Deploying Avaya Aura® AE Services on Infrastructure as a Service Environment
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

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/getGenericDetailsDetailsId=2009112112456651010 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.

"Hosted Service" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in the Hosted SAS or other service description documentation regarding the applicable hosted service. If you purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCSESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHODOWNLOADS, 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 Heritange Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

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").
Heritage Nortel Software

“Heritage Nortel Software” means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/Licenselnfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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. Unless otherwise stated, 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.

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.

The following applies only if the H.264 (AVC) codec is distributed with the product, in whole or in part, including any code and software.

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT
Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

## Chapter 1: Introduction

- Purpose ............................................................................................................ 8
- Prerequisites ...................................................................................................... 8
- Change history ................................................................................................ 9

## Chapter 2: Overview

- Overview of Infrastructure as a Service environment ....................................... 10
- Supported applications in Infrastructure as a Service Environment .................. 11
- Topology .......................................................................................................... 11
- Connection types for Infrastructure as a Service .............................................. 13
- Networking considerations ............................................................................... 13
- Unsupported features of Avaya Aura® application on Infrastructure as a Service ... 14
- Software details of Application Enablement Services ....................................... 14
- Supported browsers on Infrastructure as a Service ........................................... 15
  - Supported browsers for Amazon Web Services Management Console .......... 15
  - Supported browsers for Microsoft Azure ......................................................... 15
  - Supported browsers for Google Cloud Platform ............................................. 16
- Disk partitioning ............................................................................................... 16
- Third party software requirements .................................................................... 16
- Application Enablement Services license requirements .................................... 16

## Chapter 3: Planning

- Planning for deploying ISO on Amazon Web Services ....................................... 17
  - Planning checklist .......................................................................................... 17
  - Supported footprints for AE Services on AWS .............................................. 17
- Planning for deploying ISO on Microsoft Azure ................................................ 18
  - Planning checklist .......................................................................................... 18
  - Hardware resources configuration matrix ....................................................... 18
- Planning for deploying ISO on Google Cloud Platform ..................................... 19
  - Planning checklist .......................................................................................... 19
  - Hardware resources configuration matrix ....................................................... 19
- Downloading software from PLDS ................................................................... 20
- Latest software updates and patch information ................................................. 21
- Required software ........................................................................................... 21
- Configuration tools and utilities ......................................................................... 22

## Chapter 4: Pre-deployment configuration

- Preconfiguration for deploying OVA on Amazon Web Services ......................... 23
  - Checklist for converting Avaya Aura® application OVA to an Amazon Machine Image ................................................ 23
  - Creating a bucket for uploading the OVAs for AMI conversion ..................... 23
  - Uploading the Avaya Aura® application OVA ............................................... 24
  - Creating a Linux Amazon EC2 virtual server instance ................................... 24
Contents

Creating a user access key.......................................................... 26
Obtaining the virtual server instance user ID................................. 26
Converting the OVA to AMI............................................................ 26
Predeployment tasks for deploying ISO on Amazon Web Services... 29
Predeployment checklist for Amazon Web Services......................... 29
Creating RHEL virtual machine on Amazon Web Services............. 30
Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services... 31
Configuring Yum on Amazon Web Services virtual machine........... 32
Predeployment tasks for deploying ISO on Microsoft Azure.......... 32
Predeployment checklist for Microsoft Azure.............................. 32
Creating RHEL virtual machine on Microsoft Azure.................... 33
Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure... 33
Predeployment tasks for deploying ISO on Google Cloud Platform... 34
Predeployment checklist for Google Cloud Platform...................... 34
Creating a PPK file.................................................................. 34
Creating RHEL instance on Google Cloud Platform..................... 35
Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform... 36
Verifying the ISO image on a Linux-based computer..................... 37

Chapter 5: Deploying...................................................................... 38
Deploying the AE Services server software................................ 38
Deploying Avaya Aura® Software-Only ISO image using Solution Deployment Manager...... 40
Installing the AE Services patch from CLI................................ 43
Amazon Web Services instance management.............................. 43
Starting an AWS instance............................................................ 44
Stopping an AWS instance........................................................... 44
Rebooting an AWS instance........................................................ 44

Chapter 6: Configuring................................................................. 46
Opening an ssh session to AE Services........................................ 46
Logging on to the AE Services Management web console........... 47
Editing the NIC configuration (optional)..................................... 48

Chapter 7: Post-installation verification........................................ 49
Verifying the software version.................................................... 49
Verifying the license................................................................. 49
Verifying the AE Service IP (Local IP) settings......................... 49
Verifying the Network Configure settings............................... 50
Verifying the time zone and NTP server settings....................... 51

Chapter 8: Resources................................................................. 52
Application Enablement Services documentation........................ 52
Finding documents on the Avaya Support website....................... 53
Accessing the port matrix document....................................... 54
Avaya Documentation Portal navigation................................... 54
Training................................................................................... 55
Viewing Avaya Mentor videos.................................................. 55
Chapter 1: Introduction

Purpose

This document describes the procedure to deploy Avaya Aura® Application Enablement Services on the following Infrastructure as a Service platforms:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

This document is intended for people who install and configure Avaya Aura® Application Enablement Services.

Prerequisites

Before deploying the Avaya Aura® Application Enablement Services on Infrastructure as a Service, ensure that you have the following knowledge and tools.

Knowledge

- Infrastructure as a Service platform that you use
- Linux® Operating System

Tools

For information about tools and utilities, see Configuration tools and utilities on page 22.
# Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
</table>
| 7     | September 2019| Updated the [Deploying the AE Services server software](#) on page 38 section. Added the following sections:  
• [Configuring an LDAP server for User Management](#) on page 58  
• [Creating an LDAP User account](#) on page 60                                                                                   |
| 6     | May 2019      | Updated the “Supported footprints for AE Services on AWS” section.                                                                                     |
| 5     | April 2019    | Updated the “Supported applications in Infrastructure as a Service Environment” section.                                                                |
| 4     | February 2019 | Updated the “Supported applications in Infrastructure as a Service Environment” section.                                                                |
| 3     | February 2019 | Updated the “Supported footprints for AE Services on AWS” section.                                                                                     |
| 2     | December 2018 | Updated the following sections:  
• Overview of Infrastructure as a Service environment  
• Release details of Avaya Aura® application                                                                                   |
| 1     | July 2018     | Initial release.                                                                                                                                          |
Chapter 2: Overview

Overview of Infrastructure as a Service environment

Infrastructure as a Service (IaaS) environment enables enterprises to securely run applications on the virtual cloud. The supported Avaya Aura® applications on IaaS can also be deployed on-premises. Avaya Aura® application supports the following platforms within this offer:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform
- IBM Bluemix

For information about Bluemix, see IBM Bluemix product documentation.

Supporting the Avaya Aura® applications on the IaaS platforms provide the following benefits:

- Minimizes the capital expenditure on infrastructure. The customers can move from capital expenditure to operational expense.
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.
- Allows you to pay per-use licensing.
- Allows you to upgrade at a minimal cost.
- Supports mobility to move from one network to another.
- Allows you to stay current with latest security updates provided by the service provider.

You can connect the following applications to the Avaya Aura® IaaS instances from the customer premises:

- Avaya Aura® Conferencing Release 8.0 and later
- Avaya Aura® Messaging Release 6.3 and later
- G430 Branch Gateway, G450 Branch Gateway, and G650 Media Gateway

Supported third-party applications

With the software-only (ISO) offer, you can install third-party applications on the system and get more control on the system. For the list of supported third-party software applications in Release 8.0 and later, see the Avaya Product Support Notice at PSN020360u.
## Supported applications in Infrastructure as a Service Environment

<table>
<thead>
<tr>
<th>Application</th>
<th>Release</th>
<th>Amazon Web Services</th>
<th>Microsoft Azure</th>
<th>Google Cloud Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Avaya Aura® System Manager</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya WebLM</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presence Services using Avaya Breeze® platform</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Avaya Aura® Device Services</td>
<td>Release 7.1.3</td>
<td>Y</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services (Software only)</td>
<td>Release 8.0.1</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Aura® Media Server (Software only)</td>
<td>Release 8.0</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Diagnostic Server (Software only)</td>
<td>Release 3.x</td>
<td>Y</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Avaya Session Border Controller for Enterprise</td>
<td>Release 8.0</td>
<td>Y</td>
<td>—</td>
<td>—</td>
</tr>
</tbody>
</table>

### Topology

The following diagram depicts the architecture of the Avaya applications on the Infrastructure as a Service platform. This diagram is an example setup of possible configuration offered by Avaya.  

⚠️ **Important:**  

The setup must follow the Infrastructure as a Service deployment guidelines, but does not need to include all the applications.
Deploying Avaya Aura® AE Services on Infrastructure as a Service Environment

Comments on this document? infodev@avaya.com
Connection types for Infrastructure as a Service

Amazon Web Services
You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

<table>
<thead>
<tr>
<th>Connection type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN connection</td>
<td>For more information, see <a href="https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html">https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/vpn-connections.html</a>.</td>
</tr>
<tr>
<td>Direct connection</td>
<td>For more information, see <a href="https://aws.amazon.com/directconnect/">https://aws.amazon.com/directconnect/</a></td>
</tr>
</tbody>
</table>

Microsoft Azure
You can connect applications in a hybrid network on the Virtual Networks (VNet) in the following ways:

<table>
<thead>
<tr>
<th>Connection type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN connection</td>
<td>For more information, see <a href="https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal">https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal</a></td>
</tr>
<tr>
<td>Direct connection</td>
<td>For more information, see <a href="https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction">https://docs.microsoft.com/en-us/azure/expressroute/expressroute-introduction</a></td>
</tr>
<tr>
<td>Express route</td>
<td>For more information, see <a href="https://docs.microsoft.com/en-us/azure/networking/networking-overview#on-premises-connectivity">https://docs.microsoft.com/en-us/azure/networking/networking-overview#on-premises-connectivity</a></td>
</tr>
</tbody>
</table>

Google Cloud Platform
You can connect applications in a hybrid network on the Virtual Private Cloud (VPC) in the following ways:

<table>
<thead>
<tr>
<th>Connection type</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>VPN connection</td>
<td>For more information, see <a href="https://cloud.google.com/vpn/docs/concepts/overview">https://cloud.google.com/vpn/docs/concepts/overview</a></td>
</tr>
<tr>
<td>GCN Direct</td>
<td>For more information, see <a href="https://cloud.google.com/interconnect/docs/concepts/dedicated-overview">https://cloud.google.com/interconnect/docs/concepts/dedicated-overview</a></td>
</tr>
</tbody>
</table>

Networking considerations
When you deploy an Avaya application at main location or at a branch location on Infrastructure as a Service, ensure that you follow the networking requirements, such as, the WAN network topology, bandwidth and latency of the Avaya applications. You must adhere to the Avaya network recommendations and Infrastructure as a Service networking rules.

Infrastructure as a Service has some limitations for establishing public internet VPNs and direct connections.

For more information about Amazon VPC Limits, see the Amazon Web Services documentation at https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html.
For more information about Microsoft Azure VPN connection limits and VPN Gateway, see the Microsoft Azure documentation at https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-about-vpngateways.

⚠️ Important:

Avaya recommends the use of direct connection in combination of a private WAN connection with Service Level Agreement that measures to ensure that the network quality is appropriate for signaling and voice traffic.

Avaya is not responsible for network connections between Infrastructure as a Service and customer premises.

---

Unsupported features of Avaya Aura® application on Infrastructure as a Service

**Amazon Web Services**
The Avaya Aura® application does not support the following features on Amazon Web Services:

- Out of Band Management configurations
- IPv6 addresses

**Microsoft Azure**
The Avaya Aura® application does not support the following features on Microsoft Azure:

- Out of Band Management configurations
- IPv6 addresses

**Google Cloud Platform**
The Avaya Aura® application does not support the following features on Google Cloud Platform:

- IPv6 addresses

---

Software details of Application Enablement Services

The following table lists the software details of all the supported platform for the application. You can download the softwares from the Avaya PLDS website at http://plds.avaya.com/.
Table 1: Application Enablement Services build details

<table>
<thead>
<tr>
<th>Release</th>
<th>Bundle offer type</th>
<th>Installer files</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.0.1</td>
<td>OVA</td>
<td>• AVP and VMware: AES-8.0.1.0.0.5.20181122-e65-00.ova</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• KVM: AES-8.0.1.0.0.5.20181122-kvm-001.ova</td>
</tr>
<tr>
<td>8.0.1</td>
<td>ISO</td>
<td>swonly-8.0.1.0.0.5-20181122.iso</td>
</tr>
<tr>
<td>8.0.1</td>
<td>Pre-upgrade Patch file</td>
<td>AES801_PreUpgradePatch.bin</td>
</tr>
<tr>
<td>8.0.1</td>
<td>Patch file</td>
<td>aesvcs-8.0.1.0.0.5-featurepack.bin</td>
</tr>
<tr>
<td>8.0.1</td>
<td>Super Patch file</td>
<td>aesvcs-8.0.1.0.1-superpatch.bin</td>
</tr>
<tr>
<td>8.0.1</td>
<td>Solution Deployment Manager Client</td>
<td>Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip contains the Avaya_SDMClient_win64_8.0.1.0.0332099_11.exe file.</td>
</tr>
</tbody>
</table>

Supported browsers on Infrastructure as a Service

Supported browsers for Amazon Web Services Management Console

Amazon Web Services Management Console supports the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest 3 versions</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Latest 3 versions</td>
</tr>
<tr>
<td>Microsoft Internet Explorer</td>
<td>11</td>
</tr>
<tr>
<td>Microsoft Edge</td>
<td>12</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>9, 8, 7</td>
</tr>
</tbody>
</table>

Supported browsers for Microsoft Azure

Microsoft Azure portal supports the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Chrome</td>
<td>Latest version</td>
</tr>
</tbody>
</table>
## Supported browsers for Google Cloud Platform

Google Cloud Platform supports the following web browsers:

<table>
<thead>
<tr>
<th>Browser</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Edge</td>
<td>Latest version</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>11</td>
</tr>
<tr>
<td>Apple Safari</td>
<td>Latest version. Applicable for Mac only.</td>
</tr>
<tr>
<td>Google Chrome</td>
<td>Latest version</td>
</tr>
<tr>
<td>Mozilla Firefox</td>
<td>Latest version</td>
</tr>
</tbody>
</table>

## Disk partitioning

You must allocate 10 GB size for `/var` partition.

## Third party software requirements

You can deploy the Avaya Aura® application ISO file on a Red Hat Enterprise Linux 7.4 virtual machine by using the bash command line or by using the Solution Deployment Manager.

## Application Enablement Services license requirements

To get the full functionality for Application Enablement Services you must install the Application Enablement Services product license. The product license specifies the features you are permitted to use. For more information about licensed features, see the Avaya Aura® Application Enablement Services Overview and Specification.
Chapter 3: Planning

Planning for deploying ISO on Amazon Web Services

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application ISO on Amazon Web Services:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Purchase the required licenses. Register for PLDS and perform the following:</td>
<td>Go to the Avaya Product Licensing and Delivery System at <a href="https://plds.avaya.com/">https://plds.avaya.com/</a>.</td>
</tr>
<tr>
<td></td>
<td>• Obtain the license file.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Activate license entitlements in PLDS.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td>Download the required software.</td>
<td>See <a href="#">Downloading software from PLDS</a> on page 20.</td>
</tr>
<tr>
<td>3.</td>
<td>Verify that you have a valid Red Hat subscription.</td>
<td>Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription.</td>
</tr>
</tbody>
</table>

Supported footprints for AE Services on AWS

<table>
<thead>
<tr>
<th>AES Deployment Type</th>
<th>Footprint</th>
<th>AWS instance type</th>
<th>AWS vCPU</th>
<th>AWS RAM (GB)</th>
<th>HDD (GB)</th>
<th>NICs</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES (Software only)</td>
<td>Profile 1</td>
<td>m3.medium</td>
<td>1</td>
<td>4(3.75)</td>
<td>30 GB</td>
<td>2</td>
</tr>
<tr>
<td>AES (Software only)</td>
<td>Profile 2</td>
<td>c4.large</td>
<td>2</td>
<td>4(3.75)</td>
<td>30 GB</td>
<td>2</td>
</tr>
<tr>
<td>AES (Software only)</td>
<td>Profile 3</td>
<td>c3.xlarge</td>
<td>4</td>
<td>6(7.5)</td>
<td>30 GB</td>
<td>2</td>
</tr>
</tbody>
</table>
Planning for deploying ISO on Microsoft Azure

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application on Microsoft Azure:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Purchase the required licenses. Register for PLDS and perform the following • Obtain the license file. • Activate license entitlements in PLDS.</td>
<td>Go to the Avaya Product Licensing and Delivery System at <a href="https://plds.avaya.com/">https://plds.avaya.com/</a></td>
</tr>
<tr>
<td>2.</td>
<td>Download the required Avaya Aura® application ISO.</td>
<td>See Downloading software from PLDS on page 20.</td>
</tr>
</tbody>
</table>

Hardware resources configuration matrix

AE Services 8.0 ISO provides 3 AE ServicesProfiles with different CPU and memory sizes during the installation process. The specified CPU and memory is assigned and reserved to that particular AE ServicesVirtualized Environment. Profile 1 has 1 CPU 2 GB resource, being the lowest footprint, Profile 2 has 2 CPU 2 GB resources, and Profile 3 has 4 CPU 4 GB resources. Each footprint/Profile has different capacities based on the number of users and BHCC.

AE Services 8.0 supports the following footprint matrix:

<table>
<thead>
<tr>
<th>Footprint</th>
<th>DMCC — Third party call control: Microsoft OCS/Lync, IBM Sametime, Avaya Aura® Contact Center</th>
<th>DMCC — First Party call control</th>
<th>TSAPI, DLG, CVLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum number of users or agents</td>
<td>Maximum number of users or agents</td>
<td>Maximum Messages per second (MPS) Rate</td>
</tr>
<tr>
<td>1 CPU and 2 GB RAM</td>
<td>1K 10K</td>
<td>20K BHCC 6K BHCC</td>
<td>1K 9K BHCC 1K MPS</td>
</tr>
</tbody>
</table>

Table continues…
### Planning for deploying ISO on Google Cloud Platform

#### Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application on Google Cloud Platform:

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
</table>
| 1.  | Purchase the required licenses. Register for PLDS and perform the following  
|    |   • Obtain the license file.  
|    |   • Activate license entitlements in PLDS. | Go to the Avaya Product Licensing and Delivery System at [https://plds.avaya.com/](https://plds.avaya.com/). |
| 2.  | Download the required Avaya Aura® application ISO. | See [Downloading software from PLDS](#) on page 20. |

#### Hardware resources configuration matrix

AE Services 8.0 ISO provides 3 AE Services Profiles with different CPU and memory sizes during the installation process. The specified CPU and memory is assigned and reserved to that particular AE Services Virtualized Environment. Profile 1 has 1 CPU 2 GB resource, being the
AE Services 8.0 supports the following footprint matrix:

<table>
<thead>
<tr>
<th>Footprint</th>
<th>Maximum number of users or agents</th>
<th>Maximum BHCC</th>
<th>Maximum number of users or agents</th>
<th>Maximum BHCC</th>
<th>Maximum Messages per second (MPS) Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 CPU and 2 GB RAM</td>
<td>1K</td>
<td>20K BHCC</td>
<td>1K</td>
<td>9K BHCC</td>
<td>1K MPS</td>
</tr>
<tr>
<td></td>
<td>10K</td>
<td>6K BHCC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 CPU and 2 GB RAM</td>
<td>2.5K</td>
<td>50K BHCC</td>
<td>2.4K</td>
<td>18K BHCC</td>
<td>1K MPS</td>
</tr>
<tr>
<td></td>
<td>12K</td>
<td>12K BHCC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 CPU and 4 GB RAM</td>
<td>5K</td>
<td>100K BHCC</td>
<td>8K</td>
<td>36K BHCC</td>
<td>2K MPS</td>
</tr>
<tr>
<td></td>
<td>20K</td>
<td>24K BHCC</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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](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](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.

---

**Latest software updates and patch information**

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the product or solution on the Avaya Support web site at [https://support.avaya.com/](https://support.avaya.com/).

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

---

**Required software**

Application Enablement Services Software-Only installation requires that you install the AE Services Software-only template.

Download the AE Services software from the Product Licensing and Delivery System (PLDS) web site, then verify the ISO image. For new installations you must write the ISO image to a CD. For upgrade installations, download the .bin file to the AE Services server.
Configuration tools and utilities

To deploy and configure the applications, you need the following tools and utilities:

• A browser for accessing the Amazon Web Services Management Console.
• PuTTY, PuTTYgen, WinSCP, and WinZip.
Chapter 4: Pre-deployment configuration

Preconfiguration for deploying OVA on Amazon Web Services

Checklist for converting Avaya Aura® application OVA to an Amazon Machine Image

Ensure that you complete the following before converting the Avaya Aura® application OVA to an Amazon Machine Image (AMI).

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td>Create a bucket for uploading the OVAs.</td>
<td>Creating a bucket for uploading the OVAs for AMI conversion on page 23</td>
</tr>
<tr>
<td>2.</td>
<td>Upload the Avaya Aura® application OVA.</td>
<td>Uploading the Avaya Aura application OVA on page 24.</td>
</tr>
<tr>
<td>5.</td>
<td>Obtain the virtual server instance user ID.</td>
<td>Obtaining the virtual server instance user ID on page 26.</td>
</tr>
<tr>
<td>6.</td>
<td>Convert OVA to AMI.</td>
<td>Converting the OVA to AMI on page 26.</td>
</tr>
</tbody>
</table>

Creating a bucket for uploading the OVAs for AMI conversion

Procedure

1. Sign in to the Amazon Web Services Management console.
2. Go to Services > Storage, and click S3.
The system displays the S3 Management Console page.

3. Click **Create bucket**.
   The system displays the Create bucket dialog box.

4. In **Bucket name**, type a unique bucket name.
   Only use lowercase letters for the name.

5. In the **Region** field, click a region for your bucket.
   For more information about creating a bucket and selecting a region, see Amazon S3 Documentation.

6. Click **Create**.

---

**Uploading the Avaya Aura® application OVA**

**Procedure**

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services > Storage**, and click **S3**.
   The system displays the S3 Management Console page.
3. From the **All Buckets** section, select a bucket.
4. Click **Upload**.
   The system displays the Upload - Select Files and Folders dialog box.
5. Click **Add Files**.
6. On the Choose File to Upload dialog box, select Avaya Aura® application OVA file from your local system, and click **Open**.
7. Click **Upload**.

---

**Creating a Linux Amazon EC2 virtual server instance**

**Procedure**

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services > Compute**, and click **EC2**.
   The system displays the EC2 Management Console page.
3. Click **Launch Instance**.
4. On the Choose an Amazon Machine Image (AMI) page, search for a Linux AMI, and click **Select**.
5. On the Choose an Instance Type page, select an instance type according to your profile, and click **Next: Configure Instance Details**.

6. On the Configure Instance Details page, do the following:
   a. In the **Network** field, click a VPC network.
   b. In the **Network interfaces** section, assign an IP address.

7. Click **Next: Add Storage**.

8. On the Add Storage page, add partitions according to your profiles, and click **Next: Add Tags**.

9. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.

10. On the Configure Security Group page, create a new security group or select an existing security group, and click **Review and Launch**.

11. On the Review Instance Launch page, review the details of each configuration, and then click **Launch**.

12. On the Select an existing key pair or create a new key pair dialog box, select one of the following options:
   
   - **Choose an existing key pair**: If you select this option, perform the following:
     a. From the **Select a key pair** drop-down list, select a key pair.
     b. Select the **I acknowledge that I have access to the selected private key file (<example.pem>), and that without this file, I won't be able to log into my instance** check box.
   
   - **Create a new key pair**: If you select this option, perform the following:
     a. In the **Key pair name** field, type a name for the private key file. The extension of the private key file is `.pem`.
     b. Click **Download Key Pair**.
     c. Save the file in a secure and accessible location.
   
   - **Note**: You will not be able to download the file again.

   - **Proceed without a key pair**: If you select this option, select the **I acknowledge that I will not be able to connect to this instance unless I already know the password built into this AMI** check box.

13. Click **Launch Instances**.

   The system creates the virtual server instance.

14. Click **Launch Status**, and click **View instance**.

   When the system creates an instance, the **Status Checks** column displays the message: **2/2 checks passed**.
Creating a user access key

Procedure
1. Sign in to the Amazon Web Services Management console.
2. Go to Services > Security, Identity & Compliance, and click IAM.
   The system displays the Welcome to Identity and Access Management page.
3. In the left navigation pane, click Users.
4. Click on a user name.
5. On the Summary page, click the Security Credentials tab.
6. In the Access Keys section, click Create Access Key.
   The system displays the message: Your access key has been created successfully.

⚠️ Important:
When you create a security access key, you must save it. If you lose the security access key, you cannot retrieve it.

Obtaining the virtual server instance user ID

Procedure
1. Sign in to the Amazon Web Services Management console.
2. Go to Services > Compute, and click EC2.
   The system displays the EC2 Management Console page.
3. In the left navigation pane, click Instances.
4. Select a server instance, and click Connect.
5. On the Connect To your Instance page, view the user ID.

   Example:
   `ssh -i "example.pem" ec2-user@<IP address>`

   The user name is ec2-user. Use this user ID to connect to the Linux server.

Converting the OVA to AMI

Before you begin
- Create an access key. For more information, see “Creating an access key”.

• Obtain the user id. For more information, see “Obtaining the virtual server instance user id”.
• Converting the *.pem file to the *.ppk format and configure PuTTY for establishing an SSH connection. For more information, see “Configuring PuTTY”.

Procedure

1. Open an SSH session.
2. In Host Name (or IP address), type the IP Address of the virtual server instance, and click Open.
3. Log in to the Linux server, and run the command: `aws`.
4. To configure the AWS details, run the command: `aws configure`, and do the following:
   a. In AWS Access Key ID, type the AWS access key ID.
   b. In AWS Secret Access Key, type the AWS secret access key ID.
   c. In Default region name, type the region name.
      For example: us-west-2.
   d. In Default output format, type text or json.
5. To check whether the EC2 instance is ready to use, run the command: `aws s3 ls`.
      The system displays the S3 bucket that you created.
6. To view the content of the S3 bucket, run the command: `aws s3 ls s3://<nameofbucket>`.

   Note:
   If DNS resolution for the VPC is disabled, the execution of the `aws s3 ls s3://<nameofbucket>` command fails.
7. To allow importing files into the EC2 instance, create a vmimport role, and attach policies as mentioned in the following sub-steps:
   a. Create a file named trust-policy.json with the following policy:

   ```json
   ```
   b. Use the create-role command to create a role named vmimport and give VM Import/Export access to it.
      Ensure that you specify the full path to the location of the trust-policy.json file, and prefix file:// to it:
      ```command
      aws iam create-role --role-name vmimport --assume-role-policy-document file://trust-policy.json
      ```
   c. Create a file named role-policy.json with the following policy:
      Where <your_bucket_name> is the bucket where the OVA is stored:

      ```json
      { "Version": "2012-10-17", 
      ```
"Statement": [
    {
        "Effect": "Allow",
        "Action": [
            "s3:ListBucket",
            "s3:GetBucketLocation"
        ],
        "Resource": [
            "arn:aws:s3:::<your_bucket_name>
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:GetObject"
        ],
        "Resource": [
            "arn:aws:s3:::<your_bucket_name>/*
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:ModifySnapshotAttribute",
            "ec2:CopySnapshot",
            "ec2:RegisterImage",
            "ec2:Describe*"
        ],
        "Resource": "*"
    }
]

---

**d. Use the following put-role-policy command to attach the policy to the role created above.**

Ensure that you specify the full path to the location of the `role-policy.json` file.

```bash
aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-document file://role-policy.json
```

**8. To import the ova for conversion, type the following command:**

```bash
aws ec2 import-image --cli-input-json "{"Description": "<Server OVA>",
\"DiskContainers": [{ "Description": "<text description of task>",
\"UserBucket": { \"S3Bucket": "<your_bucket_name>", \"S3Key" : "<server.ova>" } }]
"
```

Ensure to replace appropriate values wherever brackets <> are present in above command.

The system displays the **Status** and the **ImportTaskId** parameters.

**9. To check the status of the import image, run the command:**

```bash
aws ec2 describe-import-image-tasks --cli-input-json "{"ImportTaskIds": [
\"<Your_ImportTaskId>\"], \"NextToken\": \"abc\", \"MaxResults\": 10 }"
```

Where, **ImportTaskId** is the one from the output of the Step 8. For example: `import-ami-ffmanv5x`
The conversion process takes up to 30 minutes. You can run the above command repeatedly. When the AMI conversion is successful, the system displays the **Status** as **completed** and also displays **ImageId**.

In the following example, the process is at the update stage and is 30% complete.

```
[ec2-user@ip-10-143-10-81 ~]$ aws ec2 describe-import-image-tasks --cli-input-json "{"ImportTaskIds": ["import-ami-ffgji45r"], "NextToken": "abc", "MaxResults": 10 }" IMPORTIMAGETASKS <product_name>8.0.xxx-aws-001.ova import-ami-ffgji45r 30 active updating
```

In the following example, the process is preparing the AMI and is 76% complete.

```
IMPORTIMAGETASKS x86_64 <product_name>8.0.xxx-aws-001.ova import-ami-ffgji45r BYOL Linux 76 active preparing ami
```

The output format varies depending on the selection of the text or JSON format on the aws CLI configuration.


10. Sign in to the Amazon Web Services Management console.

11. Go to **Services > Compute**, and click **EC2**.

   The system displays the EC2 Management Console page.

12. In the left navigation pane, click **IMAGES > AMIs**.

   You can search the converted AMI with **ImageId**. The system displays the newly converted AMI **ImageId** in the **AMI ID** column.

   You can give an appropriate name for the AMI **ImageId**.

---

**Predeployment tasks for deploying ISO on Amazon Web Services**

---

**Predeployment checklist for Amazon Web Services**

Perform the following tasks to deploy Avaya Aura® application ISO on Amazon Web Services.

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a virtual machine.</td>
<td>See <a href="#">Creating RHEL virtual machine on Amazon Web Services</a> on page 30</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Assign the required resources to the virtual machine.</td>
<td>See <a href="#">Disk partitioning</a> on page 16</td>
</tr>
<tr>
<td>3</td>
<td>Copy the ISO to the virtual machine.</td>
<td>See <a href="#">Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services</a> on page 31</td>
</tr>
<tr>
<td>4</td>
<td>Configure Yum.</td>
<td>See <a href="#">Configuring Yum on Amazon Web Services virtual machine</a> on page 32</td>
</tr>
</tbody>
</table>

### Creating RHEL virtual machine on Amazon Web Services

**About this task**

Use this procedure to create RHEL virtual machine on Amazon Web Services.

**Note:**

Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

Also, please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Amazon Web Services documentation.

**Procedure**

1. Sign in to the Amazon Web Services Management console.
2. Go to **Services > Compute**, and click **EC2**.
   
The system displays the EC2 Management Console page.
3. Click **Launch Instance**.
4. On the Choose an Amazon Machine Image (AMI) page, search for RHEL 7.4, and click **Select**.
5. On the Choose an Instance Type page, select the instance type according to your profile, and click **Next: Configure Instance Details**.
6. On the Configure Instance Details page, do the following:
   a. In the **Network** field, click a VPC network.
   b. In the **Subnet** field, add the required details.
   c. In the **Network interfaces** section, assign an IP address.
7. Click **Next: Add Storage**.
8. On the Add Tags page, add a tag, and click **Next: Configure Security Group**.
9. On the Configure Security Group page, create a new security group or select an existing security group, and click Review and Launch.

10. On the Review Instance Launch page, review the details of each configuration, and then click Launch.

11. On the Select an existing key pair or create a new key pair dialog box, select one of the following options:

   • **Choose an existing key pair**: If you select this option, perform the following:
     a. From the Select a key pair drop-down list, select a key pair.
     b. Select the I acknowledge that I have access to the selected private key file (<example.pem>), and that without this file, I won't be able to log into my instance check box.

   • **Create a new key pair**: If you select this option, perform the following:
     a. In the Key pair name field, type a name for the private key file. The extension of the private key file is .pem.
     b. Click Download Key Pair.
     c. Save the file in a secure and accessible location.

   🌟 **Note**: You will not be able to download the file again.

12. Click Launch Instances.

   The system creates the RHEL instance.

13. Click Launch Status, and click View instance.

   When the system creates an instance, the Status Checks column displays the message: 2/2 checks passed.

---

**Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services**

**About this task**
You can upload the ISO file using WinSCP.

**Before you begin**
Create a virtual machine instance on Amazon Web Services
Create a ppk file

**Procedure**
1. Open WinSCP.
2. From the advance section, choose the authentication and browse to the .ppk file, and click login.
3. Enter the login credentials.
4. Upload the .iso to the virtual machine instance by using the IP address of the virtual machine.

---

**Configuring Yum on Amazon Web Services virtual machine**

**Procedure**

1. Log on to your virtual machine as a root user.
2. Run the following command to edit the `redhat-rhui.repo` file:
   ```
   vi /etc/yum.repos.d/redhat-rhui.repo
   ```
   In the enabled field, enter 1.
3. Set `enable=1` for:
   ```
   [rhui-REGION-rhel-server-optional]
   name=Red Hat Enterprise Linux Server 7 Optional (RPMs)
   ```
   and
   ```
   [rhui-REGION-rhel-server-rhscl]
   Name=Red Hat Enterprise Linux Server 7 RHSCL (RPMs)
   ```

---

**Predeployment tasks for deploying ISO on Microsoft Azure**

**Predeployment checklist for Microsoft Azure**

Perform the following tasks to deploy Avaya Aura® application ISO on Microsoft Azure.

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a virtual machine.</td>
<td>See <a href="#">Creating RHEL virtual machine on Microsoft Azure</a> on page 33</td>
</tr>
<tr>
<td>2</td>
<td>Assign the required resources to the virtual machine.</td>
<td>See <a href="#">Disk partitioning</a> on page 16</td>
</tr>
<tr>
<td>3</td>
<td>Copy the ISO to the virtual machine.</td>
<td>See <a href="#">Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure</a> on page 33</td>
</tr>
</tbody>
</table>
Creating RHEL virtual machine on Microsoft Azure

Before you begin
Create an account on Microsoft Azure.

⚠️ Important:
Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

⚠️ Note:
Please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Microsoft Azure documentation.

Procedure
1. Log on to the Azure portal.
2. In the search box, search for the customized image you uploaded and click on that image.
3. On disk page, click on Create VM link. A virtual machine is created.
4. In the Basics tab, enter the required details and click OK.
   
   Ensure that you select authentication type as password instead of SSH public key.
5. Select the subnet created for main interface.
6. In the Settings tab, enter or select the required details, and click OK.
7. In the Summary tab, click Create.
   
   The deployment begins. After the successful deployment, shut down the virtual machine.
8. On the Virtual Machines page, click on the RHEL virtual machine name that you created.
9. Ensure that the hard disk size is 30 GB.

Next steps
Uploading the ISO on to the RHEL virtual machine instance on Microsoft Azure.

Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure

Before you begin
Create RHEL virtual machine instance on Microsoft Azure.

Procedure
1. Open WinSCP session with your RHEL machine on Microsoft Azure by using the user ID and password that you provided at the time of creating the virtual machine.
2. From the advance section, choose the authentication and browse to the .ppk file, and click login.
3. Enter the login credentials.
4. Upload the .iso file to the virtual machine instance.

---

**Predeployment tasks for deploying ISO on Google Cloud Platform**

**Predeployment checklist for Google Cloud Platform**

Perform the following tasks to deploy Avaya Aura® application ISO on Google Cloud Platform.

<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Create a PPK file</td>
<td>See <a href="#">Creating a PPK file</a> on page 34.</td>
</tr>
<tr>
<td>2</td>
<td>Create RHEL virtual machine instance</td>
<td>See <a href="#">Creating RHEL instance on Google Cloud Platform</a> on page 35.</td>
</tr>
<tr>
<td>3</td>
<td>Assign the required resources to the RHEL virtual machine instance</td>
<td>See <a href="#">Disk partitioning</a> on page 16.</td>
</tr>
<tr>
<td>4</td>
<td>Copy the ISO to the RHEL virtual machine instance</td>
<td>See <a href="#">Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform</a> on page 36</td>
</tr>
</tbody>
</table>

**Creating a PPK file**

**Procedure**

1. Open puttygen file, and click **Load**.
2. Under the **Parameters** section, select SSH-2 RSA.
3. Under **Actions** section, click **Generate**.
   
   You will be instructed to move the mouse cursor around within the PuTTY Key Generator window as a randomizer to generate the private key.

4. Enter a value in the **Key passphrase** and enter the same value in the **Confirm passphrase** field to protect the private key.
5. Click **Save private key**, and save the file to your local computer.
6. The box under **Public key for pasting into OpenSSH authorized_keys file:** contains the public key.
7. Copy the public key.
8. Open a text editor and paste the public key into the text editor and save the file.

---

**Creating RHEL instance on Google Cloud Platform**

**Before you begin**
Create an account on Google Cloud Platform.
Create a ppk file.

⚠️ **Important:**
Avaya recommends installing only required RPMs to the system for security and stability. Do not install complete Red Hat system.

🌟 **Note:**
Please note that the steps provided in this section are for reference purpose only. For the most up-to-date information, see the Google Cloud Platform documentation.

**Procedure**

1. Log on to the Google Cloud Platform.
2. Go to **Compute Engine > VM Instances.**
3. In the VM Instances page, click **CREATE INSTANCE**
4. In the **Create an instance** page, do the following:
   a. In the **Name** field, enter the name of your product.
   b. In the **Zone** field, select the required zone.
   c. In the **Machine type** field, select the number of CPUs and memory needed for your deployment.
5. Under the **Boot disk** section, click **Change** and do the following:
   a. Select the RHEL image.
   b. In the **Size (GB)** field, enter the required disk size and click **Select.**
Create an instance page appears.
6. Click **Networking** and do the following:
   a. In the **Network** field, select VPC network.
   b. In the **Subnetwork** field, select an appropriate subnet.
   c. In the **Primary Internal IP** field, select Ephemeral Custom.
   d. In the **Custom ephemeral IP address** field, enter an IP address that is within the range of your network.
e. In the **External IP** field, select None

7. Click **Done**.

8. Click **SSH Keys**.

9. In the **Enter entire key data** section, copy your private key details.

![SSH Keys](image)

When you paste the key, a login user is also created.

10. Click **Create**

    Virtual machine instance will be deployed.

**Next steps**

Uploading the ISO on to the RHEL virtual machine instance.

---

**Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform**

**About this task**

You can upload the ISO file using WinSCP.

**Before you begin**

Create a virtual machine instance on Google Cloud Platform.

Reuse the PPK file that was created earlier.

**Procedure**

1. Open WinSCP.

2. From the advance section, choose the authentication and browse to the .ppk file, and click login.

3. Enter the login credentials.
4. Upload the .iso to the virtual machine instance by using the IP address of the virtual machine.

---

**Verifying the ISO image on a Linux-based computer**

**About this task**

Use this procedure to verify that the md5 checksum of the downloaded ISO image matches the md5 checksum that is displayed for the ISO image on the PLDS Web site.

Use this procedure if you downloaded ISO images to a Linux-based computer.

**Procedure**

1. Enter `md5sum file name`, where `file name` is the name of the ISO image. Include the .iso file name extension.
2. Compare the md5 checksum of the ISO image to be used for installation with the md5 checksum that is displayed for the ISO image on the PLDS Web site.
3. Ensure that both numbers are the same.
4. If the numbers are different, download the ISO image again and reverify the md5 checksum.
Chapter 5: Deploying

Deploying the AE Services server software

About this task

- You can install the AE Services software from either a CD, DVD, or an ISO image. For information about obtaining the ISO image, see Required software on page 21.
- The procedure uses the following packages:
  - cs-cusldap: The LDAP Configuration package for AE Services. This is a mandatory package.
  - aesvcs-linuxconfig: The Linux Configuration package for AE Services. This is an optional package.
- `mountpoint` is the name of the media directory. For example, if the media directory is `/media/cdrom`, replace `mountpoint` with `/media/cdrom`.

Note:

You must install the AE Services server software using the ISO file from a window that emulates xterm or is recognized by Linux. If you install the server software from a DOS window, you might have display problems.

Procedure

1. Open an ssh session to the AE Services server and open an account with root privileges.
2. List the contents of `/etc/fstab` to find out the name of the media directory. The media directory is the mount point for this procedure.
3. If you install from a CD or DVD, insert the disk into the DVD or CD drive on the AE Services server.
   If you have installed and configured the Autorun RPM on the server, the installation program starts automatically. Do the following steps if the installation program does not start automatically:
   a. Type the command `mount mountpoint` to ensure that the media directory is properly mounted.
   b. Type the command `mountpoint/install` to start the installation program manually.

The installation wizard displays the Navigating the dialog boxes screen. Go to step 5.
4. If you install the AE Services server software from an ISO image, download the ISO image to the /tmp directory of the AE Services server, and then do one of the following:

   • Mount the image using the `mount` command. For example `mount -t iso9660 -o loop /tmp/swonly-<build-number>.iso mountpoint`

   • Start the installation program manually, by typing the command: `/mountpoint/install`

   The installation wizard displays the Navigating the dialog boxes screen.

5. Press **Enter** to continue with the installation.

   The installation wizard displays the Select Installation Media screen.

6. Select the media and press **Enter**.

7. In the Enter RPM URL screen, type the path name. For example, type the path name as `/media/cdrom/Releases`.

8. Highlight **OK** and press **Enter**.

   The installation wizard displays the Select Release Version screen with the latest version selected by default.

9. Press **Enter**.

10. In the Co-residency warning screen, highlight **Yes** and press **Enter**.

11. In the Choose Installation Method screen, verify that **Install/Update** is selected; then highlight **OK** and press **Enter**.

    The installation wizard displays the Choose Installation Packages screen with the following packages selected:

    • MVAP Avaya AE Services
    • Third Party Third_Party_Packages

12. Highlight **OK** and press **Enter**.

    The installation wizard displays the Optional Package screen with the `aesvcs-linuxconfig` package selected.

13. Select the Optional Package.

    The installation wizard selects the default package, aesvcs-linuxconfig. It is the Linux Configuration package for AE Services.

    Avaya recommends that you accept the default.

**Caution:**

If you use your own implementation of LDAP, cs-cusldap will overwrite your existing LDAP directory. To use the existing LDAP directory with AE Services manually configure your LDAP implementation for compatibility with AE Services User Management. For this procedure, see Configuring the LDAP server on page 59.
The installation wizard displays the Enable and Disable Enhanced Access Security Gateway options.

14. Select the appropriate Security Gateway option.

★ Note:

Enhanced Access Security Gateway option enables or disables Avaya Services logins to access your system. Register your product using Avaya Global Registration Tool to enable Avaya Remote Connectivity. You can also enable this feature after deploying the application by using the command `EASGManage`.

The installation wizard displays the Last chance to abort -- Ready to Proceed? screen.

15. Select Yes to continue.

16. Verify the installation command. If all options are correct, press Enter to select Yes.

The time required to install the software depends on the packages and the server processing power. Allow 5 to 10 minutes for the installation. When the installation is complete, the program displays the following message:

    Success, Installation/Update completed

17. During the installation, press Enter to Exit.

    • If the installation is successful, the wizard displays the following message:

        Installation Successful — Install/Upgrade log file is in /var/disk/logs

    • If the installation is unsuccessful, the wizard displays the following message:

        Installation/Update failed

18. Press Enter to select OK.

19. Please remove the DVD or CD. if you used it for the AE Services installation

20. Reboot the server.

Next steps
Install the AE Services license. See license requirements on page 16.

---

Deploying Avaya Aura® Software-Only ISO image using Solution Deployment Manager

About this task

Use this procedure to deploy the Avaya Aura® application ISO image file in a Software-Only environment.
Before you begin

• Add a location.
• Add a platform
• Add an Operating System user on RHEL instance
  For example, you can add a user using the following commands: `adduser <username>`, `passwd <username>`
• Set the password for the root user
  For example, you can set the password using the following command: `passwd <root>`

Procedure

1. To start the Solution Deployment Manager client, click **Start > All Programs > Avaya > Avaya SDM Client** or click the SDM icon on the desktop.

2. Click **Application Management**.

3. In **Application Management Tree**, select a location.

4. On the **Applications** tab, click **New**.
   The system displays the Application Deployment dialog box.

5. In the Select Location and Platform section, do the following:
   a. In **Select Location**, select a location if not already selected.
   b. In **Select Platform**, select a platform to deploy the **Software-Only ISO image**.
      The system displays the IP Address and FQDN of the platform in the **Platform IP** and **Platform FQDN** fields.
      Avaya recommends to keep the FQDN value short because when the FQDN of RHEL system on Google Cloud Platform is greater than 45 characters, the HTTPD service of Application Enablement Services fails to start. If the FQDN in the /etc/hosts file becomes more than 45 characters, you must remove the FQDN from the file, restart the system, and then install Application Enablement Services.

6. In the Provide admin and root Credentials section, do the following:
   a. In **Admin User of OS**, type the admin user name.
   b. In **Admin Password of OS**, type the admin user password.
   c. In **Root User of OS**, type the root user name.
   d. In **Root Password of OS**, type the root user password.
   e. **(Optional)** Click **Test Connection**.
      The system logs in to the platform by using the credentials to test the platform connectivity. If connectivity is established, the system displays the message: **Test Connection Successful**.
   f. Click **OK**.
7. Click **Next**.

8. To select the required application, on the **ISO** tab, click one of the following:
   - **SW Library / Select from software library**: Select the local library where the **ISO image** is available.
     
     If you are deploying the **ISO image** from the Solution Deployment Manager client, you can use the default software library that is set during the Solution Deployment Manager Client installation.
   - **Browse**: Select the **ISO image** from your local computer, and click **Submit File**.
   - **URL**: Click **URL** and provide the path to the **ISO image**.

Select the required application, click **Submit**.

If the application **ISO image** supports the patch deployment, the system enables the **Service or Feature Pack** tab.

9. **(Optional)** To install the patch file for the application, click **Service or Feature Pack**, and enter the appropriate parameters.
   a. Click **URL**, and provide the absolute path to the latest service or feature pack.
   b. Click **SW Library / Select from software library**, and select the latest service or feature pack.
   c. Click **Browse**, and select the latest service or feature pack.

You can install the Avaya Aura® application Release 8.0 bin file now or after completing the Avaya Aura® application deployment.

If you do not provide the Avaya Aura® application Release 8.0 bin file at the time of deploying the Avaya Aura® application, the system displays the following message:

**Installation of the latest <application> patch is mandatory. Are you sure you want to skip the patch installation? If Yes, ensure to manually install the <application> patch later.**

10. In **Flexi Footprint**, select the footprint size for the application.

11. In **Test Your Operating System Compatibility Against Element Software Package**, click **Test Environment Compatibility**.

    The installer checks if the platform has all the dependent rpms, network, cpu, memory, and hard disk configuration as specified for the element. This process takes about 4-5 minutes. After the process starts, you cannot proceed further until the process is complete. If you get any error or warning, make the necessary changes before the next steps.

    **Note:**
    - If the browser hangs, the system provides the option to end the script or wait. Always click **Wait**.

12. **(Optional)** To view the installer compatibility results in a separate window, click **View Output**.

    The system displays the Environment Check Output window.
13. Click Next.
14. On the Configuration Parameters page, provide all the information required.
   For a Software-Only application deployment, the Network Parameters tab is disabled.
15. Click Deploy.
16. On the EULA Acceptance window, click Accept.
   After accepting EULA, the system displays Software only Installation Warning for software-
   only application deployment.
17. To continue with the deployment, click Accept.
   The system displays the deployment status in the Current Action Status column and the
   deployed application on the Applications tab.
18. To view details, click Status Details.

---

**Installing the AE Services patch from CLI**

**About this task**
Use this procedure to install the AE Services patch from CLI.

**Procedure**
1. Log in to the AE Services command line interface.
2. Copy the patch file on the AE Services server.
3. To provide executable permission, run the command: `chmod +x <patch_file_name>`.
4. Switch to the root user.
5. To install the patch, run the command: `./<patch file_name>`.
6. To accept the license terms, read the End User License Agreement, and type Y.
7. Run the command: `swversion` to verify the AE Services version.

---

**Amazon Web Services instance management**

Using EC2 Management Console, you can start, stop, reboot, and terminate an instance.

⚠️ **Note:**
With the stop and start operations, the instance might move to a different host that might change the IP Address and MAC Address if not statically allocated. Rebooting the instance will not change the host, IP Address, and MAC Address in AWS.
Starting an AWS instance

Procedure

1. Sign in to the Amazon Web Services Management console.

2. Go to Services > Compute, and click EC2.
   The system displays the EC2 Management Console page.

3. In the left navigation pane, click Instances.

4. Select one or more instance, click Actions > Instance State > Start.
   The system displays a message to start the instances.

5. Click Yes, Start.
   When the system starts the instance, the Instance State column displays the state as running.

Stopping an AWS instance

Procedure

1. Sign in to the Amazon Web Services Management console.

2. Go to Services > Compute, and click EC2.
   The system displays the EC2 Management Console page.

3. In the left navigation pane, click Instances.

4. Select one or more instance, click Actions > Instance State > Stop.
   The system displays a message to stop the instances.

5. Click Yes, Stop.
   When the system stops the instance, the Instance State column displays the state as stopped.

Rebooting an AWS instance

Procedure

1. Sign in to the Amazon Web Services Management console.

2. Go to Services > Compute, and click EC2.
   The system displays the EC2 Management Console page.

3. In the left navigation pane, click Instances.
4. Select one or more instance, click **Actions > Instance State > Reboot**.
   The system displays a message to reboot the instances.

5. Click **Yes, Reboot**.
Chapter 6: Configuring

Opening an ssh session to AE Services

About this task
This procedure assumes that you have a secure shell (ssh) client, such as PuTTY or PuTTYtel running on your administrative workstation.

Procedure

1. Start your ssh client, and complete the information in the dialog box that it presents to open a session. For example, specify the following information to open a session to the AE Services server.
   - Host Name (or IP address) - enter the host name or IP address of your AE Services server, for example, aeserver.example.com.
   - Port - enter 22.
   - Connection type - enter SSH.
   - Click Open.

   ✩ Note:
   The server displays the PuTTY Security Alert window the first time you connect to the SAMP. If you see this window, click Yes to accept the server’s host key.

   The system displays the PuTTY window.

2. If you are an Avaya service technician or Business Partner, log in as follows:
   a. At the login as: prompt, type craft.
   b. At the prompt, type the challenge/password.
   c. At the command prompt, type su - sroot.
   d. At the prompt, type the challenge/password.

3. If you are a customer, log in as follows:
   a. At the login as: prompt, type cust.
   b. At the password prompt, type the password for the cust account.
   c. At the command prompt, type su - root.
   d. At the password prompt, type the password for the root account.
Logging on to the AE Services Management web console

About this task

⚠️ Important:
You cannot log in to the AE Services Management web console with root credentials.

Procedure

1. On the web browser, type `https://<Fully Qualified Domain Name/IP address>`, the AE Services URL.
   For example: `https://aserver.example.com`

   If you are accessing the AE Services server for the first time, the browser displays a security alert for an SSL certificate.

   If the SSL certificate is not presented, verify that the address bar on your browser displays https and the fully qualified domain name or IP address of the AE Services server.

2. On the Security alert window, click Yes to accept the certificate.

3. On the Application Enablement Services welcome page, click Continue To Login.

4. On the Application Enablement Services Management web console login page, in Username, type the login ID.

5. Click Continue.

6. In Password, type the password.

   When logged in as a service technician, and if the Enhanced Access Security Gateway (EASG) is present, your login ID is challenged by EASG. You must enter a proper response in the Response field to log in successfully.

   For customer user login credentials, these options are not presented.

7. Click Login.

   The browser displays the Application Enablement Services Management web console. The main menu is in the left pane and the welcome page is in the right pane.

🌟 Note:

   If you are logging in for the first time, AE Services displays the End User License Agreement page.
Editing the NIC configuration (optional)

About this task
Network interfaces are configured during the AE Services installation process on the Configure Network Information page. Use this procedure only if you need to change the NIC settings from Auto-Negotiate to Lockdown (100M links only).

The values that are initially displayed on the Network Configure page reflect the negotiated values between the NICs on the AE Services server and the Ethernet switch on your network.

⚠️ Important:
AE Services has been tested at 1000BaseT full duplex and 100BaseT full duplex. These are the required speed and duplex mode settings for both network interfaces (eth0 and eth1).

Procedure
1. From the AE Services Management Console main menu, select Networking > Network Configure.
2. From the Network Configure page, edit any of the settings that you need to change, and click Apply Changes.

🌟 Note:
Changing the settings for a NIC will cause the NIC to restart. Once you change the settings, they remain in effect until you reset them. Rebooting the AE Services server will not reset any of the values.
Chapter 7: Post-installation verification

Verifying the software version

About this task
You can see the software version in the upper-right corner of the AE Services Management Console window. If not, you can run the `swversion` command.

Procedure
1. Open an ssh session to the AE Services server.
2. In the command line in a terminal window, run the `swversion` command.
3. Verify the version number and build number.

Verifying the license

Procedure
1. Log in to AE Services Management Console. Use an info tag for this information, see Logging into the Management Console in Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment.
3. On the Web License Manager main menu, click Licensed Products > Application_Enablement.
4. On the Application Enablement (Standard License file) page, verify the Licensed Features settings.

Verifying the AE Service IP (Local IP) settings

Procedure
1. From your browser, log in to AE Services Management Console.
2. From the main menu, select Networking > AE Service IP (Local IP).
The settings on the AE Services IP (Local IP) page should match the settings you specified when you installed Linux.

- If you set up a single NIC configuration, the IP settings in the Client Connectivity, Switch Connectivity, and Media Connectivity fields should be the same.
- If you set up a dual NIC configuration, the IP settings should match the settings you specified when you installed Linux.

**Note:**
The private network segment should contain one subnet; this is the only supported configuration. You can configure any default gateway for public and private network segments. However, Avaya recommends using a public gateway as the default gateway to enable access to AES through both public and private network segments. After deployment, you must add static routes through CLI to make AES accessible from the private network segment.

---

**Verifying the Network Configure settings**

**Procedure**

1. From your browser, log in to AE Services Management Console.
2. From the main menu, select **Networking > Network Configure**.
3. On the Network Configure page, check the following settings:
   - The Hostname field should display the host name you specified when you installed Linux.
   - The DNS Domain Name field should display the fully-qualified DNS domain name you specified when you installed Linux.
   - The Primary DNS Server field should display the IP address you specified when you installed Linux.
   - The Default Gateway field should display the IP address you specified when you installed Linux.
   - The Auto_Neg/Speed/Duplex field should display one of the following values:
     - off / 100 / full if using Lockdown mode
     - on / 100 / full or on / 1000 / full if using Auto-Negotiation mode
   - The Physical IP Address for the Network Interfaces (eth0, eth2, or eth3) should match the settings you specified when you installed Linux. See [Verifying the AE Service IP (Local IP) settings](#) on page 49.
   - The Netmask for the Network Interfaces (eth0, eth2, eth3) should match the settings you specified when you installed Linux.
Verifying the time zone and NTP server settings

Procedure

1. From your browser, log in to AE Services Management Console.
2. From the main menu, select Maintenance > Date Time/NTP Server.

The settings for the time zone and NTP server should match the settings you typed on the Date/Time Initialization screen when you installed the software.
Chapter 8: Resources

Application Enablement Services documentation

The following table lists the documents related to Application Enablement Services. Download the documents from the Avaya Support website at [http://support.avaya.com](http://support.avaya.com).

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Design</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services Overview and Specification</td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services TSAPI and CVLAN Client and SDK Installation Guide</td>
<td>Installing TSAPI and CVLAN Client and SDK</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Using</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Upgrading Avaya Aura® Application Enablement Services</td>
<td>Upgrading Application Enablement Services applications</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Administering Avaya Aura® Application Enablement Services</td>
<td>Administering Application Enablement Services applications and install patches on Application Enablement Services applications</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services for Microsoft® Lync Server Products</td>
<td>Deploy Application Enablement Services applications in Microsoft Lync Server Products</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtual Appliance</td>
<td>Deploy Application Enablement Services applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Deploying Avaya Aura® Application Enablement Services in Virtualized Environment</td>
<td>Deploy Application Enablement Services applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

Table continues...
<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Deploying Avaya Aura® Application Enablement Services in Infrastructure as a Service Environment</em></td>
<td>Deploy Application Enablement Services applications in Infrastructure as a Service Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><em>Deploying Avaya Aura® Application Enablement Services in a Software-Only Environment</em></td>
<td>Deploy Application Enablement Services applications in Software-Only Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><strong>Maintenance and Troubleshooting</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Maintaining Avaya Aura® Application Enablement Services</em></td>
<td>Maintaining Application Enablement Services applications and install patches on Application Enablement Services applications.</td>
<td>System administrators and IT personnel</td>
</tr>
</tbody>
</table>

**Related links**

- Finding documents on the Avaya Support website on page 53
- Accessing the port matrix document on page 54
- Avaya Documentation Portal navigation on page 54

---

### Finding documents on the Avaya Support website

**Procedure**

1. Go to [https://support.avaya.com/](https://support.avaya.com/).
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product > Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.
   
   For example, for user guides, click **User Guides** in the **Content Type** filter. The list displays the documents only from the selected category.
7. Click **Enter**.

**Related links**

- Application Enablement Services documentation on page 52
**Accessing the port matrix document**

**Procedure**

1. Go to [https://support.avaya.com](https://support.avaya.com).
2. Log on to the Avaya website with a valid Avaya user ID and password.
3. On the Avaya Support page, click **Support By Product > Documents**.
4. In **Enter Your Product Here**, type the product name, and then select the product from the list of suggested product names.
5. In **Choose Release**, select the required release number.
6. In the **Content Type** filter, select one or more of the following categories:
   - Application & Technical Notes
   - Design, Development & System Mgt
   The list displays the product-specific Port Matrix document.
7. Click **Enter**.

**Related links**

- [Application Enablement Services documentation](#) on page 52

---

**Avaya Documentation Portal navigation**

Customer documentation for some programs is now available on the Avaya Documentation Portal at [https://documentation.avaya.com/](https://documentation.avaya.com/).

**Important:**

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open [https://support.avaya.com/](https://support.avaya.com/).

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs (⭐)**.
Navigate to the My Content > My Docs menu, and do any of the following:
- Create, rename, and delete a collection.
- Add content from various documents to a collection.
- Save a PDF of selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive content that others have shared with you.

* Add yourself as a watcher by using the Watch icon (👀).

Navigate to the My Content > Watch list menu, and do the following:
- Set how frequently you want to be notified, starting from every day to every 60 days.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the portal.

- Share a section on social media platforms, such as Facebook, LinkedIn, Twitter, and Google +.
- Send feedback on a section and rate the content.

⚠️ Note:
Some functionality is only available when you log in to the portal. The available functionality depends on the role with which you are logged in.

Related links
- Application Enablement Services documentation on page 52

### Training

The following courses are available on the Avaya Learning website at [http://www.avaya-learning.com](http://www.avaya-learning.com). After logging in to the website, enter the course code or the course title in the Search field and click Go to search for the course.

<table>
<thead>
<tr>
<th>Course code</th>
<th>Course title</th>
</tr>
</thead>
<tbody>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.0</td>
</tr>
</tbody>
</table>

### 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 https://support.avaya.com/ and do one of the following:
  - In Search, type Avaya Mentor Videos to see a list of the available videos.
  - In Search, type the product name. On the Search Results page, select Video in the Content Type column on the left.

• To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - 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 https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Related links
Using the Avaya InSite Knowledge Base on page 56

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

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

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

2. Log on to the Avaya website with a valid Avaya user ID and password. The system displays the Avaya Support page.
3. Click Support by Product > Product Specific Support.
4. In Enter Product Name, enter the product, and press Enter.
5. Select the product from the list, and select a release.
6. Click the Technical Solutions tab to see articles.
7. Select relevant articles.

Related links
Support on page 56
Chapter 9: Configuring an LDAP server for User Management

About this task
To use your existing Lightweight Directory Access Protocol (LDAP) directory with AE Services, you need to configure your LDAP implementation for compatibility with AE Services User Management. After installing AE Services server, if you face any discrepancy with LDAP, perform the following procedure.

Before you begin

- Ensure that you have installed AE Services server software.

  Note:
  - AE Services server software installs the cs-cusldap and cs-userservice packages. To verify whether the packages are installed, run `rpm -q ‘cs-userservice|cs-cusldap’` command.
  - Back up the files on your system as mentioned in Deploying the AE Services server software on page 38.

  AE Services server software installs the cs-cusldap and cs-userservice packages. To verify whether the packages are installed, run `rpm -q ‘cs-userservice|cs-cusldap’` command.

- Ensure that your LDAP implementation must be an OPEN LDAP of version 2.1.22-28.

Procedure

1. Restore `/etc/ldap.conf` file from the backup.
2. Merge `/etc/sssd/sssd.conf` file with your modified `sssd.conf` file.
3. Restart sssd service using the command `service sssd restart`.
4. Restart sshd service using the command `service sshd restart`.
5. Add admin user to the following groups: securityadmin, usrsvc_admin and susers. Run the following command to access sudo commands and web interface for an LDAP user:

   ```
   usermod -a -G securityadmin,usrsvc_admin,susers admin_username
   ```

6. If your security policy doesn't allow multiple users with ID equals to zero, modify the user ID for sroot to an unused ID using the command `usermod -u new_UID sroot`.
7. If required, add root shell permission for cust and sroot user types to `/etc/sudoers`.

Comments on this document? infodev@avaya.com
8. Reboot the server.

Related links
- Configuring the LDAP server on page 59
- Creating an LDAP User account on page 60

Configuring the LDAP server

About this task
Follow this procedure to manually configure your LDAP server for User Management.

Procedure

1. Copy the mvapus schema file (mvapus.schema) from /var/mvap/config/cus to the LDAP schema directory (/etc/openldap/schema).

2. Edit the /etc/openldap/schema/core.schema file as follows:
   a. Locate the userid attribute specification section.
   b. Add the following specification element:
      
      after the EQUALITY caseIgnoreMatch line, add ORDERING caseIgnoreOrderingMatch
      
   c. Save the schema file.

3. Edit the /etc/openldap/slapd.conf file as follows:
   a. Add the following include statement to the already existing set of \include statements:

      include /etc/openldap/schema/mvapus.schema

   b. Note the suffix value used in the current slapd.conf file.
   c. Save and close the slapd.conf file.

4. Modify the init.ldif file to match the chosen organizationalUnit for the \users and the existing suffix used by the enterprise as follows:
   a. Eliminate the first entry in the init.ldif file.
   b. Revise the second entry to reflect the desired organizationalUnit \ (for example, ou=users).
   c. Revise the DN attribute of the next two entries to reflect the chosen organizationalUnit and suffix in use in the enterprise.
   d. Save and close the init.ldif file.

5. Restart the LDAP server.

6. Use the ldapadd tool or equivalent to add the entries in the ldif.init file into the LDAP server:

   For example, ldapadd -x -D bind credentials DN -W -f init.ldif
Creating an LDAP User account

About this task
You must now create an LDAP user account for the user service. This account must have privileges to add, modify, and delete avayauuser class entries in the specified region of the Directory Information Tree (DIT).

Procedure
1. Open the /var/mvap/config/cus/user.properties file for editing.
2. Edit the LDAP storage section to reflect the LDAP configuration work completed in Configuring the LDAP server on page 59:
   a. Set the LDAP provider to the correct host and suffix combination.
   b. Set the userroot property to the suffix value in use.
   c. Set the principal to the DN of the LDAP you created in Configuring the LDAP server on page 59.
   d. Set the password attribute to the generated encrypted value.
      Run /usr/share/tomcat5/webapps/axis/WEB-INF/lib/makepassword.sh against the plain text password furnished by the enterprise LDAP administrator for the User account you created.
   e. Set the orgunit property to the organizationalUnit selected for the user data space.
3. Save and close the modified user.properties file.
4. Make identical changes to the corresponding properties in the var/mvap/config/cus/ldapfilter.properties file.
5. If the relevant Tomcat/Axis server has not already deployed the User Management service, deploy the service:
   a. Verify the Tomcat service is running.
   b. Go to:
      /usr/share/tomcat5/webapps/axis/WEB-INF/lib/
   c. Run the org.apache.axis.clientAdminController application against the cusdeploy.wsdd file.
      For example:
      
      java -classpath Axis jar files
      org.apache.axis.clientAdminController cusdeploy.wsdd
6. Restart the Tomcat service that is the container for the user service.

Related links

Configuring an LDAP server for User Management on page 58
Chapter 10: Appendix

Configuring PuTTY

Converting the *.pem file to the *.ppk format

Before you begin
Download the PuTTYGen software.

Procedure
1. Double-click the downloaded puttygen.exe file.
2. In the PuTTY Key Generator dialog box, click Conversions > Import key.
3. On Load private key, select a .pem file from your local computer, and click Open.
   The system displays the key in the Key section.
4. Click Generate.
   The system takes a few minutes.
5. Click Save private key.

Configuring PuTTY for an SSH session

Before you begin
Convert the *.pem file to the *.ppk format.

Procedure
1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click Connections > SSH > Auth.
3. In the Authentication parameters section, click Browse.
4. On Select a private key, select a .ppk file from your local computer, and click Open.
Signing in to the Amazon EC2 virtual server instance

Before you begin

• Convert the *.pem file to the *.ppk format.
• Configure PuTTY for an SSH session

Procedure

1. Open a PuTTY session for SSH.
2. On the PuTTY Configuration dialog box, in the left navigation pane, click Session.
3. In Host Name (or IP Address), type admin@<IP_Address>, where <IP_Address> is the IP address of the Amazon EC2 virtual server instance.
4. Click Open.
# Index

## A

- accessing port matrix .......................................................... 54  
- AES software  
  - installing ........................................................................ 38  
- Amazon EC2 virtual server instance  
  - create .................................................................................. 24, 30  
- Application Enablement Services ........................................... 14  
- applications  
  - footprints ........................................................................ 17  
  - instance type ........................................................................ 17  
  - vCPU, RAM, HDD, NICs ....................................................... 17  
- Avaya support website support .................................................. 56  

## C

- checklist  
  - converting OVA to AMI ....................................................... 23  
  - deploying ISO on Amazon Web Services ............................ 29  
  - deploying ISO on Google Cloud Platform ............................ 34  
  - deploying ISO on Microsoft Azure ...................................... 32  
  - OVA to Amazon Machine Image ......................................... 23  
  - planning .............................................................................. 18, 19  
  - planning for deployment ..................................................... 17  
- collection  
  - delete .................................................................................. 54  
  - edit name ............................................................................. 54  
  - generating PDF .................................................................... 54  
  - sharing content .................................................................... 54  
- configuring  
  - .PuTTY for SSH ................................................................. 62  
  - yum on RHEL ........................................................................ 32  
- Configuring  
  - LDAP server for User Management ..................................... 58  
- connection types  
  - IaaS .................................................................................. 13  
- content  
  - publishing PDF output ....................................................... 54  
  - searching .............................................................................. 54  
  - sharing .................................................................................. 54  
  - watching for updates ......................................................... 54  
- convert  
  - .pem file to .ppk .................................................................. 62  
- copying  
  - ISO to RHEL machine on Microsoft Azure ......................... 33  
- creating  
  - bucket ................................................................................ 23  
  - PPK file .............................................................................. 34  
  - RHEL machine on Azure ...................................................... 33  
  - RHEL machine on Google Cloud Platform ......................... 35  
  - user access key ................................................................... 26  

## D

- deploying  
  - Communication Manager ISO using SDM Client .................. 40  
  - disk partitioning ................................................................... 16  
  - disk resizing .......................................................................... 16  
- documentation  
  - Application Enablement Services .......................................... 52  
  - documentation portal .......................................................... 54  
  - finding content ..................................................................... 54  
  - navigation ............................................................................. 54  
  - document changes ................................................................ 9  
- downloading software  
  - using PLDS ......................................................................... 20  

## F

- finding content on documentation portal .................................. 54  
- finding port matrix .................................................................. 54  

## H

- hardware  
  - footprint ............................................................................ 18, 19  

## I

- IaaS  
  - overview ............................................................................ 10  
- importing OVA for conversion .................................................. 26  
- Infrastructure as a Service  
  - overview ........................................................................... 10  
- InSite Knowledge Base ............................................................. 56  
- Installing the AE Services patch  
  - CLI ....................................................................................... 43  
- instance  
  - reboot .................................................................................. 43  
  - start ..................................................................................... 43  
  - stop ..................................................................................... 43  
- ISO image  
  - verifying on Linux-based computer ........................................ 37  

## L

- latest software patches .......................................................... 21  
- LDAP  
  - creating a user account ....................................................... 60  
  - licensed features  
    - specific features ............................................................... 16  
- logging  
  - AE Services Management web console ................................. 47  
  - logging on to
logging on to (continued)
Amazon EC2 virtual server instance ............................ 63
Linux server ................................................................. 63

M
matrix
agents ................................................................. 18, 19
table ................................................................. 18, 19
My Docs ................................................................. 54

N
Network configure settings ........................................ 50
networking considerations
Avaya applications ........................................................ 13
NIC configuration, editing ........................................... 48

O
obtaining
virtual server instance user id .................................... 26
opening an ssh session ................................................. 46
OVA to AMI conversion ........................................... 26

P
patch information ........................................................ 21
PCN ................................................................. 21
PLDS
  downloading software ........................................... 20
port matrix ............................................................... 54
PSN ................................................................. 21

R
rebooting
Amazon instance ...................................................... 44
AWS instance ........................................................ 44
release notes for latest software patches ..................... 21
required software ...................................................... 21
requirements
  third-party software ............................................. 16
resources
  DMCC ............................................................. 18, 19

S
searching for content .................................................. 54
sharing content .......................................................... 54
software details .......................................................... 14
software patches ......................................................... 21
starting
Amazon instance ...................................................... 44
AWS instance ........................................................ 44
stopping (continued)
Amazon instance ...................................................... 44
AWS instance ........................................................ 44
support ................................................................. 56
supported applications
  Infrastructure as a Service .................................... 11

T
tools and utilities
configuration .............................................................. 22
topology
  Avaya applications on Infrastructure as a Service
    platform ......................................................... 11
training ................................................................. 55

U
unsupported features .................................................. 14
uploading
  ISO to virtual machine instance on Amazon Web
    Services ............................................................ 31
  iso to virtual machine instance on Google Cloud Platform
    ........................................................................... 36
  OVA .................................................................... 24

V
verifying
  license ................................................................. 49
videos ................................................................. 55

W
watch list ................................................................. 54