



# **Deploying Avaya Diagnostic Server using VMware® in the Virtualized Environment**

Release 2.0  
Issue 4  
December 2016

## Notice

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

## Documentation disclaimer

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

## Link disclaimer

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

## Warranty

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

## Licenses

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

Avaya grants you a license within the scope of the license types described below, with the exception of Heritage Nortel Software and Support Tools, for which the scope of the license is detailed below

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

## License types

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

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

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

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

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

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

## Support tools

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

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

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

### Copyright

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

### Virtualization

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

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.

### 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.

### 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.

### 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.

# Contents

|                                                                               |    |
|-------------------------------------------------------------------------------|----|
| <b>Chapter 1: Introduction</b>                                                | 7  |
| Purpose                                                                       | 7  |
| Intended audience                                                             | 7  |
| Document changes since the last issue                                         | 7  |
| Related resources                                                             | 7  |
| Documentation                                                                 | 7  |
| Viewing Avaya Mentor videos                                                   | 8  |
| Support                                                                       | 9  |
| <b>Chapter 2: Architecture overview</b>                                       | 10 |
| Avaya Aura® Virtualized Environment Overview                                  | 10 |
| VMware components                                                             | 11 |
| <b>Chapter 3: Planning and configuration</b>                                  | 12 |
| Planning                                                                      | 12 |
| Server hardware and resources                                                 | 13 |
| Avaya Diagnostic Server virtual appliance resource requirements               | 13 |
| VMware software requirements                                                  | 14 |
| WebLM                                                                         | 14 |
| Specifications of bundled software in the OVA                                 | 15 |
| Capacity of Avaya Diagnostic Server in a virtualized environment              | 15 |
| <b>Chapter 4: Initial setup and predeployment</b>                             | 16 |
| Registering for PLDS                                                          | 16 |
| Downloading software from PLDS                                                | 16 |
| Registering SAL Gateway                                                       | 17 |
| <b>Chapter 5: Deploying the Avaya Diagnostic Server OVA</b>                   | 19 |
| Avaya Diagnostic Server OVA deployment overview                               | 19 |
| Deployment checklist                                                          | 19 |
| Deploying the Avaya Diagnostic Server OVA to vCenter                          | 20 |
| Properties field descriptions                                                 | 24 |
| Deploying the Avaya Diagnostic Server OVA directly to the ESXi server         | 29 |
| Deployment of cloned and copied OVAs                                          | 30 |
| <b>Chapter 6: Initial configuration</b>                                       | 31 |
| Starting the virtual machine                                                  | 31 |
| Configuring the Avaya Diagnostic Server parameters and the network parameters | 31 |
| Configuring the virtual machine automatic startup settings                    | 34 |
| <b>Chapter 7: Post-installation verification and testing</b>                  | 36 |
| Verification of the SAL Gateway implementation                                | 36 |
| Testing the alarming service of SAL Gateway                                   | 36 |
| Testing the remote access service of SAL Gateway                              | 36 |
| Testing the SAL Gateway UI                                                    | 37 |

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| Testing the SAL Watchdog service.....                                           | 38        |
| Verification of the SLA Mon implementation.....                                 | 38        |
| Testing the slamonsrvr service.....                                             | 38        |
| Testing the slamonweb service.....                                              | 39        |
| Testing the slamondb service.....                                               | 39        |
| <b>Chapter 8: Postinstallation customer responsibilities.....</b>               | <b>40</b> |
| <b>Chapter 9: Reconfiguring the virtual machine.....</b>                        | <b>41</b> |
| Enabling reconfiguration of software parameters on the virtual machine.....     | 41        |
| Reconfiguring the virtual machine deployed through vCenter.....                 | 42        |
| Reconfiguring the virtual machine deployed directly on an ESXi server.....      | 42        |
| <b>Chapter 10: Managing the authentication file.....</b>                        | <b>44</b> |
| Access Security Gateway and the authentication file.....                        | 44        |
| Installing an authentication file.....                                          | 45        |
| <b>Chapter 11: Maintenance procedures.....</b>                                  | <b>46</b> |
| Backup and restore overview.....                                                | 46        |
| Backing up the virtual machine.....                                             | 46        |
| Restoring a virtual machine from a backup.....                                  | 47        |
| Creating a snapshot.....                                                        | 48        |
| Restoring a snapshot.....                                                       | 48        |
| <b>Chapter 12: Upgrading the Avaya Diagnostic Server virtual appliance.....</b> | <b>50</b> |
| Upgrading from the SAL Gateway virtual appliance.....                           | 50        |
| Validating an upgrade operation.....                                            | 51        |
| <b>Chapter 13: Troubleshooting.....</b>                                         | <b>53</b> |
| FAQ.....                                                                        | 53        |
| <b>Appendix A: VMware best practices for performance.....</b>                   | <b>56</b> |
| BIOS.....                                                                       | 56        |
| Intel Virtualization Technology.....                                            | 56        |
| Dell PowerEdge Server .....                                                     | 57        |
| HP ProLiant Servers.....                                                        | 57        |
| VMware Tools.....                                                               | 58        |
| Timekeeping.....                                                                | 58        |
| Configuring timing.....                                                         | 59        |
| VMware networking best practices .....                                          | 60        |
| Thin vs. thick deployments.....                                                 | 61        |
| Best practices for VMware features.....                                         | 62        |
| VMware Snapshots.....                                                           | 62        |
| VMware vMotion.....                                                             | 63        |
| VMware High Availability.....                                                   | 64        |
| Hyperthreading.....                                                             | 64        |
| <b>Appendix B: Password management.....</b>                                     | <b>65</b> |
| Password policies.....                                                          | 65        |
| Resetting the password of an operating system account.....                      | 65        |

Resetting the password of the admin user..... 66

Resetting the password of the root user..... 66

**Glossary**..... 67

# 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.

---

## Intended audience

The primary audience for this document is anyone who installs, configures, and verifies Avaya Diagnostic Server in a VMware® vSphere™ 5.0 or 5.1 virtualization environment at a customer site. The audience includes implementation engineers, field technicians, business partners, solution providers, and customers.

---

## Document changes since the last issue

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

- Added ESXi 6.0 to the list of supported VMware software versions.

---

## Related resources

---

### Documentation

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

| Title                                                           | Description                                                                                                                                                                                    | Audience                                                                        |
|-----------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>Design</b>                                                   |                                                                                                                                                                                                |                                                                                 |
| <i>Avaya Aura® Virtualized Environment Solution Description</i> | 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              |
| <b>Implementation</b>                                           |                                                                                                                                                                                                |                                                                                 |
| <i>Deploying Avaya Diagnostic Server</i>                        | Describes the implementation requirements and procedures to deploy Avaya Diagnostic Server in a non-virtualized environment.                                                                   | Sales engineers, solution architects, implementation engineers, and customers   |
| <b>Administration</b>                                           |                                                                                                                                                                                                |                                                                                 |
| <i>Administering Avaya Diagnostic Server with SLA Mon™</i>      | 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 |
| <i>Administering Avaya Diagnostic Server with SAL Gateway</i>   | Provides information about configuring and administering SAL Gateway for remote servicing and alarm transfer facilities of Avaya products at a customer site.                                  | Solution architects, implementation engineers, support personnel, and customers |

## Viewing Avaya Mentor videos

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

### About this task

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

### Procedure

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

- Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

 **Note:**

Videos are not available for all products.

---

## Support

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

# Chapter 2: Architecture overview

---

## Avaya Aura® Virtualized Environment Overview

Avaya Aura® Virtualized Environment integrates real-time Avaya Aura® applications with VMware® virtualized server architecture. Virtualized Environment provides the following benefits:

- simplifies IT management using common software administration and maintenance.
- requires fewer servers and racks which reduces the footprint.
- lowers power consumption and cooling requirements.
- enables capital equipment cost savings.
- lowers operational expenses.
- uses standard operating procedures for both Avaya and non-Avaya products.
- customers can deploy Avaya products in a virtualized environment on customer-specified servers and hardware.
- business can scale rapidly to accommodate growth and to respond to changing business requirements.

For existing customers who have a VMware IT infrastructure, Avaya Aura® Virtualized Environment provides an opportunity to 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 is only for VMware and is not intended to include any other industry hypervisor. Virtualized Environment is inclusive of the Avaya Aura® portfolio.

### **Note:**

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

- server and host
- reservations and configuration values

### **Customer deployment**

Deployment into the blade, cluster, and server is managed by vCenter Server and vSphere Client.

The customer provides the servers and the VMware infrastructure including the VMware licenses.

## Software delivery

The software is delivered as one or more pre-packaged Open Virtualization Appliance (OVA) files that are posted on the Avaya Product Licensing and Download System (PLDS) and the Avaya support site. Each OVA contains the following components:

- the application software and operating system.
- pre-installed VMware tools.
- preset configuration details for
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

## Patches and upgrades

A minimum patch level can be required for each supported application. For more information regarding the application patch requirements, see the compatibility matrix tool at <http://support.avaya.com/CompatibilityMatrix/Index.aspx>.

## Performance and capacities

The OVA template is built with configuration values which optimize performance and follow recommended Best Practices.



### Caution:

Modifying these values can have a direct impact on the performance, capacity, and stability of the virtual machine. It is the responsibility of the customer to understand the aforementioned impacts when changing configuration values. Avaya Global Support Services (GSS) may not be able to assist in fully resolving a problem if the virtual hardware or resource allocation has been changed to unsupported values for a virtual application. Avaya GSS could require the customer to reset the values to the optimized values before starting to investigate the issue.

---

# VMware components

| VMware software component | Description                                                                                                                                                                                                                                                                      |
|---------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| ESXi Host                 | The physical machine running the ESXi Hypervisor software.                                                                                                                                                                                                                       |
| 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.                                                                                          |

# 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 <a href="https://plds.avaya.com">https://plds.avaya.com</a> .                                           | See <a href="#">Registering for PLDS</a> on page 16.                                                                                                                                                                                                                             |   |
| 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 <a href="#">Server hardware and resources</a> on page 13.                                                                                                                                                                                                                    |   |
| 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. | See <a href="#">Avaya Diagnostic Server virtual appliance resource requirements</a> on page 13.                                                                                                                                                                                  |   |
| 5 | Ensure that the SAL Gateway registration process is complete and you have received the Solution Element ID and Alarm ID for the new SAL Gateway.                                       | See <a href="#">Registering SAL Gateway</a> on page 17.<br><br>You must provide a registered Solution Element ID to make the SAL Gateway component of Avaya Diagnostic Server operational. Until you enter a correct Solution Element ID, the SAL Gateway services do not start. |   |
| 6 | 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                                                                                                                                         |   |

*Table continues...*

| # | Action                                                                  | Notes                                                                                                                             | ✓ |
|---|-------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------|---|
|   |                                                                         | deploy and use an external WebLM server.                                                                                          |   |
| 7 | 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 5.0 with update 3 or later, ESXi 5.1 with any updates, ESXi 5.5 with any updates, or ESXi 6.0 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 GHz         |
| Memory              | 8 GB          |
| Storage reservation | 220 GB        |
| Shared NIC          | 1 @ 1000 Mbps |
| IOPS                | 1875          |

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 GHz or higher.

---

## VMware software requirements

The following are the supported VMware software versions:

- VMware vSphere ESXi 5.0 with update 3 or later
- VMware vSphere ESXi 5.1
- VMware vSphere ESXi 5.5
- VMware vSphere ESXi 6.0
- VMware vCenter Server 5.0
- VMware vCenter Server 5.1
- VMware vCenter Server 5.5
- VMware vCenter Server 6.0
- VMware vSphere Client 5.0
- VMware vSphere Client 5.1
- VMware vSphere Client 5.5
- VMware vSphere Client 6.0

You can add ESXi 5.0 under vCenter Server 5.0 and vCenter Server 5.1. However, you can add ESXi 5.1 only under vCenter Server 5.1. See *VMware Product Interoperability Matrixes* at [http://partnerweb.vmware.com/comp\\_guide2/sim/interop\\_matrix.php](http://partnerweb.vmware.com/comp_guide2/sim/interop_matrix.php) to view compatibility with other solution releases.

**\* Note:**

ESXi 4.1 does not support Avaya Diagnostic Server virtual appliance.

---

## 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.

|                             |                             |
|-----------------------------|-----------------------------|
| <b>Operating system</b>     | CentOS 5.9, 64-bit          |
| <b>Java</b>                 | Oracle JRE 1.7.0_51         |
| <b>Application software</b> | Avaya Diagnostic Server 2.0 |

---

## 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*.

# 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](mailto: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 OVA supports two modes of deployment on a VMware vSphere 5.0 or 5.1 environment:

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

Based on the VMware environment you have, select one of the two methods of deployment.

---

## 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.                                                     |                                                                                                                                                                                                           |   |
| 2   | Ensure that you have the Solution Element ID and the Product ID for the SAL Gateway component. | You receive these IDs after you register SAL Gateway with Avaya. For more information, see <a href="#">Registering SAL Gateway</a> on page 17.                                                            |   |
| 3   | Deploy the OVA.                                                                                | See <a href="#">Deploying the Avaya Diagnostic Server OVA to vCenter</a> on page 20 or <a href="#">Deploying the Avaya Diagnostic Server OVA directly to the ESXi server</a> on page 29.                  |   |
| 4   | 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. |   |

*Table continues...*

| No. | Action | Link/Notes                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | ✓ |
|-----|--------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---|
|     |        | <p>See <a href="#">Resetting the password of an operating system account</a> on page 65 and <a href="#">Password policies</a> on page 65.</p> <p> <b>Caution:</b></p> <p>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.</p> <p>Note that 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.</p> |   |

## 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 two disk formats, and click **Next**.

- **Thick Provision Lazy Zeroed:** Allocates the required 220-GB disk space during the creation of the virtual disk for the Avaya Diagnostic Server virtual appliance.
- **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 61.

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.
- b. In the **Hostname** field, enter a host name or fully qualified domain name for the Avaya Diagnostic Server virtual appliance.

- c. In the **Avaya Diagnostic Server Components** field, select one of the following options to indicate which Avaya Diagnostic Server components you want to install:

- **Both:** To install both components, SAL Gateway and SLA Mon server.
- **SAL Gateway:** To install only the SAL Gateway component.
- **SLAMon Server:** To install only the SLA Mon server component.

 **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>.

- d. If you chose to install the SLA Mon server component, in the **WebLM Hostname** field, enter the host name or IP address of an external WebLM server.

 **Important:**

A WebLM server address is mandatory for the SLA Mon server deployment. If you chose not to install the SLA Mon server, you can leave this field with the default value.

- e. If you chose to install the SAL Gateway component, complete the following fields to configure SAL Gateway:

 **Note:**

If you chose not to install SAL Gateway, leave these fields with the default values.

- **Automatic Software Update**
- **SMTP Hostname / IP Address**
- **SMTP Port**
- **Administrator's E-mail Address**
- (Optional) **SMTP Username**
- (Optional) **SMTP Password**
- (Optional) **Secondary E-mail Address**
- **Solution Element ID**

 **Note:**

You must provide a registered Solution Element ID to make SAL Gateway operational. Until you enter a correct Solution Element ID, the SAL Gateway services do not start.

- **Alarm ID**
- **Platform Qualifier**
- **Primary Destination Core**
- **Port**
- **Primary Destination Remote**
- **Port**
- (Optional) **Proxy Type**
- (Optional) **Proxy Hostname**
- (Optional) **Proxy Port**
- (Optional) **Proxy User**
- (Optional) **Proxy Password**
- (Optional) **Policy Server Hostname**
- (Optional) **Policy Server Port**
- **Master Agent Hostname**
- **Master AgentX Port**
- **Role**

 **Important:**

You must replace the default values in most of the fields with correct values that match your environment. However, accept the default values in the **Platform Qualifier**, **Primary Destination Core**, **Primary Destination Remote**, and **Port** fields, unless you have valid reasons to change these values.

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

- f. In the Network Properties section of the Properties window, complete the following fields according to your network settings:

- **Default Gateway**
- **DNS**
- **Network 1 IP Address**
- **Network 1 Netmask**

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

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.

### Related links

[Starting the virtual machine](#) on page 31

## 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 Avaya Diagnostic Server configuration information through the Properties window of the deployment wizard .

### Important:

For the Avaya Diagnostic Server components to function correctly, you must replace the default values in the Properties window with correct values that match your environment. In addition, provide correct SMTP details to receive software update notifications from Avaya.

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

| Name                                      | Description                                                                                                                                                                                                                                                                                                                                                                                           |
|-------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Timezone setting</b>                   | The appropriate time zone for the location where you deploy the Avaya Diagnostic Server virtual appliance.                                                                                                                                                                                                                                                                                            |
| <b>Hostname</b>                           | The host name or fully qualified domain name of the Avaya Diagnostic Server virtual appliance.                                                                                                                                                                                                                                                                                                        |
| <b>Avaya Diagnostic Server Components</b> | <p>The Avaya Diagnostic Server components you want to install. You can select one of the following options:</p> <ul style="list-style-type: none"> <li>• <b>Both:</b> To install both components, SAL Gateway and SLA Mon server.</li> <li>• <b>SAL Gateway:</b> To install only the SAL Gateway component.</li> <li>• <b>SLAMon Server:</b> To install only the SLA Mon server component.</li> </ul> |

*Table continues...*

| Name                                                                                                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>WebLM Hostname</b>                                                                                                                                                     | <p>The host name or IP address of an external WebLM server to configure the SLA Mon server licensing.</p> <p>A WebLM server address is mandatory for the SLA Mon server deployment. If you chose not to install the SLA Mon server, you can leave this field with the default value.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| The following fields are for the configuration of the SAL Gateway component. If you chose not to install SAL Gateway, you can leave these fields with the default values. |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Automatic Software Update</b>                                                                                                                                          | <p>A drop-down list to enable or disable automatic software update for Avaya Diagnostic Server. You can select one of the following two options:</p> <ul style="list-style-type: none"> <li>• <b>Yes:</b> To enable the Automatic Software Update feature. If you do not install the downloaded software packages within the grace period set for the packages, the packages are applied automatically.</li> <li>• <b>No:</b> To disable the Automatic Software Update feature. You must install the downloaded software packages manually.</li> </ul> <p> <b>Note:</b></p> <p>The Automatic Software Update feature is implemented through the SAL Gateway component of Avaya Diagnostic Server. Therefore, this feature is available for Avaya Diagnostic Server that has both components or only SAL Gateway installed. For Avaya Diagnostic Server that has only the SLA Mon server, the Automatic Software Update feature is not available.</p> |
| <b>SMTP Hostname / IP Address</b>                                                                                                                                         | The host name or the IP address of the Simple Mail Transfer Protocol (SMTP) server that SAL Gateway is to use for sending email notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SMTP Port</b>                                                                                                                                                          | The port number of the SMTP server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Administrator's E-mail Address</b>                                                                                                                                     | The administrator email address where you want to receive email notifications about download and installation status of software updates.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| <b>SMTP Username</b>                                                                                                                                                      | <p>(Optional) The user name for the SMTP server.</p> <p>The field is mandatory only when the SMTP server is configured to authenticate users.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>SMTP Password</b>                                                                                                                                                      | <p>(Optional) The password of the user to be authenticated by the SMTP server.</p> <p>The field is mandatory only when the SMTP server is configured to authenticate users.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Secondary E-mail Address</b>                                                                                                                                           | (Optional) A secondary email address where you want to receive email notifications.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

*Table continues...*

| Name                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Solution Element ID</b>      | <p>A unique identifier in the format (nnn)nnn-nnnn, where n is a digit from 0 through 9. Using this ID, Avaya Services or Avaya Partners can uniquely identify and connect to this SAL Gateway.</p> <p>You must replace the default value with the Solution Element ID you receive from Avaya. Otherwise, the remote access and product alarm functionalities through SAL Gateway are affected. You receive this ID after you register SAL Gateway with Avaya.</p> <p> <b>Note:</b></p> <p>Register your SAL Gateway before you perform the deployment so that you have the Solution Element ID and Product ID ready for the deployment. You must provide a registered Solution Element ID to make SAL Gateway operational. If you do not enter a correct Solution Element ID, the SAL Gateway services do not start after the deployment.</p> |
| <b>Alarm ID</b>                 | <p>A unique 10-character ID, also called Product ID, assigned to a device, for example, this SAL Gateway. The Product ID is included in alarms that are sent to alarm receivers from the managed device. Avaya uses the Alarm ID to identify the device that generated the alarm.</p> <p>You must replace the default value with the Product ID you receive from Avaya. Otherwise, the remote access and product alarm transfer functionalities through SAL Gateway are affected. You receive this ID after you register SAL Gateway with Avaya.</p>                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Platform Qualifier</b>       | <p>An alphanumeric string to establish a channel for communication between SAL Gateway and Secure Access Concentrator Core Server.</p> <p>The default platform qualifier is <code>Enterprise-production</code>.</p> <p> <b>Important:</b></p> <p>Do not change the default value unless you receive instructions to do so.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| <b>Primary Destination Core</b> | <p>The host name of the Concentrator Core Server that SAL Gateway first contacts.</p> <p>The default value is <code>secure.alarming.avaya.com</code>, which is used to communicate with the Concentrator Core Server located at Avaya.</p> <p>If you have a local Concentrator Core Server or one at a partner location, you must enter the host name or the IP</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |

*Table continues...*

| Name                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|-----------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                   | address of that server. Otherwise, you must retain the default value to communicate with Avaya.                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Port</b>                       | <p>The port number for the primary Concentrator Core Server.</p> <p>The default port is 443.</p> <p>For the Avaya Concentrator Core Server, you must retain the default value. For a local Concentrator Core Server, you must enter the value as 8443.</p>                                                                                                                                                                                                                                                            |
| <b>Primary Destination Remote</b> | <p>The host name or IP address of the primary Secure Access Concentrator Remote Server that requests and facilitates remote access for service personnel.</p> <p>The default value is <code>remote.sal.avaya.com</code>.</p> <p>To communicate with the Avaya Concentrator Remote Server, retain the default value. If you have a local Concentrator Remote Server, enter the host name of that server.</p>                                                                                                           |
| <b>Port</b>                       | <p>The port number of the primary Secure Access Concentrator Remote Server.</p> <p>The default value is 443.</p>                                                                                                                                                                                                                                                                                                                                                                                                      |
| <b>Proxy Type</b>                 | <p>(Optional) The type of channel that the virtual machine uses to communicate with the servers outside your network. This field is required only if you use a proxy server for internet access outside the firewall of your network. The options are:</p> <ul style="list-style-type: none"> <li>• <b>HTTP:</b> For an HTTP proxy without authentication.</li> <li>• <b>Authenticated HTTP:</b> For an HTTP proxy with authentication.</li> <li>• <b>SOCKS:</b> For a SOCKS proxy without authentication.</li> </ul> |
| <b>Proxy Hostname</b>             | <p>(Optional) The host name or IP address of the proxy server. This field is required only if you have a proxy server for Internet access outside your network.</p>                                                                                                                                                                                                                                                                                                                                                   |
| <b>Proxy Port</b>                 | (Optional) The port number of the proxy server.                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Proxy User</b>                 | <p>(Optional) The user name for the authenticated HTTP proxy. This field is required only if the proxy type is authenticated HTTP.</p>                                                                                                                                                                                                                                                                                                                                                                                |
| <b>Proxy Password</b>             | <p>(Optional) The password for the authenticated HTTP proxy. This field is required only if the proxy type is authenticated HTTP.</p>                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Policy Server Hostname</b>     | <p>(Optional) The host name or the IP address of Policy Server installed on your network.</p> <p>The use of Policy Server is optional. You can add the Policy Server information later through the SAL Gateway user interface (UI).</p>                                                                                                                                                                                                                                                                               |

*Table continues...*

| Name                         | Description                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Policy Server Port</b>    | (Optional) The port number that Policy Server uses for communication with SAL Gateway.                                                                                                                                                                                                                                                                                                                                                             |
| <b>Master Agent Hostname</b> | <p>The host name or IP address of the SNMP master agent to which the SNMP subagent must connect.</p> <p>The default value is 127.0.0.1.</p> <p>If you did not configure an SNMP master agent before the OVA deployment, you must update the SNMP master agent information on the SAL Gateway UI after you complete OVA deployment.</p> <p>For information about SNMP master agent configuration, see <i>Deploying Avaya Diagnostic Server</i>.</p> |
| <b>Master AgentX Port</b>    | <p>The AgentX listener port number of the SNMP master agent.</p> <p>The default value is 705.</p> <p>Retain the default value unless another application is already using the port.</p>                                                                                                                                                                                                                                                            |
| <b>Role</b>                  | <p>The role or permission level of the Avaya support personnel to the SAL Gateway UI. Avaya support personnel can have one of the following roles:</p> <ul style="list-style-type: none"> <li>• <b>Administrator:</b> With full permissions to all the SAL Gateway UI pages except a few.</li> <li>• <b>Browse:</b> With the read-only access to all pages.</li> <li>• <b>Deny:</b> Without access to the SAL Gateway UI.</li> </ul>               |

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

| Name                        | Description                                                                                                                                          |
|-----------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Default Gateway</b>      | The IP address of the default gateway on your network. You can leave this field blank if you plan to use Dynamic Host Configuration Protocol (DHCP). |
| <b>DNS</b>                  | The comma-separated addresses of the Domain Name Servers (DNS) for the virtual machine. You can leave this field blank if you plan to use DHCP.      |
| <b>Network 1 IP Address</b> | The IP address of the network interface. You can leave this field blank if you plan to use DHCP.                                                     |
| <b>Network 1 Netmask</b>    | The netmask or prefix for the network interface. You can leave this field blank if you plan to use DHCP.                                             |

---

# 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.

During this direct deployment, you cannot configure the Avaya Diagnostic Server components. After the deployment, when you start the virtual machine console for the first time, the console displays a series of prompts to set the parameters to configure the SAL Gateway and SLA Mon components of Avaya Diagnostic Server.

## 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, accept the default disk format, **Thick Provision Lazy Zeroed**, which allocates the required 220-GB disk space for the Avaya Diagnostic Server virtual appliance, and click **Next**.

For more information about virtual disk, see [Thin vs. thick deployments](#) on page 61.

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 parameters for the Avaya Diagnostic Server components.

### Related links

[Starting the virtual machine](#) on page 31

[Configuring the Avaya Diagnostic Server parameters and the network parameters](#) on page 31

---

## 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.

# 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. The system starts the system services, and the SAL Gateway and SLA Mon 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, Avaya Diagnostic Server is deployed with some default configuration values. When you start the virtual machine for the first time, you must configure the network parameters and the Avaya Diagnostic Server 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 Avaya Diagnostic Server components and the network parameters after starting the virtual machine for the first time.

**! Important:**

You must replace the default configuration values of the Avaya Diagnostic Server components with correct values to make the Avaya Diagnostic Server instance functional.

**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 IP address of the default gateway on your network.

**\* Note:**

Set the IP address and 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 proxy server information.
  - The IP address allocated to 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. When the system prompts you to choose the Avaya Diagnostic Server components you want to install, enter one of the following options:
    - **1:** To install only the SAL Gateway component.
    - **2:** To install only the SLA Mon server component.
    - **3:** To install both components, SAL Gateway and SLA Mon server.

**! 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>.

5. For the SLA Mon server component, when the system prompts, enter the host name or IP address of an external WebLM server.
6. When the system prompts, complete the following SAL Gateway configuration parameters:

 **Note:**

To accept the default or current values, press **Enter** at each prompt.

- **Automatic Software Update**
- **SMTP Hostname or IP Address**
- **SMTP Server Port**
- **Administrator's E-mail Address**
- (Optional) **SMTP Username**
- (Optional) **SMTP Password**
- (Optional) **Secondary E-mail Address**
- **SAL Gateway Solution Element ID**

 **Note:**

You must provide a registered Solution Element ID to make SAL Gateway operational. Until you enter a correct Solution Element ID, the SAL Gateway services do not start.

- **SAL Gateway Alarm ID**
- **Platform Qualifier**
- **Primary Destination Core Server**
- **Primary Destination Core Server Port**
- **Primary Destination Remote Server**
- **Primary Destination Remote Server Port**

 **Important:**

You must accept the default values in the **Platform Qualifier**, **Primary Destination Core Server**, **Primary Destination Core Server Port**, **Primary Destination Remote Server**, and **Primary Destination Remote Server Port** fields, unless you have valid reasons to change these values.

To accept the default values, press **Enter** at each prompt.

- (Optional) **Proxy Type**

- (Optional) **Proxy Server Hostname**
- (Optional) **Proxy Server Port**
- (Optional) **Policy Server Hostname**
- (Optional) **Policy Server Port**
- **Master Agent Hostname**
- **Master Agent Port**

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

7. When the system prompts, select the role to be assigned to Avaya service personnel.
8. Confirm the configuration changes.

The system configures the Avaya Diagnostic Server components according to the settings you entered.

## Result

After the configuration is complete, the system starts the SAL Gateway and the SLA Mon services and prompts you to log on to the virtual machine.

## Related links

[Properties field descriptions](#) on page 24

---

# Configuring the virtual machine automatic startup settings

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.

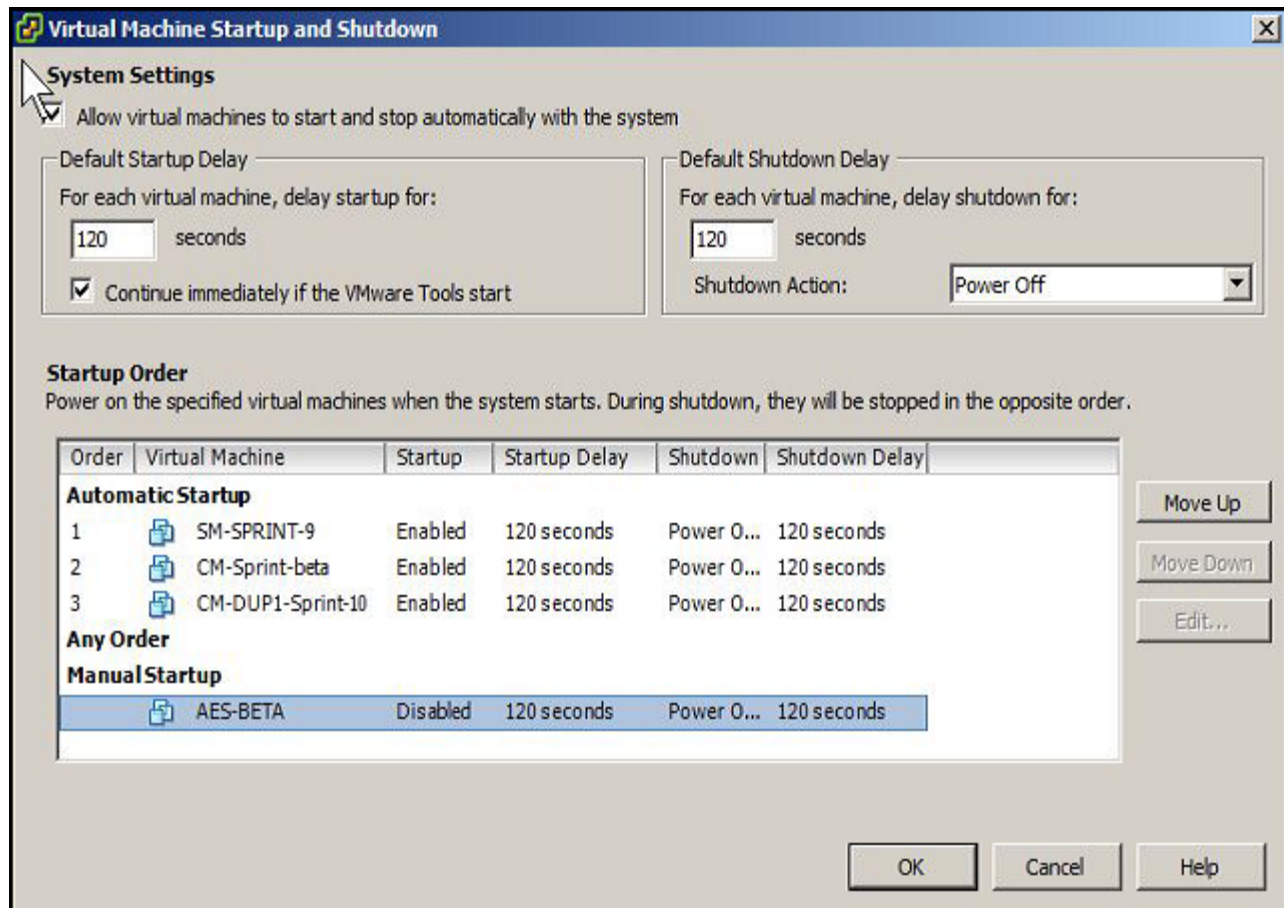
## Procedure

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: 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:  
`service spiritAgent status`
3. If the service is not running, run the following command to start the service:  
`service spiritAgent start`
4. Check the status again to verify that the service is running properly.

---

## Testing the remote access service of SAL Gateway

### About this task

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

## Procedure

1. Log on to the 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:  
`service axedaAgent status`
3. If the service is not running, run the following command to start the service:  
`service axedaAgent start`
4. Check the status again to verify that the service is running properly.

---

## Testing the SAL Gateway UI

### About this task

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

### Procedure

1. From another terminal on the network where SAL Gateway is deployed, open a web browser.
2. In the address bar, type the following URL:  
`https://<IP address of the Avaya Diagnostic Server virtual appliance>:7443`  
  
You can replace the host IP with the DNS host name if the host server is registered under DNS.  
  
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 Avaya Diagnostic Server virtual machine as admin, and switch to the root user.
  - b. Run the following command to check the status of the gatewayUI service:  
`service gatewayUI status`
  - c. If the service is not running, run the following command to start the service:  
`service gatewaUI start`
  - d. Check the status again to verify that the service is running properly.

---

## Testing the SAL Watchdog service

### About this task

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

### Procedure

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

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

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

---

## Verification of the SLA Mon implementation

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

### Note:

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

---

## Testing the slamonsrvr service

### About this task

Use this procedure to confirm 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:  

```
service slamonsrvr status
```

Expected output sample:

```
slamonsrvr Running
```

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

```
service slamonsrvr start
```

---

## Testing the slamonweb service

### About this task

Use this procedure to confirm 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:

```
service slamonweb status
```

Expected output sample:

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

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

```
service slamonweb start
```

---

## Testing the slamondb service

### About this task

Use this procedure to confirm 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:

```
service slamondb status
```

Expected output sample:

```
postmaster (pid 21287 21286 21285 21284 21282 21280 15031 15027  
10402 10387 10370) is running...
```

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

```
service slamondb start
```

# Chapter 8: 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 9: Reconfiguring the virtual machine

---

## Enabling reconfiguration of software parameters on the virtual machine

### About this task

After you deploy the Avaya Diagnostic Server virtual machine, you can change the configuration, including network and time zone, of the virtual machine at any time. The virtual machine reconfiguration procedures differ based on the type of deployment, which can be a vCenter deployment or a direct ESXi deployment. However, reconfiguration of the Avaya Diagnostic Server software parameters during the virtual machine reconfiguration is disabled by default.

Use this procedure to be able to change the configuration of the Avaya Diagnostic Server software parameters on a virtual machine for both vCenter and direct ESXi host deployment. This procedure is an one time function. After you enable reconfiguration of the software parameters, you can change the Avaya Diagnostic Server software parameters at any time.

### Procedure

1. Perform one of the following:
  - For a vCenter deployment, connect to the vCenter server through a vSphere client.
  - For a direct ESXi deployment, connect to the ESXi server through a vSphere client.
2. Right click the Avaya Diagnostic Server virtual machine, and click **Open Console**.
3. Log on to the virtual machine as admin, and switch to the root user.
4. Run the following command:

```
reconfigurevm -e
```

The Avaya Diagnostic Server software parameters are now available for reconfiguration through the virtual machine reconfiguration procedures.

5. Run the following command to disable reconfiguration of the software parameters:

```
reconfigurevm -d
```

---

## Reconfiguring the virtual machine deployed through vCenter

### About this task

The virtual machine reconfiguration procedures differ based on the type of deployment, which can be a vCenter deployment or a direct ESXi deployment. Use this procedure to reconfigure the virtual machine deployed using vCenter.

### Procedure

1. Connect to the vCenter server through the vSphere client.
2. Shut down the virtual machine.
3. Right click the virtual machine, and click **Edit Settings**.
4. On the Edit Settings window, select the **Options** tab, and click **Properties**.
5. Modify the properties according to your requirements.
6. Click **OK**.
7. Power on the virtual machine.

### Result

When the virtual machine boots up, all the settings are applied automatically.

### Related links

[Enabling reconfiguration of software parameters on the virtual machine](#) on page 41

---

## Reconfiguring the virtual machine deployed directly on an ESXi server

If you deploy the Avaya Diagnostic Server virtual appliance directly on an ESXi host, then at every reboot, a script runs during the boot up process that waits for user inputs. By following the interactive messages from the script, you can reconfigure the virtual machine. The script waits for your input for 30 seconds before proceeding with the normal boot process. If you do not provide any input within 30 seconds, the script skips the reconfiguration of the virtual machine and proceeds with the normal boot process.

### About this task

Use this procedure only when you need to reconfigure the virtual machine deployed directly on an ESXi host server.

### Procedure

1. Connect to the ESXi host server through the vSphere client.
2. Shut down the virtual machine.

3. Start the virtual machine, and open the virtual machine console.

As part of the startup, the system prompts you to configure the virtual machine.

4. Follow the interactive messages that the system displays to reconfigure the virtual machine.

**Related links**

[Enabling reconfiguration of software parameters on the virtual machine](#) on page 41

# Chapter 10: Managing the authentication file

---

## Access Security Gateway and the authentication file

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

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

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

### Note:

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

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

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

```
service slamonsrvr status  
service slamondb restart
```

```
service slamonweb stop
```

- Install an authentication file through the **asgloadauth** script. For example:

```
asgloadauth /tmp/<authfile_name>
```

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

### Important:

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

---

## Installing an authentication file

### Before you begin

Create and download the authentication file from AFS.

### Note:

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

### About this task

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

### Procedure

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

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

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

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

```
asgloadauth /tmp/<auth_filename>
```

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

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

# Chapter 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: Upgrading the Avaya Diagnostic Server virtual appliance

---

## Upgrading from the SAL Gateway virtual appliance

### About this task

Use this procedure to upgrade from an existing SAL Gateway virtual appliance to an Avaya Diagnostic Server virtual appliance.

### Procedure

1. Take a backup of the existing SAL Gateway virtual appliance, and copy the backup file to an external host.

For more information, see [Backing up the virtual machine](#) on page 46.

2. Shut down the existing SAL Gateway virtual appliance.
3. Deploy the new Avaya Diagnostic Server OVA on an ESXi host server.

You can accept the default values for configuring the virtual appliance and the Avaya Diagnostic Server software as you are going to restore the configuration values from the backup file of the earlier virtual appliance.

#### Important:

- While deploying the new Avaya Diagnostic Server OVA, you must configure the same network parameters, including host name, IP address, netmask, and default gateway, as the earlier virtual appliance.
  - If you want to install SLA Mon server as part of Avaya Diagnostic Server, you must also configure the hostname or IP address of an external WebLM server.
4. Start the new Avaya Diagnostic Server virtual appliance.
  5. Log on to the new virtual machine as admin, and switch to the root user.
  6. Copy the backup file from the external host to a directory on the new virtual machine.
  7. Restore the backup file on the new virtual machine.

For more information, see [Restoring a virtual machine from a backup](#) on page 47.

**Next steps**

Check the network configuration, services, SAL Gateway configuration, and SLA Mon server configuration to validate that the upgrade process is successful.

After you validate the upgrade process, you can remove the earlier virtual machine from the host 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-2.0.0.0-e50-05.

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:

```
service spiritAgent status
```

```
service axedaAgent status
```

```
service gatewayUI status
```

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:

```
service slamonsrvr status
```

```
service slamondb status
```

**service slamonweb status**

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 13: Troubleshooting

---

## 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 reconfigure my virtual appliance after I have deployed the virtual appliance?

A. For information about reconfiguring your virtual appliance, see [Reconfiguring the virtual machine deployed through vCenter](#) on page 42 and [Reconfiguring the virtual machine deployed directly on an ESXi server](#) on page 42.

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 59.

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?

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.

*Table continues...*

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?

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
```

*Table continues...*

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.

# 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>.

---

## 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.

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 a 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 VMkernel vNICs to the same IP Maximum Transmission Unit (MTU).

## References

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

## 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                            | <a href="#">Best Practices for virtual machine snapshots in the VMware environment</a> |
| Understanding virtual machine snapshots in VMware ESXi and ESX                                    | <a href="#">Understanding virtual machine snapshots in VMware ESXi and ESX</a>         |
| Working with snapshots                                                                            | <a href="#">Working with snapshots</a>                                                 |
| Configuring VMware vCenter Server to send alarms when virtual machines are running from snapshots | <a href="#">Send alarms when virtual machines are running from snapshots</a>           |
| Consolidating snapshots in vSphere 5.x                                                            | <a href="#">Consolidating snapshots in vSphere 5.x</a>                                 |

## 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 iSCSI 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

---

## 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 65

---

## 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 **Ctrl**.
3. Select the first entry, and type **e**.
4. Select the second entry, **kernel**, and type **e**.
5. Edit the entry as the following:
  - a. Remove **rhgb quiet**.
  - b. Enter **init=/bin/sh**.
6. Press **Enter**.
7. Press **b**, and let the booting process to continue.
8. When the process stops at the shell prompt **sh-4.1#**, run the following command:

```
mount -rw -o remount /
```

9. Run the following command:

```
passwd
```

10. When the system prompts, type the new password.
11. Restart the virtual machine using the VMware console.

# Glossary

|                        |                                                                                                                                                                                                                                                                                                                                                   |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>AFS</b>             | 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.                                                                                                                                                    |
| <b>Application</b>     | A software solution development by Avaya that includes a guest operating system.                                                                                                                                                                                                                                                                  |
| <b>Avaya Appliance</b> | 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.                            |
| <b>Blade</b>           | 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. |
| <b>ESXi</b>            | A virtualization layer that runs directly on the server hardware. Also known as a <i>bare-metal hypervisor</i> . Provides processor, memory, storage, and networking resources on multiple virtual machines.                                                                                                                                      |
| <b>Hypervisor</b>      | 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.                                                                                                                                                      |
| <b>MAC</b>             | Media Access Control address. A unique identifier assigned to network interfaces for communication on the physical network segment.                                                                                                                                                                                                               |
| <b>OVA</b>             | 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.                                                                                                                                |
| <b>PLDS</b>            | Product Licensing and Download System. The Avaya PLDS provides product licensing and electronic software download distribution.                                                                                                                                                                                                                   |
| <b>Reservation</b>     | A reservation specifies the guaranteed minimum required amounts of CPU or memory for a virtual machine.                                                                                                                                                                                                                                           |

|                          |                                                                                                                                                                                                                                                                                                                              |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>RFA</b>               | 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. |
| <b>SAN</b>               | 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.                                            |
| <b>Snapshot</b>          | 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.                                                                                           |
| <b>Storage vMotion</b>   | A VMware feature that migrates virtual machine disk files from one data storage location to another with limited impact to end users.                                                                                                                                                                                        |
| <b>vCenter Server</b>    | 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.                                                                                                                       |
| <b>virtual appliance</b> | A virtual appliance is a single software application bundled with an operating system.                                                                                                                                                                                                                                       |
| <b>VM</b>                | 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.                                                                                                                |
| <b>vMotion</b>           | 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.                                                                                                  |
| <b>VMware HA</b>         | 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.       |
| <b>vSphere Client</b>    | The vSphere Client is a downloadable interface for administering vCenter Server and ESXi.                                                                                                                                                                                                                                    |

# Index

## A

|                                   |                    |
|-----------------------------------|--------------------|
| Access Security Gateway .....     | <a href="#">44</a> |
| admin user                        |                    |
| reset password .....              | <a href="#">66</a> |
| application software parameters   |                    |
| enable reconfiguration .....      | <a href="#">41</a> |
| ASG .....                         | <a href="#">44</a> |
| ASG authentication file           |                    |
| install .....                     | <a href="#">45</a> |
| authentication file               |                    |
| install .....                     | <a href="#">45</a> |
| authentication file for ASG ..... | <a href="#">44</a> |
| automatic restart                 |                    |
| virtual machine .....             | <a href="#">34</a> |
| Avaya applications                |                    |
| networking .....                  | <a href="#">60</a> |
| Avaya Diagnostic Server           |                    |
| capacity .....                    | <a href="#">15</a> |

## B

|                                       |                    |
|---------------------------------------|--------------------|
| back up virtual application .....     | <a href="#">46</a> |
| best practices                        |                    |
| performance .....                     | <a href="#">56</a> |
| BIOS .....                            | <a href="#">56</a> |
| BIOS for HP servers .....             | <a href="#">57</a> |
| BIOS settings                         |                    |
| for Dell servers .....                | <a href="#">57</a> |
| bundled software specifications ..... | <a href="#">15</a> |

## C

|                                           |                    |
|-------------------------------------------|--------------------|
| capacity of Avaya Diagnostic Server ..... | <a href="#">15</a> |
| checklist                                 |                    |
| deployment procedures .....               | <a href="#">19</a> |
| planning procedures .....                 | <a href="#">12</a> |
| clones                                    |                    |
| virtual appliances .....                  | <a href="#">30</a> |
| components .....                          | <a href="#">11</a> |
| VMware .....                              | <a href="#">11</a> |
| configure                                 |                    |
| Avaya Diagnostic Server parameters .....  | <a href="#">31</a> |
| network parameters .....                  | <a href="#">31</a> |
| configuring                               |                    |
| timing .....                              | <a href="#">59</a> |
| virtual machine automatic restart .....   | <a href="#">34</a> |
| creating a snapshot .....                 | <a href="#">48</a> |
| customer responsibilities                 |                    |
| postinstallation .....                    | <a href="#">40</a> |

## D

|                          |                    |
|--------------------------|--------------------|
| database service, slamon |                    |
| test .....               | <a href="#">39</a> |
| deploying clones .....   | <a href="#">30</a> |
| deploying OVA            |                    |
| directly to ESXi .....   | <a href="#">29</a> |
| to vCenter .....         | <a href="#">20</a> |
| deployment               |                    |
| thick .....              | <a href="#">61</a> |
| thin .....               | <a href="#">61</a> |
| deployment procedures    |                    |
| checklist .....          | <a href="#">19</a> |
| document changes .....   | <a href="#">7</a>  |
| document purpose .....   | <a href="#">7</a>  |
| downloading software     |                    |
| using PLDS .....         | <a href="#">16</a> |

## E

|                                              |                    |
|----------------------------------------------|--------------------|
| enable                                       |                    |
| reconfiguration of software parameters ..... | <a href="#">41</a> |

## F

|                            |                    |
|----------------------------|--------------------|
| FAQ .....                  | <a href="#">53</a> |
| field descriptions         |                    |
| properties page .....      | <a href="#">24</a> |
| forgot root password ..... | <a href="#">66</a> |

## G

|               |                    |
|---------------|--------------------|
| Gateway UI    |                    |
| testing ..... | <a href="#">37</a> |

## H

|                         |                    |
|-------------------------|--------------------|
| high availability ..... | <a href="#">64</a> |
| hyperthreading .....    | <a href="#">64</a> |

## I

|                                       |                    |
|---------------------------------------|--------------------|
| install                               |                    |
| authentication file .....             | <a href="#">45</a> |
| Intel Virtualization Technology ..... | <a href="#">56</a> |
| intended audience .....               | <a href="#">7</a>  |

## L

|                       |                    |
|-----------------------|--------------------|
| license manager ..... | <a href="#">14</a> |
|-----------------------|--------------------|

**M**

|                         |                    |
|-------------------------|--------------------|
| managing licenses ..... | <a href="#">14</a> |
|-------------------------|--------------------|

**N**

|                                     |                    |
|-------------------------------------|--------------------|
| networking Avaya applications ..... | <a href="#">60</a> |
| networking best practices .....     | <a href="#">60</a> |
| network parameters                  |                    |
| configure .....                     | <a href="#">31</a> |
| NTP time source .....               | <a href="#">58</a> |

**O**

|                          |                    |
|--------------------------|--------------------|
| os account password      |                    |
| resetting .....          | <a href="#">65</a> |
| overview .....           | <a href="#">10</a> |
| backup and restore ..... | <a href="#">46</a> |
| OVA deployment .....     | <a href="#">19</a> |

**P**

|                                                  |                    |
|--------------------------------------------------|--------------------|
| password policies .....                          | <a href="#">65</a> |
| password reset .....                             | <a href="#">65</a> |
| performance best practices .....                 | <a href="#">56</a> |
| planning procedures                              |                    |
| checklist .....                                  | <a href="#">12</a> |
| PLDS .....                                       | <a href="#">16</a> |
| downloading software .....                       | <a href="#">16</a> |
| postinstallation customer responsibilities ..... | <a href="#">40</a> |
| properties page                                  |                    |
| field descriptions .....                         | <a href="#">24</a> |
| purpose of document .....                        | <a href="#">7</a>  |

**R**

|                                         |                    |
|-----------------------------------------|--------------------|
| reconfiguration                         |                    |
| enable for application parameters ..... | <a href="#">41</a> |
| reconfiguring virtual machine           |                    |
| at ESXi host .....                      | <a href="#">42</a> |
| at vCenter .....                        | <a href="#">42</a> |
| recover root password .....             | <a href="#">66</a> |
| register                                |                    |
| SAL Gateway .....                       | <a href="#">17</a> |
| registering .....                       | <a href="#">16</a> |
| related documentation .....             | <a href="#">7</a>  |
| remote access service                   |                    |
| test status .....                       | <a href="#">36</a> |
| requirements                            |                    |
| virtual machine resources .....         | <a href="#">13</a> |
| reset password                          |                    |
| admin user .....                        | <a href="#">66</a> |
| os accounts .....                       | <a href="#">65</a> |
| reset root password .....               | <a href="#">66</a> |
| resource requirements .....             | <a href="#">13</a> |

|                            |                    |
|----------------------------|--------------------|
| restoring                  |                    |
| virtual machine .....      | <a href="#">47</a> |
| restoring a snapshot ..... | <a href="#">48</a> |
| root user                  |                    |
| reset password .....       | <a href="#">66</a> |

**S**

|                                                            |                    |
|------------------------------------------------------------|--------------------|
| SAL Gateway                                                |                    |
| register .....                                             | <a href="#">17</a> |
| test alarming services .....                               | <a href="#">36</a> |
| SAL Gateway implementation                                 |                    |
| test remote access service .....                           | <a href="#">36</a> |
| verify .....                                               | <a href="#">36</a> |
| SAL Gateway parameters                                     |                    |
| configure .....                                            | <a href="#">31</a> |
| SAL Gateway virtual appliance                              |                    |
| upgrade to Avaya Diagnostic Server virtual appliance ..... | <a href="#">50</a> |
| server hardware .....                                      | <a href="#">13</a> |
| server resources .....                                     | <a href="#">13</a> |
| SLA Mon server implementation                              |                    |
| verify .....                                               | <a href="#">38</a> |
| slamonsrvr service                                         |                    |
| test .....                                                 | <a href="#">38</a> |
| slamonweb service                                          |                    |
| test .....                                                 | <a href="#">39</a> |
| snapshot                                                   |                    |
| creating .....                                             | <a href="#">48</a> |
| restoring .....                                            | <a href="#">48</a> |
| snapshots .....                                            | <a href="#">62</a> |
| specifications                                             |                    |
| bundled software .....                                     | <a href="#">15</a> |
| starting virtual machine .....                             | <a href="#">31</a> |
| support .....                                              | <a href="#">9</a>  |
| supported VMware versions .....                            | <a href="#">14</a> |

**T**

|                               |                    |
|-------------------------------|--------------------|
| test                          |                    |
| alarming service .....        | <a href="#">36</a> |
| remote access service .....   | <a href="#">36</a> |
| slamon database service ..... | <a href="#">39</a> |
| slamonsrvr service .....      | <a href="#">38</a> |
| slamonweb service .....       | <a href="#">39</a> |
| testing                       |                    |
| Gateway UI .....              | <a href="#">37</a> |
| SAL Watchdog service .....    | <a href="#">38</a> |
| thick deployment .....        | <a href="#">61</a> |
| thin deployment .....         | <a href="#">61</a> |
| timekeeping .....             | <a href="#">58</a> |
| configuring .....             | <a href="#">59</a> |

**U**

|                                     |                    |
|-------------------------------------|--------------------|
| upgrade                             |                    |
| SAL Gateway virtual appliance ..... | <a href="#">50</a> |

|                   |                    |
|-------------------|--------------------|
| upgrade operation |                    |
| validating .....  | <a href="#">51</a> |

## V

|                                             |                    |
|---------------------------------------------|--------------------|
| validating                                  |                    |
| upgrade operation .....                     | <a href="#">51</a> |
| verify                                      |                    |
| SAL Gateway implementation .....            | <a href="#">36</a> |
| SLA Mon server implementation .....         | <a href="#">38</a> |
| videos .....                                | <a href="#">8</a>  |
| virtual appliance                           |                    |
| backup .....                                | <a href="#">46</a> |
| restore .....                               | <a href="#">47</a> |
| virtual machine                             |                    |
| automatic restart configuration .....       | <a href="#">34</a> |
| starting .....                              | <a href="#">31</a> |
| virtual machine resource requirements ..... | <a href="#">13</a> |
| vMotion .....                               | <a href="#">63</a> |
| VMware software                             |                    |
| supported .....                             | <a href="#">14</a> |
| VMware Tools .....                          | <a href="#">58</a> |
| VT support .....                            | <a href="#">56</a> |

## W

|             |                    |
|-------------|--------------------|
| WebLM ..... | <a href="#">14</a> |
|-------------|--------------------|