Deploying Avaya Aura® System Manager on Infrastructure as a Service Environment
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.

License

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

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License as set forth below in the Designated System(s) License (DS) section as applicable. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors up to the number indicated in the order; or 2) each copy or an Instance of the Software only: 1) on a number of Designated Processors or Designated Processors that may be identified 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. "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/LICENSEINFO 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.

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 or Designated Processors that may be identified 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.
Copyright

Except where expressly stated otherwise, no use should be made of materials on the Document, and 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. THIS PRODUCT 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 THE H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

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

Chapter 1: Introduction.................................................................................................................. 7
  Purpose........................................................................................................................................ 7
  Prerequisites................................................................................................................................. 7
  Change history.............................................................................................................................. 7

Chapter 2: Overview..................................................................................................................... 9
  Overview of Infrastructure as a Service environment................................................................. 9
  Supported applications in Infrastructure as a Service Environment......................................... 10
  Topology....................................................................................................................................... 10
  Connection types for Infrastructure as a Service....................................................................... 11
  Networking considerations......................................................................................................... 12
  Unsupported features of Avaya Aura® application on Infrastructure as a Service ....................... 13
  Software details of System Manager.......................................................................................... 13
  Third-party software requirements............................................................................................. 14
  System capacities for applications............................................................................................. 14
  Supported footprints for the System Manager on AWS............................................................. 14
  Supported footprints of System Manager ISO on Microsoft Azure............................................. 15
  Supported footprints of System Manager ISO on Google Cloud Platform.................................... 15

Chapter 3: Planning and pre-deployment configuration............................................................. 16
  Downloading software from PLDS............................................................................................. 16
  Latest software updates and patch information......................................................................... 17
  Planning checklist for deploying OVA on Amazon Web Services............................................ 17
    Planning checklist.................................................................................................................. 17
    Signing in to the Amazon Web Services Management console............................................. 18
    Creating a key pair................................................................................................................. 18
    Configuration tools and utilities............................................................................................. 19
    Preconfiguration for deploying OVA on Amazon Web Services........................................... 19
  Preconfiguration for deploying ISO on Amazon Web Services.............................................. 25
    Checklist for deploying ISO on Amazon Web Services........................................................... 25
    Creating RHEL instance on Amazon Web Services............................................................... 26
    Uploading the Avaya Aura® application ISO to RHEL machine on Amazon Web Services.... 28
    Configuring Yum on Amazon Web Services........................................................................ 28
  Preconfiguration for deploying ISO on Microsoft Azure........................................................ 29
    Checklist for deploying ISO on Microsoft Azure.................................................................... 29
    Creating RHEL instance on Microsoft Azure...................................................................... 30
    Uploading the Avaya Aura® application ISO to RHEL machine on Microsoft Azure............. 31
  Preconfiguration for deploying ISO on Google Cloud Platform............................................. 32
    Checklist for deploying ISO on Google Cloud Platform....................................................... 32
    Creating a PPK file................................................................................................................ 33
    Creating RHEL instance on Google Cloud Platform.............................................................. 33
Contents

Uploading the Avaya Aura® application ISO to RHEL machine on Google Cloud Platform... 35

Chapter 4: Deploying

Deploying Avaya Aura® application OVA on Amazon Web Services... 36
Deploying Avaya Aura® application AMI... 36
Installing the System Manager patch from CLI... 37
Amazon Web Services instance management... 38
Deploying Avaya Aura® application ISO on Infrastructure as a Service... 39
Adding a location... 39
Adding a software-only platform... 40
Deploying the System Manager Software-Only ISO image using bash CLI... 41
Deploying the System Manager Software-Only ISO image by using Solution Deployment Manager Client... 52
Installing the System Manager service pack or patch from CLI... 55

Chapter 5: Configuring

Configuring the AMI on Amazon Web Services... 56
Configuring the System Manager instance... 56
Allocating dedicated hosts... 59
Dual data center configuration... 60

Chapter 6: Post-installation verification

Post-installation steps... 61
Verifying the installation of System Manager... 61
Installing language pack on System Manager... 61
Enhanced Access Security Gateway (EASG) overview... 62
Managing EASG from CLI... 63
Viewing the EASG certificate information... 64
EASG product certificate expiration... 64
EASG site certificate... 64
Managing site certificates... 64

Chapter 7: Resources

System Manager documentation... 66
Finding documents on the Avaya Support website... 67
Accessing the port matrix document... 67
Avaya Documentation Center navigation... 68
Training... 69
Viewing Avaya Mentor videos... 69
Support... 70
Using the Avaya InSite Knowledge Base... 70

Chapter 8: Appendix

Configuring PuTTY... 72
Converting the *.pem file to the *.ppk format... 72
Configuring PuTTY for an SSH session... 72
Signing in to the Amazon EC2 virtual server instance... 73
Identifying the SSH user name of the RHEL instance on AWS... 73

Comments on this document? infodev@avaya.com
Chapter 1: Introduction

Purpose

This document describes the procedure to deploy Avaya Aura® System Manager on the following Infrastructure as a Service platforms:

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

This document is intended for people who install and configure Avaya Aura® System Manager.

Prerequisites

Before deploying the Avaya Aura® System Manager 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 19.

Change history

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>May 2020</td>
<td>For Release 8.1.2, updated the section: Unsupported features of Avaya Aura application on Infrastructure as a Service on page 13</td>
</tr>
<tr>
<td>3</td>
<td>December 2019</td>
<td>Updated the “Configuring the System Manager instance” section.</td>
</tr>
</tbody>
</table>

Table continues…
## Issue History

<table>
<thead>
<tr>
<th>Issue</th>
<th>Date</th>
<th>Summary of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>October 2019</td>
<td>For Release 8.1.1, updated the following section:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• <a href="#">Software details of System Manager</a> on page 13</td>
</tr>
<tr>
<td>1</td>
<td>June 2019</td>
<td>Release 8.1 document.</td>
</tr>
</tbody>
</table>

### Software details of System Manager

- [Software details of System Manager](#) on page 13

Comments on this document? infodev@avaya.com
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 (IBM Cloud)

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

Software security updates

Avaya Security Service Packs (SSP) and Kernel Service Packs (KSP) are built for customers who do not use the software-only distribution. Software-only installation is in the control of the operating system and is responsible for applying the relevant security patches from Red Hat.
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 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 8.1.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya WebLM</td>
<td>Release 8.1.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Aura® Session Manager</td>
<td>Release 8.1.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Avaya Aura® Communication Manager</td>
<td>Release 8.1.2</td>
<td>Y</td>
<td>Y</td>
<td>Y</td>
</tr>
<tr>
<td>Presence Services using Avaya Breeze® platform</td>
<td>Release 8.1.2</td>
<td>Y</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Avaya Aura® Application Enablement Services (Software only)</td>
<td>Release 8.1.2</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>
</tbody>
</table>

For information about other Avaya product compatibility information, go to https://support.avaya.com/CompatibilityMatrix/Index.aspx.

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.
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, go to <a href="https://docs.aws.amazon.com/VPC/">https://docs.aws.amazon.com/VPC/</a> and search for “VPN connections” section.</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> section.</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>
</table>
| VPN connection  | For more information, go to [https://docs.microsoft.com/en-us/](https://docs.microsoft.com/en-us/) and search for “Create a Site-to-Site connection in the Azure portal” section.  
For more information, go to [https://docs.microsoft.com/en-us/](https://docs.microsoft.com/en-us/) and search for “Azure networking” section. |
| Direct connection| For more information, go to [https://docs.microsoft.com/en-us/](https://docs.microsoft.com/en-us/) and search for “ExpressRoute overview” section. |

**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, go to <a href="https://cloud.google.com/vpn/docs/">https://cloud.google.com/vpn/docs/</a> and search for “Cloud VPN overview” section.</td>
</tr>
<tr>
<td>GCN Direct</td>
<td>For more information, go to <a href="https://cloud.google.com/interconnect/docs/">https://cloud.google.com/interconnect/docs/</a> and search for “Dedicated Interconnect Overview” section.</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](https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Appendix_Limits.html).

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
• Data Encryption

Microsoft Azure
The Avaya Aura® application does not support the following features on Microsoft Azure:
• Out of Band Management configurations
• IPv6 addresses
• Data Encryption

Google Cloud Platform
The Avaya Aura® application does not support the following features on Google Cloud Platform:
• Out of Band Management configurations
• IPv6 addresses
• Data Encryption

Software details of System Manager
For Avaya Aura® application software build details of OVA, ISO, service patch, Data migration Utility, or Solution Deployment Manager Client, see Avaya Aura® Release Notes on the Avaya Support website at http://support.avaya.com/.
Third-party software requirements

You can deploy the Avaya Aura® application ISO file on a Red Hat Enterprise Linux 7.6 virtual machine by using the bash command line or by using the Solution Deployment Manager.

For the list of supported browsers and their versions, see the respective third-party documentation.

System capacities for applications

For information about the system capacities, such as, number of users, gateways, and endpoints, see the product specific documentation on the Avaya Support website at http://support.avaya.com.

Supported footprints for the System Manager on AWS

<table>
<thead>
<tr>
<th>Footprint</th>
<th>Profile 2</th>
<th>Profile 3</th>
<th>Profile 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS instance type</td>
<td>m4.2xlarge or higher</td>
<td>m4.2xlarge or higher</td>
<td>m4.4xlarge or higher</td>
</tr>
<tr>
<td>AWS vCPU</td>
<td>8</td>
<td>8</td>
<td>18</td>
</tr>
<tr>
<td>AWS RAM (GB)</td>
<td>32</td>
<td>32</td>
<td>36</td>
</tr>
<tr>
<td>HDD (GB)</td>
<td>Total: 105</td>
<td>Total: 250</td>
<td>Total: 850</td>
</tr>
<tr>
<td></td>
<td>• HDD1: 44</td>
<td>• HDD1: 150</td>
<td>• HDD1: 650</td>
</tr>
<tr>
<td></td>
<td>• HDD2: 25</td>
<td>• HDD2: 30</td>
<td>• HDD2: 30</td>
</tr>
<tr>
<td></td>
<td>• HDD3: 15</td>
<td>• HDD3: 20</td>
<td>• HDD3: 20</td>
</tr>
<tr>
<td></td>
<td>• HDD4: 21</td>
<td>• HDD4: 50</td>
<td>• HDD4: 150</td>
</tr>
<tr>
<td>NICs</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

*Note:*

From Release 8.0 and later, System Manager Profile 1 is not supported. If System Manager is on a pre Release 8.0 and using the Profile 1, ensure that the server has the required resources to configure Profile 2 on Release 8.0 and later.
### Supported footprints of System Manager ISO on Microsoft Azure

<table>
<thead>
<tr>
<th>Footprint</th>
<th>Instance type</th>
<th>vCPU</th>
<th>RAM (GB)</th>
<th>HDD (GB)</th>
<th>NICs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 2</td>
<td>D4_v2 (Standard) or higher</td>
<td>8</td>
<td>32</td>
<td>105</td>
<td>1</td>
</tr>
<tr>
<td>Profile 3</td>
<td>D4_v2 (Standard) or higher</td>
<td>8</td>
<td>32</td>
<td>250</td>
<td>1</td>
</tr>
<tr>
<td>Profile 4</td>
<td>D16_v3 (Standard) or higher</td>
<td>18</td>
<td>36</td>
<td>850</td>
<td>1</td>
</tr>
</tbody>
</table>

### Supported footprints of System Manager ISO on Google Cloud Platform

<table>
<thead>
<tr>
<th>Footprint</th>
<th>vCPU</th>
<th>RAM (GB)</th>
<th>HDD (GB)</th>
<th>NICs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile 2</td>
<td>6</td>
<td>12</td>
<td>Total: 105 • HDD1: 44 • HDD2: 25 • HDD3: 15 • HDD4: 21</td>
<td>1</td>
</tr>
<tr>
<td>Profile 3</td>
<td>8</td>
<td>18</td>
<td>Total: 250 • HDD1: 150 • HDD2: 30 • HDD3: 20 • HDD4: 50</td>
<td>1</td>
</tr>
<tr>
<td>Profile 4</td>
<td>18</td>
<td>36</td>
<td>850       • HDD1: 650 • HDD2: 30 • HDD3: 20 • HDD4: 150</td>
<td>1</td>
</tr>
</tbody>
</table>
Chapter 3: Planning and pre-deployment configuration

Downloading software from PLDS

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

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

Note:

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

Procedure

1. Enter http://plds.avaya.com in your Web browser to access the Avaya PLDS website.
2. Enter your login ID and password.
3. On the PLDS home page, select Assets.
4. Click View Downloads.
5. Click on the search icon (magnifying glass) for Company Name.
6. In the %Name field, enter Avaya or the Partner company name.
7. Click Search Companies.
8. Locate the correct entry and click the Select link.
9. Enter the Download Pub ID.
10. Click Search Downloads.
11. Scroll down to the entry for the download file and click the Download link.
12. In the Download Manager box, click the appropriate download link.
Note:
The first link, Click to download your file now, uses the Download Manager to download the file. The Download Manager provides features to manage the download (stop, resume, auto checksum). The click here link uses your standard browser download and does not provide the download integrity features.

13. If you use Internet Explorer and get an error message, click the install ActiveX message at the top of the page and continue with the download.

14. Select a location where you want to save the file and click Save.

15. If you used the Download Manager, click Details to view the download progress.

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/.

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.

Planning checklist for deploying OVA on Amazon Web Services

Planning checklist

Ensure that you complete the following before deploying the Avaya Aura® application OVA on Amazon Web Services Management console:
<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 software.                                      | See [Configuration tools and utilities](#) on page 19.                     |
|     |                                                                    | See [Downloading software from PLDS](#) on page 16.                        |
| 3.  | Log on to the Amazon Web Services Management console.                 | See [Signing in to the Amazon Web Services Management console](#) on page 18 |
| 4.  | Create a key pair.                                                    | See [Creating a key pair](#) on page 18                                    |

### Signing in to the Amazon Web Services Management console

**Before you begin**

Ensure that you have an Amazon Web Services account.

**Procedure**

1. In your web browser, type the URL [https://aws.amazon.com/](https://aws.amazon.com/).
2. Under **My Account**, click **AWS Management Console**.
3. In the **Email address of your AWS account** field, type the account ID or account alias.
4. Click **Next**.
5. In the **IAM user name** field, type the user name or registered email ID.
6. In the **Password** field, type the password.
7. Click **Sign In**.

The system displays the Amazon Web Services Management Console page.

### Creating a key pair

**About this task**

A key pair is a set of public and private keys. The public key is used to encrypt data, such as the login password. The private key is used to decrypt the encrypted data. You provide this key pair...
when you create a CloudFormation stack, and use it for SSH access to the Amazon Machine Instances.

**Procedure**

1. Sign in to the Amazon Web Services Management console.
2. In the left navigation pane, go to **NETWORK & SECURITY**, and click **Key Pairs**.
3. Click **Create Key Pair**.
4. In the Create Key Pair dialog box, in the **Key pair name** field, type a name for the key pair.
5. Click **Create**.

   The system generates a *.pem file and prompts you to save the file on your computer. You can also view the created key pair name in the Key pair name column.

   **Important:**
   When you create a key pair, save it. If you lose the key, you cannot retrieve it and you will not be able to access the instance.

---

**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.

---

**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>
<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 20</td>
<td>✔</td>
</tr>
<tr>
<td>2.</td>
<td>Upload the Avaya Aura® application OVA.</td>
<td>Uploading the Avaya Aura application OVA on page 20.</td>
<td></td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>No.</th>
<th>Task</th>
<th>Link/Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>3.</td>
<td>Convert OVA to AMI.</td>
<td>Converting the OVA to AMI on page 23</td>
</tr>
<tr>
<td>4.</td>
<td>Create a Linux Amazon EC2 virtual server instance.</td>
<td>Creating a Linux Amazon EC2 virtual server instance on page 21</td>
</tr>
<tr>
<td>5.</td>
<td>Create an access key.</td>
<td>Creating a user access key on page 22</td>
</tr>
<tr>
<td>6.</td>
<td>Obtain the virtual server instance user ID.</td>
<td>Obtaining the virtual server instance user ID on page 22</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
      {
        "Version":"2012-10-17",
        "Statement": [
          {
            "Sid": "",
            "Effect": "Allow",
            "Principal": { "Service": "vmie.amazonaws.com" },
            "Action": "sts:AssumeRole",
            "Condition": { "StringEquals": { "sts:ExternalId": "vmimport" } } }
        ]
      }
      ```
   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:

```
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:

```
{
  "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.

```
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:

```
aws ec2 import-image --cli-input-json "{"Description": "<Server OVA>", "DiskContainers": [{ "Description": "{text description of task}" }, { "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: `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 } "
```

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

```
IMPORTIMAGETASKS x86_64 <product_name>8.x.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 Imageld. The system displays the newly converted AMI Imageld in the AMI ID column.

You can give an appropriate name for the AMI Imageld.

---

**Preconfiguration for deploying ISO on Amazon Web Services**

**Checklist for deploying ISO on Amazon Web Services**

Ensure that you complete the following before deploying Avaya Aura® System Manager 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>Purchase the required licenses.</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>Register for PLDS and perform the following:</td>
<td></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 16.</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>
<tr>
<td>4</td>
<td>Ensure that you have the required resources.</td>
<td>See <a href="#">Supported footprints for the System Manager on AWS</a> on page 14.</td>
</tr>
<tr>
<td>5</td>
<td>Create an RHEL instance.</td>
<td>See <a href="#">Creating RHEL instance on Amazon Web Services</a> on page 26.</td>
</tr>
<tr>
<td>6</td>
<td>Copy the ISO to the RHEL instance.</td>
<td>See <a href="#">Uploading the Avaya Aura application ISO to RHEL machine on Amazon Web Services</a> on page 28</td>
</tr>
<tr>
<td>7</td>
<td>Configure Yum.</td>
<td>See <a href="#">Configuring Yum on Amazon Web Services</a> on page 28.</td>
</tr>
</tbody>
</table>

---

**Creating RHEL instance 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.

In a software-only installation, the customer will also install the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, it is recommended to check the list of tested RPMs and follow the instructions in the PSN periodically published by Avaya. PSN is available at [PSN020361u](#).

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 the supported RHEL version, and click Select.
   For the supported RHEL version, see “Third party software requirements” section.

5. (Optional) If the required RHEL version is not available, then, on the Choose an Amazon Machine Image (AMI) page, click Community AMIs, and click Red Hat, and search for the supported RHEL version and click Select.

6. On the Choose an Instance Type page, select the instance type according to your required footprints, and click Next: Configure Instance Details.
   For System Manager, select m4.2x large or higher.

7. Click Next: Add Storage.
   Change the size of the default Hard Disk size from 10 to 44 GB. Additionally, add three more hard disks in the below sequence.
   • HDD2: 25
   • HDD3: 15
   • HDD4: 21
   Make sure that you enable the "Delete on Termination" check box for the additionally added hard disks.

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

   Remember the name entered for the tag. The name entered for the tag is used to identify the RHEL instance after the instance is created.

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.

13. Click **Launch Instances**.
   The system creates the RHEL instance.

14. 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**

**Before you begin**
• Converting the *.pem file to the *.ppk format.
• Configuring PuTTY for an SSH session.
• Find the SSH user name of the instance you deployed.
For more information, see “Appendix”.

Procedure

1. Log on to the RHEL virtual machine using SSH.
   Use the SSH user name to log on.
2. Switch to root user by using the following command: `sudo su`
3. Run the following command to edit the `redhat-rhui.repo` file:
   ```
   vi /etc/yum.repos.d/redhat-rhui.repo
   ```
   Set `enabled=1` for:
   ```
   [rhui-REGION-rhel-server-rhsc1]
   Name=Red Hat Enterprise Linux Server 7 RHSCL (RPMs)
   enabled=0
   ```
   and
   ```
   [rhui-REGION-rhel-server-extras]
   Name=Red Hat Enterprise Linux Server 7 Extra(RPMs)
   enabled=0
   ```
   and
   ```
   [rhui-REGION-rhel-server-optional]
   Name=Red Hat Enterprise Linux Server 7 Optional (RPMs)
   enabled=0
   ```
4. Run the following command to save the file: `wq`

---

Preconfiguration for deploying ISO on Microsoft Azure

Checklist for deploying ISO on Microsoft Azure

Ensure that you complete the following before deploying Avaya Aura® System Manager ISO on Microsoft Azure.
## Planning and pre-deployment configuration

<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 software. | See [Downloading software from PLDS](#) on page 16. |
| 3   | Verify that you have a valid Red Hat subscription. | Ensure that you have a valid Red Hat subscription either through Amazon Web Services or by your own Red Hat Cloud Access subscription. |
| 4   | Ensure that you have the required resources. | See [Supported footprints of System Manager ISO on Microsoft Azure](#) on page 15 |
| 5   | Create an RHEL instance. | See [Creating RHEL instance on Microsoft Azure](#) on page 30 |
| 6   | Copy the ISO to the RHEL instance. | See [Uploading the Avaya Aura application ISO to RHEL machine on Microsoft Azure](#) on page 31 |

---

### Creating RHEL instance 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.

In a software-only installation, the customer will also install the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, it is recommended to check the list of tested RPMs and follow the instructions in the PSN periodically published by Avaya. PSN is available at [PSN020361u](#).
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 Size tab, select the profile as D4_v2, and click Select.
7. In the Settings tab, enter or select the required details, and click OK.
8. In the Summary tab, click Create.
   The deployment begins. After the successful deployment, shut down the virtual machine.
9. On the Virtual Machines page, click on the RHEL virtual machine name that you created.
10. Change the hard disk size from 32 GB to 44 GB and save the configuration.
    System Manager requires four hard disks. By default, one hard disk is available. You must create additional three hard disks. You must create the hard disks in the same sequence as mentioned in the Supported footprints of System Manager ISO on Microsoft Azure on page 15.

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.

---

**Preconfiguration for deploying ISO on Google Cloud Platform**

---

**Checklist for deploying ISO on Google Cloud Platform**

Ensure that you complete the following before deploying Avaya Aura® System Manager 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>Purchase the required licenses.</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>Register for PLDS and perform the following:</td>
<td></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 16.</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>
<tr>
<td>4</td>
<td>Create a PPK file.</td>
<td>See <a href="#">Creating a PPK file</a> on page 33</td>
</tr>
<tr>
<td>5</td>
<td>Ensure that you have the required resources.</td>
<td>See <a href="#">Supported footprints of System Manager ISO on Google Cloud Platform</a> on page 15</td>
</tr>
<tr>
<td>6</td>
<td>Create an RHEL instance.</td>
<td>See <a href="#">Creating RHEL instance on Google Cloud Platform</a> on page 33</td>
</tr>
<tr>
<td>7</td>
<td>Copy the ISO to the RHEL instance.</td>
<td>See <a href="#">Uploading the Avaya Aura application ISO to RHEL machine on Google Cloud Platform</a> on page 35</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.

In a software-only installation, the customer will also install the Red Hat provided RPM updates. To avoid possible issues or incompatibilities with new RPMs, it is recommended to check the list of tested RPMs and follow the instructions in the PSN periodically published by Avaya. PSN is available at [PSN020361u](#).

⚠️ **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 vCPUs and memory needed for your deployment.

   It is recommended to take the required CPUs only. For CPU, memory, and hard disk details, see [Supported footprints of System Manager ISO on Google Cloud Platform](#) on page 15.

5. Under the **Boot disk** section, click **Change** and do the following:
   a. Select the appropriate RHEL image. For the supported RHEL version, see “Third party software requirements” section.
   b. In the **Size (GB)** field, enter the required disk size and click **Select**.

   For more information about the disk size requirements, see [Supported footprints of System Manager ISO on Google Cloud Platform](#) on page 15.

   You will return to the Create an instance page.

6. Click **Networking** and click in the **Networking interfaces** field, 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 **Security**.

9. Under the **SSH Keys** section, in the **Enter entire key data** section, copy your private key details.
When you paste the key, a login user is also created.

10. Click **Create**.

Virtual machine instance will be deployed and will appear under the VM instances page.

System Manager requires four hard disks. By default, one hard disk is available. You must create additional three hard disks.

11. To create the additional hard disks, perform the following steps:
   a. Click on the RHEL instance and click **Edit**.
   b. Under the **Boot disk and local disk** section, click **Add item**.
   c. Select the drop-down and click **Create disk**.
   d. Enter the required details.

You must create the hard disks in the same sequence as mentioned in the [Supported footprints of System Manager ISO on Google Cloud Platform](#) on page 15.

**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 and enter the login credentials.
2. Click **Advanced**, and select **Advanced**.
3. In the left pane of the Advanced Site Settings window, click **Authentication**.
4. In the right pane, click the browse icon under the **Private key file** field and browse to the .ppk file.
5. Click **OK**, and click **Login**.
6. Upload the .iso to the virtual machine instance.
Chapter 4: Deploying

Deploying Avaya Aura® application OVA on Amazon Web Services

Deploying Avaya Aura® application AMI

About this task
You can deploy Avaya Aura® application AMI on Amazon Web Services

Before you begin
Convert the Avaya Aura® application OVA to AMI. See Checklist for converting Avaya Aura application OVA to an Amazon Machine Image on page 19.

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 IMAGES > AMIs.
   The system displays the list of AMIs.
4. Select the Avaya Aura® application AMI, and click Launch.
   You must select the correct instance type for deploying the AMI. If you select an incorrect instance type, usability of the system might be impacted.
5. On the Choose an Instance Type page, select an instance type, and click Next: Configure Instance Details.
6. Click Next: Add Storage.
7. On the Add Storage page, leave the default settings, and click Next: Add Tags.
9. On the Configure Security Group page, create a new security group or select an existing security group, and click Review and Launch.
You must select the security group that has the required ports enabled. For information about accessing ports, see “Accessing the port matrix document” section.

10. 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.

11. Click *Launch Instances*.

The system creates the instance and displays it on the Instances page.

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

---

### Installing the System Manager patch from CLI

**About this task**

From System Manager Release 7.1 and later, you must install the patch after the ova deployment is complete.

**Before you begin**

Download the latest System Manager patch file and save the patch file to the `/swlibrary` location of System Manager.

**Procedure**

1. Log in to the System Manager command line interface.
2. Run the command: `SMGRPatchdeploy /swlibrary/<System_Manager_R8.1.x.x_xxxxxxxxx.bin>`.
Next steps

Note:
Modifying the network or management configuration is not recommended before the patch deployment.

Log on to the System Manager web console. At your first log in, change the System Manager web console credentials.
Click About and check the software 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.

---

**Deploying Avaya Aura® application ISO on Infrastructure as a Service**

You can deploy the Avaya Aura® application on Infrastructure as a Service by using the following methods:

- Bash CLI
- Avaya SDM client

**Related links**

- [Adding a location](#) on page 39
- [Adding a software-only platform](#) on page 40
- [Deploying the System Manager Software-Only ISO image by using Solution Deployment Manager Client](#) on page 52

---

**Adding a location**

**About this task**

You can define the physical location of the host and configure the location specific information. You can update the information later.

**Procedure**

1. On the **Locations** tab, in the Locations section, click **New**.
2. In the New Location section, perform the following:
   a. In the Required Location Information section, type the location information.
   b. In the Optional Location Information section, type the network parameters for the virtual machine.

3. Click Save.
   The system displays the new location in the Application Management Tree section.

Related links
Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39

Adding a software-only platform

About this task
Use this procedure to add an operating system on Solution Deployment Manager. In Release 8.1.2, the system supports the Red Hat Enterprise Linux Release 7.6 64-bit operating system.

Before you begin
Add a location.

Procedure
1. On the Platforms tab, click Add.
2. In Platform Name, type the name of the platform.
3. In Platform FQDN or IP, type the FQDN or IP address of the base operating system.
4. In User Name, type the user name of the base operating system.
   For a software-only deployment, the user name must be a direct access admin user. If the software-only application is already deployed, provide the application cli user credentials.
5. In Password, type the password of the base operating system.
6. In Platform Type, select OS.
7. Click Save.
   If the platform has some applications running, the system automatically discovers those applications and displays the applications in the Applications tab.
   • If Solution Deployment Manager is unable to establish trust, the system displays the application as Unknown.
   • If you are adding OS, only Add and Remove operations are available on the Platforms tab. You cannot perform any other operations. On the Applications tab, the system enables the New option. If the application is System Manager, the system enables Update App on Solution Deployment Manager Client.

The system displays the added base operating system on the Platforms tab.
Related links
Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39

Deploying the System Manager Software-Only ISO image using bash CLI

Preparing for software-only deployments

About this task
Use this procedure to prepare the setup for software-only deployments.

Procedure

1. Create an RHEL instance with required resources. For more information on creating RHEL instance, see Red Hat documentation.
   
   For more information about the required resources, see Supported footprints information for respective environments.

2. Register the RHEL instance to the Red Hat subscription or create local repository for RPM installation or updates.
   
   For example,
   ```bash
   subscription-manager repos --enable rhel-7-server-rpms
   ```

3. To create a directory, run the following command:
   ```bash
   mkdir /var/installer
   ```

4. Download the Avaya Aura® application ISO to the RHEL instance.

5. Run the following command to mount the ISO:
   ```bash
   mount -o loop AvayaAuraSystemManager-8.1.x.0.xxxxxx_v47.iso /mnt
   ```

6. Run the following command to copy the ISO to the directory:
   ```bash
   cp -rvf /mnt/* /var/installer
   ```

7. Run the following command to install dependencies:
   ```bash
   yum install SMGR-Dependencies-0.1-1.noarch.rpm -y
   ```

8. Run the following command to unmount the /mnt directory:
   ```bash
   umount /mnt
   ```

9. Run the following commands to install required RPMs:
   ```bash
   cd pre-install_rpms
   rpm -Uvh *.rpm --nodeps
   ```

For the list of tested Avaya Aura® Software-Only RPMs, see Avaya PSN020361u at PSN020361u.
Important:
The PSN PSN020361u provides details of the latest RPMs tested with Avaya applications. These RPM versions should be used when installing and updating the operating system. Using the RPM versions that are not tested might result in an operational impact to the Avaya application.

10. Disable SELinux if already enabled.

For disabling SELinux, see Red Hat documentation.

11. For AWS, run the following commands to remove cloud-init package:

   ```
   systemctl stop cloud-init
   systemctl disable cloud-init
   yum remove cloud-init -y
   ```

12. Reboot the system.

Related links
Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39

Checking the environment

Before you begin
- Create an RHEL instance.
- Create a user before running the installer.
- Install required RPMs.

Procedure
1. Log in to the RHEL instance as a default user and switch to the root account.
   You must run the installer as a root user.
2. Go to, `cd /var/installer`.
3. To check for installer environment check, do one of the following:
   - For profile 2, type the following command:
     ```
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 250Kuser
     ```
   - For profile 3, type the following command:
     ```
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 250Kuser-prof3
     ```
   - For profile 4, type the following command:
     ```
     ./Install_System_Manager_8.1.0.0.xxxxxx -c -p 300Kuser-prof4
     ```
   The system checks for the environment against the installer. During this time, you cannot perform any other action.
   If the check fails, take necessary steps to fix errors and perform the installer check again.

Related links
Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39
Deploying System Manager *Software-Only ISO image* using the OS console

About this task

Use this procedure to deploy the System Manager ISO image in a Software-Only environment.

Before you begin

- Create an operating system instance.
- Copy the installer and check the environment.

Procedure

1. Log on to the RHEL instance.
2. Go to the `/var/install` directory.
3. Run the following installation script as a root user:
   ```bash
   ./Install_System_Manager_8.1.0.0.xxxxxx
   ```
   The system runs the command and displays the installation status of the required RPMs.
4. Read the prompt messages.
5. Press Enter to continue.
   
   The installer checks the package and environment settings.
   
   The system displays the following message:
   
   A reboot will be required in order to complete this. Please exit any other sessions before continuing.
6. Press Enter to continue.
7. If the installer does not find old network interfaces naming scheme (eth0 and eth1), when prompted, type yes to convert network interfaces to old scheme.
   
   The system displays the message: Rebooting the system and please re-run the SMGR install after reboot.
8. After reboot of the system, go to `/var/installer`, and re-run the following installation script as a root user:
   ```bash
   ./Install_System_Manager_8.1.0.0.xxxxxx
   ```
9. On the End User License Agreement page, press Y to start the installation process.
10. The system starts the installation and prompts you to configure the System Manager configuration and network parameters such as IPv4 address, IPv4 netmask, IPv4 gateway, short hostname, domain name, DNS server IP, IPv6 address, IPv6 network prefix, IPv6 gateway address, default search list, NTP IP, virtual hostname, virtual domain name, SNMP V3 parameters, SMGR CLI username and Password before proceeding to the next step. For more information on configuration and network parameters, see Network and configuration field descriptions on page 45.
11. In the Enter profile page, select the required System Manager profile from the following:
   • Press 1 for profile 2
   • Press 2 for profile 3
   • Press 3 for profile 4
12. On the Enhanced Access Security Gateway (EASG) page, read the EASG information, and click OK.
13. Select one of the following options to enable or disable EASG and click OK:
   • Enable EASG (Recommended)
   • Disable EASG
14. Verify the configuration details and press Enter to continue.
15. Select the required Backup definition parameter for System Manager schedule backup.
16. Click Yes to install Avaya’s version of bash RPM.
   Installing Avaya’s customized bash is optional, but Avaya recommends to install Avaya’s customized bash to help Avaya support.
   This step is applicable only if the installed version of the bash RPM is older than the Avaya provided bash RPM.
17. Click Continue to reboot the system for post installation configuration.
18. To verify post installation status, run the following command:
   ```bash
   cd/var/log/Avaya/PostDeployLogs/
tailf post_install_sp.log
   ```
   ✶ Note:
   On successful post installation, exit status of eject command is 0 is displayed.
19. Access System Manager web interface using IP address or FQDN. If installation is successful, Installation of latest System manager patch is mandatory is displayed.
   ✶ Note:
   For more information on mandatory patch installation, see “Installing mandatory patch” in *Upgrading Avaya Aura® System Manager*

Related links
   Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39
## Network and configuration field descriptions

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management IPv4 Address (or Out of Band Management IPv4 Address)</td>
<td>The IPv4 address of the System Manager application for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the inbound signaling network.</td>
</tr>
<tr>
<td>Management Netmask</td>
<td>The Out of Band Management subnetwork mask to assign to the System Manager application.</td>
</tr>
<tr>
<td>Management Gateway</td>
<td>The gateway IPv4 address to assign to the System Manager application.</td>
</tr>
<tr>
<td>IP Address of DNS Server</td>
<td>The DNS IP addresses to assign to the primary, secondary, and other System Manager applications. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>Management FQDN</td>
<td>The FQDN to assign to the System Manager application.</td>
</tr>
<tr>
<td>Note:</td>
<td>System Manager hostname is case sensitive. The restriction applies only during the upgrade of System Manager.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the System Manager application for out of band management. The field is optional.</td>
</tr>
<tr>
<td>IPv6 Network prefix</td>
<td>The IPv6 subnetwork mask to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Default Search List</td>
<td>The search list of domain names. The field is optional.</td>
</tr>
<tr>
<td>NTP Server IP/FQDN</td>
<td>The IP address or FQDN of the NTP server. The field is optional. Separate the IP addresses with commas (,).</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The timezone where the System Manager application is located. A list is available where you select the name of the continent and the name of the country.</td>
</tr>
</tbody>
</table>

**Note:**

You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public IP Address</td>
<td>The IPv4 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public Netmask</td>
<td>The IPv4 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public Gateway</td>
<td>The gateway IPv4 address to assign to the System Manager application. The field is optional.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public FQDN</td>
<td>The FQDN to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Address</td>
<td>The IPv6 address to enable public access to different interfaces. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Network Prefix</td>
<td>The IPv6 subnetwork mask to assign to System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Public IPv6 Gateway</td>
<td>The gateway IPv6 address to assign to the System Manager application. The field is optional.</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Virtual Hostname</td>
<td>The virtual hostname of the System Manager application.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong></td>
</tr>
<tr>
<td></td>
<td>• The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.</td>
</tr>
<tr>
<td></td>
<td>• VFQDN is a mandatory field.</td>
</tr>
<tr>
<td></td>
<td>• By default, VFQDN entry gets added in the /etc/hosts file during installation. Do not remove VFQDN entry from the /etc/hosts file.</td>
</tr>
<tr>
<td></td>
<td>• VFQDN entry will be below FQDN entry and mapped with IP address of system. Do not manually change the order and value.</td>
</tr>
<tr>
<td></td>
<td>• You must keep VFQDN domain value same as of FQDN domain value.</td>
</tr>
<tr>
<td></td>
<td>• If required, VFQDN value can be added in DNS configuration, ensure that the value can be resolved.</td>
</tr>
<tr>
<td></td>
<td>• Secondary Server (Standby mode) IP address value is mapped with VFQDN value in hosts file of Primary server IP address. After Secondary Server is activated, then the IP address gets updated with Secondary Server IP address.</td>
</tr>
<tr>
<td></td>
<td>• In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.</td>
</tr>
<tr>
<td></td>
<td>• After System Manager installation, if you require to change the System Manager VFQDN value, perform the following:</td>
</tr>
<tr>
<td></td>
<td>1. Log in to System Manager with administrator privilege credentials.</td>
</tr>
<tr>
<td></td>
<td>2. Run the <code>changeVFQDN</code> command.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>When you run the <code>changeVFQDN</code> command on System Manager, data replication synchronization between System Manager with Session Manager and other elements fails To correct VFQDN on other elements and to retrieve new VFQDN from System Manager, see product-specific Administering document.</td>
</tr>
<tr>
<td>Virtual Domain</td>
<td>The virtual domain name of the System Manager application.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SNMPv3 User Name Prefix</td>
<td>The prefix for SNMPv3 user.</td>
</tr>
<tr>
<td>SNMPv3 User Authentication Protocol Password</td>
<td>The password for SNMPv3 user authentication.</td>
</tr>
</tbody>
</table>

Table continues…
### Name | Description
--- | ---
Confirm Password | The password that you retype to confirm the SNMPv3 user authentication protocol.
SNMPv3 User Privacy Protocol Password | The password for SNMPv3 user privacy.
Confirm Password | The password that you must provide to confirm the SNMPv3 user privacy protocol.

### Name | Description
--- | ---
SMGR command line user name | The user name of the System Manager CLI user.
**Note:** Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsc, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.
SMGR command line user password | The password for the System Manager CLI user.
Confirm Password | The password that you retype to confirm the System Manager CLI user authentication.

### Name | Description
--- | ---
Schedule Backup? | • **Yes**: To schedule the backup jobs during the System Manager installation.  
• **No**: To schedule the backup jobs later.
**Note:** If you select No, the system does not display the remaining fields.
Backup Server IP | The IP address of the remote backup server.
**Note:** The IP address of the backup server must be different from the System Manager IP address.
Backup Server Login Id | The login ID of the backup server to log in through the command line interface.
Backup Server Login Password | The SSH login password to log in to the backup server from System Manager through the command line interface.
Confirm Password | The password that you reenter to log in to the backup server through the command line interface.
Backup Directory Location | The location on the remote backup server.
File Transfer Protocol | The protocol that you can use to create the backup. The values are SCP and SFTP.

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Repeat Type</td>
<td>The type of the backup. The possible values are:</td>
</tr>
<tr>
<td></td>
<td>• Hourly</td>
</tr>
<tr>
<td></td>
<td>• Daily</td>
</tr>
<tr>
<td></td>
<td>• Weekly</td>
</tr>
<tr>
<td></td>
<td>• Monthly</td>
</tr>
<tr>
<td>Backup Frequency</td>
<td>The frequency of the backup taken for the selected backup type.</td>
</tr>
<tr>
<td></td>
<td>The system generates an alarm if you do not schedule a System Manager backup every seven days.</td>
</tr>
<tr>
<td>Backup Start Year</td>
<td>The year in which the backup must start. The value must be greater than or equal to the current year.</td>
</tr>
<tr>
<td>Backup Start Month</td>
<td>The month in which the backup must start. The value must be greater than or equal to the current month.</td>
</tr>
<tr>
<td>Backup Start Day</td>
<td>The day on which the backup must start. The value must be greater than or equal to the current day.</td>
</tr>
<tr>
<td>Backup Start Hour</td>
<td>The hour in which the backup must start. The value must be six hours later than the current hour.</td>
</tr>
<tr>
<td>Backup Start Minutes</td>
<td>The minute when the backup must start. The value must be a valid minute.</td>
</tr>
<tr>
<td>Backup Start Seconds</td>
<td>The second when the backup must start. The value must be a valid second.</td>
</tr>
<tr>
<td>Public</td>
<td>The port number that is mapped to public port group.</td>
</tr>
<tr>
<td></td>
<td>You must configure Public network configuration parameters only when you configure Out of Band Management. Otherwise, Public network configuration is optional.</td>
</tr>
<tr>
<td>Out of Band Management</td>
<td>The port number that you must assign to the Out of Band Management port group. The field is mandatory.</td>
</tr>
</tbody>
</table>

**Enhanced Access Security Gateway (EASG) - EASG User Access**

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG</td>
<td>Enables or disables Avaya Logins for Avaya Services to perform the required maintenance tasks.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• 1: To enable EASG.</td>
</tr>
<tr>
<td></td>
<td>• 2: To disable EASG.</td>
</tr>
<tr>
<td></td>
<td>Avaya recommends to enable EASG.</td>
</tr>
<tr>
<td></td>
<td>You can also enable EASG after deploying or upgrading the application by using the command: <strong>EASGManage --enableEASG</strong>.</td>
</tr>
</tbody>
</table>
Customer Root Account

Note:
The Customer Root Account field is applicable only in case of deploying application OVA on Appliance Virtualization Platform and VMware by using Solution Deployment Manager. The system does not display the Customer Root Account field, when you deploy an application:

- OVA on VMware by using VMware vSphere Web Client.
- ISO on Red Hat Enterprise Linux by using Solution Deployment Manager.

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Customer Root Account for this Application</td>
<td>Enables or disables the customer root account for the application. Displays the ROOT ACCESS ACCEPTANCE STATEMENT screen. To accept the root access, click <strong>Accept</strong>. When you accept the root access statement, the system displays the Customer Root Password and Re-enter Customer Root Password fields.</td>
</tr>
<tr>
<td>Customer Root Password</td>
<td>The root password for the application</td>
</tr>
<tr>
<td>Re-enter Customer Root Password</td>
<td>The root password for the application</td>
</tr>
</tbody>
</table>

Data Encryption

Note:

- From Release 8.1.2, Data Encryption is supported only for Appliance Virtualization Platform and VMware Virtualized Environment.
- For data encryption, you must use a new encryption capable variant of Release 8.1E OVA.

For more information, see the application-specific Data Privacy Guidelines on the Avaya Support website.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Encryption</td>
<td>Enables or disables the data encryption.</td>
</tr>
<tr>
<td></td>
<td>The options are:</td>
</tr>
<tr>
<td></td>
<td>• 1: To enable the data encryption.</td>
</tr>
<tr>
<td></td>
<td>• 2: To disable the data encryption.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong></td>
</tr>
<tr>
<td></td>
<td>• An encrypted system cannot be changed to a non-encrypted system without a</td>
</tr>
<tr>
<td></td>
<td>new OVA installation and vice-versa.</td>
</tr>
<tr>
<td></td>
<td>• While using vCenter, when you enable data encryption and do not enter the</td>
</tr>
<tr>
<td></td>
<td>encryption passphrase, the system does not block the deployment due to vCen-</td>
</tr>
<tr>
<td></td>
<td>ter limitation. Therefore, ensure that you enter the encryption passphrase,</td>
</tr>
<tr>
<td></td>
<td>if data encryption is enabled.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On Solution Deployment Manager:</strong> When the Data Encryption field is set</td>
</tr>
<tr>
<td></td>
<td>to 1, the system enables the <strong>Encryption Pass-Phrase</strong> and **Re-enter En-</td>
</tr>
<tr>
<td></td>
<td>tryption Pass-Phrase** fields to enter the encryption passphrase.</td>
</tr>
<tr>
<td></td>
<td>• <strong>On vCenter or ESXi:</strong> When the Data Encryption field is set to 1, enter</td>
</tr>
<tr>
<td></td>
<td>the encryption passphrase in the <strong>Password</strong> and <strong>Confirm Password</strong></td>
</tr>
<tr>
<td>Encryption Pass-Phrase</td>
<td>This field is applicable when data encryption is enabled.</td>
</tr>
<tr>
<td></td>
<td>The passphrase for data encryption.</td>
</tr>
<tr>
<td></td>
<td>When you deploy the application by using Solution Deployment Manager, the</td>
</tr>
<tr>
<td></td>
<td>system applies the passphrase complexity rules.</td>
</tr>
<tr>
<td></td>
<td>When you deploy the application by using vCenter or ESXi, the system does</td>
</tr>
<tr>
<td></td>
<td>not apply the passphrase complexity rules.</td>
</tr>
<tr>
<td>Re-enter Encryption Pass-Phrase</td>
<td>The passphrase for data encryption.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Require Encryption Pass-Phrase at Boot-Time</td>
<td>If the check box is selected, you need to type the encryption passphrase whenever the application reboots. By default the Require Encryption Pass-Phrase at Boot-Time check box is selected. <strong>Important:</strong> You must remember the data encryption pass-phrase as the system prompts you to enter the encryption passphrase with every reboot of the application. If you lose the data encryption passphrase, the only option is to reinstall the OVA. If the check box is not selected, the application creates the Local Key Store and you are not required to type the encryption passphrase whenever the application reboots. This might make the system less secure. You can also set up the remote key server by using the <code>encryptionRemoteKey</code> command after the deployment of the application.</td>
</tr>
</tbody>
</table>

**Related links**

[Deploying Avaya Aura application ISO on Infrastructure as a Service](#) on page 39

---

**Deploying the System Manager Software-Only ISO image by using Solution Deployment Manager Client**

**About this task**

Use this procedure to deploy the System Manager ISO image in a Software-Only environment.

**Before you begin**

- Add a location.
  
  See [Adding a location](#) on page 39
- Add a platform
  
  See [Adding a software-only platform](#) on page 40
- 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>`
- Install System Manager dependencies on RHEL instance.
- Delete the `/var/installer` folder from RHEL machine, after installing the dependencies.
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.
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 System Manager Release 8.1.2 bin file now or after completing the System Manager deployment.

If you do not provide the System Manager Release 8.1.2 bin file at the time of deploying the System Manager, the system displays the following message:

> Installation of the latest System Manager patch is mandatory. Are you sure you want to skip the patch installation? If Yes, ensure to manually install the System Manager 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. After the check is completed successfully, the system displays a message “Environment check is successful”.

   ![Note:](image)

   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 more information, see [Network and configuration field descriptions](#) on page 45

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.

Related links
Deploying Avaya Aura application ISO on Infrastructure as a Service on page 39

Installing the System Manager service pack or patch from CLI

Before you begin
• To reach the System Manager command line interface, use one of the following methods:
  - Open vSphere Web Client and click on the Console tab or the icon.
  - Use PuTTY.
• Log in to System Manager with administrator privilege credentials.
• Take a snapshot of the System Manager virtual machine.

Procedure
Type SMGRPatchdeploy <absolute path to the service pack or patch for System Manager>.

If you do not provide the name of the patch or service pack, the console displays menu items. Provide the absolute path to the patch or service pack that you want to install for System Manager.

Next steps
Delete the snapshot after you verify the System Manager functionality.
Chapter 5: Configuring

Configuring the AMI on Amazon Web Services

Configuring the System Manager instance

About this task
Use the following procedure for the System Manager first boot configuration.

Before you begin
Download and install the System Manager license file.

Procedure

1. Log in to the System Manager command line interface with the user name as admin and password as admin.
   
   For example: ssh admin@<IP Address>
   
   At your first login, the system prompts you to change your admin password.

2. To configure the System Manager network and other parameters, run the command: smgrSetup.

3. Read the End User License Agreement (EULA).

4. To accept the EULA, in Do you accept the Avaya Software License Terms? (Y)es/(N)o, type Y.
   
   The system displays the message: Starting SMGR post-install first boot.

5. To specify configuration details, type y.

6. In Management IP Address, type the IP address of the System Manager instance.

7. In Management Netmask, type the subnetwork mask of the System Manager instance.

8. In Management Gateway, type the gateway IP address of the System Manager instance.

9. In Management Interface Short Hostname, type the host name of the System Manager instance.
   
   The value of the System Manager hostname is case-sensitive. The restriction applies only during the upgrade of System Manager.
10. In **Management Interface Domain Name**, type the domain name of the System Manager instance.

11. In **IP Address of DNS Server**, type the domain name of the primary, secondary, and System Manager instances.
   
   Separate the IP addresses with commas (,).

12. **(Optional)** In **Default Search List**, type the search list of domain names.

13. **(Optional)** In **NTP Server IP or FQDN**, type the IP address or FQDN of the NTP server.
   
   Separate the IP addresses with commas (,).

14. In **Time Zone Detail**, select the timezone where the System Manager instance is located.
   
   The system displays a list of available continents and countries.


16. At the **Virtual FQDN** prompt, perform the following for the System Manager instance.
   
   a. In **Virtual FQDN**, type the virtual FQDN name.
   
   b. In **Virtual Hostname**, type the virtual hostname.
   
   c. In **Virtual Domain name**, type the virtual domain name.

   The VFQDN value must be unique and different from the FQDN value of System Manager and the elements.

   • **VFQDN** is a mandatory field.

   • Do not add VFQDN entries in the DNS configuration.

   • Do not add **VFQDN** in the `/etc/hosts` file on System Manager.

   • Adding **VFQDN** in the `/etc/hosts` file might cause failures.

   • In Geographic Redundancy, the primary and secondary System Manager must use the same VFQDN.

   • After the System Manager installation, you cannot change the VFQDN unless you reinstall System Manager.

17. At the **SNMPv3** prompt, perform the following:

   a. In **User Name Prefix**, type the user name prefix.

   b. In **Authentication Protocol Password**, type the authentication protocol password.


   d. In **Privacy Protocol Password**, type the privacy protocol password.

   e. In **Re-type Privacy Protocol Password**, retype the privacy protocol password.
18. At the **SMGR CLI USER** prompt, perform the following:

   a. In **SMGR command line user name**, type the user name of the System Manager CLI user.

      Do not provide the common user names, such as, admin, csaadmin, postgres, root, bin, daemon, adm, sync, dbus, vcsa, ntp, saslauth, sshd, tcpdump, xfs, rpc, rpcuser, nfsnobody, craft, inads, init, rasaccess, sroot, postgres, smgr, and nortel.

   b. In **SMGR command line user password**, type the password for the System Manager CLI user.

   c. In **Confirm Password**, retype the password to confirm the System Manager CLI user authentication.

19. To schedule the remote backup during the System Manager installation, in **Schedule SMGR Backup**, type one of the following:

   a. 1: To schedule the backup.

   b. 2: To schedule the backup later.

20. At the **Enhanced Access Security Gateway (EASG)** prompt, read the following messages, and type one of the following:

    **Enable: (Recommended)**

    By enabling Avaya Logins you are granting Avaya access to your system.
    This is necessary to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.
    In addition to enabling the Avaya Logins, this product should be registered with Avaya and technically onboarded for remote connectivity and alarming. Please see the Avaya support site (support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.

    **Disable:**

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

    a. 1: To enable EASG.

       Avaya recommends to enable EASG.

       You can also enable EASG after deploying or upgrading the application by using the command: `EASGManage --enableEASG`.

    b. 2: To disable EASG.
21. At the **Customer Root Account** prompt, perform the following:
   a. In **Enable Customer Root Account for this Application**, click **Accept** to accept the root access.
   b. In **Customer Root Password**, type the root password for the System Manager.
   c. In **Re-enter Customer Root Password**, retype the password for the System Manager.

22. In 

23. To confirm the System Manager Configuration parameters, in **Do you want to continue**, type **Y**.
   
The system starts the configuration of the network parameters. The deployment process takes about 60–70 minutes to be completed.

Do not reboot the system until the configuration is complete.

You can monitor the System Manager post deployment configuration from the `/var/log/Avaya/PostDeployLogs/post_install_sp.log` file. Once the configuration is complete, the log file displays the message: `exit status of eject command is 0`.

**Next steps**

To verify that the System Manager installation is complete and the system is ready for patch deployment, do one of the following:

- **On the web browser**, type `https://<Fully Qualified Domain Name>/SMGR`, and ensure that the system displays the System Manager Log on page.
  
The system displays the message: Installation of latest System Manager patch is mandatory.

- **On the Command Line Interface**, log on to the System Manager console, and verify that the system does not display the message: Maintenance: SMGR Post installation configuration is In-Progress.
  
  It should only display the message: Installation of latest System Manager patch is mandatory.

---

**Allocating dedicated hosts**

**Procedure**

1. Sign in to the Amazon Web Services Management console.
2. Go to **Instances > Dedicated Hosts**.
3. Click **Allocate a Host**.
   
The system displays the Allocate Dedicated Host page.
4. In the **Instance type** field, select **c4.xlarge**.
5. In the **Availability Zone** field, select the appropriate zone.
6. In the **Quantity** field, type 2.
7. Click **Allocate host**.

---

**Dual data center configuration**

For configuring the applications in a dual data center environment, the instances must be configured in the same network region in two zones on the same Virtual Private Cloud (VPC).
Chapter 6: Post-installation verification

Post-installation steps

Procedure

Recreate all licenses with the new host ID format, and install the new license files.

System Manager on VMware uses a new host ID format for Avaya WebLM server. Therefore, all licenses previously installed becomes invalid. For instructions to install the license file, see Managing licenses in Administering Avaya Aura® System Manager.

Verifying the installation of System Manager

About this task

Perform the following verification procedure after you install System Manager Release 8.1.2 and configure System Manager.

Procedure

1. On the web browser, type https://<fully qualified domain name of System Manager>, and ensure that the system displays the System Manager web console.

2. On the upper-right corner, click and click About.

   The system displays the About SMGR window with the build details.

3. Verify the System Manager version number.

Installing language pack on System Manager

About this task

After you install, upgrade, or apply a service or a feature pack, run the language pack to get the localization support for the French language.

⚠️ Note:

After installing the language pack, you cannot uninstall the language pack.
Procedure

1. Log in to the System Manager command line interface with administrator privilege CLI user credentials.

2. Type `locate LocalizationScript.sh`, and press Enter.

   System Manager displays the path of the localization script.

   For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/script/LocalizationScript.sh`

3. Type `locate FrenchResourceBundle.zip`, and press Enter.

   The System Manager displays the path of the `FrenchResourceBundle.zip` script.

   For example: `/opt/Avaya/Mgmt/8.1.x/CommonConsole/localization/common_console/FrenchResourceBundle.zip`

   This is just an example of the path, the path might vary based on actual path that you get.

4. Type `cd $MGMT_HOME/CommonConsole/script/` to go to the localization script folder.

5. To run the localization script, type `sudo ./LocalizationScript.sh $MGMT_HOME/` CommonConsole/localization/common_console/FrenchResourceBundle.zip.

6. If you are running the data migration through SSH connection, then do not close the SSH session or terminate the connection.

   If you close the SSH session or terminate the connection, System Manager kills the process and the installation fails.

   **Note:**

   During this activity, System Manager restarts the JBoss service. Therefore, the System Manager web console will not be accessible. If System Manager is in the Geographic Redundancy mode then apply these steps on the secondary System Manager server also after secondary server is active.

7. Change the browser language setting to French.

---

**Enhanced Access Security Gateway (EASG) overview**

EASG provides a secure method for Avaya services personnel to access the Avaya Aura® application remotely and onsite. Access is under the control of the customer and can be enabled or disabled at any time. EASG must be enabled for Avaya Services to perform tasks necessary for the ongoing support, management and optimization of the solution. EASG is also required to enable remote proactive support tools such as Avaya Expert Systems® and Avaya Healthcheck.
Managing EASG from CLI

About this task
After deploying or upgrading an Avaya Aura® application, you can enable, disable, or view the status of EASG.

Before you begin
Log in to the application CLI interface.

Procedure
1. To view the status of EASG, run the command: `EASGStatus`.
   The system displays the status of EASG.

2. To enable EASG, do the following:
   a. Run the command: `EASGManage --enableEASG`.
      The system displays the following message.
      By enabling Avaya Services Logins you are granting Avaya access to your system. This is required to maximize the performance and value of your Avaya support entitlements, allowing Avaya to resolve product issues in a timely manner.
      The product must be registered using the Avaya Global Registration Tool (GRT, see https://grt.avaya.com) to be eligible for Avaya remote connectivity. Please see the Avaya support site (https://support.avaya.com/registration) for additional information for registering products and establishing remote access and alarming.
      b. When the system prompts, type yes.
      The system displays the message: EASG Access is enabled.

3. To disable EASG, do the following:
   a. Run the command: `EASGManage --disableEASG`.
      The system displays the following message.
      By disabling Avaya Services Logins you are denying Avaya access to your system. This is not recommended, as it can impact Avaya's ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Services Logins should not be disabled.
      b. When the system prompts, type yes.
      The system displays the message: EASG Access is disabled.
Viewing the EASG certificate information
Procedure
1. Log in to the application CLI interface.
2. Run the command: `EASGProductCert --certInfo`.
   The system displays the EASG certificate details, such as, product name, serial number, and certificate expiration date.

EASG product certificate expiration
The Avaya Aura® application raises an alarm if the EASG product certificate has expired or is about to expire in 365 days, 180 days, or 30 days. To resolve this alarm, the customer must apply the patch for a new certificate or upgrade to the latest release. Else, the customer loses the ability for Avaya to provide remote access support.

If the EASG product certificate expires, EASG access is still possible through the installation of EASG site certificate.

EASG site certificate
EASG site certificates are used by the onsite Avaya technicians who do not have access to the Avaya network to generate a response to the EASG challenge. The technician will generate and provide the EASG site certificate to the customer. The customer loads this EASG site certificate on each server to which the customer has granted the technician access. The EASG site certificate will only allow access to systems on which it has been installed, and will only allow access to the given Avaya technician and cannot be used by anyone else to access the system including other Avaya technicians. Once this is done, the technician logs in with the EASG challenge/response.

Managing site certificates
Before you begin
1. Obtain the site certificate from the Avaya support technician.
2. You must load this site certificate on each server that the technician needs to access. Use a file transfer tool, such as WinSCP to copy the site certificate to `/home/cust` directory, where `cust` is the login ID. The directory might vary depending on the file transfer tool used.
3. Note the location of this certificate and use in place of `installed_pkcs7_name` in the commands.
4. You must have the following before loading the site certificate:
   • Login ID and password
   • Secure file transfer tool, such as WinSCP
   • Site Authentication Factor

Procedure

1. To install the site certificate:
   a. Run the following command: `sudo EASGSiteCertManage --add <installed_pkcs7_name>`.
   b. Save the Site Authentication Factor to share with the technician once on site.

2. To view information about a particular certificate: run the following command:
   • `sudo EASGSiteCertManage --list`: To list all the site certificates that are currently installed on the system.
   • `sudo EASGSiteCertManage --show <installed_pkcs7_name>`: To display detailed information about the specified site certificate.

3. To delete the site certificate, run the following command:
   • `sudo EASGSiteCertManage --delete <installed_pkcs7_name>`: To delete the specified site certificate.
   • `sudo EASGSiteCertManage --delete all`: To delete all the site certificates that are currently installed on the system.
## System Manager documentation

The following table lists the documents related to System Manager. 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><strong>Avaya Aura® System Manager Overview and Specification</strong></td>
<td>Understand high-level product features and functionality.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Administering Avaya Aura® System Manager</strong></td>
<td>Administering System Manager applications and install patches on System Manager applications.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td><strong>Avaya Aura® System Manager Certificate Management</strong></td>
<td>Understand certificate management.</td>
<td>Customers and sales, services, and support personnel</td>
</tr>
<tr>
<td>Using</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Using the Solution Deployment Manager client</strong></td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td><strong>Avaya Aura® System Manager Solution Deployment Manager Job-Aid</strong></td>
<td>Deploy System Manager applications and install patches on System Manager applications.</td>
<td>System administrators</td>
</tr>
<tr>
<td>Implementation</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Upgrading Avaya Aura® System Manager</strong></td>
<td>Upgrade the Avaya Aura® System Manager application to Release 8.1.x.</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><strong>Deploying Avaya Aura® System Manager in Virtual Appliance</strong></td>
<td>Deploy System Manager applications in Virtual Appliance</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><strong>Deploying Avaya Aura® System Manager in Virtualized Environment</strong></td>
<td>Deploy System Manager applications in Virtualized Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td><strong>Deploying Avaya Aura® System Manager in Infrastructure as a Service Environment</strong></td>
<td>Deploy System Manager applications in Infrastructure as a Service Environment</td>
<td>Implementation personnel</td>
</tr>
</tbody>
</table>

Table continues…
### Title and Description

<table>
<thead>
<tr>
<th>Title</th>
<th>Description</th>
<th>Audience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Deploying Avaya Aura® System Manager in Software-Only Environment</td>
<td>Deploy System Manager applications in Software-Only Environment</td>
<td>Implementation personnel</td>
</tr>
<tr>
<td>Maintenance and Troubleshooting</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Avaya Aura® System Manager Fault Management and monitoring using SNMP</td>
<td>Monitor System Manager using SNMP.</td>
<td>System administrators and IT personnel</td>
</tr>
<tr>
<td>Troubleshooting Avaya Aura® System Manager</td>
<td>Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.</td>
<td>System administrators and IT personnel</td>
</tr>
</tbody>
</table>

### 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 the appropriate release number.

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

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

### 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.

Avaya Documentation Center navigation

Customer documentation for some programs is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

⚠️ Important:

For documents that are not available at Avaya Documentation Center, click More Sites > Support on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Center, you can:

- Search for content using one of the following:
  - Type a keyword in Search, and click Filters to search for content by product, release.
  - From Products & Solutions, select a solution and product, and select the appropriate document from the list.
- Sort documents on the search results page by last updated dated and relevance.
- 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 Manage Content > My Docs menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add topics 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 collection that others have shared with you.
- Add yourself as a watcher by using the Watch icon (👁).

Navigate to the Manage Content > Watchlist menu, and do the following:
  - Enable Include in email notification to receive email alerts.
  - 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 website.

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

★ Note:

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

Training

The following courses are available on the Avaya Learning website at http://www.avaya-learning.com. After you log into 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>20460W</td>
<td>Virtualization and Installation Basics for Avaya Team Engagement Solutions</td>
</tr>
<tr>
<td>20970W</td>
<td>Introducing Avaya Device Adapter</td>
</tr>
<tr>
<td>20980W</td>
<td>What's New with Avaya Aura® Release 8.1</td>
</tr>
<tr>
<td>71200V</td>
<td>Integrating Avaya Aura® Core Components</td>
</tr>
<tr>
<td>72200V</td>
<td>Supporting Avaya Aura® Core Components</td>
</tr>
<tr>
<td>20130V</td>
<td>Administering Avaya Aura® System Manager Release 8.1</td>
</tr>
<tr>
<td>21450V</td>
<td>Administering Avaya Aura® Communication Manager Release 8.1</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.

• 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, click Clear All and select Video in the Content Type.
  - In Search, type the product name. On the Search Results page, click Clear All and select Video in the Content Type.
The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to [www.youtube.com/AvayaMentor](http://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 a topic name to see the list of videos available for the topic. For example, Contact Centers.

**Note:**

Videos are not available for all products.

---

### Support

Go to the Avaya Support website at [https://support.avaya.com](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](#)

### 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 70
Chapter 8: 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.

Identifying the SSH user name of the RHEL instance on AWS

About this task
You will require the user name to login to the RHEL instance. This is applicable for software-only deployments.

Before you begin
Create RHEL instance on Amazon Web Services.

Procedure
  1. Log on to the Amazon Web Services management console.
  2. Click Servers > EC2.
  3. In the right-pane, select the RHEL instance you created.
  4. On the top of the page, click Actions > Connect.

In the page that opens, under the Example, user name of the RHEL instance appears. For example: ssh -i "<Key_Pair.pem>" abc-user@<IP address>. In this example, “abc-user” is the user name to login to the RHEL instance using SSH.
Index

A
accessing port matrix .......................................................... 67
adding
  location ............................................................................. 39
  software-only platform .................................................. 40
adding location ................................................................. 39
Amazon EC2 virtual server instance
  create .................................................................................. 21, 26
applications
  footprints ........................................................................ 14, 15
  instance type ................................................................. 14, 15
  system capacities .......................................................... 14
  vCPU, RAM, HDD, NICs .................................................. 14, 15
Avaya support website .......................................................... 70

C
checklist
  converting OVA to AMI .................................................... 19
  deploying ISO on Amazon Web Services ......................... 25
  deploying ISO on Google Cloud Platform ......................... 32
  deploying ISO on Microsoft Azure .................................... 29
  OVA to Amazon Machine Image ........................................ 19
  planning .............................................................................. 17
collection
  delete ................................................................................. 68
  edit name .......................................................................... 68
  generating PDF ................................................................ 68
  sharing content ................................................................. 68
configuring
  .PuTTY for SSH .................................................................. 72
  System Manager ................................................................ 56
  yum on RHEL ...................................................................... 28
connection types
  IaaS .................................................................................. 11
content
  publishing PDF output ..................................................... 68
  searching ........................................................................... 68
  sharing .............................................................................. 68
  sort by last updated .......................................................... 68
  watching for updates ....................................................... 68
convert
  .pem file to .ppk ............................................................... 72
copy
  Avaya WebLM ISO image on the OS ................................. 42
copying
  ISO to RHEL machine on Microsoft Azure ....................... 31
courses .............................................................................. 69
creating
  bucket ............................................................................... 20
  PPK file ............................................................................ 33
  RHEL instance on Azure .................................................. 30
creating (continued)
  RHEL machine on Google Cloud Platform ....................... 33
  user access key ............................................................... 22
  creating a key pair .......................................................... 18

D
dedicated hosts
  allocating .......................................................................... 59
deploying
  AMI .................................................................................. 36
  ISO on IaaS ...................................................................... 39
  System Manager ISO image using console ..................... 43
  System Manager ISO image using Solution Deployment
    Manager ........................................................................... 52
documentation
  System Manager ............................................................... 66
documentation center ........................................................ 68
  finding content ............................................................... 68
  navigation ......................................................................... 68
documentation portal ........................................................ 68
  finding content ............................................................... 68
  navigation ......................................................................... 68
document changes ............................................................. 7
downloading software
  using PLDS ....................................................................... 16
dual data center
  configuration .................................................................... 60

E
EASG
  certificate information ..................................................... 64
  disabling .......................................................................... 63
  enabling .......................................................................... 63
  status ............................................................................... 63
  EASG product certificate expiration .................................. 64
  EASG site certificate ........................................................ 64
  Enhanced Access Security Gateway
    EASG overview ............................................................. 62

F
finding content on documentation center ......................... 68
finding port matrix ............................................................ 67
first boot
  network and configuration .............................................. 45

I
IaaS
  overview ............................................................................ 9
Index

U

unsupported features ........................................................... 13
uploading
  ISO to virtual machine instance on Amazon Web Services .............................................................. 28
  iso to virtual machine instance on Google Cloud Platform ........................................................................ 35
  OVA s ................................................................................. 20

V

verify
  System Manager installation .............................................. 61
  videos .................................................................................. 69

W

watch list .............................................................................. 68