



Upgrading Avaya Aura[®] Session Manager

Draft

Release 10.2.x
Issue 10
March 2026

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

1 © 2013-2026, Avaya LLC

2 All Rights Reserved.

3 Notice

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

10 Documentation disclaimer

11 "Documentation" means information published in varying media
12 which may include product information, subscription or service
13 descriptions, operating instructions and performance specifications
14 that are generally made available to users of products.
15 Documentation does not include marketing materials. Avaya shall
16 not be responsible for any modifications, additions, or deletions
17 to the original published version of Documentation unless such
18 modifications, additions, or deletions were performed by or on the
19 express behalf of Avaya. End user agrees to indemnify and hold
20 harmless Avaya, Avaya's agents, servants and employees against
21 all claims, lawsuits, demands and judgments arising out of, or in
22 connection with, subsequent modifications, additions or deletions to
23 this documentation, to the extent made by End user.

24 Link disclaimer

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

33 Warranty

34 Avaya provides a limited warranty on Avaya hardware and software.
35 Please refer to your agreement with Avaya to establish the terms of
36 the limited warranty. In addition, Avaya's standard warranty language
37 as well as information regarding support for this product while under
38 warranty is available to Avaya customers and other parties through
39 the Avaya Support website: [https://support.avaya.com/helpcenter/
40 getGenericDetails?detailId=C20091120112456651010](https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010) under the link
41 "Warranty & Product Lifecycle" or such successor site as designated
42 by Avaya. Please note that if the product(s) was purchased from an
43 authorized Avaya channel partner outside of the United States and
44 Canada, the warranty is provided by said Avaya Channel Partner and
45 not by Avaya.

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

56 Hosted Service

57 THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN
58 AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR
59 AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS
60 OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE
61 AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo)
62 UNDER THE LINK "Avaya Terms of Use for Hosted Services"
63 OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND
64 ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE
65 HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED
66 SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON
67 BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE
68 DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY
69 AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE.
70 IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A
71 COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT
72 YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

73 TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY,
74 OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF
75 USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE
76 OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED
77 SERVICE.

78 Copyright

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

93 Virtualization

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

101 Third Party Components

102 The following applies only if the H.264 (AVC) codec is distributed
103 with the product. THIS PRODUCT IS LICENSED UNDER THE AVC
104 PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A
105 CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE
106 REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH
107 THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC
108 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A
109 PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO
110 PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE
111 IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.
112 ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA,
113 L.L.C. SEE [HTTP://WWW.MPEGLA.COM](http://www.mpegla.com).

114 Service Provider

115 WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL
116 PARTNER IS HOSTING ANY PRODUCTS THAT USE OR
117 EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA
118 CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE
119 AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND
120 ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC)
121 CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO
122 LICENSE FOR THE PERSONAL USE OF A CONSUMER
123 OR OTHER USES IN WHICH IT DOES NOT RECEIVE
124 REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH
125 THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC
126 VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A
127 PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO
128 PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE
129 IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE.
130 ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC)
131 CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE [HTTP://
132 WWW.MPEGLA.COM](http://www.mpegla.com).

133 Compliance with Laws

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

139 Preventing Toll Fraud

140 "Toll Fraud" is the unauthorized use of your telecommunications
141 system by an unauthorized party (for example, a person who is not a
142 corporate employee, agent, subcontractor, or is not working on your
143 company's behalf). Be aware that there can be a risk of Toll Fraud
144 associated with your system and that, if Toll Fraud occurs, it can

1 result in substantial additional charges for your telecommunications
2 services.

3 **Avaya Toll Fraud intervention**

4 If You suspect that You are being victimized by Toll Fraud and You
5 need technical assistance or support, please contact your Avaya
6 Sales Representative.

7 **Security Vulnerabilities**

8 Information about Avaya's security support policies can be
9 found in the Security Policies and Support section of [https://](https://support.avaya.com/security)
10 support.avaya.com/security.

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

14 **Downloading Documentation**

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

18 **Contact Avaya Support**

19 See the Avaya Support website: <https://support.avaya.com> for
20 Product or Cloud Service notices and articles, or to report a
21 problem with your Avaya Product or Cloud Service. For a list of
22 support telephone numbers and contact addresses, go to the Avaya
23 Support website: <https://support.avaya.com> (or such successor site
24 as designated by Avaya), scroll to the bottom of the page, and select
25 Contact Avaya Support.

26 **Trademarks**

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

37 Avaya is a registered trademark of Avaya LLC.

38 All non-Avaya trademarks are the property of their respective owners.

Contents

Chapter 1: Introduction	8
Purpose	8
Changes to platform support	8
Prerequisites	9
Change history	9
Chapter 2: Upgrade overview and considerations	13
Upgrade overview and considerations	13
Supported upgrade paths for Session Manager	15
Removal of default certificates	16
Branch Session Manager upgrade overview	17
Solution Deployment Manager	17
Chapter 3: Planning and preconfiguration	20
Prerequisites	20
Customer configuration data for Session Manager	21
Supported servers	22
Supported servers for Avaya Aura® applications	22
Supported hardware for VMware	24
Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)	24
Software requirements	24
Supported ESXi version	25
Supported ASP R6.0.x (KVM on RHEL 8.10) version	26
Latest software updates and patch information	27
Upgrade sequence for Avaya components	27
Optional Upgrade Sequence	30
Verify the software version of the Survivable Remote Servers	33
Optional Upgrade Sequence for Avaya components	34
Supported browsers	37
Software details of Session Manager and Branch Session Manager	38
Capacity limits	38
Supported footprints of Session Manager on VMware	38
Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10)	40
Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)	41
Supported footprints of Branch Session Manager on VMware	41
Chapter 4: Preupgrade tasks	43
Configuring the User settings	43
Obtaining a company ID	43
Establishing PLDS connection to Avaya	43
Adding trusted certificates	46
Creating a software library	48

Downloading software from PLDS.....	48
Downloading the OVA file to System Manager.....	49
Preparing Session Manager 8.x for upgrading to Release 10.2.x.....	50
Session Manager backup and restore commands.....	50
Applications pre-upgrade functions.....	51
Refreshing elements.....	51
Analyzing software.....	51
Downloading the software.....	52
File Download Manager field descriptions.....	53
Performing the preupgrade check.....	54
Preupgrade Configuration field descriptions.....	55
Upgrading VMware ESXi version.....	56
Virtual machine management.....	57
Application management.....	57
Managing the location.....	57
Managing the platform.....	60
Downloading the OVA file to System Manager.....	66
Managing the application.....	67
Managing vCenter.....	71
Chapter 5: Migrating from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	78
Migrating Session Manager or Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	78
Obtaining existing VMware details.....	79
Performing prerequisite tasks to migrate Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	79
Performing prerequisite tasks to migrate Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	81
Obtaining Session Manager configuration details.....	82
Obtaining Branch Session Manager configuration details.....	83
Restoring backup of Session Manager or Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10).....	84
Chapter 6: Migrate Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1.....	85
Migrating Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1.....	86
Upgrading Branch Session Manager Release 8.1.x to Release 10.2.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager	88
Migrating Appliance Virtualization Platform deployed on S8300D with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1.....	91
Chapter 7: Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.0.....	93
Migrating Appliance Virtualization Platform deployed on Common Server 1, 2, or 3 with Session Manager to Avaya Solutions Platform 130 Release 5.0.....	93

Migrating Appliance Virtualization Platform deployed on Avaya Solutions Platform 120 with Session Manager to Avaya Solutions Platform 130 Release 5.0.....	94
Chapter 8: Upgrading Session Manager to Release 10.2.x on Avaya Solution Platform130 or on VMware.....	97
Upgrading Session Manager by using System Manager Solution Deployment Manager.....	97
Upgrading Session Manager or Branch Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using System Manager Solution Deployment Manager	97
Upgrading VMware-based Session Manager Release 6.3.22 to Release 10.2.x using System Manager Solution Deployment Manager	100
Upgrade Management field descriptions.....	101
Upgrade Configuration field descriptions.....	103
Edit Upgrade Configuration field descriptions.....	104
Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using data migration utility.....	111
Upgrading Session Manager from Release 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through command-line interface.....	113
Upgrading non-edge Branch Session Manager to edge Branch Session Manager Release 10.2.x.....	114
Upgrading Branch Session Manager instances in bulk.....	115
Downloading the bulk import spreadsheet template.....	115
Filling the bulk import spreadsheet for upgrading Branch Session Manager instances in bulk.....	116
Upgrading Branch Session Manager instances in bulk by using System Manager Solution Deployment Manager.....	119
patchSM command.....	120
Installing software patches.....	121
Installing a Session Manager or Branch Session Manager patch with the snapshot option..	121
Chapter 9: Upgrading Session Manager to Release 10.2.x on Software-only environment.....	123
Upgrade path for Software-only environment.....	123
Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x on Software-only and IaaS.....	123
Chapter 10: Post-upgrade verification.....	126
Post-upgrade checklist for Session Manager or Branch Session Manager.....	126
Configuring Session Manager in a System Manager geographically redundant environment.....	127
Testing the Session Manager instance.....	127
Installing the license file.....	127
Verifying Data Replication.....	128
Troubleshooting Data Replication.....	128
Viewing the Security Module status.....	129
Troubleshooting Security Module Sanity failure.....	129
Verifying the Enrollment Password status.....	130
Viewing the Session Manager entity link connection status.....	130
Accepting new service.....	131

Enhanced Access Security Gateway.....	132
Checking EASG status.....	132
Enabling and disabling EASG using CLI.....	132
Enabling and disabling EASG through System Manager.....	133
EASGManage.....	133
Loading and managing site certificate.....	134
Alarming Configuration.....	135
Network Management Systems Destinations.....	135
Activating and managing the Session Manager serviceability agent.....	136
Alarming configuration checklist.....	136
Adding Session Manager to the SAL Gateway.....	136
Generating a test alarm.....	138
Chapter 11: Resources	139
Session Manager documentation.....	139
Finding documents on the Avaya Support website.....	140
Accessing the port matrix document.....	140
Avaya Documentation Center navigation.....	141
Training.....	142
Viewing Avaya Mentor videos.....	142
Support.....	143
Using the Avaya InSite Knowledge Base.....	143
Appendix A: OS-level logins for Session Manager	145
Appendix B: Upgrading RHEL	147
Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines.....	147
Appendix C: Product notifications	149
Viewing Product Correction Notices and Product Support Notices.....	149
Registering for product notifications.....	150
Appendix D: Archiving logs	151
Log harvester.....	151
Accessing the Log Harvester service.....	152
Creating a new log harvesting profile.....	152
Create New Profile field descriptions.....	152
Submitting a request for harvesting log files.....	153
Appendix E: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10)	155
Virtual Machine Backups (clone) as an alternative to snapshots.....	155
Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10).....	155
Calculating space for the clone.....	158
Validating a Virtual Machine Backup (clone).....	160
Rolling back using the Virtual Machine Backup (clone).....	162
Appendix F: Security Service Pack	165
Avaya Aura® Security Service Packs overview.....	165
Glossary	167

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya Aura® Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x on:

- Avaya Solutions Platform 130 (Avaya supplied ESXi 7.0) environment.
- VMware in customer-provided Virtualized Environment.
- Avaya Solutions Platform 130 Release 6.0 (Avaya supplied Kernel-Based Virtual Machine on Red Hat Enterprise Linux R8.10) environment.
- Customer-provided Software-only environment.
- Amazon Web Services (AWS), Google Cloud, and Microsoft Azure setup in Infrastructure as a service (IaaS).

This document:

- Includes upgrade checklists and maintenance procedures.
- Does not include optional or customized aspects of a configuration.

The primary audience for this document is anyone who upgrades, configures, and verifies Session Manager upgrade at a customer site.

Changes to platform support

As of January 1, 2026, Avaya has refined its infrastructure support strategy for Avaya Aura® and Surround Applications. This update specifically impacts Software-Only and Infrastructure as a Service (IaaS) deployment models. To ensure your environment remains compliant and supported, review the following changes to supported platforms:

Discontinued Platforms:

- Hypervisor: Microsoft Hyper-V
- Cloud Platforms: Microsoft Azure, Google Cloud Platform (GCP), IBM Cloud

Supported platforms for Software Only and Infrastructure as a Service (IaaS) deployment models:

- Cloud Platform: AWS

- On-premises platforms: KVM, Nutanix, VMware

Prerequisites

Before upgrading the Avaya Aura® application, ensure that you have the following knowledge, skills, and tools:

Knowledge

- Avaya Solutions Platform
- **For VMware:** VMware® vSphere™ virtualized environment
- **For KVM:** ASP R6.0.x (KVM on RHEL 8.10) virtualized environment
- **For Amazon Web Services (AWS):** AWS environment
- **For Google Cloud:** Google Cloud environment
- **For Azure:** Microsoft Azure environment
- **For IBM Cloud:** IBM Cloud for VMware Solutions environment
- Linux® Operating System
- System Manager

Skills

- Solution Deployment Manager
- VMware® vSphere™ virtualized environment
- KVM hypervisor
- AWS Management Console
- Google cloud
- Microsoft Azure
- IBM Cloud for VMware Solutions

Change history

Issue	Date	Summary of changes
10	March 2026	Added the section: Changes to platform support on page 8

Table continues...

Issue	Date	Summary of changes
9	February 2026	Updated the following sections: • Supported servers on page 22 • Supported servers for Avaya Aura applications on page 22 • Software requirements on page 24 • Supported ASP R6.0.x (KVM on RHEL 8.10) version on page 26 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 155 • Calculating space for the clone on page 158 • Validating a Virtual Machine Backup (clone) on page 160
8	October 2025	Updated the following sections: • Upgrade sequence for Avaya components on page 27 • Optional Upgrade Sequence for Avaya components on page 34
7	August 2025	Updated the following sections: • Upgrade sequence for Avaya components on page 27 • Optional Upgrade Sequence for Avaya components on page 34
6	April 2025	Updated the section for R10.2.1.1: • Supported ESXi version on page 25
5	January 2025	Updated the following sections: • Obtaining existing VMware details on page 79 • Obtaining Session Manager configuration details on page 82 • Obtaining Branch Session Manager configuration details on page 83

Table continues...

Issue	Date	Summary of changes
4	December 2024	Added the following sections for R10.2.1: • Optional Upgrade Sequence on page 30 • Verify the software version of the Survivable Remote Servers on page 33 • Optional Upgrade Sequence for Avaya components on page 34 • Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines on page 147 • Supported footprints of Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 40 • Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10) on page 41 • Migrating Session Manager or Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 78 • Obtaining existing VMware details on page 79 • Performing prerequisite tasks to migrate Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 79 • Performing prerequisite tasks to migrate Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 81 • Obtaining Session Manager configuration details on page 82 • Obtaining Branch Session Manager configuration details on page 83 • Restoring backup of Session Manager or Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10) on page 84 • Virtual Machine Backups (clone) as an alternative to snapshots on page 155 • Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10) on page 155 • Validating a Virtual Machine Backup (clone) on page 160 • Rolling back using the Virtual Machine Backup (clone) on page 162 Updated the following sections for R10.2.1: • Prerequisites on page 9 • Adding a software-only platform on page 63 • Avaya Aura Security Service Packs overview on page 165 • Supported servers for Avaya Aura applications on page 22 • Supported servers on page 22

Table continues...

Issue	Date	Summary of changes
3	March 2024	Added the section: Avaya Aura Security Service Packs overview on page 165
2	February 2024	Updated the section: Upgrade sequence for Avaya components on page 27
1	December 2023	10.2 Document Release.

Draft

Chapter 2: Upgrade overview and considerations

Upgrade overview and considerations

You can upgrade to Avaya Aura® Session Manager Release 10.2.x from the following:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 8.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 7.x on Avaya Aura® Virtualized Appliance, VMware-based or KVM-based Virtualized Environment, and Amazon Web Services.

! Important:

For upgrading Session Manager and Branch Session Manager to Release 10.2.x:

- Before upgrading Session Manager to Release 10.2.x, Avaya recommends that the older Session Manager Release version must be on the latest version of its releases with the latest Security Service Pack (SSP). The latest version for Release 7.1.x, 8.0.x, and 8.1.x are Release 7.1.3.8, 8.0.1.2, and 8.1.3.8 respectively.

When you are on a latest release, you can use the **backupSM** and **restoreSM** commands or the data migration utility to upgrade to Release 10.2.x.

- To upgrade Session Manager from Release 7.0.x to Release 10.2 and later, first upgrade Session Manager Release 7.0.x to 10.1.x, and then upgrade to Release 10.2 and later.

You cannot directly upgrade from Release 7.0.x to Release 10.2 and later. If you upgrade directly from Release 7.0.x to Release 10.2 and later, the upgrade might fail.

- In a scenario where upgrade of more than one Session Manager is from releases 7.x and 8.x, Cassandra has two distinct clusters, one on Session Manager Release 7.x or 8.x and the other on Session Manager Release 10.2. In this case, the User Storage Data under **System Status** on System Manager shows failed. Therefore, it is recommended that you upgrade the Session Managers running Release 7.x and 8.x to release 10.2 as soon as possible.

- 1 • To upgrade Session Manager to Release 10.2.x and later, you must install the latest
2 Security Service Pack (SSP) on Session Manager Release 8.1.x and later system before
3 upgrading System Manager to Release 10.2.x and later.
- 4 • For upgrading Session Manager from Release 6.x to Release 10.1 and later, first
5 upgrade Session Manager 6.x to 8.1.x, and then upgrade to Release 10.1 and later.
6 You cannot directly upgrade the Release 6.x system to Release 10.1 and later.
- 7 • From Release 10.1 and later, Appliance Virtualization Platform is no longer supported
8 for deploying or upgrading the Avaya Aura® applications. To upgrade the Avaya Aura®
9 applications, migrate Appliance Virtualization Platform to Avaya Solutions Platform 130
10 (Avaya-Supplied ESXi 7.0) Release 5.1.
- 11 • From Release 10.1 and later, Avaya Aura® applications will no longer have the Amazon
12 Web Services (AWS). Alternately, you can continue to deploy the application by using
13 the software-only offer. For more information, see the product-specific Software-only and
14 Infrastructure As a Service Environments guide.
- 15 • Upgrade the Session Manager servers one at a time to limit service degradation and
16 outages.
- 17 • Upgrade all Session Manager instances to the new release as soon as practical,
18 preferably in a single maintenance window. Session Manager clusters are designed
19 to operate with a mix of two supported releases within the cluster during the upgrade
20 interval, however, some features may not perform optimally while in this configuration.
21 Under no circumstance should there be more than two separate releases of Session
22 Manager within a cluster.
- 23 • Schedule the upgrade during hours of little or no system activity. The active call count of
24 Session Manager determines when the upgrade must occur. Ideally, the active call count
25 should be zero.
- 26 • Most SIP endpoints are assigned to a primary and a secondary SIP Proxy Server
27 (Session Manager). When upgrading the primary Session Manager, the endpoint does
28 not lose service because the secondary Session Manager handles the call.
- 29 • Verify firewall settings when performing a system installation or upgrade. For more
30 information, see the Avaya Aura® Port Matrix document for Avaya Aura® Session
31 Manager at Avaya Support website.

32 During an upgrade, the call processing traffic of the Session Manager server that is getting
33 upgraded is handled by the other Session Managers. Calls that are active when the upgrade takes
34 place will remain active. However, the Session Manager server denies any changes to the SIP
35 session, for example, transferring the call.

*** Note:**

- 36 • If you upgrade from Release 6.3.22 to Release 8.1.x using Solution Deployment
37 Manager, the call logs are stored and backed up automatically.
- 38 • Ensure to take User Data Storage backup before upgrading.

- 1 For information about backing up the call history using User Data Storage, see
 2 *Administering Avaya Aura® Session Manager*.

3 Supported upgrade paths for Session Manager

- 4 The following table displays all the upgrade paths from earlier releases to Release 10.2.x.
 5 For information about terms used in this table, see “Glossary”.

From offer	From Release	Session Manager	Branch Session Manager	To Software-only (VMware, KVM, RHVH, Hyper-V, AWS, GoogleCloud, or Azure) 10.2 (ISO)	To ASP 130 (OVA)/ VMware 10.2 (OVA)
AVP	7.x		✓	Migration using CLI	Migration using CLI
	7.1.3.x	✓	✓	Migration using CLI	Migration using CLI
	8.0.1	✓	✓	Migration using CLI	Migration using CLI
	8.1.x	✓	✓	Migration using CLI	Fully automated upgrade using SDM
VMware	7.x		✓	Migration using CLI	Migration using CLI
	7.1.3.x	✓	✓	Migration using CLI	Migration using CLI
	8.0.x	✓	✓	Migration using CLI	Migration using CLI
	8.1.x	✓	✓	Migration using CLI	Fully automated upgrade using SDM
	10.1.x	✓	✓	Migration using CLI	Fully automated upgrade using SDM
ASP 130	8.1.x	✓	✓	Migration using CLI	Fully automated upgrade using SDM
	10.1.x	✓	✓	Migration using CLI	Fully automated upgrade using SDM
KVM/ OpenStack/ RHVH (OVA)	7.1.x	✓	✓	Migration using CLI	Migration using CLI
	8.0.x	✓	✓	Migration using CLI	Migration using CLI
	8.1.x	✓	✓	Migration using CLI	Migration using CLI
Software-only	8.0.x	✓	✓	Migration using CLI	NA
	8.1.x	✓	✓	Migration using CLI	NA
	10.1.x	✓	✓	Migration using CLI	NA
AWS (OVA)	7.1.x	✓		Migration using CLI	Migration using CLI
	8.x	✓		Migration using CLI	Migration using CLI

! Important:

- 6 • Before starting the application upgrade, upgrade the platform and hypervisor.

- 1 • To upgrade System Manager, use Solution Deployment Manager Client. To upgrade
2 applications other than System Manager, use System Manager Solution Deployment
3 Manager.
- 4 • Upgrade or migration using Solution Deployment Manager is only supported with the
5 same IP Address of the application in a Software-only environment.
6 Software-only upgrade is supported for VMware, KVM, RHVH, Hyper-V, AWS,
7 GoogleCloud, and Azure.
- 8 • If the application supports the upgrade using Solution Deployment Manager, you can
9 also use the CLI for upgrading that application.
- 10 • To upgrade the application from Release 6.x to Release 10.x, upgrade the application
11 from 6.x to 8.1.x, and then upgrade to Release 10.x. You cannot directly upgrade the
12 Release 6.x system to Release 10.1 and later.
- 13 • Before upgrading Session Manager to Release 10.2.x, Avaya recommends that the older
14 Session Manager Release version must be on the latest version of its releases with the
15 latest Security Service Pack (SSP). The latest version for Release 7.1.x, 8.0.x, and 8.1.x
16 are Release 7.1.3.8, 8.0.1.2, and 8.1.3.8 respectively.
- 17 When you are on a latest release, you can use the **backupSM** and **restoreSM**
18 commands or the data migration utility to upgrade to Release 10.2.x.
- 19 • To upgrade Session Manager from Release 7.0.x to Release 10.2 and later, first upgrade
20 Session Manager Release 7.0.x to 10.1.x, and then upgrade to Release 10.2 and later.
21 You cannot directly upgrade from Release 7.0.x to Release 10.2 and later. If you upgrade
22 directly from Release 7.0.x to Release 10.2 and later, the upgrade might fail.
- 23 • In a scenario where upgrade of more than one Session Manager is from releases 7.x
24 and 8.x, Cassandra has two distinct clusters, one on Session Manager Release 7.x or
25 8.x and the other on Session Manager Release 10.2. In this case, the User Storage Data
26 under **System Status** on System Manager shows failed. Therefore, it is recommended
27 that you upgrade the Session Managers running Release 7.x and 8.x to release 10.2 as
28 soon as possible.

29 Removal of default certificates

30 Avaya SIP CA issued certificates are no longer supported for new installations. Default
31 certificates, also known as demo certificates, are non-unique identity certificates that were
32 automatically installed on newly shipped Session Manager servers. Default certificates are not
33 secure and do not meet current NIST standards.

34 New Session Manager servers no longer use the Avaya SIP Product CA issued Default
35 Certificates. New customer networks can request an Identity Certificate from the System Manager
36 Trust Management that is signed by the System Manager Certificate Authority.

37 For upgrades, Session Manager preserves the previous certificate. If a demo certificate was in use
38 in the previous release, the certificate is preserved through the upgrade.

39 Avaya recommends that customers use the newer certificates as soon as possible.

1 Branch Session Manager upgrade overview

See the PCN issued for the Session Manager software release. The Branch Session Manager (BSM) upgrade, in some cases, could involve upgrading Communication Manager Survivable Remote templates as outlined in the document, *Upgrading Avaya Aura® Communication Manager*. See [Product notifications](#) on page 149 for more information about PCNs and PSNs.

* Note:

- If you are upgrading an active Branch Session Manager, ensure that Branch Session Manager is administered on System Manager and the **Enrollment Password** is active.
- Before installing or upgrading the Branch Session Manager, ensure that all the Branch Session Managers are configured in DNS or added to the `/etc/hosts` file on System Manager.

An example of the contents of the `/etc/hosts` file is:

```
123.45.6.78      bsm.co.avaya.com bsm
123.45.6.88      core-asml.ca.avaya.com core-asml
```

The first entry is the IP address, the second entry is the FQDN, and the third entry is the short hostname (FQDN without the domain name).

- Ensure that the date and time is in sync between System Manager and System Platform. A clock shift can cause certificate and DRS replication problems.
- You must upgrade Branch Session Manager to be the same level as the core Session Manager.

20 Solution Deployment Manager

Solution Deployment Manager simplifies and automates the deployment and upgrade process.

With Solution Deployment Manager, you can deploy the following applications:

- System Manager
- Session Manager
- Branch Session Manager
- Communication Manager
- Application Enablement Services
- Avaya WebLM
- Avaya Diagnostic Server (Secure Access Link)
- Avaya Session Border Controller Release 8.0 and later
- Avaya Breeze® platform Release 3.3 and later
- Avaya Aura® Media Server

For the latest and most accurate information about other Avaya product compatibility information, go to **TOOLS > Product Compatibility Matrix** on the Avaya Support website.

*** Note:**

- 1 When an application is deployed on a KVM host, Solution Deployment Manager does not
- 2 support that application.

3 With Solution Deployment Manager, you can migrate, upgrade, and update the following
4 applications:

- 5 • Hardware-based Session Manager
- 6 • System Platform-based Communication Manager
 - 7 - Duplex CM Main / Survivable Core with Communication Manager
 - 8 - Simplex CM Main / Survivable Core with Communication Manager, Communication
 - 9 Manager Messaging, and Utility Services
 - 10 - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and
 - 11 Utility Services
 - 12 - Embedded CM Main with Communication Manager, Communication Manager Messaging,
 - 13 and Utility Services
 - 14 - Embedded Survivable Remote with Communication Manager, Branch Session Manager,
 - 15 and Utility Services
- 16 • System Platform-based Branch Session Manager
 - 17 - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and
 - 18 Utility Services
 - 19 - Embedded Survivable Remote with Communication Manager, Branch Session Manager,
 - 20 and Utility Services
- 21 • Session Manager Release 7.1.3.x and later
- 22 • Communication Manager Release 7.x and later
- 23 • Branch Session Manager Release 7.x and later
- 24 • Application Enablement Services Release 7.x and later
- 25 • Avaya Breeze® platform Release 3.3 and later
- 26 • System Manager Release 7.1.3.x and later (using SDM client only)
- 27 • WebLM Release 7.x and later

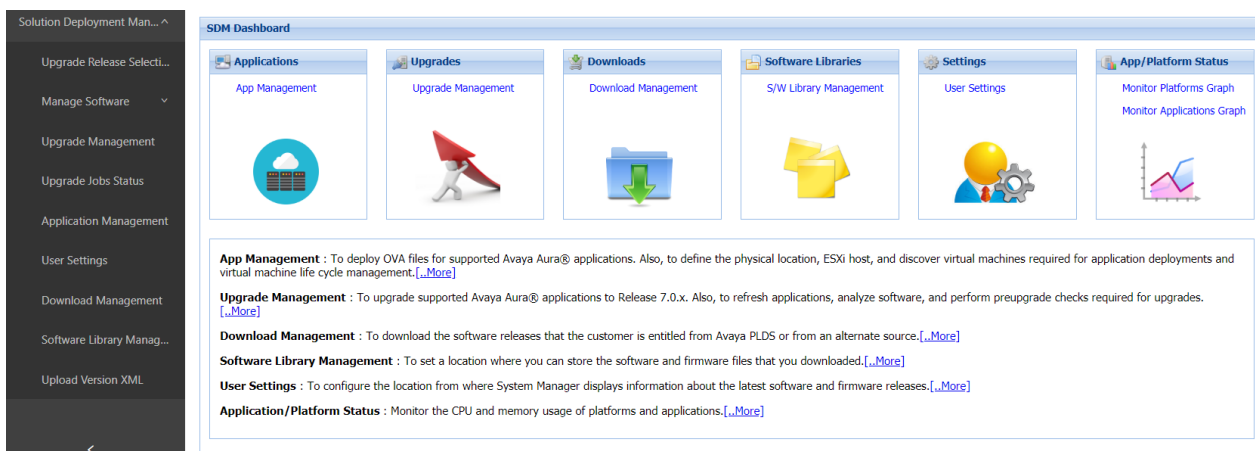
*** Note:**

- 28 You must manually migrate the Services virtual machine that is part of the template.

29 The centralized deployment and upgrade process provides better support to customers who want
30 to upgrade their systems to Avaya Aura® Release 10.2.x. The process reduces the upgrade time
31 and error rate.

32 **Solution Deployment Manager dashboard**

33 You can access the Solution Deployment Manager dashboard from the System Manager web
34 console or by installing the Solution Deployment Manager client.



Solution Deployment Manager capabilities

With Solution Deployment Manager, you can perform deployment and upgrade-related tasks by using the following links:

- **Upgrade Release Setting:** To select **Release 7.x Onwards** or **6.3.8** as the target upgrade. **Release 7.x Onwards** is the default upgrade target.
- **Manage Software:** To analyze, download, and upgrade the IP Office, Unified Communications Module, and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **Application Management:** To deploy OVA files for the supported Avaya Aura® application.
 - Configure Remote Syslog Profile.
 - Generate the Appliance Virtualization Platform Release 8.x or earlier Kickstart file.
 - Generate the platform Kickstart file for the following Appliance Virtualization Platform or Avaya Solutions Platform platforms:
 - Appliance Virtualization Platform 8.0.x
 - Appliance Virtualization Platform 8.1.x
 - Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1
- **Upgrade Management:** To upgrade Avaya Aura® applications to Release 10.2.x.
- **User Settings:** To configure the location from where System Manager displays information about the latest software and firmware releases.
- **Download Management:** To download the OVA files and firmware to which the customer is entitled. The download source can be the Avaya PLDS or an alternate source.
- **Software Library Management:** To configure the local or remote software library for storing the downloaded software and firmware files.
- **Upload Version XML:** To save the `version.xml` file to System Manager. You require the application-specific `version.xml` file to perform upgrades.

Chapter 3: Planning and preconfiguration

Prerequisites

Serial Number	Prerequisites	Tasks/ Notes
1	Upgrade System Manager to Release 10.2.x.	See the application-specific upgrade document.
2	Upgrade Appliance Virtualization Platform and AVP Utilities to Avaya Solutions Platform 130 Release 5.1 and later.	See the application-specific upgrade document.
3	Download the Session Manager or Branch Session Manager software.	See Software details of Session Manager and Branch Session Manager on page 38.
4	Verify that the existing server is compatible with Release 10.2.x version of the application. If the existing server is incompatible, change the server accordingly.	See Supported servers on page 22.
5	Keep the following information handy to create a backup on the remote server: • IP address • Directory • User Name • Password	-
6	Ensure that all virtual machines running on the host are on the same subnet mask. If Out of Band Management is configured in a virtual environment deployment, you need two subnet masks based on following requirements: • Public or signaling traffic: To route signaling traffic of all virtual machines. • Management traffic: To route management traffic of all virtual machines.	-

Customer configuration data for Session Manager

The following table identifies the required customer configuration information for deployment and configuration. An asterisk (*) indicates a required field.

Configuration Data	Field	Example value for the System	✓
Network Settings	Short hostname*	example-sm-1	
	Network domain*	Mycompany.com	
	IPv4 address*		
	Netmask*		
	Default gateway*		
	IPv6 address		
	IPv6 prefix		
	IPv6 gateway		
System Time Settings	Local time zone*		
	NTP server(s) Comma-separated list, up to 3 servers	Timeserver.ex.com, TS1.ex2.com	
DNS Settings	DNS server(s) Comma-separated list, up to 3 servers	123.4.56.789, 142.67.2.123	
	Search Domain List Comma-separated list	avaya.com	
System Manager Settings	Primary System Manager IP address*		
	Enrollment password*  Note: Verify the enrollment password is active.		
Login Settings	Login Name*		
	Password*		
Survivable Remote Note:  This configuration data is only for Branch Session Manager.	• LSP IPv4 • LSP IPv6  Note: This field takes either of the two values.		
EASG status	EASG	Enable or Disable	

Table continues...

Configuration Data	Field	Example value for the System	✓
Data Encryption	Data Encryption	Enable or Disable	
Edge Topology BSM	Edge Topology BSM	Enable or Disable	
 Note: This configuration data is only for Branch Session Manager.			

1 Supported servers

2 The following servers are supported for deployments and upgrades to Release 10.2.x and later:

- 3 • Avaya Solutions Platform S8300 for Communication Manager and Branch Session Manager
- 4 • Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660xs

5 For fresh installations, use Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640.

6 Supported servers for Avaya Aura® applications

7 The following table lists the Avaya sourced supported servers for the Avaya Aura® applications:

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
S8300D	Y	N	N	N	N
S8300E ¹	Y	Y	Y	Y	Y
HP ProLiant DL360 G7 (CSR1)	Y	N	N	N	N
HP ProLiant DL360p G8 (CSR2)	Y	Y	Y	N	N
HP ProLiant DL360 G9 (CSR3)	Y	Y	Y	N	N
Dell™ PowerEdge™ R610 (CSR1)	Y	N	N	N	N
Dell™ PowerEdge™ R620 (CSR2)	Y	Y	Y	N	N
Dell™ PowerEdge™ R630 (CSR3)	Y	Y	Y	N	N

Table continues...

Supported servers	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
Avaya Solutions Platform 120 Appliance: Dell PowerEdge R640 2	N	Y	Y	N	N
Avaya Solutions Platform 130 Appliance: Dell PowerEdge R640 and R660xs 3	N	Y	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.x/6.x	Y Avaya Solutions Platform 130 Release 5.1/6.x
Avaya Solutions Platform S8300 4	N	N	N	Y Release 5.1	Y Release 5.1/6.x

¹ You can migrate the S8300E server to Avaya Solutions Platform S8300 Release 6.x. For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* on the Avaya Support website.

² Avaya Solutions Platform 120 Appliance uses Appliance Virtualization Platform to support virtualization.

³ You can migrate the Avaya Solutions Platform 120 Appliance to Avaya Solutions Platform 130 Appliance Release 6.x. For information, see *Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130* on the Avaya Support website.

Avaya Solutions Platform 130 Appliance 5.1.x uses VMware vSphere ESXi software to support virtualization. Avaya Solutions Platform 130 Appliance 6.x uses KVM on RHEL software to support virtualization.

⁴ Avaya Solutions Platform S8300 5.1.x supports virtualization using VMware vSphere ESXi foundation license for Communication Manager and Branch Session Manager. Avaya Solutions Platform S8300 6.x supports virtualization using KVM on RHEL 8.10 software.

Avaya Solutions Platform 130 Appliance R4/5 uses VMware vSphere ESXi Standard License to support virtualization

*** Note:**

- Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL website, this results in an unsupported configuration.
- From Avaya Aura® Release 10.1 and later, Avaya-provided HP ProLiant DL360p G8, HP ProLiant DL360 G9, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, and Avaya Solutions Platform 120 servers are not supported.

1 However, in Release 10.2.x, Avaya Solutions Platform 120 can be upgraded to Avaya
2 Solutions Platform 130 Release 6.0.

- 3 • From Avaya Aura® Release 8.0 and later, S8300D, Dell™ PowerEdge™ R610, and HP
4 ProLiant DL360 G7 servers are not supported.

5 With the introduction of Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), you no longer
6 need a specific license key as was the case with Avaya Solutions Platform 5.1.x and earlier
7 versions running on ESXi. However, it is imperative that customers have a record in PLDS for
8 each and every instance of the server hypervisor as customers and Avaya will be subject to audits
9 to ensure right to use royalties have been paid.

10 Supported hardware for VMware

11 VMware offers compatibility guides that list servers, system, I/O, storage, and backup compatibility
12 with VMware infrastructure. For more information about VMware-certified compatibility guides and
13 product interoperability matrices, see the Broadcom website (formerly VMware).

14 Supported hardware for ASP R6.0.x (KVM on RHEL 8.10)

15 The only supported hardware for the KVM images is Avaya Solutions Platform 130 Release 6.0.x
16 and Avaya Solutions Platform S8300 Release 6.0.x.

17 Software requirements

18 Avaya Aura® supports the following software versions:

- 19 • Avaya Solutions Platform 130 (Avaya-supplied KVM on RHEL 8.10): Dell PowerEdge R660xs
20 or R640.
21 • Avaya Solutions Platform S8300 (Avaya-supplied KVM on RHEL 8.10): S8300E.

22 **Note:**

23 Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs, S8300e) is a
24 single host server with preinstalled KVM on RHEL 8.10 software.

- 25 • Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0): S8300E
26 • Customer-provided Virtualized Environment offer supports the following software versions:
27 - VMware® vSphere ESXi 7.0 or 8.0
- VMware® vCenter Server 7.0 or 8.0

To view compatibility with other solution releases, see Broadcom website (formerly VMware) and search for VMware Product Interoperability Matrix.

- Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single host server with a preinstalled KVM on RHEL 8.10 software.
- Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) 8.10 for Communication Manager and Branch Session Manager.

*** Note:**

- Avaya Aura® Release 10.2 and later does not support vSphere ESXi 6.7.
 - Avaya Aura® Release 10.1 and later does not support vSphere ESXi 6.0 and 6.5.
 - Avaya Aura® Release 8.1.x and later supports ASP R6.0.x (KVM on RHEL 8.10) hypervisor.
- For more information about upgrading from RHEL 8.4 to RHEL 8.10, see *Upgrading Avaya Aura® Session Manager*

Supported ESXi version

The following table lists the supported ESXi versions of Avaya Aura® applications:

ESXi version	Avaya Aura® Release				
	7.1.x	8.0.x	8.1.x	10.1.x	10.2.x
ESXi 5.0	N	N	N	N	N
ESXi 5.1	N	N	N	N	N
ESXi 5.5	Y	N	N	N	N
ESXi 6.0	Y	Y	Y	N	N
ESXi 6.5	Y	Y	Y	N	N
ESXi 6.7	N	Y	Y	Y	N
ESXi 7.0	N	N	Starting from Release 8.1.3: Y	Y	Y
ESXi 8.0	N	N	N	N	Y

*** Note:**

- Avaya Solutions Platform 130 Appliance and Avaya Solutions Platform S8300 R6.0 supports Avaya-supplied KVM on RHEL 8.10. The Avaya-provided environments (ASP 130/S8300) only support Avaya-provided updates. If you update directly from a Dell or RHEL website, this results in an unsupported configuration.
- Avaya Aura® Release 10.2.x supports VMware 8.0, VMware 8.0 Update 2, and VMware 8.0 Update 3.

- 1 Avaya Aura® Release 10.2.x does not support VMware 8.0 Update 1. For information
2 about known issues, see VMware 8.0 Update 1 Release Notes on the Broadcom website
3 (formerly VMware).
- 4 • As of October 15, 2022, VMware has ended support for VMware vSphere 6.x. Therefore,
5 it is recommended to upgrade to supported vSphere versions.
- 6 For customer-provided environments and how to upgrade to supported vSphere version,
7 see the VMware website.
- 8 • Avaya Solutions Platform 130 Appliance Release 5.x and Avaya Solutions Platform
9 S8300 Release 5.1 support only ESXi 7.0. ASP 6.0 moves the Avaya-supplied software
10 from ESXi to KVM on RHEL. The Avaya-provided environments (ASP 130/S8300) only
11 support Avaya-provided updates. If you update directly from a Dell, VMware, or RHEL
12 website, this results in an unsupported configuration.
- 13 • From VMware vSphere ESXi 6.7 onwards, only HTML5 based vSphere Client is
14 supported.
- 15 • Avaya Aura® applications support the particular ESXi version and its subsequent update.
16 For example, the subsequent update of VMware ESXi 7.0 can be VMware ESXi 7.0
17 Update 3.
- 18 • WebLM Release 10.1.2 OVA and higher are certified with ESXi 8.0, ESXi 8.0 Update 2
19 (U2) deployments, and ESXi 8.0 Update 3 (U3) deployments.

20 Supported ASP R6.0.x (KVM on RHEL 8.10) version

21 The following table lists the supported KVM versions of Avaya Aura® applications:

Avaya Solutions Platform (KVM on RHEL 8.10)	Avaya Aura® Release		
	8.1.x	10.1.x	10.2.x
KVM Release 8.10	Y	Not supported for Session Manager	Y

* Note:

- 22 • Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x are Avaya-
23 supplied KVM on RHEL 8.10. The Avaya Solutions Platform 130 can be either a Dell
24 R660xs or Dell R640. The Dell R660xs only ships with and supports KVM on RHEL
25 8.10. The initial Release of Avaya Solutions Platform 130 Release 4.0 supported Avaya-
26 supplied ESXi 6.5 and Avaya Solutions Platform 130/S8300 R5.x supported Avaya-
27 supplied ESXi 7.0.
- 28 • Avaya Solutions Platform 130 and Avaya Solutions Platform S8300 R6.0.x software is
29 KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R660xs server only supports
30 KVM on RHEL 8.10. The Avaya Solutions Platform 130 Dell R640 and the ASP S8300

- 1 S8300E support both ESXi 7.0 and KVM on RHEL 8.10. Avaya Solutions Platform 130
- 2 Dell R640 Release 4.0 supported ESXi 6.5
- 3 • Avaya Solutions Platform 130 Release 6.0 (Dell PowerEdge R640, R660xs) is a single
- 4 host server with a preinstalled KVM on RHEL R8.10 software.
- 5 • Avaya Solutions Platform S8300 Release 6.0 is shipped with a preinstalled Kernel-Based
- 6 Virtual Machine (KVM) on Red Hat Enterprise Linux (RHEL) R8.10 for Communication
- 7 Manager and Branch Session Manager.
- 8 • Avaya Solutions Platform130 Release 6.0.x (Dell PowerEdge R640, R660xs, S8300E) is
- 9 a single host server with preinstalled KVM on RHEL R8.10 software.
- 10 • With the introduction of Avaya Solutions Platform R6.0.x there is no longer a specific
- 11 license key needed as was present with Avaya Solutions Platform 5.1.x and earlier
- 12 versions running on ESXi. However, it is imperative that customers have a record in
- 13 PLDS for each and every instance of the server hypervisor as customers and Avaya will
- 14 be subject to audits to ensure right to use royalties have been paid.

15 Latest software updates and patch information

16 Before you start the deployment or upgrade of an Avaya product or solution, download the latest
 17 software updates or patches for the product or solution. For more information, see the latest
 18 release notes, Product Support Notices (PSNs), and Product Correction Notices (PCNs) for the
 19 product or solution on the Avaya Support website at <https://support.avaya.com/>.

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

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

24 Upgrade sequence for Avaya components

25 Upgrade Avaya components and solution in the following sequence. If any of the Avaya
 26 components are not part of your solution, you can skip that particular component and move to
 27 the next component.

28 Disclaimer on Upgrade Sequence Flexibility

29 While Avaya recommends following the documented upgrade sequence to maintain solution
 30 stability and validated integration, the sequence allows flexibility in specific scenarios. Avaya
 31 supports component versions that may be ahead or behind others in the upgrade path, provided
 32 they are documented in the Product Compatibility Matrix published on the Avaya Support site.
 33 Customers may upgrade individual components out of sequence where such configurations are
 34 certified to be interoperable.

Refer to the Product Compatibility Matrix before performing any upgrades out of sequence.

For the latest and most accurate compatibility information, go to <http://support.avaya.com/CompatibilityMatrix/Index.aspx>.

*** Note:**

If you are using ASP130/S8300 5.0 or earlier, you *must* first upgrade to ASP130/S8300 5.1 or 6.0 before upgrading to Avaya Aura® Release 10.2.x.

To upgrade the Avaya Aura® applications to Release 10.2.x, upgrade the hypervisor to a supported version.

For information about the supported ESXi version, see [Supported ESXi version](#) on page 25.

For information about the supported KVM version, see [Supported ASP R6.0.x \(KVM on RHEL 8.10\) version](#) on page 26.

With Aura® R10.2.x, Avaya Messaging R11.0 is compatible. Upgrade Avaya Messaging to R11.0 or later before upgrading Aura® components to R10.2.x.

1. Hard Endpoints- H.323 and SIP
2. Standalone Avaya WebLM.

*** Note:**

With Avaya Aura® Release 10.2, WebLM is not available. To upgrade WebLM, use the latest WebLM Release 10.1.3.x. If you upgrade Communication Manager or Application Enablement Services to 10.2 and have a standalone WebLM in the setup, upgrade the standalone WebLM to Release 10.1.3.1 or later. Otherwise, the licensing for Communication Manager and Application Enablement Services will not work.

3. SAL Gateway
4. Avaya Aura® System Manager includes System Manager WebLM and System Manager Solution Deployment Manager.

Starting with 10.2.x, if AAM is managed by System Manager then before upgrading System Manager, clean the AAM data from System Manager.

In the:

- Non-Geography Redundancy setup, update standalone System Manager.
- Geography Redundancy setup, update the primary System Manager.

5. Avaya Aura® Session Manager, Core Session Managers only
6. Avaya Breeze® platform and other Snap-ins
7. Avaya Call Management System
8. Avaya Experience Portal
9. Avaya Oceana®
10. Avaya Aura® Device Services
11. Avaya Aura® Media Server
12. G4XX Media Gateways

*** Note:**

- 1 To successfully upgrade to Release 43.x, use Gateway 38.21.2 or later. If the
- 2 gateway runs older loads, the download fails and displays the following message:
- 3 Incompatible software image. To resolve, upgrade to 38.21.2 (G430) / 38.21.3
- 4 (G450).

- 5 13. Avaya Aura® Branch Session Manager
- 6 14. Avaya Aura® Communication Manager Survivable Remote Servers, formerly known as
- 7 Local Survivable Processors
- 8 15. Avaya Aura® Application Enablement Services (AES)
- 9 16. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform
- 10 17. Avaya Aura® Communication Manager Survivable Core Servers, formerly known as
- 11 Enterprise Survivable Servers
- 12 18. Avaya Aura® Communication Manager feature servers and evolution servers
- 13 In a duplex configuration, update the following:
- 14 • Standby Communication Manager server
- 15 • Active Communication Manager server
- 16 19. Avaya IP Office™ platform
- 17 20. Avaya Messaging, formerly known as Avaya IX™ Messaging and Officelinx

! Important:

- 18 Avaya Messaging must be upgraded to R11.0 or later before upgrading Aura®
- 19 components to R10.2.x.

- 20 21. Avaya Aura® Web Gateway
- 21 22. Workplace Clients
- 22 Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.
- 23 23. Avaya Session Border Controller (ASBCE)

*** Note:**

- 24 • System Manager is an integral part of the Avaya Aura® solution.
- 25 • System Manager must be on the same or higher release than the application you are
- 26 upgrading. For example, you must upgrade System Manager to 10.2 before you upgrade
- 27 Communication Manager to 10.2.
- 28 All applications supported by System Manager do not follow the general Avaya Aura®
- 29 Release numbering schema. Therefore, for application versions System Manager
- 30 supports, see Avaya Aura® Release Notes on the Avaya Support website.
- 31 • Uninstall the old Solution Deployment Manager Client and install the latest Solution
- 32 Deployment Manager Client.
- 33 Solution Deployment Manager Client must be on the same or higher release than the
- 34 OVA you are deploying. For example, if you are deploying Communication Manager 10.2

- 1 OVA, Solution Deployment Manager Client version must be on Release 10.2. Solution
- 2 Deployment Manager Client cannot be on Release 10.1 or Release 8.1.

3 For information about upgrading the application, see the application-specific upgrade guide on the

4 Avaya Support website.

Optional Upgrade Sequence

6 With the Optional Upgrade Sequence feature, you can upgrade your core Communication

7 Manager before upgrading your Survivable Remote Servers, formerly known as Local Survivable

8 Processors (LSP). This sequence of upgrading has a limitation of configurations not synchronizing

9 between the upgraded core Communication Manager and yet-to-be-upgraded Survivable Remote

10 servers (LSP).

Caution:

- 11 Ensure that you read the [Limitations of Optional Upgrade Sequence](#) on page 33 before
- 12 implementing this upgrade sequence.

Note:

- 13 The Optional Upgrade Sequence feature does not apply to Survivable Core Server (SCS),
- 14 formerly known as Enterprise Survivable Server (ESS). Always upgrade Survivable Core
- 15 Server (ESS) before the core Communication Manager.
- 16 If you are using Avaya Solutions Platform (ASP) 130/S8300, ensure that the Optional
- 17 Upgrade Sequence is feasible for your setup. To verify the feasibility, review the latest ASP
- 18 documentation for compatibility of Communication Manager release with the underlying Avaya
- 19 Solutions Platform hypervisor release.

20 With the Optional Upgrade Sequence feature, you can have your core Communication Manager

21 and Survivable Remote Servers (LSP) in different compatible versions.

- 22 • Supported versions of Core Communication Manager: Release 10.1.3.3 and later versions,
- 23 Release 10.2.1 and later versions.
- 24 • Supported versions of Survivable Remote Servers (LSP): Release 8.1.3.x, Release 10.1.x.

25 Traditionally, the existing upgrade sequence requires that all the Survivable Remote Servers (LSP)

26 are upgraded before the core Communication Manager. In environments with a large number

27 of survivable remote sites, the upgrade of the core Communication Manager has to wait until

28 the end of the Communication Manager upgrade to use the latest features and fixes. With the

29 Optional Upgrade Sequence feature, you can upgrade your core Communication Manager to the

30 latest software version and use the latest features and functionalities of the upgraded software

31 before you upgrade your Survivable Remote Servers (LSP). The Optional Upgrade Sequence

32 feature ensures that the Survivable Remote Servers (LSP) running a lower software version

33 continue registering to the core Communication Manager running on a higher version. However,

34 the configurations on the core Communication Manager do not synchronize with Survivable

35 Remote Servers (LSP) because of the difference in the software versions. *Any administrative*

changes to the upgraded core Communication Manager are unavailable to the Survivable Remote Servers (LSP) running on a lower software version. The core Communication Manager generates a warning File synchronization (FSY) alarm for the software version mismatch. The core Communication Manager clears the warning alarm after you upgrade the Survivable Remote Servers (LSP) to the same or a higher software version than your core Communication Manager. The administrative changes are also available after the upgrade. Use Optional Upgrade Sequence if you do not expect changes at the branch locations. Select Survivable Remote Servers (LSP) for later upgrades such that they will not be impacted by the limitations of Optional Upgrade Sequence feature.

While you use the latest features from the core Communication Manager, you can continue to upgrade your Survivable Remote Servers (LSP) to the same or a later software version than your core Communication Manager. For example, if you want to upgrade to Avaya Aura® R10.2 which offers Trellix Antivirus support, identify the Survivable Remote Server (LSP) locations where you do not expect administrative changes and upgrade them after you upgrade your core Communication Manager. The upgraded core Communication Manager can utilize the Trellix Antivirus feature at the main location. Note that the configurations from the upgraded core Communication Manager do not synchronize with the yet-to-be-upgraded Survivable Remote Servers (LSP). The yet-to-be-upgraded Survivable Remote Servers (LSP) can register with the core Communication Manager.

Optional Upgrade Sequence comparison

Use the Optional Upgrade Sequence feature if you require your core Communication Manager to utilize the features of the latest release before some of your Survivable Remote Servers (LSP). For example, in a setup with one core Communication Manager, one Survivable Core Server (ESS), and three Survivable Remote Servers (LSP), with the existing Upgrade Sequence feature, you must follow the order of upgrading. With the Optional Upgrade Sequence feature, you can upgrade the core Communication Manager before the Survivable Remote Servers (LSP). The following table provides a few examples of the upgrade paths:

Existing Upgrade Sequence	Optional Upgrade Sequence
• Survivable Core Server (ESS) Release 10.2 • Survivable Remote Server (LSP)1 Release 10.2 • Survivable Remote Server (LSP)2 Release 10.2 • Survivable Remote Server (LSP)3 Release 10.2 • Core Communication Manager Release 10.2 As the software versions of the Survivable Remote Servers (LSP) and the Core Communication Manager are same, the configurations synchronize between these servers and the admin changes are available on all servers.	Example 1: • Survivable Core Server (ESS) Release 10.2.1 • Core Communication Manager Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.1 • Survivable Remote Server (LSP)2 Release 10.1 • Survivable Remote Server (LSP)3 Release 10.1 Example 2: • Survivable Core Server (ESS) Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.2.1 • Main Communication Manager Release 10.2.1 Warning alarm for yet-to-be upgraded LSPs. • Survivable Remote Server (LSP)2 Release 8.x • Survivable Remote Server (LSP)3 Release 10.1 Example 3: • Survivable Core Server (ESS) Release 10.2.1 • Survivable Remote Server (LSP)1 Release 10.2.1 • Survivable Remote Server (LSP)2 Release 10.2.1 • Main Communication Manager Release 10.2.1 Warning alarm for yet-to-be upgraded LSPs.

Existing Upgrade Sequence	Optional Upgrade Sequence
	Survivable Remote Server (LSP)³ Release 10.1

! Important:

- 1 • Plan carefully before you implement Optional Upgrade Sequence.
- 2 • Optional Upgrade Sequence is available for Survivable Remote Servers (LSP). There is
- 3 no change to the upgrade sequence for other Avaya Aura[®] components.

*** Note:**

- 4 The fixes for any issues with the Optional Upgrade Sequence feature will be available in the
- 5 latest supported versions. For more information, see [Avaya Product Lifecycle Matrix](#).

6 Limitations of Optional Upgrade Sequence

7 The configurations on the core Communication Manager do not synchronize with the Survivable
8 Remote Servers (LSP) because of the difference in the software versions. Any administrative
9 changes to the upgraded core Communication Manager are unavailable to the Survivable Remote
10 Servers (LSP) running on a lower software version. The core Communication Manager generates
11 a warning File synchronization (FSY) alarm for the software version mismatch.

12 The alarm clears automatically, and the administrative changes synchronize from the core server
13 after you upgrade the Survivable Remote Servers (LSP) to the same or a later software version
14 than your core Communication Manager.

15 For more information about the FSY alarm, see

16 *Avaya Aura[®] Communication Manager Alarms, Events, and Logs Reference*

17 Related links

18 [Verify the software version of the Survivable Remote Servers](#) on page 33

19 [Optional Upgrade Sequence for Avaya components](#) on page 34

20 Verify the software version of the Survivable Remote Servers

21 If you use the Optional Upgrade Sequence feature, your core Communication Manager and
22 Survivable Remote Servers (LSP) might not run on the same software version. You can check
23 the software version of each Survivable Remote Server (LSP) in your network and upgrade them
24 to the same or a later software version than your core Communication Manager. To view the
25 software version, log in to the core Communication Manager through SAT and run the `list`
26 `survivable-processor` command. The list displays all the Survivable Remote Servers (LSP)
27 and their current software version.

```
list survivable-processor
```

SURVIVABLE PROCESSORS						
Record Number	Name/ IP Address	Type	Reg	Act	Translations Updated/ SWVersion	Net Rgn
1	Hermes101ASPLSP [REDACTED] No V6 Entry	LSP	y	y	8:43 5/16/2024 R020x.01.0.974.0	2
2	Hermes101ESS [REDACTED] No V6 Entry	ESS S	n			1
3	Hermes101LSP [REDACTED] No V6 Entry	LSP	y	n	8:43 5/16/2024 R020x.01.0.974.0	2
4	lsp54 [REDACTED] No V6 Entry	LSP	y	n	3:52 5/3/2024 R018x.01.0.890.0	2

Command successfully completed

Command: [REDACTED]

ESC-x=Cancel Esc-e=Submit Esc-p=Prev Pg Esc-n=Next Pg Esc-h=Help Esc-r=Refresh

To read the software version numbers displayed on the SAT screen, refer to the Software version field description topic in *Administering Avaya Aura® Communication Manager*.

Related links

[Optional Upgrade Sequence](#) on page 30

Optional Upgrade Sequence for Avaya components

Upgrade Avaya components and solution in the following sequence. If any of the Avaya components are not part of your solution, you can skip that particular component and move to the next component.

If you choose the Optional Upgrade Sequence feature, you can upgrade the core Communication Manager before you upgrade your Survivable Remote Servers (LSP). In the following Optional Upgrade Sequence, you can skip steps 12 to 14. Note that if you skip the order of sequence, skip all the optional steps. For more information, read [Optional Upgrade Sequence](#) on page 30.

Disclaimer on Upgrade Sequence Flexibility

While Avaya recommends following the documented upgrade sequence to maintain solution stability and validated integration, the sequence allows flexibility in specific scenarios. Avaya supports component versions that may be ahead or behind others in the upgrade path, provided they are documented in the Product Compatibility Matrix published on the Avaya Support site. Customers may upgrade individual components out of sequence where such configurations are certified to be interoperable.

Refer to the Product Compatibility Matrix before performing any upgrades out of sequence.

For the latest and most accurate compatibility information, go to <http://support.avaya.com/CompatibilityMatrix/Index.aspx>.

*** Note:**

- 3 If you are using ASP130/S8300 5.0 or earlier, you *must* first upgrade to ASP130/S8300 5.1 or
- 4 6.0 before upgrading to Avaya Aura® Release 10.2.x.
- 5 To upgrade the Avaya Aura® applications to Release 10.2.x, upgrade the hypervisor to a
- 6 supported version.
- 7 For information about the supported ESXi version, see [Supported ESXi version](#) on page 25.
- 8 For information about the supported KVM version, see [Supported ASP R6.0.x \(KVM on RHEL](#)
- 9 [8.10\) version](#) on page 26.
- 10 With Aura® R10.2.x, Avaya Messaging R11.0 is compatible. Upgrade Avaya Messaging to
- 11 R11.0 or later before upgrading Aura® components to R10.2.x.
- 12 1. Hard Endpoints- H.323 and SIP
- 13 2. Standalone Avaya WebLM.

*** Note:**

- 14 With Avaya Aura® Release 10.2, standalone WebLM is not available. To upgrade
- 15 standalone WebLM, use the latest standalone WebLM Release 10.1.3.x. If you
- 16 upgrade Communication Manager or Application Enablement Services to 10.2 and
- 17 have a standalone WebLM in the setup, upgrade the standalone WebLM to Release
- 18 10.1.3.1 or later. Otherwise, the licensing for Communication Manager and Application
- 19 Enablement Services will not work.
- 20 3. SAL Gateway
- 21 4. Avaya Aura® System Manager includes System Manager WebLM and System Manager
- 22 Solution Deployment Manager.
- 23 In the:
- 24 • Non-Geography Redundancy setup, update standalone System Manager.
- 25 • Geography Redundancy setup, update the primary System Manager.
- 26 5. Avaya Aura® Session Manager, Core Session Managers only
- 27 6. Avaya Breeze® platform and other Snap-ins
- 28 7. Avaya Call Management System
- 29 8. Avaya Experience Portal
- 30 9. Avaya Oceana®
- 31 10. Avaya Aura® Device Services
- 32 11. Avaya Aura® Media Server
- 33 12. **Optional:** G4XX Media Gateways

*** Note:**

- 1 To successfully upgrade to Release 43.x, use Gateway 38.21.2 or later. If the
- 2 gateway runs older loads, the download fails and displays the following message:
- 3 Incompatible software image. To resolve, upgrade to 38.21.2 (G430) / 38.21.3
- 4 (G450).
- 5 If you skip the order of sequence, skip all the optional steps.

! Important:

- 6 Ensure to read the [Limitations of Optional Upgrade Sequence](#) on page 33 before you
- 7 skip this step.

8 13. **Optional:** Avaya Aura® Branch Session Manager

*** Note:**

- 9 If you skip the order of sequence, skip all the optional steps.

! Important:

- 10 Ensure to read the [Limitations of Optional Upgrade Sequence](#) on page 33 before you
- 11 skip this step.

12 14. **Optional:** Avaya Aura® Communication Manager Survivable Remote Servers formerly

13 known as Local Survivable Processors.

*** Note:**

- 14 If you skip the order of sequence, skip all the optional steps.

! Important:

- 15 Ensure to read the [Limitations of Optional Upgrade Sequence](#) on page 33 before you
- 16 skip this step.

17 15. Avaya Aura® Application Enablement Services

18 16. Avaya Aura® Presence Services Snap-in on Avaya Breeze® platform

19 17. Avaya Aura® Communication Manager Survivable Core Servers, formerly known as

20 Enterprise Survivable Servers

21 18. Avaya Aura® Communication Manager feature servers and evolution servers

22 In a duplex configuration, update the following:

- 23 • Standby Communication Manager server
- 24 • Active Communication Manager server

25 19. Avaya IP Office™ platform

26 20. Avaya Messaging, formerly known as Avaya IX™ Messaging and Officelinx

! Important:

- 27 Avaya Messaging must be upgraded to R11.0 or later before upgrading Aura®
- 28 components to R10.2.x.

21. Avaya Aura® Web Gateway

22. Workplace Clients

Clients are dependent on Avaya Aura® Device Services in Avaya Aura® Platform.

23. Avaya Session Border Controller (ASBCE)

*** Note:**

- System Manager is an integral part of the Avaya Aura® solution.
- System Manager must be on the same or higher release than the application you are upgrading. For example, you must upgrade System Manager to 10.2 before you upgrade Communication Manager to 10.2.
- All applications supported by System Manager do not follow the general Avaya Aura® Release numbering schema. Therefore, for application versions System Manager supports, see Avaya Aura® Release Notes on the Avaya Support website.
- Uninstall the old Solution Deployment Manager Client and install the latest Solution Deployment Manager Client.
- Solution Deployment Manager Client must be on the same or higher release than the OVA you are deploying. For example, if you are deploying Communication Manager 10.2 OVA, Solution Deployment Manager Client version must be on Release 10.2. Solution Deployment Manager Client cannot be on Release 10.1 or Release 8.1.

For information about upgrading the application, see the application-specific upgrade guide on the Avaya Support website.

Related links

[Optional Upgrade Sequence](#) on page 30

Supported browsers

The following are the minimum tested versions of the supported browsers:

- Microsoft Chromium Edge Release 93
- Google Chrome Release 91
- Mozilla Firefox Release 93

*** Note:**

- From Avaya Aura® Release 10.1 and later, Microsoft Internet Explorer is no longer supported.
- Later versions of the browsers can be used. However, it is not explicitly tested.

Related links

[Software details of Session Manager and Branch Session Manager](#) on page 38

1 Software details of Session Manager and Branch Session Manager

3 For Avaya Aura® application software build details, see Avaya Aura® Release Notes on the Avaya
4 Support website at <https://support.avaya.com/>.

5 Related links

6 [Supported browsers](#) on page 37

7 Capacity limits

8 Supported footprints of Session Manager on VMware

9 The following table summarizes single Session Manager capacities for all Session Manager
10 footprints.

*** Note:**

11 The capacities listed here are only for Session Manager. For information about capacity limits
12 for AADS, see the AADS documentation.

*** Note:**

13 Avaya Aura® Session Manager supports VMware hosts with Hyperthreading enabled at the
14 BIOS level.

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices	10K to 23.3K Devices	23.3K to 66.7K Devices
CPU Minimum	2200MHz					
vCPUs	3	5	8	12	20	53
CPU MHz Reservation	3300	5500	8800	13200	22000	58300
Memory Reservation	5132MiB	7828 MiB	10552 MiB	13368 MiB	24370 MiB	74064 MiB
SIP Devices ¹ (Normal/Failure) ²	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K	66.7K/72K
CC Agents (Normal/Failure)	1.6K/2K	3.75K/4166	5.8K/6666	8333/10K	18K/21K	21.6K/25.2K
Presence Users (Normal/Failure)	2K/2.4K	4.5K/5K	7K/8K	10K/12K	18K/21K	21.6K/25.2K
Sessions (Sec/ Hour/Max)	20/72K/ 17.9K	45/162K/ 37.4K	70/256K/ 59.8K	100/360K/90 K	150/540K/ 170K	180/648K/ 510K

Table continues...

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices	10K to 23.3K Devices	23.3K to 66.7K Devices
HDD for VMware OVA (GiB) ³	100	100	135	135	210	210
HDD for Software-Only ISO (GiB) ⁴	100	100	135	135	210	210

Notes:

1. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints.
2. Normal/Failure: Normal refers to capacity of the Session Manager in Sunny Day scenario and Failure refers to capacity of the Session Manager in Rainy Day scenario. A Session Manager in a rainy day scenario can have more number of users registered as it has registrations from the users whose Primary Session Manager is down.
3. HDD for VMware OVA: When deployed with SDM. Other deployment methods require that disk size be resized manually.
4. You can deploy Session Manager software-only *ISO image* on VMware, KVM, Hyper-V, Amazon Web Services, Google Cloud Platform, and Microsoft Azure platforms.

Session Manager instances are intended to operate as redundant, homogeneous servers to provide high reliability if a Session Manager failure or a network component failure occurs. Each Session Manager should have similar system resources and a balanced number of devices.

Session Manager instances must be similarly sized in both processing power and available memory to accommodate distributions of devices during failover. Small and large footprints are not intended to be mixed in a solution. However, closely sized footprints, such as one size with the next size down in the table above, can be mixed temporarily as capacities increase. You must ensure that the number of devices failing over to a smaller footprint does not exceed the device capacities of that footprint.

You can implement a system that consists of a mixture of Session Manager instances hosted on VMware platforms as well as Session Manager instances hosted on the existing non-VMware platforms. You must configure the VMware-based Session Manager to be similar to the non-VMware-based Session Manager across the enterprise. Similar configurations ensure the best use of system resources and handling failover scenarios. Be careful when configuring the system where a large non-VMware Session Manager can failover to Session Manager running in VMware environment. You must ensure that the target Session Manager can handle the total capacities.

Avaya Aura[®] deployment supports a geo-redundant Session Manager configuration of up to 28 Session Manager instances that are interconnected and aware of each other. Configurations that exceed this limit are not expected to have problems, but these configurations are not guaranteed to be supported.

The following table summarizes the number of soft clients supported per Session Manager when the soft clients are using Avaya Aura[®] Device Services.

Session Manager profile	Total SIP devices	Number of Workplace devices	Previous Workplace devices
Profile 1	2,000	1,200	750
Profile 2	4,500	2,700	1350
Profile 3	7,000	4,200	2100
Profile 4	10,000	6,000	3000
Profile 5	23,300	13,900	5240
Profile 6	66,700	13,900	-

1 Supported footprints of Session Manager on ASP R6.0.x (KVM on 2 RHEL 8.10)

3 The following table summarizes single Session Manager capacities for all Session Manager
4 footprints.

* Note:

- 5 Avaya Aura® Session Manager supports KVM hosts with Hyperthreading enabled at the BIOS
6 level.

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint)	23.5K to 72K Devices
CPU Minimum	2200 MHz					
vCPUs	3	5	8	12	20	53
CPU MHz Reservation ¹	3300	5500	8800	13200	22000	58300
Memory Reservation ¹	5132 MiB	7828 MiB	10552 MiB	13368 MiB	24370 MiB	74064 MiB
SIP Devices ² (Normal/Failure) ³	2K/2.4K	4.5K/5K	7K/8K	10K/12K	23.3K/ 25K	66.7K/72K
CC Agents (Normal/Failure)	1.6K/2K	3.75K/4166	5.8K/6666	8333/10K	18K/21K	21.6K/25.2K
Presence Users (Normal/Failure)	2K/2.4K	4.5K/5K	7K/8K	10K/12K	18K/21K	21.6K/25.2K
Sessions (Sec/ Hour/Max)	20/72K/ 17.9K	45/162K/ 37.4K	70/256K/ 59.8K	100/360K/90 K	150/540K/ 170K	180/648K/ 510K
HDD for VMware OVA (GiB)	100	100	135	135	210	210

Table continues...

Session Manager Device Footprints	Up to 2K Devices	2K to 4.5K Devices	4.5K to 7K Devices	7K to 10K Devices (R1 footprint)	10K to 23.5K Devices (R2 footprint)	23.5K to 72K Devices
* Note: 1. Ensure to consider reservations for deploying Avaya Aura® applications on Avaya Solutions Platform 130 and Avaya Solutions Platform S8300. 2. SIP devices: It includes all hard endpoints, soft clients, AST/NON-AST SIP endpoints and third-party endpoints. 3. Normal/Failure: Normal refers to capacity of the Session Manager in Sunny Day scenario and Failure refers to capacity of the Session Manager in Rainy Day scenario. A Session Manager in a rainy day scenario can have more number of users registered as it has registrations from the users whose Primary Session Manager is down.						

1 Supported footprints of Branch Session Manager on ASP R6.0.x (KVM on RHEL 8.10)

2 The following table summarizes single Branch Session Manager capacities for all Branch Session Manager footprints.

*** Note:**

- 5 Avaya Aura® Session Manager supports KVM hosts with Hyperthreading enabled at the BIOS level.
- 7 A gibibyte = 1024^3 and gigabyte = 1000^3
- 8 The terms mebibyte and megabyte are closely related and often used as synonyms, though they don't technically refer to the same amount of capacity. However, they are close in size,
- 10 One mebibyte equals 1.048576 megabytes.

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
CPU Minimum	2200 MHz	
vCPUs	2	4
CPU MHz Reservation	2200	4400
Memory Reservation	3164 MiB	4952 MiB
CC Agents Max	583	4167
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K
HDD (GiB)	50	50

11 Supported footprints of Branch Session Manager on VMware

12 The following table summarizes single Branch Session Manager capacities for all Branch Session Manager footprints.

*** Note:**

- 1 Avaya Aura® Session Manager supports VMware hosts with Hyperthreading enabled at the
- 2 BIOS level.
- 3 A gibibyte (GiB) and a gigabyte (GB) are sometimes used as synonyms, though they do not
- 4 describe the same output of capacity technically. However, they are close in size. A gibibyte =
- 5 1024^3 and gigabyte = 1000^3 .
- 6 The terms mebibyte and megabyte are closely related and often used as synonyms, though
- 7 they don't technically refer to the same amount of capacity. However, they are close in size,
- 8 One mebibyte equals 1.048576 megabytes.

Branch Session Manager Device Footprints	Up to 1K Devices	1k to 5K Devices
CPU Minimum	2200 MHz	
vCPUs	2	4
CPU MHz Reservation	2200	4400
Memory Reservation	3164 MiB	4952 MiB
CC Agents Max	583	4167
Sessions (Sec/Hour/Max)	3/10.8K/4.8K	30/108K/35K
HDD (GiB)	50	50

Chapter 4: Preupgrade tasks

Configuring the User settings

Obtaining a company ID

Before you begin

Ensure that you have access and user credentials to log in to the PLDS website at <https://plds.avaya.com>.

Procedure

1. On the web browser, type the PLDS URL, `https://plds.avaya.com`.
2. In the **Email address** field, enter the user name, and in the **Password** field, enter the password.
3. Click **Submit**.
4. After successful log in, on the Home page, click **Administration > My Company**.

The system displays the company ID followed by a company name.

Establishing PLDS connection to Avaya

About this task

Use the procedure to configure the location from where System Manager displays information about the latest software and firmware releases during Analyze operation. The entitlements depend on the credentials that you provide on the **User Settings** page.

Before you begin

- Obtain a company ID to configure PLDS.
- Add the required ports and websites to a firewall of customer.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > User Settings**.
2. On the User Settings page, click **Edit**.
3. Select the **Use Avaya Support Site** check box, and provide the SSO username and SSO password for PLDS, and the company ID.

4. Configure the PLDS settings and proxy settings for the software download.
5. If your network configuration requires a proxy, select the **Use Proxy** check box, and provide the details.

*** Note:**

- If you are using a proxy server that uses certificates, add the full CA certificate chain of the identity certificate that is used to secure the proxy server into the System Manager trust store. Failure to do so will result in errors when System Manager tries to connect to the proxy server to reach out to Avaya PLDS.
- For more information about how to add a CA certificate to the System Manager trust store, see [Adding trusted certificates](#) on page 46.

6. Click **Commit**.

Related links

[User Settings field descriptions](#) on page 44

User Settings field descriptions

Source configuration

Name	Description
Use Avaya Support site	The option to find the information and download the software releases from the Avaya Support website. * Note: - To download the firmware and analyze the software on System Manager, you must gain access to <code>plds.avaya.com</code>, <code>pldsxml.avaya.com</code>, and <code>downloads.dlavaya.com</code>. - Select the Use Avaya Support Site check box, to use Avaya Support Site. Enter the SSO user name, SSO password, and Company ID details. The SSO authentication is required to get entitlements for Analyze and artifacts for download. - If you select the check box, the Alternate Source is unavailable.

Table continues...

Name	Description
Alternate Source	The website location from where you can get the latest software. The alternate source is an HTTP URL and an alternate to the Avaya Support website. You must set the alternate source. For more information, see <i>Setting up an alternate source</i>.  Note: - The XML files compare the available software version and the latest available version in PLDS. - Clear the Use Avaya Support Site check box, to use alternate source repository. You must enter a http URL, for example: <code>http://10.10.10.10/SUMDATA/</code>. - The IP address of the alternate source can be the same as the IP address of the software library. However, ensure that the URL location and the server path for software library configuration are different.

1 PLDS configuration

Name	Description
SSO User Name	The user name used as a single sign on for PLDS.
SSO Password	The single sign on password for PLDS.
Confirm SSO Password	The SSO password that you retype in this field.
Company ID	The company ID for PLDS. For more information, see Obtaining a company ID.  Note: After upgrading System Manager, if the system does not auto populate the Company ID field, then you must manually edit the field with appropriate value after the upgrade.

2 Proxy settings

3 You require proxy settings to use the Avaya PLDS and the Avaya Support site. If your network
4 configuration requires a proxy, enter the details in the **Proxy Settings** section.

Name	Description
Use Proxy	The option to use the proxy server for PLDS.
Host	The host name of the proxy.
Port	The port of the proxy.
Password	The password of the proxy server for the Avaya Support website.
Confirm Password	The password of the proxy server that you retype for the Avaya Support website.

Button	Description
Edit	Displays the edit page to change the user settings.
Commit	To save the changes to the user settings.
Reset to Default	To reset the page and clear the values.
Cancel	To cancel the changes and return to the previous page.

1 Related links

- 2 [Establishing PLDS connection to Avaya](#) on page 43

3 Adding trusted certificates

4 About this task

- 5 Use the following procedure to import the certificates that you want to add as trusted certificate in
6 the trust store of the element.

* Note:

- 7 From Release 8.1, you can add trusted certificates for multiple elements. All the elements
8 must be of same **Type** and **Version**. When you add trusted certificates for multiple elements,
9 the system creates a scheduled job. To view the certificate management job status, select the
10 element, and click **View Certificate Add Status** on the Manage Elements page.
- 11 If you select multiple elements, click **More Actions > Manage Trusted Certificates**, and the
12 version of the elements is not up to date or empty then System Manager displays the following
13 error message:
- 14 `ElementType and Version of Selected Elements do not match.`

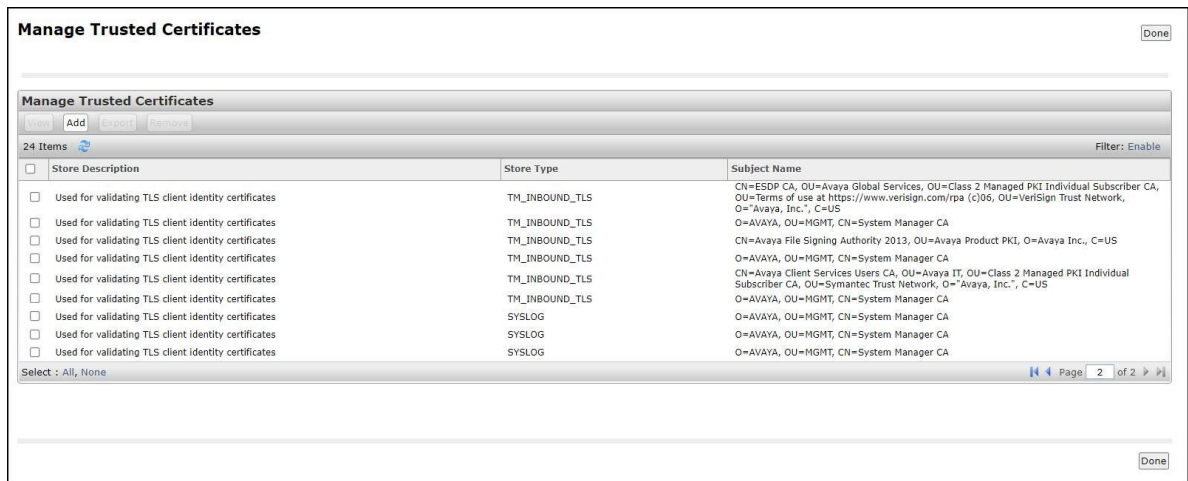
15 Before you begin

16 Perform the **Refresh Element(s)** operation under **Pre-upgrade Actions** on the **Services >**
17 **Solution Deployment Manager > Upgrade Management** page and ensure that the version in
18 the **Current Version** column is up to date for all the elements on which you plan to add trusted
19 certificates at once.

20 Procedure

- 21 On the System Manager web console, click **Services > Inventory > Manage Elements**.
- 22 On the Manage Elements page, select one or more elements, and click **More Actions >**
23 **Manage Trusted Certificates**.

3. On the Manage Trusted Certificates page, click **Add**.



4. On the Add Trusted Certificates page, in **Select Store Type to add trusted certificate**, select a store type or select **All** if you are unsure of the store type.
5. To import certificates from a file, do the following:
- Click **Import from file**.
 - Type the file name or click **Browse** to select a file.
- Note:**
- System Manager validates the file type. If you provide an invalid file type, the system displays an error message.
- Click **Retrieve Certificate**.
6. To import certificates in the PEM format, do the following:
- Locate the PEM certificate.
 - Open the certificate in the Notepad application.
 - Select and copy the contents in the file.
 - On the Add Trusted Certificates page, click **Import as PEM certificate**.
 - Paste the contents from the PEM file in the text box provided on the Add Trusted Certificates page.
7. To import certificates from existing certificates, do the following:
- Click **Import from existing certificates**.
 - In the Global Trusted Certificate section, select a certificate.
8. To import certificates by using TLS, do the following:
- Click **Import using TLS**.
 - In **IP Address**, type the IP address of the computer.

- c. In **Port**, type the port of the computer.
- d. Click **Retrieve Certificate**.
9. Click **Commit**.
10. Restart the System Manager Application server.

Creating a software library

About this task

Note:

- 7 You cannot set System Manager as a software library. You must set an external server as a software library.
- 9 For more information about configuring external server as a remote software library, see
- 10 *Administering Avaya Aura® System Manager*.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Software Library Management**.
2. Click **New**.
3. Complete the Add Software Library page.
4. Click **Commit**.
 - To reset the page, click **Clear Configuration**.

Downloading software from PLDS

Procedure

1. On your web browser, type <http://plds.avaya.com> 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 the search icon  for Company Name.
6. In the Search Companies dialog box, do the following:
 - a. In the **%Name** field, type `Avaya` or the Partner company name.
 - b. Click **Search Companies**.

- c. Locate the correct entry and click the **Select** link.
7. Search for the available downloads by using one of the following:
 - In **Download Pub ID**, type the download pub ID.
 - In the **Application** field, click the application name.
8. Click **Search Downloads**.
9. In the **Download Manager** box, click the appropriate **Download** link.

 Note:

- 7 The first link, **Click to download your file now**, uses the Download Manager to
- 8 download the file. The Download Manager provides features to manage the download
- 9 (stop, resume, auto checksum). The **click here** link uses your standard browser
- 10 download and does not provide the download integrity features.
- 11 10. If you use the Download Manager, click **Details** to view the download progress.
- 12 11. Select a location where you want to save the file, and click **Save**.
- 13 12. **(Optional)** When the system displays the security warning, click **Install**.
- 14 When the installation is complete, PLDS displays the downloads again with a check mark
- 15 next to the downloads that have completed successfully.

Downloading the OVA file to System Manager

About this task

You can download the software from Avaya PLDS or from an alternate source to System Manager. Use the procedure to download the OVA files to your computer and upload the file to System Manager.

Before you begin

Set the local software library.

Procedure

1. Download the OVA file on your computer.
2. On the System Manager web console, click **Services > Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:
 - a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
 - b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.

c. Click **Download**.

The system displays the Upload File page.

5. In the **Software Library** field, select a local System Manager software library.

6. Complete the details for the product family, device type, and the software type.

7. Click **Browse** and select the OVA file from the location on the system.

8. Provide a valid file type.

This system uploads the OVA file from local computer to the designated software library on System Manager.

 Note:

9 If the file type is invalid, System Manager displays an error.

Preparing Session Manager 8.x for upgrading to Release 10.2.x

Procedure

1. To place the Session Manager in **Deny New Service**, follow the steps below,
 - a. On the System Manager web console, click **Elements > Session Manager**.
 - b. On the Session Manager **Dashboard** page, select the appropriate Session Manager or Branch Session Manager in the Session Manager **Instances** table.
 - c. Click **Service State**.
 - d. Select **Deny New Service**.
 - e. Click **Confirm**.
2. On the Session Manager **Dashboard** page, wait until **Active Call Count** is zero. Refresh the screen to update the count.

Session Manager backup and restore commands

backupSM

```
# backupSM
```

You can run this command using the customer account or the services account. This command creates the `Session_Manager_backup.tgz` file and places it in the home directory of the account running the command. For example, if the `cust` user runs the command then the backup file is placed in `/home/cust`.

restoreSM

This command requires the path to the backup file generated using the **backupSM** command.

```
# restoreSM <path to backup file>
```

Applications pre-upgrade functions

Refreshing elements

Before you begin

- On the User Settings page, configure the user settings.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
 - a. Select one or more devices.
 - b. Click **Pre-upgrade Actions > Refresh Element(s)**.
4. On the Job Schedule page, click one of the following:
 - **Run Immediately**: To perform the job.
 - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays  and the **Current Version** column displays the current version of the element.

Analyzing software

About this task

Analyze works on the version of OVA, service pack, and feature pack files uploaded to the software library. To get the correct entitle update or upgrade version, the version field must contain valid value. You can get the version values from versions files that are available on PLDS.

Custom patching does not require the analyze operation.

Before you begin

- On the Roles page, set the Software Management Infrastructure permission.
- Perform the Refresh elements operation.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
 - a. Select a device that you want to analyze.
 - b. Click **Pre-upgrade Actions > Analyze**.
4. On the Job Schedule page, click one of the following:
 - **Run Immediately**: To perform the job.
 - **Schedule later**: To perform the job at a scheduled time.
5. If you select **Schedule later**, select the date, time, and timezone.
6. Click **Schedule**.

The **Last Action Status** column displays a , the **Current Version** column displays the current version of the element, and the **Entitled Upgrade Version** column displays the next version of the element for which the element is entitled to be upgraded.

Downloading the software

About this task

You can download the software releases that you are entitled from Avaya PLDS, or from an alternate source to System Manager.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
 2. In the left navigation pane, click **Download Management**.
- The system displays the File Download Manager page.
3. To change the display settings, click one of the following:
 - **Tree View**: To view the list of elements in the tree format. The system displays each element with the list of components associated with the element that you selected.
 - **List View**: To view the list of elements in the list format. Every element is displayed individually.
 4. In **Select Software/Hardware Types**, select the software or firmware that you want to download.
 5. To get the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page, click **Refresh Families**.

The time to complete the refresh operation depends on the source configuration in **User Settings**.

6. Click **Show Files**.

7. In **Select Files Download Details**, do the following:

- a. In **Source**, click **Avaya PLDS/Alternate Source** or **My Computer** from where you want to download the files.
- b. Select the files that you want to download.
- c. Click **Download**.

In File Download Status, the system displays the file that you selected for download.

File Download Manager field descriptions

Select Software/Hardware Types

Name	Description
Family Name	The name of the device family.
Hardware/Software	The name of the associated software or hardware.

Select Files Download Details

Name	Description
Source	The source from where Download Manager gets the software or firmware files. The options are: • Avaya PLDS/Alternate Source • My Computer

Name	Description
File name	The file name.
Version	The file version.
Entitled	The file entitlements.
File Size (in bytes)	The file size in bytes.
Hardware/Software	The name of the hardware or the software.
Family Name	The name of the device family.
Content Type	The type of the content.
Software Library	The status of the file download.
File Description	A description of the file that you download.

Button	Description
Refresh Families	Gets the latest details of the software for the supported product families from alternate source or Avaya Support Site, and update the information on the File Download Manager page. * Note: When you add or update details in the <code>versions.xml</code> file, you must click Refresh Families to get the updated information.
Show Files	Displays the files associated with the element that you selected.

1 File Download Status

Name	Description
File Name	The file name of the software or firmware file.
Job Name	The name of the download job.
Current Step	The current status.
Percentage Completed	The status of completion.
Status	The status of the download activity.
Scheduled By	The user who scheduled the download job.

Button	Description
Delete	Deletes the files that you have selected.

2 Performing the preupgrade check

3 Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, do the following:
 - a. Select an application to upgrade.
 - b. Click **Pre-upgrade Actions > Pre-upgrade Check**.
4. On the Pre-upgrade Configuration page, fill in the required information.

* **Note:**

- 10 To upgrade to different server, in **Target Host**, select the target server host.
5. On the Job Schedule page, click one of the following:
 - **Run Immediately:** To perform the job.
 - **Schedule later:** To perform the job at a scheduled time.
6. Click **Schedule**.

On the Upgrade Management page, the status of the **Last Action Status** and **Pre-upgrade Check Status** columns display a .

Preupgrade Configuration field descriptions

Pre upgrade Configuration Parameters

Name	Description
Element name	The name of the application that you want to upgrade.
Parent name	The parent of the application that you want to upgrade.
IP Address	The IP address of the application that you want to upgrade.
Current Version	The current version of the application that you want to upgrade.
Target Platform	The Appliance Virtualization Platform or ESXi host of the virtual machine.
Data Store	The data store. When you set the Target Host as Same Box , the system enables the Data Store field.
New Target Platform	The Appliance Virtualization Platform or ESXi host to which you want to upgrade the virtual machine. For upgrades on a different server, add Appliance Virtualization Platform or ESXi host from Application Management.
Upgrade Source	The location where OVA or the software patches are available in the local storage or remote server.
Upgrade/Update To	The OVA file or the software patch to which you want to upgrade.
Flexi Footprint	The file based on the storage, CPU, and memory capacity of your system.

Job Schedule

Name	Description
Schedule Job	The option to schedule a job: • Run immediately: To run the upgrade job immediately. • Schedule later: To run the upgrade job at the specified date and time.
Date	The date on which you want to run the job. The date format is mm:dd:yyyy. Use the calendar icon to choose a date. This field is available when you select the Schedule later option for scheduling a job.
Time	The time when you want to run the job. The time format is hh:mm:ss and 12 (AM or PM) or 24-hour format. This field is available when you select the Schedule later option for scheduling a job.

Table continues...

Name	Description
Time Zone	The time zone of your region. This field is available when you select the Schedule later option for scheduling a job.
Name	Description
Schedule	Runs the job or schedules to run at the time that you configured in Job Schedule.

1 Upgrading VMware ESXi version

2 About this task

3 If the ESXi upgrade is required for upgrading the application to Release 10.2.x, use the following
4 procedure to upgrade the ESXi to a supported ESXi version.

5 For information about the supported ESXi version, see [Supported ESXi version](#) on page 25.

6 Before you begin

7 Take the backup of the application and keep it on remote servers. For information about creating a
8 data backup on a remote server, see the application-specific document.

9 Procedure

10 1. Shut down all the virtual machines that are hosted on the ESXi.

11 2. Put the ESXi into maintenance mode.

12 For information about performing steps on ESXi, see VMware product documentation
13 website.

14 3. Upgrade ESXi to supported ESXi version.

15 For information about upgrading ESXi, see VMware product documentation website.

16 4. After upgrading the ESXi host, log in to the host UI, and exit from the ESXi maintenance
17 mode.

18 5. Apply the license key for the upgraded ESXi.

19 6. Power on the virtual machines.

1 Virtual machine management

2 Application management

3 The Application Management link from Solution Deployment Manager provides the application
4 management capabilities that you can use to do the following.

- 5 • Defines the physical location for Avaya Aura® Appliance Virtualization Platform Release
6 8.x or earlier, ESXi host, or Avaya Solutions Platform 130 (Avaya-Supplied ESXi 7.0), and
7 discovers virtual machines that are required for application deployments and virtual machine
8 life cycle management.
- 9 • Supports password change and patch installation of the Avaya Aura® Appliance Virtualization
10 Platform Release 8.x or earlier host. Restart, shutdown, and certificate validation of
11 Appliance Virtualization Platform Release 8.x or earlier and ESXi hosts. Also, enables and
12 disables SSH on the host.
- 13 • Manages lifecycle of the OVA applications that are deployed on the Avaya Aura® Appliance
14 Virtualization Platform Release 8.x or earlier or ESXi host. The lifecycle includes start, stop,
15 reset virtual machines, and establishing trust for virtual machines.

* Note:

16 For the Avaya Aura® Messaging element, trust re-establishment is not required.

- 17 • Deploys Avaya Aura® application OVAs on customer-provided Virtualized Environment and
18 Avaya Aura® Virtualized Appliance environment.
- 19 • Removes the Avaya Aura® application OVAs that are deployed on a virtual machine.
- 20 • Deploys Avaya Aura® application ISOs in Software-only environment.
- 21 • Configures application and networking parameters required for application deployments.
- 22 • Supports flexible footprint definition based on capacity required for the deployment of the
23 Avaya Aura® application OVA.

24 You can deploy the OVA or ISO file on the platform by using System Manager Solution
25 Deployment Manager or the Solution Deployment Manager client.

26 Managing the location

27 Viewing a location

28 Procedure

- 29 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
30 **Application Management**.
- 31 2. Click the Locations tab.

32 The Locations section lists all locations.

1 Adding a location

2 About this task

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

5 Procedure

- 6 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
7 **Application Management**.
- 8 2. On the **Locations** tab, in the Locations section, click **New**.
- 9 3. In the New Location section, do the following:
 - 10 a. In Required Location Information, type the location information.
 - 11 b. In Optional Location Information, type the network parameters for the virtual machine.
- 12 4. Click **Save**.

13 System Manager displays the new location in the **Application Management Tree** section.

14 Related links

15 [New and Edit location field descriptions](#) on page 59

16 Editing the location

17 Procedure

- 18 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
19 **Application Management**.
- 20 2. On the **Locations** tab, in the Locations section, select a location that you want to edit.
- 21 3. Click **Edit**.
- 22 4. In the Edit Location section, make the required changes.
- 23 5. Click **Save**.

24 Related links

25 [New and Edit location field descriptions](#) on page 59

26 Deleting a location

27 Procedure

- 28 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
29 **Application Management**.
- 30 2. On the **Locations** tab, in the Locations section, select one or more locations that you want
31 to delete.
- 32 3. Click **Delete**.
- 33 4. In the Delete confirmation dialog box, click **Yes**.

The system does not delete the applications that are running on the platform and moves the platform to **Unknown location Platform mapping**.

New and Edit location field descriptions

Required Location Information

Name	Description
Name	The location name.
Avaya Sold-To #	The customer contact number. Administrators use the field to check entitlements.
Address	The address where the host is located.
City	The city where the host is located.
State/Province/Region	The state, province, or region where the host is located.
Zip/Postal Code	The zip code of the host location.
Country	The country where the host is located.

Optional Location Information

Name	Description
Default Gateway	The IP address of the virtual machine gateway. For example, 172.16.1.1.
DNS Search List	The search list of domain names.
DNS Server 1	The DNS IP address of the primary virtual machine. For example, 172.16.1.2.
DNS Server 2	The DNS IP address of the secondary virtual machine. For example, 172.16.1.4.
NetMask	The subnet mask of the virtual machine.
NTP Server	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,).

Button	Description
Save	Saves the location information and returns to the Locations section.
Edit	Updates the location information and returns to the Locations section.
Delete	Deletes the location information, and moves the host to the Unknown location section.
Cancel	Cancels the add or edit operations, and returns to the Locations section.

1 Managing the platform

2 Adding an Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 host

4 About this task

5 Use this procedure to add an Appliance Virtualization Platform Release 8.x or earlier, ESXi, or
6 Avaya Solutions Platform 130 Release 5.1 host. You can associate an ESXi host with an existing
7 location.

8 If you add a standalone ESXi host to the System Manager Solution Deployment Manager or the
9 Solution Deployment Manager client, add the standalone ESXi host using its FQDN.

* Note:

10 You can add a VMware ESXi host in Solution Deployment Manager if the Standard or
11 Enterprise VMware license is applied on the VMware ESXi host.

12 If the VMware vSphere Hypervisor Free License is applied on the VMware ESXi host or the
13 VMware ESXi host is in the evaluation period, you cannot add that VMware ESXi host in
14 Solution Deployment Manager.

15 Solution Deployment Manager supports the Avaya Aura® Appliance Virtualization Platform and
16 VMware ESXi hosts. If you try to add another host, System Manager displays the following error
17 message:

18 Retrieving host certificate info is failed: Unable to communicate with
19 host. Connection timed out: connect. Solution Deployment Manager only
20 supports host management of VMware-based hosts and Avaya Appliance
21 Virtualization Platform (AVP).

22 Solution Deployment Manager 10.2.1 does not support ASP 130/S8300 R6.0.x (KVM on RHEL
23 8.10). You can add Avaya Solutions Platform 130 Release 5.0 (Avaya Supplied ESXi) similar to
24 VMware ESXi host.

* Note:

- 25 • To add an Appliance Virtualization Platform host, ensure that you accept the AVP EULA
26 before you add the host to the SDM inventory.
- 27 • To add an ESXi host in Solution Deployment Manager, set the vmk0 interface as the IP
28 Address of the ESXi host. Otherwise, Solution Deployment Manager does not support
29 adding the ESXi host in Solution Deployment Manager.
- 30 • To add an Avaya Solutions Platform host, ensure that you use the FQDN. Do not use the
31 IP address to add an Avaya Solutions Platform host.

32 Before you begin

33 Add a location.

34 Procedure

- 35 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
36 **Application Management**.
- 37 2. In **Application Management Tree**, select a location.

3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
 - a. Provide details such as the platform name, platform FQDN or IP address, username, and password.
For Appliance Virtualization Platform and VMware ESXi deployment, you can also provide the root username.
 - b. In **Platform Type**, select **AVP/ESXi**.
 - c. Set the Platform IP address of Appliance Virtualization Platform to 192.168.13.6, if you are connected through the services port.

5. Click **Save**.

6. In the Certificate dialog box, click **Accept Certificate**.

System Manager generates the certificate and adds the Appliance Virtualization Platform host. For the ESXi host, you can accept the certificate. If the certificate is invalid, Solution Deployment Manager displays the error. To generate the certificate, see the VMware documentation.

In the Application Management Tree section, System Manager displays the new host in the specified location and discovers applications.

7. To view the discovered application details, such as name and version, do the following to establish trust between the application and System Manager:
 - a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
 - b. Click **More Actions > Re-establish connection**.
For more information, see “Re-establishing trust for Solution Deployment Manager elements”.
 - c. Click **More Actions > Refresh App**.

 Important:

- 27 To change the IP address or FQDN of the Appliance Virtualization Platform host from
- 28 the local inventory, you require AVP Utilities. To get the AVP Utilities application name
- 29 during the IP address or FQDN change, refresh AVP Utilities to ensure it is available.

8. On the **Platforms** tab, select the required platform and click **Refresh Host**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element > Inventory**. This is due to the absence of the **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.

2. Ensure that System Manager populates the **Application Name** and **Application Version** for each virtual machine.

Adding an Avaya Solutions Platform 130 Release 5.1 host

About this task

Use this procedure to add an Avaya Solutions Platform 130 Release 5.1 host. You can associate an Avaya Solutions Platform 130 Release 5.1 host with an existing location.

Before you begin

- If you are connected to the Avaya Solutions Platform 130 host through the services port using the SDM client, perform the following:
 1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
 2. Add the host in the format `192.11.13.6 <changed FQDNname>`
 For example: `192.11.13.6 esxihost6.hostdomain.com`
- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform 130 Release 5.1 is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform 130 Release 5.1 host.
- Regenerate the self-signed certificate using the FQDN.
 See "Regenerating Avaya Solutions Platform 130 self-signed certificate with FQDN using the command line interface".
- Add Avaya Solutions Platform 130 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform 130 Release 5.1 host.

Procedure

1. To add an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, choose one of the following:
 - For System Manager SDM, on the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
 - For SDM client, on the **SDM Client** web console, click **Application Management**.
2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
 - a. Provide details of Platform name, Platform FQDN, username, and password.
 For Avaya Solutions Platform 130 deployment, you can also provide the root username.
 - b. In **Platform Type**, select **ASP 130/S8300**.

5. Click **Save**.

The Avaya Solutions Platform 130 certificate is updated based on the platform FQDN.
After adding an Avaya Solutions Platform 130 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.

7. In the Certificate dialog box, click **Accept Certificate**.

System Manager generates the certificate and adds the Avaya Solutions Platform 130 host.

In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.

8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:

- a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
- b. Click **More Actions > Re-establish connection**.
- c. Click **More Actions > Refresh App**.

9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

After adding a new host under Application Management Tree, the **Refresh Platform** operation might fail to add the virtual machine entry under **Manage Element > Inventory**. This is due to the absence of **Application Name** and **Application Version** for the virtual machines discovered as part of the host addition. After adding the host, do the following:

1. In Application Management Tree, establish trust for all the virtual machines deployed on the host.
2. Ensure that the system populates **Application Name** and **Application Version** for each virtual machine.

Adding a software-only platform

About this task

Use this procedure to add an operating system to Solution Deployment Manager. In Release 10.2.x, System Manager supports the Red Hat Enterprise Linux (RHEL) 8.4, or RHEL 8.10 (64-bit) operating system.

Before you begin

Add a location.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. On the **Platforms** tab, click **Add**.

3. In **Platform Name**, type the name of the platform.

4. In **Platform FQDN or IP**, type the FQDN or IP address of the base operating system.

5. In **User Name**, type the username of the base operating system.

For a software-only deployment, the username must have the permission to log in through SSH. If the software-only application is already deployed, provide the application CLI user credentials.

6. In **Password**, type the password of the base operating system.

7. In **Platform Type**, select **OS**.

8. Click **Save**.

Any other application running on the platform is automatically discovered and displayed in the **Applications** tab.

- If the Solution Deployment Manager cannot establish trust, the application is displayed as Unknown.
- If you add the OS, only **Add** and **Remove** operations are available on the **Platforms** tab. **New** option is enabled on the **Applications** tab. If the application is System Manager, **Update App** is enabled on Solution Deployment Manager Client.

System Manager displays the added base operating system on the **Platforms** tab.

Shutting down the Appliance Virtualization Platform host

About this task

You can perform the shutdown operation on one Appliance Virtualization Platform host at a time. You cannot schedule the operation.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select an Appliance Virtualization Platform host.
4. Click **More Actions > Lifecycle Action > Host Shutdown**.

The Appliance Virtualization Platform host and virtual machines shut down.

Shutting down Appliance Virtualization Platform host from CLI

About this task

From Solution Deployment Manager, shut down the virtual machines that are running on the host.

Procedure

1. Start an SSH session and log in to the Appliance Virtualization Platform host.
2. At the prompt, type `/opt/avaya/bin/avpshutdown.sh`.
The system displays `Are you sure you want to stop all VMs and shutdown?`
3. To confirm the shutdown operation, type `Y`.
The system shuts down Appliance Virtualization Platform host, and stops all virtual machines running on the Appliance Virtualization Platform host. The host does not restart automatically.
You must manually turn on the Appliance Virtualization Platform server. All virtual machines running on Appliance Virtualization Platform automatically start.

Restarting Appliance Virtualization Platform or an ESXi host

About this task

The restart operation fails, if you restart the host on which System Manager itself is running. If you want to restart the host, you can do this either through vSphere Web Client or through the Solution Deployment Manager client.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> area, select a platform.
4. Click **More Actions > Lifecycle Action > Host Restart**.
5. On the confirmation dialog box, click **Yes**.
The system restarts the host and virtual machines running on the host.

Removing a platform

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, select one or more platforms that you want to delete.
3. Click **Remove**.
4. On the Delete page, click **Yes**.

1 Add and Edit platform field descriptions

Name	Description
Location	The location where the platform is available. The field is read-only.
Platform Name	The platform name of OS, Appliance Virtualization Platform, ESXi, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
Platform FQDN or IP	The IP address or FQDN of the platform.  Note: To add Avaya Solutions Platform, use the FQDN only. Do not use the IP address to add Avaya Solutions Platform.
User Name	The user name to log in to the platform.  Note: For Appliance Virtualization Platform, provide the admin credentials you configure when generating the Kickstart file.
Password	The password to log in to the platform.
Platform Type	The options are the following: • OS: For Red Hat Enterprise Linux. • AVP/ESXi: For Appliance Virtualization Platform, ESXi, or Avaya Solutions Platform 130 Release 5.0. You can add Avaya Solutions Platform 130 Release 5.0 as a standalone ESXi. • ASP 130/S8300: For Avaya Solutions Platform 130 Release 5.1 and Avaya Solutions Platform S8300 Release 5.1 hosts. Do not select this option to add Avaya Solutions Platform 130 Release 5.0.

Button	Description
Save	Saves the host information and returns to the Platforms for Selected Location <location name> section.

2 Downloading the OVA file to System Manager

3 About this task

4 You can download the software from Avaya PLDS or from an alternate source to System
 5 Manager. Use the procedure to download the OVA files to your computer and upload the file
 6 to System Manager.

7 Before you begin

8 Set the local software library.

9 Procedure

10 1. Download the OVA file on your computer.

2. On the System Manager web console, click **Services > Solution Deployment Manager**.
3. In the navigation pane, click **Download Management**.
4. On the Download Management page, perform the following:

- a. In the Select Software/Hardware Types section, select the family name, and click **Show Files**.
- b. In the Select Files Download Details section, in the **Source** field, select **My Computer**.
- c. Click **Download**.

The system displays the Upload File page.

5. In the **Software Library** field, select a local System Manager software library.
6. Complete the details for the product family, device type, and the software type.
7. Click **Browse** and select the OVA file from the location on the system.
8. Provide a valid file type.

This system uploads the OVA file from local computer to the designated software library on System Manager.

 Note:

- 16 If the file type is invalid, System Manager displays an error.

Managing the application

Editing an application

Before you begin

- Install the Solution Deployment Manager client.
- An ESXi host must be available.
- When you change the IP address or FQDN:
 - AVP Utilities must be available and must be discovered.
 - If AVP Utilities is discovered, the system must display AVP Utilities in the **App Name** column. If the application name in **App Name** is empty, click **More Actions > Re-establish connection** to establish trust between the application and System Manager.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In **Application Management Tree**, select a location.
3. On the **Applications** tab, in the Applications for Selected Location <location name> section, select an application, and click **Edit**.

The system displays the Edit App section.

4. To update the IP address and FQDN of the application in the local Solution Deployment Manager inventory, perform the following:

a. Click **More Actions > Re-establish connection**.

*** Note:**

To update IP address or FQDN for AVP Utilities, establish trust on all applications that are running on the host on which AVP Utilities resides.

b. Click **More Actions > Refresh App**.

*** Note:**

To update IP address or FQDN for AVP Utilities, refresh all applications that are running on the host on which AVP Utilities resides.

c. Click **Update IP/FQDN in Local Inventory**.

d. Click **Update App IP/FQDN**.

e. Provide the IP address and FQDN of the application.

Update IP/FQDN in Local Inventory updates the IP address or FQDN of the application only in the local database in System Manager. The actual IP address or FQDN of the host does not change. Use **Update Network Params** in the **Platforms** tab to update the IP address or FQDN of the host.

5. Click **Save**.

Starting an application from Solution Deployment Manager

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the **Application Management Tree**, select a platform to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to start.
4. Click **Start**.

In **Application State**, the system displays **Started**.

Stopping an application from Solution Deployment Manager

About this task

System Manager is operational and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.

2. From the **Application Management Tree**, select a ESXi or vCenter host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to stop.
4. Click **Stop**.

In **Application State**, the system displays *Stopped*.

Restarting an application from Solution Deployment Manager

Before you begin

- System Manager is operational, and ESXi or vCenter is added to the Application Management page to deploy Avaya Aura® Application OVA on ESXi applications.
- Applications must be in the running state.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. From the application management tree, select a host to which you added applications.
3. On the **Applications** tab, select one or more applications that you want to restart.
4. Click **Restart**.

In **Application State**, the system displays *Stopped* and then *Started*.

Re-establishing trust for Solution Deployment Manager elements

About this task

Use this procedure to re-establish trust with an application.

Before you begin

- Add a location.
- Add an Appliance Virtualization Platform host to the location.

Procedure

1. To access Solution Deployment Manager, do one of the following:
 - On the System Manager web console, click **Services > Solution Deployment Manager**.
 - On the desktop, click the Solution Deployment Manager icon ().
2. Click **Application Management**.
3. In **Application Management Tree**, select a platform.
4. On the **Applications** tab, in the Applications for Selected Location <location name> area, select an application.
5. Click **More Actions > Re-establish connection**.

6. Select the release version of the product deployed on the application.

The options are:

- **6.3 and below:** When you select this, the system displays the following message:

Trust cannot be established for this version VM.

- **7.0**
- **7.1 and above**
- **others**

 Note:

- 8 When you select the version as **7.0** or **others**, you need to provide the user name and password of the application.

7. When you select the version **7.0** or **others**, in **User Name**, type the user name of the application.

8. When you select the version **7.0** or **others**, in **Password**, type the password of the application.

9. Click **Reestablish Connection**.

Common causes for application deployment failure

If the application is not reachable from System Manager Solution Deployment Manager or Solution Deployment Manager Client, the OVA deployment fails at the sanity stage, because you might have:

- Provided an IP which is not on the network.
- Provided wrong network values that causes the network configuration for the application to not work properly.
- Chosen a private virtual network.

The following are some examples of wrong network values and configuration that can result in the OVA deployment failure:

- Using an IP which is already there on the network (duplicate IP).
- Using an IP which is not on your network at all.
- Using a DNS value, such as 0.0.0.0.
- Deploying on an isolated network on your VE deployment.

You can check the deployment status in the **Current Action Status** column on the **Applications** tab.

1 Reestablish Connection field descriptions

Name	Description
Select Version	Select the required version. The options are: • 6.3 and below • 7.0 • 7.1 and above • others  Note: When you select the version as 7.0 or others, you need to provide the user name and password of the application.
Application Name	The name of the application.
VM IP/FQDN	The IP address or FQDN of the application.
User Name	The user name of the application.  Note: When you select the version as 7.0 or others, you need to provide the user name and password of the application.
Password	The password of the application.  Note: When you select the version as 7.0 or others, you need to provide the user name and password of the application.

Button	Description
Reestablish Connection	Establishes connection between System Manager and the application.
Cancel	Cancels the changes and returns to the previous page.

2 Managing vCenter

3 Creating a role for a user

4 About this task

To manage a vCenter or ESXi in Solution Deployment Manager, you must provide complete administrative-level privileges to the user.

Use the following procedure to create a role with administrative-level privileges for the user.

8 Procedure

1. Log in to vCenter Server.
2. On the Home page, click **Administration > Roles**.
The system displays the Create Role dialog box.

3. In **Role name**, type a role name for the user.
4. To provide complete administrative-level privileges, select the **All Privileges** check box.
5. **(Optional)** To provide minimum mandatory privileges, do the following.

a. In All Privileges, select the following check boxes:

- **Datastore**
- **Datastore cluster**
- **Distributed switch**
- **Folder**
- **Host profile**
- **Network**
- **Resource**
- **Tasks**
- **Virtual machine**
- **vApp**

*** Note:**

You must select all the subprivileges under the list of main set of privileges. For example, when you select the **Distributed switch** check box, ensure that you select all the related subprivileges. This is applicable for all the main privileges mentioned above. If you do not select all the subprivileges, the system might not work properly.

b. In All Privileges, expand **Host**, and select the **Configuration** check box.

*** Note:**

You must select all the subprivileges under **Configuration**.

6. Click **OK** to save the privileges.

Next steps

Assign this role to the user for mapping vCenter in Solution Deployment Manager. To assign the role to the user, see the VMware documentation.

Adding a vCenter to Solution Deployment Manager

About this task

System Manager Solution Deployment Manager supports virtual machine management in vCenter 6.0, 6.5, 6.7, 7.0, and 8.0. When you add vCenter, System Manager discovers the ESXi hosts that this vCenter manages, adds them to the repository, and displays in the Managed Hosts section. Also, System Manager discovers virtual machines running on the ESXi host and adds to the repository.

System Manager displays vCenter, ESXi host, and virtual machines on the Manage Elements page.

Before you begin

Ensure that you have the required permissions.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager > Application Management**.
2. In the lower pane, click **Map vCenter**.
3. On the Map vCenter page, click **Add**.
4. In the New vCenter section, provide the following vCenter information:
 - a. In **vCenter FQDN**, type FQDN of vCenter.
 - For increased security when using a vCenter with Solution Deployment Manager, use an FQDN for the vCenter. vCenter does not put IP addresses in its certificates. Therefore, you need FQDN to confirm the server identity through the certificate in Solution Deployment Manager.
 - The FQDN value must match the value of the **SAN** field of the vCenter certificate. The FQDN value is case-sensitive.
 - b. In **User Name**, type the username to log in to vCenter.
 - c. In **Password**, type the password to log in to vCenter.
 - d. In **Authentication Type**, select **SSO** or **LOCAL** as the authentication type.

If you select the authentication type as **SSO**, Solution Deployment Manager displays the **Is SSO managed by Platform Service Controller (PSC)** field.
 - e. **(Optional)** If PSC is configured to facilitate the SSO service, select **Is SSO managed by Platform Service Controller (PSC)**.

PSC must have a valid certificate.

The system enables **PSC IP or FQDN**, and you must provide the IP or FQDN of PSC.
 - f. **(Optional)** In **PSC IP or FQDN**, type the IP or FQDN of PSC.
5. Click **Save**.
6. On the certificate dialog box, click **Accept Certificate**.

The system generates the certificate and adds vCenter.

In the Managed Hosts section, the system displays the ESXi hosts that this vCenter manages.

Note:

- System Manager does not support vCenter with Cluster level.
- If there is a large data center with multiple hosts in a vCenter, there can be a delay in discovering all the VMs of those hosts when mapping that vCenter in the Solution

- 1 Deployment Manager. If you select a smaller number of hosts rather than all hosts,
- 2 this process can be faster.

3 Related links

- 4 [Editing vCenter](#) on page 74
- 5 [Map vCenter field descriptions](#) on page 75
- 6 [New vCenter and Edit vCenter field descriptions](#) on page 75

7 Editing vCenter

8 Before you begin

9 Ensure that you have the required permissions.

10 Procedure

- 11 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
- 12 **Application Management**.
- 13 2. In the lower pane, click **Map vCenter**.
- 14 3. On the Map vCenter page, select a vCenter server and click **Edit**.
- 15 4. In the Edit vCenter section, change the vCenter information as appropriate.
- 16 5. If vCenter is migrated from an earlier release, on the Certificate page, click **Save**, and then
- 17 click **Accept Certificate**.
- 18 6. To edit the location of ESXi hosts, in the Managed Hosts section, do one of the following:
- 19
 - Select an ESXi host and click the edit icon (✎).
 - 20 • Select one or more ESXi hosts, select the location, click **Bulk Update > Update**.
- 21 7. Click **Commit** to get an updated list of managed and unmanaged hosts.

22 If you do not click **Commit** after you move the host from Managed Hosts to Unmanaged

23 Hosts or vice versa, and you refresh the table, the page displays the same host in both the

24 tables.

25 Deleting vCenter from Solution Deployment Manager

26 Before you begin

27 Ensure that you have the required permissions.

28 Procedure

- 29 1. On the System Manager web console, click **Services > Solution Deployment Manager >**
- 30 **Application Management**.
- 31 2. In the lower pane, click **Map vCenter**.
- 32 3. On the Map vCenter page, select one or more vCenter servers and click **Delete**.
- 33 4. Click **Yes** to confirm the deletion of servers.

34 The system deletes the vCenter from the inventory.

1 Map vCenter field descriptions

Name	Description
Name	The name of the vCenter server.
IP	The IP address of the vCenter server.
FQDN	The FQDN of the vCenter server.  Note: Use FQDN to successfully map and log in to vCenter from Solution Deployment Manager. With IP address, the system displays an error message about the incorrect certificate and denies connection.
License	The license type of the vCenter server.
Status	The license status of the vCenter server.
Certificate Status	The certificate status of the vCenter server. The options are: : The certificate is correct. : The certificate is not accepted or invalid.

Button	Description
View	Displays the certificate status details of the vCenter server.
Generate/Accept Certificate	Displays the certificate dialog box where you can generate and accept a certificate for vCenter. For vCenter, you can only accept a certificate. You cannot generate a certificate.

Button	Description
Add	Displays the New vCenter page where you can add a new ESXi host.
Edit	Displays the Edit vCenter page where you can update the details and location of ESXi hosts.
Delete	Deletes the ESXi host.
Refresh	Updates the list of ESXi hosts in the Map vCenter section.

2 New vCenter and Edit vCenter field descriptions

Name	Description
vCenter FQDN	The FQDN of vCenter.
User Name	The user name to log in to vCenter.
Password	The password that you use to log in to vCenter.

Table continues...

Name	Description
Authentication Type	The authentication type that defines how Solution Deployment Manager performs user authentication. The options are: • SSO: Global username used to log in to vCenter to authenticate to an external Active Directory authentication server. • LOCAL: User created in vCenter If you select the authentication type as SSO, Solution Deployment Manager displays the Is SSO managed by Platform Service Controller (PSC) field.
Is SSO managed by Platform Service Controller (PSC)	The check box to specify if PSC manages SSO service. When you select the check box, the system enables PSC IP or FQDN .
PSC IP or FQDN	The IP or FQDN of PSC.

Button	Description
Save	Saves any changes you make to FQDN, username, and authentication type of vCenter.
Refresh	Refreshes the vCenter details.

Managed Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
Host Name	The IP address of the ESXi host.
Location	The physical location of the ESXi host.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.

Button	Description
Edit	The option to edit the location and host.
Bulk Update	Provides an option to change the location of more than one ESXi hosts.  Note: You must select a location before you click Bulk Update.
Update	Saves the changes that you make to the location or hostname of the ESXi host.
Commit	Commits the changes that you make to the ESXi host with location that is managed by vCenter.

1

Unmanaged Hosts

Name	Description
Host IP/FQDN	The name of the ESXi host.
ESXi Version	Displays the versions of the ESXi host linked to vCenter FQDN .  Note: • For Release 10.2 and later, do not select the 6.7 version. • For Release 10.1 and later, do not select the 6.0 and 6.5 versions. • For Release 8.1 and later, do not select the 5.0 and 5.1 versions.
IPv6	The IPv6 address of the ESXi host.
Host Path	The hierarchy of the host in vCenter and also includes the host name.
Button	Description
Commit	Saves all changes that you made to vCenter on the Map vCenter page.

Chapter 5: Migrating from VMware to ASP R6.0.x (KVM on RHEL 8.10)

Migrating Session Manager or Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

You can migrate Session Manager R8.1.x ASP R5.x (VMware) to Session Manager R8.1.x ASP R6.0 (KVM). Similarly, migrate Branch Session Manager R8.1.x ASP R5.x (VMware) to Branch Session Manager R8.1.x ASP R6.0 (KVM).

When migrating, match the Session Manager version from backup to restore. Perform the backup and restore on the same Session Manager version. Similarly, match the Branch Session Manager version from backup to restore. Perform the backup and restore on the same Branch Session Manager version.

Procedure

1. Note down the existing VMware details.

For more information about the VMware details, see [Obtaining existing VMware details](#) on page 79.

2. Perform prerequisite tasks to migrate Session Manager or Branch Session Manager from VMware to KVM.

For more information about prerequisite tasks, see [Performing prerequisite tasks to migrate Session Manager from VMware to ASP R6.0.x \(KVM on RHEL 8.10\)](#) on page 79 and [Performing prerequisite tasks to migrate Branch Session Manager from VMware to ASP R6.0.x \(KVM on RHEL 8.10\)](#) on page 81.

3. Install ASP R6.0.x (KVM on RHEL 8.10).

For more information, see *Installing the Avaya Solutions Platform 130 Series* at <https://support.avaya.com/css/public/documents/101091802>.

4. Deploy Session Manager on KVM host.

For more information about deploying, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*.

5. Restore Session Manager or Branch Session Manager Backup.

For more information about restoring backup, see [Restoring backup of Session Manager or Branch Session Manager from VMware to ASP R6.0.x \(KVM on RHEL 8.10\)](#) on page 84.

Obtaining existing VMware details

About this task

Obtain the configuration details of VMware and use them for ASP R6.0.x (KVM on RHEL 8.10).

For module-specific details, see [Obtaining Session Manager configuration details](#) on page 82 and [Obtaining Branch Session Manager configuration details](#) on page 83.

Use this procedure to obtain the network IP interface details.

Procedure

1. Log in to ESXi CLI, run the following commands:

- # esxcli network ip interface ipv4 get: note down IPv4 network IP interface details.
- # esxcli network ip interface ipv6 get: note down IPv6 network IP interface details.

```
[root@localhost:~]
[root@localhost:~] esxcli network ip interface ipv4 get
Name   IPv4 Address   IPv4 Netmask   IPv4 Broadcast   Address Type   Gateway   DHCP DNS
-----
vmk0   192.168.1.1    255.255.255.0   192.168.1.255    STATIC         192.168.1.1  false
[root@localhost:~]
[root@localhost:~]
[root@localhost:~]
[root@localhost:~] esxcli network ip interface ipv6 get
Name   IPv6 Enabled   DHCPv6 Enabled   Router Adv Enabled   DHCP DNS   Gateway
-----
vmk0   true           false            true                 false      ::
```

2. Login to ESXi vSphere or vCenter and note down the VMware License serial number.

Performing prerequisite tasks to migrate Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to migrate Session Manager R8.1.x ASP R5.x (VMware) to Session Manager R8.1.x ASP R6.0 (KVM).

Before you begin

Migrate System Manager to KVM host.

Procedure

1. Log in to Session Manager CLI with root credentials.
2. To find the Session Manager profile, run the command `# profile`.

Example output:

```
[smsv@test ~]$ profile  
SM Profile 2 Max Devices 4,500
```

3. Note down Session Manager configuration details.

For more information about configuration details, see [Obtaining Session Manager configuration details](#) on page 82.

4. Set the service to Denying state.

For more information, see Denying new service for all entity links in *Administering Avaya Aura® Session Manager*.

5. To take a full backup, run the command `# backupSM`.

Example for Session Manager:

```
[smsv@test ~]$ backupSM  
Starting backup  
Backing up certificates  
Converting container_keystore.bcfks to JKS format.  
Converting spirit-identity.bcfks to JKS format.  
Backing up User Store data  
Creating backup file /home/smsv/Session_Manager_backup.tgz  
Finished backup.  
[smsv@test ~]$
```

6. Verify whether the backup file is created.

For example, the backup file is created as `Session_Manager-backup.tgz`.

7. Copy the backup file to a remote server.

8. To power off Session Manager, run the command `# shutdownSM` and enter `Y` when the screen prompts to confirm.

For example,

```
[cust@sansml #]shutdownSM  
Do you really want to continue? (y or n)  
y
```

1 Performing prerequisite tasks to migrate Branch Session Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

3 About this task

4 Use this procedure to migrate Branch Session Manager R8.1.x ASP R5.x (VMware) to Branch
5 Session Manager R8.1.x ASP R6.0 (KVM).

6 Before you begin

7 Migrate System Manager to KVM host.

8 Procedure

- 9 1. Log in to Branch Session Manager CLI with root credentials.
- 10 2. To find the Branch Session Manager profile, run the command `# profile`.

11 Example output:

```
12 [cust@sanbsml ~]$ profile  
13 BSM Profile 1 Max Devices 1,000
```

- 14 3. Note down Branch Session Manager configuration details.

15 For more information about configuration details, see [Obtaining Branch Session Manager
16 configuration details](#) on page 83.

- 17 4. Set the service to Denying state.

18 For more information, see Denying new service for all entity links in *Administering Avaya
19 Aura® Session Manager*.

- 20 5. To take a full backup, run the command `# backupSM`.

21 For example:

```
22 [root@sanbsml cust]# backupSM  
23 Starting backup  
24 Backing up certificates  
25 Converting container_keystore.bcfks to JKS format.  
26 Converting spirit-identity.bcfks to JKS format.  
27 Creating backup file /root/Session_Manager_backup.tgz  
28 Finished backup.  
29 [root@sanbsml cust]#
```

- 30 6. Verify whether the backup file is created.

31 For example, the backup file is created as `Session_Manager-backup.tgz`.

- 32 7. Copy the backup file to a remote server.

- 33 8. To power off Branch Session Manager, run the command `# shutdownSM` and enter `Y`
34 when the screen prompts to confirm.

35 For example,

```
36 [cust@sanbsml ~]# shutdownSM  
37 Do you really want to continue? (y or n)  
38 y
```

Obtaining Session Manager configuration details

Procedure

1. Log in to Session Manager CLI with root.
2. Run the script # /opt/avaya/common_services/sm_env_settings_update.sh.
3. Note down the following Session Manager configuration details:

- Hostname
- IP address
- Netmask
- Gateway
- DNS
- NTP
- Timezone
- SMGR IP
- EASG
- Data Encryption

```
[root@~]# /opt/avaya/common_services/sm_env_settings_update.sh
hostname=sm1
domain=asm.avaya.com
ip0=
netmask=
gateway=
ipv6address0=
ipv6prefix0=
ipv6gateway0=
dns=
searchlist=asm.avaya.com
ntpserver=ntp-thornt.avaya.com,ntp-us1-usae.avaya.com
ntpauth=None,None
timezone=America/Denver
CUSTLOGIN=cust
smgr_ip=
EASG_enable=1
data_encryption=1
prompt_passcode_boot_time=False
```

Obtaining Branch Session Manager configuration details

Procedure

1. Log in to Branch Session Manager CLI with root.
2. Run the script # /opt/avaya/common_services/sm_env_settings_update.sh.
3. Note down the following Branch Session Manager configuration details:
 - Hostname
 - Domain
 - IP address
 - Netmask
 - Gateway
 - DNS
 - NTP
 - Timezone
 - SMGR IP
 - LSP IP
 - EASG
 - Data Encryption

```
[root@sanity . cust]# /opt/avaya/common_services/sm_env_settings_update.sh
hostname= ' '
domain=sanity.com
ip0= ' '
netmask=:
gateway= ' '
ipv6address0=
ipv6prefix0= ' '
ipv6gateway0=
dns= ' '
searchlist=sanity.com
ntpserver= ' '
ntppath=None
timezone=Asia/Kolkata
CUSTLOGIN=cust
LSPIP= ' '
smgr_ip= ' '

EASG_enable=1
data_encryption=2
prompt_passcode_boot_time=True
[root@sanity . cust]#
```

1 Restoring backup of Session Manager or Branch Session 2 Manager from VMware to ASP R6.0.x (KVM on RHEL 8.10)

3 Procedure

- 4 1. Copy Session Manager or Branch Session Manager backup files from the remote server to
5 a newly deployed Session Manager on the KVM host.
- 6 2. Verify if the enrollment password has expired. If expired, reset the password.

7 For more information about enrollment passwords, see [Verifying the Enrollment Password](#)
8 [status](#) on page 130.

- 9 3. Log in to Session Manager CLI.

- 10 4. To restore backup, run the command `# restoreSM Session_Manager_backup.tgz`.
11 When the screen prompts, enter the enrollment password.

12 The backup is restored.

Chapter 6: Migrate Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1

To migrate Appliance Virtualization Platform deployed on S8300E to Avaya Solutions Platform S8300 Release 5.1 with Branch Session Manager deployed on it, you can have one of the following scenarios:

- **Appliance Virtualization Platform Release 8.1.x deployed on S8300E:** Migrate Appliance Virtualization Platform Release 8.1.x to Avaya Solutions Platform S8300 on the same S8300E card and then upgrade Branch Session Manager Release 8.1.x to Release 10.2.x and later with the same profile and footprint details.

For information, see [Migrating Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1](#) on page 86.

- **Appliance Virtualization Platform Release 7.x or 8.0.x deployed on S8300E:** You need to deploy Avaya Solutions Platform S8300 on the same S8300E card and then deploy Branch Session Manager with the same profile and footprint details.

For information, see [Migrating Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1](#) on page 86.

- **Appliance Virtualization Platform Release 7.x, 8.0.x, or 8.1.x deployed on S8300D:** You need to reinsert the S8300E card, deploy Avaya Solutions Platform S8300 on the it, and then deploy Branch Session Manager with the same profile and footprint details.

For information, see [Migrating Appliance Virtualization Platform deployed on S8300D with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1](#) on page 91.

Migrating Appliance Virtualization Platform deployed on S8300E with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on S8300E to Avaya Solutions Platform S8300 Release 5.1 with Branch Session Manager deployed on it.

* Note:

- If multiple applications are on the same server, follow the upgrade order.

Before you begin

Ensure that the Branch Session Manager is in **Deny New Service** state and the **Active Call Count** is zero.

! Important:

- This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform S8300.

- Use the following steps to migrate Appliance Virtualization Platform (S8300E) Release 8.1.x to Avaya Solutions Platform S8300 Release 5.1.

1. Take the backup of Branch Session Manager and keep it on remote servers.

For information about creating a backup on a remote server, see *Administering Avaya Aura® Session Manager*.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:

- a. Select the application, right-click, and then click **Guest OS > Shut down**.

The system displays the following message:

Are you sure you want to shut down <virtual_machine_name>.

- b. To proceed, click **Yes**

* Note:

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Migrate Appliance Virtualization Platform (S8300E) to Avaya Solutions Platform S8300 Release 5.1.

For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300*.

4. After successful migration, power on Branch Session Manager, if not already.
5. Upgrade Branch Session Manager Release 8.1.x to Release 10.2.x on Avaya Solutions Platform S8300 Release 5.1.

For information, see [Upgrading Branch Session Manager Release 8.1.x to Release 10.2.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager](#) on page 88.

- Use the following steps to migrate Appliance Virtualization Platform (S8300E) Release 7.x or 8.0.x to Avaya Solutions Platform S8300 Release 5.1.

1. Take the backup of Branch Session Manager and keep it on remote servers.

For information about creating a data backup on a remote server, see “Backup and restore”.

2. To do the graceful shutdown of the application, log in to the host UI through vSphere Web Client, and do the following:

- a. Select the application, right-click, and then click **Guest OS > Shut down**.

The system displays the following message:

Are you sure you want to shut down <virtual_machine_name>.

- b. To proceed, click **Yes**

 Note:

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

4. Insert the new S8300E card and deploy Avaya Solutions Platform S8300 Release 5.1.

For information about deploying Avaya Solutions Platform S8300, see *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300*.

5. Remove the existing Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only.

Do not add an Avaya Solutions Platform S8300 Release 5.1 host using the IP address.

6. Deploy Branch Session Manager Release 10.2.x with the same profile and footprint details on Avaya Solutions Platform S8300 Release 5.1 using System Manager Solution Deployment Manager.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*

7. Run the **upgradeSM** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

For information about running the data migration utility, see “Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using data migration utility”.

Upgrading Branch Session Manager Release 8.1.x to Release 10.2.x on Avaya Solutions Platform S8300 using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade Branch Session Manager Release 8.1.x running on Appliance Virtualization Platform to Release 10.2.x on Avaya Solutions Platform S8300.

For migrating Branch Session Manager on Avaya Solutions Platform S8300 Release 5.1, only the **BSM Profile 1 Max Devices 1,000** profile is supported.

* Note:

- 13 From Release 10.1 and later, Appliance Virtualization Platform is no longer available.
- 14 Therefore, if Branch Session Manager is deployed on Appliance Virtualization Platform
- 15 Release 7.x or 8.0.x, then first upgrade Appliance Virtualization Platform to Release 8.1.x
- 16 and then migrate Appliance Virtualization Platform 8.1.x to Avaya Solutions Platform S8300.

Before you begin

- Ensure to migrate Appliance Virtualization Platform to Avaya Solutions Platform S8300.

For information, see *Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300*.

- Ensure that System Manager is running on Release 10.2.
- Add a location.

For information, see [Adding a location](#) on page 58.

- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) is available in Solution Deployment Manager on the **Platforms** tab, then first remove that Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only. Do not add an ASP S8300 Release 5.1 host using the IP address.

Add the Avaya Solutions Platform S8300 host in the System Manager Solution Deployment Manager.

- Select the Branch Session Manager virtual machine and click **More Actions > Re-establish connection** to establish the trust.

For information, see [Re-establishing trust for Solution Deployment Manager elements](#) on page 69.

*** Note:**

- 1 For Branch Session Manager 7.x and later, you need to individually upgrade each
- 2 element in the following sequence:
- 3 - Utility Services or AVP Utilities
- 4 - Survivable Remote Server (SRS), formerly known as Local Survivable Processor
- 5 (LSP)
- 6 - Branch Session Manager

- Obtain the Branch Session Manager software. See “Software details of Session Manager and Branch Session Manager”.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select Branch Session Manager, and then click **Pre-Upgrade Actions > Refresh Element(s)**.
4. On the next page, click **Schedule**.

You can schedule the job now or for a later time.

5. After refresh is done, click **Pre-Upgrade Actions > Analyze**.
6. On the next page, click **Schedule**.

You can schedule the job now or for a later time.

7. After refresh is done, click **Pre-Upgrade Actions > Pre-upgrade Check**.
8. On the Pre-upgrade Configuration page, do the following:

- a. Do one of the following:

- For same server, provide the mandatory parameters along with the same target host information.
- For different server, provide the mandatory parameters along with different target host information.

For information about parameters, see [Preupgrade Configuration field descriptions](#) on page 55.

- b. In the Job Schedule section, click **Schedule**.

You can schedule the job now or for a later time.

9. Select the Branch Session Manager application.
 10. Click **Upgrade Actions > Upgrade/Update**.
 11. On the Upgrade Configuration page, select the **Override preupgrade check** check box.
- When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

12. To provide the upgrade configuration details for Branch Session Manager, click **Edit**.

13. On the Edit Upgrade Configuration page, do the following:

a. Do one of the following:

- For same server, provide the mandatory parameters along with same target host information, latest patch file, and credentials
- For different server, provide the mandatory parameters along with different target host information, latest patch file, and credentials

For information about parameters, see [Edit Upgrade Configuration field descriptions](#) on page 104.

b. Complete the details, and click **Save**.

14. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

If the field displays , review the information on the Edit Upgrade Configuration page.

15. Click **Save**.

16. To save the configuration, click **Save Configuration**.

The update configuration is saved as a job in the Upgrade Jobs Status page.

17. On the Upgrade Configuration page, click **Upgrade**.

18. On the Job Schedule page, click one of the following:

- **Run Immediately**: To perform the job.
- **Schedule later**: To perform the job at a scheduled time.

19. Click **Schedule**.

20. Click **Upgrade**.

21. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and the **Last Action Status** column displays .

22. To Commit or Rollback, do the following:

a. On the Upgrade Management page, select the element.

b. Click **Upgrade Actions > Commit/Rollback Upgrade**.

The system displays the Job Schedule page.

c. Select the action to be performed under the **Upgrade Action** column.

d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.

e. Click **Schedule**.

When you commit the changes, the system deletes the old virtual machine.

When you rollback, the system deletes the newly created virtual machine and starts the old virtual machine.

23. To view the upgrade status, perform the following:

- a. In the navigation pane, click **Upgrade Job Status**.
- b. In **Job Type**, click **Upgrade**.
- c. Click the upgrade job that you want to view.

24. Verify that the upgrade of the Branch Session Manager application is successful.

Migrating Appliance Virtualization Platform deployed on S8300D with Branch Session Manager to Avaya Solutions Platform S8300 Release 5.1

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on S8300D to Avaya Solutions Platform S8300 Release 5.1 with Branch Session Manager deployed on it.

* Note:

- 15 If multiple applications are on the same server, follow the upgrade order.

Before you begin

Ensure that the Branch Session Manager is in **Deny New Service** state and the **Active Call Count** is zero.

! Important:

- 19 This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform S8300.

Procedure

1. Take the backup of Branch Session Manager and keep it on remote servers.

For information about creating a backup on a remote server, see *Administering Avaya Aura® Session Manager*.

2. To do the graceful shutdown of the application, log in to the host UI by accessing the ESXi host, and do the following:

- a. Select the application, right-click, and then click **Guest OS > Shut down**.

The system displays the following message:

Are you sure you want to shut down <virtual_machine_name>.

b. To proceed, click **Yes**.

 Note:

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

4. Deploy Avaya Solutions Platform S8300 Release 5.1.

For information about deploying Avaya Solutions Platform S8300, see *Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300*.

5. Remove the existing Appliance Virtualization Platform and then add the Avaya Solutions Platform S8300 Release 5.1 (Avaya Supplied ESXi 7.0) host in the System Manager Solution Deployment Manager by using the FQDN only.

Do not add an Avaya Solutions Platform S8300 Release 5.1 host using the IP address.

6. Deploy Branch Session Manager Release 10.2 with the same profile and footprint details on Avaya Solutions Platform S8300 Release 5.1 using System Manager Solution Deployment Manager.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*

7. Run the **upgradeSM** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

For information about running the data migration utility, see “Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2 using data migration utility”.

Chapter 7: Migrating from Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.0

Migrating Appliance Virtualization Platform deployed on Common Server 1, 2, or 3 with Session Manager to Avaya Solutions Platform 130 Release 5.0

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on Avaya Common Server 1, 2, or 3 to Avaya Solutions Platform 130 Release 5.0 with Session Manager deployed on it.

Note:

If multiple applications are on the same server, follow the upgrade order.

Before you begin

Ensure that the **Active Call Count** is zero.

Important:

This should be a like to like migration from application perspective. So only migrate the existing applications first and do not deploy any additional application. Once all the applications are migrated successfully, then use the Avaya One Source (A1S) Configurator tool to determine if any additional applications can be deployed on Avaya Solutions Platform 130.

Procedure

1. Take the backup of Session Manager and keep it on remote servers.

For information about creating a backup on a remote server, see *Administering Avaya Aura® Session Manager*.

2. To do the graceful shutdown of the application, log in to the host UI by accessing the ESXi host, and do the following:

- a. Select the application, right-click, and then click **Guest OS > Shut down**.

The system displays the following message:

Are you sure you want to shut down <virtual_machine_name>.

- b. To proceed, click **Yes**.

*** Note:**

- If you have a virtual machine on the host, Avaya recommends to do the graceful shutdown of the virtual machine.
- Ensure that no calls are running on the system.

3. Shut down the Appliance Virtualization Platform host using the command line interface.

For information, see “Shutting down Appliance Virtualization Platform host from CLI”.

4. Deploy Avaya Solutions Platform 130 Release 6.0.

For information about deploying Avaya Solutions Platform 130, see *Installing the Avaya Solutions Platform 130 Series*.

5. Deploy Session Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.0.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*

6. Run the **upgradeSM** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

For information about running the data migration utility, see “Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2 using data migration utility”.

Related links

[Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using data migration utility](#) on page 111

[Shutting down Appliance Virtualization Platform host from CLI](#) on page 64

Migrating Appliance Virtualization Platform deployed on Avaya Solutions Platform 120 with Session Manager to Avaya Solutions Platform 130 Release 5.0

About this task

Use the following procedure to migrate Appliance Virtualization Platform that is deployed on Avaya Solutions Platform 120 to Avaya Solutions Platform 130 Release 5.0 with Session Manager deployed on it.

*** Note:**

- 1 If multiple applications are on the same server, follow the upgrade order.

Before you begin

Ensure that the **Active Call Count** is zero.

! Important:

- 4 This should be a like to like migration from application perspective. So only migrate
5 the existing applications first and do not deploy any additional application. Once all the
6 applications are migrated successfully, then use the Avaya One Source (A1S) Configurator
7 tool to determine if any additional applications can be deployed on Avaya Solutions Platform
8 130.

Procedure

1. Take the backup of Session Manager and keep it on remote servers.

For information about creating a backup on a remote server, see *Administering Avaya Aura® Session Manager*.

2. To do the graceful shutdown of the application, log in to the host UI by accessing the ESXi host, and do the following:

- a. Select the application, right-click, and then click **Guest OS > Shut down**.

The system displays the following message:

Are you sure you want to shut down <virtual_machine_name>.

- b. To proceed, click **Yes**.

*** Note:**

- 19 • If you have a virtual machine on the host, Avaya recommends to do the graceful
20 shutdown of the virtual machine.
- 21 • Ensure that no calls are running on the system.
3. Shut down the Appliance Virtualization Platform host using the command line interface.
For information, see “Shutting down Appliance Virtualization Platform host from CLI”.
4. Migrate Appliance Virtualization Platform (Dell PowerEdge R640) to Avaya Solutions Platform 130 Release 6.0.
For information, see *Migrating Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 6.0*.
5. Deploy Session Manager Release 10.1 on Avaya Solutions Platform 130 Release 5.0.
For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*
6. Run the **upgradeSM** command with data migration utility, backup file, and the service pack or feature pack as inputs to proceed.

1 For information about running the data migration utility, see “Upgrading Session Manager
2 from Release 7.x, 8.x, or 10.1.x to Release 10.2 using data migration utility”.

3 **Related links**

4 [Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using data](#)
5 [migration utility](#) on page 111

6 [Shutting down Appliance Virtualization Platform host from CLI](#) on page 64

Draft

Chapter 8: Upgrading Session Manager to Release 10.2.x on Avaya Solution Platform 130 or on VMware

Upgrading Session Manager by using System Manager Solution Deployment Manager

Upgrading Session Manager or Branch Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x using System Manager Solution Deployment Manager

About this task

Use the procedure to upgrade Session Manager or Branch Session Manager to Release 10.2.x from:

- Release 8.1.x running on Appliance Virtualization Platform, VMware, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.
- Release 10.1.x running on VMware, Avaya Solutions Platform 130, or Avaya Solutions Platform S8300.

* Note:

- From Release 10.1 and later, Appliance Virtualization Platform is no longer supported. Therefore, if Session Manager Release 8.1.x and earlier is on the Appliance Virtualization Platform host, then migrate Appliance Virtualization Platform to Avaya Solutions Platform 130 Release 5.1 before upgrading Session Manager to Release 10.2.

The procedure covers upgrades on the same server and on a different server.

Before you begin

- Ensure that System Manager is running on Release 10.2.
- Add a location.

For information, see [Adding a location](#) on page 58.

- Add the required host.

For information about adding the host, see *Managing the platform*.

For information about adding vCenter, see [Adding a vCenter to Solution Deployment Manager](#) on page 72.

! Important:

- If the application is running on the ESXi version that is not supported with Release 10.2, then first upgrade the ESXi to a supported ESXi version.
- For information about the supported ESXi version, see [Supported ESXi version](#) on page 25.
- For information about upgrading ESXi, see the VMware product documentation.
- If ESXi is managed by vCenter, ensure that the vCenter version is same or higher than the ESXi version.
- If the application is running on the server that is not supported with Release 10.2.x, then deploy Avaya Solutions Platform 130.
- For information about supported servers, see [Supported servers for Avaya Aura applications](#) on page 22.

- Select the Session Manager or Branch Session Manager virtual machine and click **More Actions > Re-establish connection** to establish the trust.

For information, see [Re-establishing trust for Solution Deployment Manager elements](#) on page 69.

*** Note:**

For Branch Session Manager 8.1.x and later, you need to individually upgrade each element in the following sequence:

- Utility Services or AVP Utilities
- Survivable Remote Server (SRS), formerly known as Local Survivable Processor (LSP)
- Branch Session Manager

- Obtain the Session Manager or Branch Session Manager software. See “Software details of Session Manager and Branch Session Manager”.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. Select Session Manager or Branch Session Manager, and then click **Pre-Upgrade Actions > Refresh Element(s)**.
4. On the next page, click **Schedule**.
You can schedule the job now or for a later time.
5. After refresh is done, click **Pre-Upgrade Actions > Analyze**.
6. On the next page, click **Schedule**.

You can schedule the job now or for a later time.

7. After refresh is done, click **Pre-Upgrade Actions > Pre-upgrade Check**.

8. On the Pre-upgrade Configuration page, do the following:

a. Do one of the following:

- For same server, provide the mandatory parameters along with the same target host information.
- For different server, provide the mandatory parameters along with different target host information.

For information about parameters, see [Preupgrade Configuration field descriptions](#) on page 55.

b. In the Job Schedule section, click **Schedule**.

You can schedule the job now or for a later time.

9. Select the Session Manager or Branch Session Manager application.

10. Click **Upgrade Actions > Upgrade/Update**.

11. On the Upgrade Configuration page, select the **Override preupgrade check** check box.

When you select the check box, the upgrade process continues even when the recommended checks fail in preupgrade check.

12. To provide the upgrade configuration details for Session Manager or Branch Session Manager, click **Edit**.

13. On the Edit Upgrade Configuration page, do the following:

a. Do one of the following:

- For same server, provide the mandatory parameters along with same target host information, latest patch file, and credentials
- For different server, provide the mandatory parameters along with different target host information, latest patch file, and credentials

For information about parameters, see [Edit Upgrade Configuration field descriptions](#) on page 104.

b. Complete the details, and click **Save**.

14. On the Upgrade Configuration page, ensure that the **Configuration Status** field displays .

If the field displays , review the information on the Edit Upgrade Configuration page.

15. Click **Save**.

16. To save the configuration, click **Save Configuration**.

The update configuration is saved as a job in the Upgrade Jobs Status page.

17. On the Upgrade Configuration page, click **Upgrade**.

18. On the Job Schedule page, click one of the following:

- **Run Immediately**: To perform the job.
- **Schedule later**: To perform the job at a scheduled time.

19. Click **Schedule**.

20. Click **Upgrade**.

21. On the Upgrade Management page, click .

The **Last Action** column displays **Upgrade**, and the **Last Action Status** column displays .

22. To Commit or Rollback, do the following:

a. On the Upgrade Management page, select the element.

b. Click **Upgrade Actions > Commit/Rollback Upgrade**.

The system displays the Job Schedule page.

c. Select the action to be performed under the **Upgrade Action** column.

d. Click **Run Immediately** to perform the job or click **Schedule later** to perform the job at a scheduled time.

e. Click **Schedule**.

When you commit the changes, the system deletes the old virtual machine.

When you rollback, the system deletes the newly created virtual machine and starts the old virtual machine.

23. To view the upgrade status, perform the following:

a. In the navigation pane, click **Upgrade Job Status**.

b. In **Job Type**, click **Upgrade**.

c. Click the upgrade job that you want to view.

24. Verify that the upgrade of the Session Manager or Branch Session Manager application is successful.

Upgrading VMware-based Session Manager Release 6.3.22 to Release 10.2.x using System Manager Solution Deployment Manager

About this task

To upgrade VMware-based Session Manager Release 6.3.22 to Release 10.2 first upgrade Session Manager 6.x to 8.1.x, and then upgrade to Release 10.1.x. You cannot directly upgrade the Release 6.3.22 system to Release 10.1 and later.

- 1 To upgrade Session Manager Release 6.3.22 to Release 8.1.x, see *Upgrading Avaya Aura®*
 2 *Session Manager* Release 8.1.x on the Avaya Support website.

3 Upgrade Management field descriptions

- 4 You can apply filters and sort each column in the devices list.

Name	Description
Name	The name of the device that you want to upgrade.
Parent	The name of the parent of the device. For example, CommunicationManager_123.
Type	The device type. For example, TN board > Communication Manager .
Sub-Type	The sub type of the device. For example, TN2302AP > Communication Manager simplex .
IP Address	The IP address of the device.
Release Status	The release status of the device. The upgrade status can be: For upgrade: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed
Update Status	The update status of the device. The upgrade status can be: • : Upgraded successfully • : Ready for upgrade • : Pending execution • : Status unknown • : Upgrade process paused • : Nonupgradable • : Operation failed

Table continues...

Name	Description
Last Action	The last action performed on the device.
Last Action Status	The status of the last action that was performed on the device.
Pre-upgrade Check Status	The status of preupgrade check of the device. The options are: • : Mandatory checks and recommended checks passed • : Mandatory checks are successful, but recommended checks failed. • : Mandatory checks and recommended checks failed You can click the icon to view the details on the Element Check Status dialog box.
Current Version	The software release status of the device.
Entitled Upgrade Version	The latest software release to which the device is entitled.
Entitled Update Version	The latest software patch or service pack to which the device is entitled.
VM Location	The location of the device.

Button	Description
Pre-upgrade Actions > Refresh Elements	Refreshes the fields that includes the status and version of the device.
Pre-upgrade Actions > Analyze	Finds if the latest entitled product release is available for a device and displays the report.
Pre-upgrade Actions > Pre-upgrade Check	Displays the Pre-upgrade Configuration page where you can configure to run the job or schedule the job to run later.
Upgrade Actions > Upgrade/Update	Displays the Upgrade Configuration page where you can configure the details of an upgrade or patch installation.
Upgrade Actions > Commit/Rollback Upgrade	Displays the Job Schedule page where you can run the upgrade job immediately or schedule it.
Upgrade Actions > Installed Patches	Displays the software patches for the element and the operations that you can perform. The operations are: install, activate, uninstall, and rollback.
Upgrade Actions > Custom Patching	Displays the Upgrade Configuration page where you configure the custom patch details. You can then install and commit the custom patch.
Upgrade Actions > Cleanup	Clears the current pending or pause state of applications. The system displays a message to check if Appliance Virtualization Platform is already installed for the same-server migration. If Appliance Virtualization Platform is already installed, you must cancel the cleanup operation and continue with the upgrade. If you continue the cleanup, the system clears the states, and you can start the upgrade process again.
Upgrade Actions > Commit	Commits the changes that you made.

Table continues...

Button	Description
Upgrade Actions > Rollback	Resets the system to the previous state.
Upgrade Actions > Resume	Resumes the upgrade process after you complete the required configuration. For example, adding the Appliance Virtualization Platform host.
Download > Download	Displays the File Download Manager page with the list of downloaded software required for upgrade or update.
Download > Bulk Import Spreadsheet	Downloads the <code>Bulk_Import_Spreadsheet_Template.xlsx</code> file on your local computer.
Show Selected Elements	Displays only the elements that you selected for preupgrade or update.

1 Upgrade Configuration field descriptions

Name	Description
Element Name	The name of the device.
Parent Name	The parent of the device. For example, <code>CommunicationManager_123</code> .
Type	The device type.
IP Address	The IP Address of the device.
Current Version	The release status of the device.
Override Preupgrade Check	The option to override preupgrade check recommendations. When you select this option, the system ignores any recommendations during preupgrade check, and continues with the upgrade operation. The system enables this option only when the system displays the upgrade status as Partial_Failure .
Override Delete VM on Upgrade Check	The option to override upgrade check recommendations. When you select this option, the system deletes the old virtual machine after the upgrade check.
Edit	Displays the Edit Upgrade Configuration page where you can provide the upgrade configuration details.
Configuration Status	An icon that defines the configuration status. ❌: Configuration incomplete. ✅: Configuration complete.

Button	Description
Import Configuration(s)	Imports the <code>Bulk_Import_Spreadsheet_Template.xlsx</code> spreadsheet. The system displays the Upload Xlsx File Configuration dialog box to upload the <code>Bulk_Import_Spreadsheet_Template.xlsx</code> spreadsheet.
Save Configuration	Saves the upgrade configuration.  Note: The system saves the configuration as a job. You can edit the job on the Upgrade Jobs Status page.
Upgrade	Commits the upgrade operation.

1 Edit Upgrade Configuration field descriptions

2 Edit Upgrade Configuration has following tabs:

- 3 • **Element Configuration**
- 4 • **AVP Configuration**

5 **Element Configuration: General Configuration Details**

Name	Description
System	The system name.
IP Address	The IP address of the device.
Operation	The operation that you want to perform on the device. The options are: • Upgrade/Migration • Update
ESXI/AVP host/Platform	The host on which you want to run the device. The options are: • Same Box • Software Only • List of hosts that you added from Application Management
New Target ESXI/AVP host/Platform	The new target host on which you want to run the device.
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, the System Manager displays the fields and populates most of the data in the Upgrade Configuration Details section.

Table continues...

Name	Description
Service/Feature Pack for auto-install after upgrade/migration	The service pack or feature pack that you want to install.

Element Configuration: Upgrade Configuration Details

The page displays the following fields when you upgrade Avaya Aura® applications. The page displays all values from the existing system. If System Manager does not populate the values, manually add the values in the mandatory fields.

Name	Description
Auto Commit	The option to automatically commit the upgrade.
Existing Administrative User	The user name with appropriate admin privileges.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields. Populates the virtual machine data of the existing virtual machine. For example, IP address, netmask, gateway.
Out of Band Management IPv4 Address	The IP address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the in-band signaling network.
Out of Band Management Netmask	The subnet mask of the virtual machine for out of band management.
Out of Band Management IPv6 Address	The IPv6 address of the virtual machine for out of band management. The field is optional network interface to isolate management traffic on a separate interface from the in-band signaling network.
Out of Band Management IPv6 Network Prefix	The IPv6 network prefix of the virtual machine for out of band management.
NTP Servers	The IP address or FQDN of the NTP server. Separate the IP addresses with commas (,). * Note: The application supports only the NTP server. It does not support the NTP pool.
DNS Servers	The DNS IP address of the virtual machine.
Search Domain List	The search list of domain names. For example, mydomain.com. Separate the domain names with commas (,).
WebLM Server IPv4 Address	The IP address of WebLM. This field is mandatory.

Table continues...

Name	Description
Flexi Footprint	The virtual resources that must be selected for the deployment of OVA based on the required capacities. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Services	The port number that is assigned to the services port. The system displays this field when Utility Services is available.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

1 The page displays the following fields when you upgrade Session Manager.

Name	Description
Existing Administrative User	The user name of the administrator.
Existing Administrative Password	The password of the administrator.
Pre-populate Data	The option to get the configuration data displayed in the fields.
IP Address	The IP address of the virtual machine.
Short Hostname	The hostname of the virtual machine. The hostname of the server and is often aligned with the DNS name of the server.
Network Domain	The domain name of the virtual machine.
Netmask	The network mask of the virtual machine.
Default Gateway	The default gateway of the virtual machine.
DNS Servers	The DNS IP address of the virtual machine.
Timezone	The timezone of the virtual machine.
Login Name	The search list of domain names. For example, mydomain.com. Separate the search names with commas (,).
Enter Customer Account Password	Password to log on to the system.
Primary System Manager IP	The IP address of System Manager.

Table continues...

Name	Description
Enrollment Password	The password that is required to establish trust between System Manager and Session Manager.
Flexi Footprint	The virtual resources that must be selected for the deployment of OVA based on the required capacities. The value depends on the server on which you deploy the OVA.
Public	The port number that you must assign to public port group.
Out of Band Management	The port number that is assigned to the out of band management port group. The field is available only when you select a different host.
Private	The port number that is assigned to an exclusive physical NIC. The installer selects a free physical server NIC during the deployment process. The field is available only when you select a different host.
Datastore	The datastore on the target ESXi host. The field is available only when you select a different host.

Element Configuration: Data Encryption

Name	Description
Data Encryption	Enables or disables the data encryption. The options are: • 1: To enable the data encryption. • 2: To disable the data encryption.  Important: • An encrypted system cannot be changed to a non-encrypted system without a new OVA installation and vice-versa. • While using vCenter, when you enable data encryption and do not enter the encryption passphrase, the system does not block the deployment due to vCenter limitation. Therefore, ensure that you enter the encryption passphrase, if data encryption is enabled. • On Solution Deployment Manager: When the Data Encryption field is set to 1, the system enables the Encryption Pass-Phrase and Re-enter Encryption Pass-Phrase fields to enter the encryption passphrase. • On vCenter or ESXi: When the Data Encryption field is set to 1, enter the encryption passphrase in the Password and Confirm Password fields.

Table continues...

Name	Description
Encryption Pass-Phrase	This field is applicable when data encryption is enabled. The passphrase for data encryption. When you deploy the application by using Solution Deployment Manager, the system applies the passphrase complexity rules. When you deploy the application by using vCenter or ESXi, the system does not apply the passphrase complexity rules.
Re-enter Encryption Pass-Phrase	The passphrase for data encryption.
Require Encryption Pass-Phrase at Boot-Time	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.  Important: 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.

1 Element Configuration: End User License Agreement

Name	Description
I Agree to the above end user license agreement	The end user license agreement. You must select the check box to accept the license agreement.

2 AVP Configuration: Existing Machine Details

Name	Description
Source IP	The source IP address.
Source Administrative User	The source user name with appropriate admin privileges.
Source Administrative Password	The source password of the administrator.
Source Root User	The source user name with appropriate root privileges.
Source Root Password	The source password of the root.

1 AVP Configuration: Configuration Details

Name	Description
Upgrade Source	The source where the installation files are available. The options are: • SMGR_DEFAULT_LOCAL • Remote Software Library
Upgrade To	The OVA file to which you want to upgrade. When you select the local System Manager library, System Manager displays the fields and populates most of the data in the Configuration Details section.
Dual Stack Setup (with IPv4 and IPv6)	Enables or disables the fields to provide the IPv6 addresses.
AVP Management IPv4 Address	IPv4 address for the Appliance Virtualization Platform host.
AVP IPv4 Netmask	IPv4 subnet mask for the Appliance Virtualization Platform host.
AVP Gateway IPv4 Address	IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
AVP Hostname	Hostname for the Appliance Virtualization Platform host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
AVP Domain	Domain for the Appliance Virtualization Platform host. If customer does not provide the host, use the default value. Format is alphanumeric string dot separated. For example, mydomain.com.
IPv4 NTP server	IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com
Secondary IPv4 NTP Server	Secondary IPv4 address or FQDN of customer NTP server. Format is x.x.x.x or ntp.mycompany.com.
Main IPv4 DNS Server	Main IPv4 address of customer DNS server. One DNS server entry in each line. Format is x.x.x.x.
Secondary IPv4 DNS server	Secondary IPv4 address of customer DNS server. Format is x.x.x.x. One DNS server entry in each line.
AVP management IPv6 address	IPv6 address for the Appliance Virtualization Platform host.
AVP IPv6 prefix length	IPv6 subnet mask for the Appliance Virtualization Platform host.
AVP gateway IPv6 address	IPv6 address of the customer default gateway on the network. Must be on the same network as the Host IP address.

Table continues...

Name	Description
IPv6 NTP server	IPv6 address or FQDN of customer NTP server.
Secondary IPv6 NTP server	Secondary IPv6 address or FQDN of customer NTP server.
Main IPv6 DNS server	Main IPv6 address of customer DNS server. One DNS server entry in each line.
Secondary IPv6 DNS server	Secondary IPv6 address of customer DNS server. One DNS server entry in each line.
Public vLAN ID (Used on S8300E only)	VLAN ID for the S8300E server. If the customer does not use VLANs, leave the default value as 1. For any other server type, leave as 1. The range is 1 through 4090. Use Public VLAN ID only on the S8300E server.
Enable Stricter Password (14 char pass length)	The check box to enable or disable the stricter password. The password must contain at least 14 characters.
AVP Super User Admin Password	Admin password for Appliance Virtualization Platform. The password must contain at least 8 characters and can include alphanumeric characters and @!\$. You must make a note of the password because you require the password to register to System Manager and the Solution Deployment Manager client.
Enhanced Access Security Gateway (EASG)	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. Enter 1 to Enable EASG (Recommended) or 2 to Disable EASG.

Table continues...

Name	Description
WebLM IP/FQDN	The IP Address or FQDN of WebLM Server.
WebLM Port Number	The port number of WebLM Server. The default port is 52233.

Button	Description
Save	Saves the changes that you made to the Edit Upgrade Configuration page.
Cancel	Cancels the changes that you made to the Edit Upgrade Configuration page.

1 Upgrading Session Manager from Release 7.x, 8.x, or 2 10.1.x to Release 10.2.x using data migration utility

3 About this task

4 Use this procedure to upgrade Session Manager using data migration utility.

5 You must perform this procedure to get data migration tool certificates to avoid the loss of alarming
6 and configuration data.

7 Procedure

- 8 1. Log in to the Session Manager with the customer account.
- 9 2. Go to the customer's home directory. For example, `cd /home/cust.`
- 10 3. Download the latest version of the data migration utility to the local directory.
- 11 4. Run the `dmutility-10.2.x.0.xxxxx.bin` utility.

```
12 $ bash dmutility-10.2.x.0.xxxxx.bin
13
14 Verifying signature... [ OK ]
15 Checking integrity of install.sh [ OK ]
16 Checking integrity of sm_backup.sh [ OK ]
17 Checking integrity of cs_functions.sh [ OK ]
18 Mounted ISO image /tmp/tmp.GUqkp31591 to /iso
19 Removing any previous backup files
20 Backing up data
21 Moving backup file to the current directory
22 Data backup is complete.
23 Copy /home/cust/Session_Manager_backup.tgz to a remote server before shutting
24 down Session Manager.
```

- 25 5. Copy the backup file to a remote server.

26 In most case, the backup file is placed in the current directory. The `dmutility` displays
27 the exact location of the backup file in the output.

- 28 6. Run the `smconfig` command and note the values of IP addresses, hostname, and other
29 parameters.

These values are required to deploy the Session Manager Release 10.2.x OVA file.

7. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Deny New Service**.

8. Run the **shutdownSM** command to shutdown Session Manager.

```
$ shutdownSM
```

```
Note: It is strongly suggested that the Session Manager
be in Deny New Service state and that one waits for all
active calls to end before shutting down the server.
Active calls through this Session Manager will drop if
it remains down too long. New calls will immediately use
an alternate Session Manager (if available) once
this Session Manager is placed in the Deny New Service state.
```

```
Do you really want to continue? (y or n)
```

9. Deploy the Release 10.2.x Session Manager or Branch Session Manager OVA.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment* on the Avaya Support website.

10. On the newly deployed Session Manager, copy the backup file to the customer's home directory.

11. Log in to the Session Manager with customer account.

12. Run the **upgradeSM** command with the backup file as an argument to run the restore utility.

```
$ upgradeSM Session_Manager_backup.tgz
Performing data migration
VSP_PROGRESS[[Starting restore]]VSP_PROGRESS
VSP_PROGRESS[[Stopping Session Manager]]VSP_PROGRESS
...
Trust Management Initialization started.
Trust Management Initialization with System Manager started.
Trust Management Initialization completed.
Upgrading saved certificates
Saving upgrade files to /opt/Avaya/prev-upgrade
Downloading System Manager root CA
Waiting for WebSphere components to startup...
Waiting for WebSphere components to startup...
...
Waiting for Management components to startup...
Waiting for Management components to startup...
Thu Apr 9 16:06:37 MDT 2015: DRS Replication registration succeeded
Please go to the System Manager Replication Page to check the synchronization
state
```

13. Run the **patchSM <name of the *.bin file>** command to apply the Release 10.2.x patch.

Go to the Session Manager Dashboard page and verify that both the **Data Replication** and the **User Data Storage Status** columns display  green check marks.

14. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Accept New Service**.

15. For VMware in customer provided Virtualized Environment, delete the old Session Manager virtual machine.

Upgrading Session Manager from Release 8.0.x, 8.1.x, or 10.1.x to Release 10.2.x through command-line interface

About this task

Use this procedure to upgrade Session Manager using command-line interface.

Procedure

1. Log in to the Session Manager with the customer account.
2. Use the **backupSM** command to create a Session Manager backup.

This command creates the `Session_Manager_backup.tgz` file and places it in the home directory of the account running the command. For example, if the cust user runs the command then the backup file is placed in `/home/cust`.
3. Copy the backup file to a remote server.
4. Run the **smconfig** command and note the values of IP addresses, hostname, and other parameters.

These values are required to deploy the Session Manager Release 10.2.x OVA file.
5. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Deny New Service**.
6. Run the **shutdownSM** command to shutdown Session Manager.

```
$ shutdownSM
```

```
Note: It is strongly suggested that the Session Manager
be in Deny New Service state and that one waits for all
active calls to end before shutting down the server.
Active calls through this Session Manager will drop if
it remains down too long. New calls will immediately use
an alternate Session Manager (if available) once
this Session Manager is placed in the Deny New Service state.
```

```
Do you really want to continue? (y or n)
```

7. Deploy the Release 10.2.x Session Manager or Branch Session Manager OVA.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment* on the Avaya Support website.
8. On the newly deployed Session Manager, copy the backup file to the customer's home directory.
9. Log in to the newly deployed Session Manager with customer account.
10. Copy the backup file.

11. Run the **restoreSM** command with the backup file as an argument to run the restore utility.

For example: **restoreSM** <path to backup file>

12. Run the **patchSM** <name of the *.bin file> command to apply the Release 10.2.x patch.

Go to the Session Manager Dashboard page and verify that both the **Data Replication** and the **User Data Storage Status** columns display  green check marks.

13. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Accept New Service**.

14. For VMware in customer provided Virtualized Environment, delete the old Session Manager virtual machine.

Upgrading non-edge Branch Session Manager to edge Branch Session Manager Release 10.2.x

Before you begin

- Deploy and configure System Manager.
- Configure Application Delivery Controller (ADC).

About this task

Use the following steps to upgrade an enterprise Branch Session Manager to an edge Branch Session Manager.

Procedure

1. Log in to Branch Session Manager with the customer account.
2. Run the **smconfig** command and note the values of IP addresses, hostname, and other parameters.
3. Run the **shutdownSM** command to shutdown Session Manager.

```
$ shutdownSM
```

Note: It is strongly suggested that the Session Manager be in Deny New Service state and that one waits for all active calls to end before shutting down the server. Active calls through this Session Manager will drop if it remains down too long. New calls will immediately use an alternate Session Manager (if available) once this Session Manager is placed in the Deny New Service state.

```
Do you really want to continue? (y or n)
```

4. Deploy the Branch Session Manager Release 10.2 OVA and ensure to select the **Edge Topology BSM** check box while deploying.

Use the values noted in step 2 to populate the other properties.

For information, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*.

*** Note:**

- 4 To deploy, use the direct method of deployment, such as vCenter or the Solution
- 5 Deployment Manager client. Do not use System Manager Solution Deployment
- 6 Manager.

5. Log in to Branch Session Manager with the customer account.

6. Install any certificates needed to establish the tunnel.

For information about configuring edge Branch Session Manager certificates, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*.

7. Run the edgeSetup command.

For information about configuring edge Branch Session Manager, see *Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment*.

Upgrading Branch Session Manager instances in bulk

Downloading the bulk import spreadsheet template

About this task

Use the following procedure to download the `Bulk_Import_Spreadsheet_Template.xlsx` file.

Procedure

1. On the System Manager web console, click **Services > Solution Deployment Manager**.
2. In the navigation pane, click **Upgrade Management**.
3. On the Upgrade Management page, click **Download > Bulk Import Spreadsheet**.

The system downloads the `Bulk_Import_Spreadsheet_Template.xlsx` file on your local computer.

1 Filling the bulk import spreadsheet for upgrading Branch Session Manager instances in bulk

Before you begin

- Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For information, see “Downloading the bulk import spreadsheet template”.

Procedure

1. On the **Element Info** sheet, do the following:

- a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.

This field supports the AVP and ESXi platforms.

- b. In **Element Type**, type BSM.

- c. In **Element IP Address**, type the IP Address of Branch Session Manager.

- d. In **Operation**, type Upgrade/Migration.

- e. In **ESXi/AVP host**, type the host IP Address of Branch Session Manager.

The value of the field must match with **SP/AVP/ESXi IP Address**.

- f. In **Migrate with AVP Install**, type `false`.

For Branch Session Manager, migration is not applicable.

- g. In **Upgrade Source**, type `SMGR_DEFAULT_LOCAL`.

- h. In **Upgrade To**, type the upgrade version of Branch Session Manager OVA.

For example: `BSM-8.1.0.0.xxxxxx-exx-0x.ova`.

- i. In **EULA**, type `true`.

- j. (Optional) In **ESXi/AVP New**, type the host IP Address of AVP or ESXi.

This field is not applicable for the same host upgrade. If you want to migrate from one AVP or ESXi host to the other, you must fill the following fields on the **BSM_Prepopulate_Data** sheet:

- **New ESXi datacentre**
- **New ESXi datastore**
- **New ESXi deployment type**

ESXi/AVP New host IP on the **AVP_VM_MAPPING** sheet.

2. On the **AVP_Info** sheet, do the following:

- a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.

You can also fill the new ESXi host here.

- b. In **Source IP**, type the IP Address of the Appliance Virtualization Platform.

c. In **Upgrade Source**, type the source where the installation files are available.

The options are:

- `SMGR_DEFAULT_LOCAL`
- Remote Software Library

d. In **Upgrade To**, type the OVA file name to which you want to upgrade.

e. In **Dual Stack Setup (with IPv4 and IPv6)**, enable or disable the fields to provide the IPv6 addresses.

The options are:

- **true**: To enable the encryption pass-phrase at boot-time.
- **false**: To disable the encryption pass-phrase at boot-time.

f. In **EASG**, type 1 to enable the EASG.

g. In **WebLM Port Number**, type the port number of WebLM Server.

The default port is 52233.

h. In **EULA**, type `true`.

3. On the **CM_Prepopulate_Data** sheet, do the following:

a. In **SP/AVP/ESXi IP Address**, type the IP Address of AVP or ESXi host.

You can also fill the new ESXi host here.

b. In **Element IP Address**, type the IP Address of Communication Manager.

c. In **NTP Server(s)**, type the IP address or FQDN of the NTP server.

Separate the IP addresses with commas (,). You can type up to three NTP servers.

d. In **Search Domain List**, type the search list of domain names.

For example, mydomain.com. Separate the search list names with commas (,).

e. In **EASG**, type 1 to enable the EASG.

f. In **Flexi Footprint**, type the footprint of Communication Manager.

For example, CM Main Max users 1,000.

g. **(Optional)** In **Customer Root Account Password**, type the customer root password.

This field is only applicable for DOD build.

 Note:

- 28 In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type
- 29 `true` for encryption pass-phrase at boot-time.

4. On the **US_Prepopulate_Data** sheet, do the following:

a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Utility Services.

- b. In **Element IP Address**, type the IP Address of Utility Services.
- c. In **Primary WebLM IP address for Licensing**, type the IP Address or FQDN of WebLM Server.
- d. In **OOBM Mode**, select the Out of Band Management mode in which you want to deploy.
The options are:
 - **OOBM_Enabled**: To enable Out of Band Management.
 - **OOBM_Disabled**: To disable Out of Band Management
- e. In **EASG**, type 1 to enable the EASG.
- f. **(Optional)** In **Customer Root Account Password**, type the customer root password.
This field is only applicable for DOD build.

 Note:

- ¹² In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type
- ¹³ `true` for encryption pass-phrase at boot-time.

5. On the **BSM_Prepopulate_Data** sheet, do the following:
 - a. In **SP/AVP/ESXi IP Address**, type the host IP Address of Branch Session Manager.
 - b. In **Search Domain List**, type `platform.avaya.com`.
 - c. In **LSP IP**, type the Communication Manager IP Address.
 - d. In **EASG User Access**, type 1 to enable the EASG.
 - e. In **Flexi Footprint**, type the footprint of Branch Session Manager.
For example, BSM Profile 1 Max Devices 1,000.
 - f. **(Optional)** In **Customer Root Account Password**, type the customer root password.
This field is only applicable for DOD build.

 Note:

- ²³ In **Data Encryption**, type 1 to enable. Fill the encryption pass-phrase and type
- ²⁴ `true` for encryption pass-phrase at boot-time.

6. On the **AVP_VM_MAPPING** sheet, do the following:
 - a. In **AVP/ESXi IP Address**, type the IP Address of the AVP or ESXi host.
You can also fill the new ESXi host here.
 - b. In **Authentication Type**, type `SSO` or `LOCAL`.
 - c. In **PSC URL**, type FQDN of PSC.
7. Save the values in the sheet.

1 Upgrading Branch Session Manager instances in bulk by using 2 System Manager Solution Deployment Manager

3 Before you begin

- 4 • On the Manage Elements page, add Branch Session Manager instances. For information
5 about adding a new element, see *Administering Avaya Aura® System Manager*.
- 6 • Refresh the element.
- 7 • Analyze the software.
- 8 • Perform the pre-upgrade check.
- 9 • Download a copy of the `Bulk_Import_Spreadsheet_Template.xlsx` spreadsheet. For
10 information, see “Downloading the bulk import spreadsheet template”.
- 11 • Fill the required system details in the `Bulk_Import_Spreadsheet_Template.xlsx`
12 spreadsheet.

* Note:

- 13 If you provide the incorrect data in the spreadsheet, the upgrade might fail.

14 Procedure

- 15 1. On the System Manager web console, click **Services** > **Solution Deployment Manager**.
- 16 2. In the navigation pane, click **Upgrade Management**.
- 17 3. On the Upgrade Management page, select Branch Session Manager instances.
- 18 4. Click **Upgrade Actions** > **Upgrade/Update**.
- 19 5. On the Upgrade Configuration page, click **Bulk Import Configuration(s)**.
- 20 6. On the Upload Xlsx File Configuration dialog box, perform the following:
 - 21 a. Click **Browse** and select the file from the local computer.
 - 22 b. To upload the spreadsheet, click **Upload**.
 - 23 c. When the spreadsheet upload is 100%, click **Submit**.

24 The system displays the file size, timestamp, and percentage complete for the
25 uploaded file. When the file upload is in-progress, do not navigate away from the
26 page.

27 On the Upgrade Management page, the system displays the message: Please
28 Wait - Saving Import Excel Sheet Configuration You must wait
29 until the system stops showing this message.

- 30 7. On the Upgrade Management page, click .

31 The **Configuration Status** column displays .

- 32 8. To save the configuration, click **Save Configuration**.

33 The update configuration is saved as a job in the Upgrade Jobs Status page.

9. On the Upgrade Configuration page, click **Upgrade**.
 10. To view the upgrade status, perform the following:
 - a. In the navigation pane, click **Upgrade Job Status**.
 - b. In the **Job Type** field, click **Upgrade**.
 - c. Click the upgrade job that you want to view.
 11. On the Upgrade Management page, click .
- The **Last Action** column displays **Upgrade**, and **Last Action Status** column displays .

patchSM command

From Release 10.2, the **patchSM** command is enhanced to take the snapshot while installing the Session Manager or Branch Session Manager patch in a virtualized environment.

Note:

- 11 The **patchSM** command is not available in a Software-Only environment.

Syntax

```
patchSM [-i <patch>] [-s <patch>] [-v <patch>] [-r <patch ID>] [-c <patch ID>] [-d]
[--snapshot]
```

- 15 **-i <patch>** 16 Installs the provided patch file. This is the default option if you just provide a patch file.
- 18 **-s <patch>** 19 Displays the patch status information.
 - 20 The -s option with the patch file displays information about the latest installed patch.
 - 22 The -s option without providing the patch file displays information about all currently installed patches.
- 24 **-v <patch>** 25 Verifies that the patch can be installed on current version of Session Manager.
- 26 **-r <patch ID>** 27 Removes the patch that matches with the provided patch ID.
- 28 **-c <patch ID>** 29 Moves the patch from the pending state to installed by removing the associated snapshot.
- 31 **-d, --debug** 32 Turn on debug logging
- 33 **--snapshot** 34 Creates a snapshot before applying the patch.

1 Installing software patches

2 About this task

3 Use the procedure to install the software patches for Session Manager.

4 Procedure

- 5 1. Log in to Session Manager and copy the 10.2.*.bin file.
- 6 2. On the Session Manager Dashboard page, change the **Service State** of the Session
- 7 Manager server to **Deny New Service**.
- 8 3. To upgrade to Release 10.2.x, run the following command:
- 9 `patchSM Session_Manager_10.2.*.bin`
- 10 4. Verify the patch installation and version using the command: `swversion`
- 11 5. After Session Manager upgrades successfully, on the Session Manager Dashboard page,
- 12 change **Service State** of the Session Manager server to **Accept New Service**.

13 Installing a Session Manager or Branch Session Manager patch 14 with the snapshot option

15 About this task

16 From Release 10.2, use this procedure to install the software patches of Session Manager or
17 Branch Session Manager with the snapshot option.

18 Procedure

- 19 1. Log in to Session Manager command-line interface and copy the 10.2 bin file.
- 20 2. On the Session Manager Dashboard page, change the **Service State** of the Session
- 21 Manager server to **Deny New Service**.
- 22 3. Type the command `patchSM -i Session_Manager_10.2.0.0.xxxxxx.bin --`
23 `snapshot`

24 Session Manager displays the following message:

25 The system will be rebooted after the patch is applied.

26 Do you wish to continue (y/n)?

- 27 4. At the prompt, type `y`.
- 28 5. In **ESXi host address**, type the IP address of the ESXi host.
- 29 6. In **ESXi username**, type the user name of the ESXi host.
- 30 7. In **ESXi password**, type the password of the ESXi host.

31 Session Manager displays the following message:

32 Snapshot complete

1 Stopping Session Manager before installing patch.

2 Session Manager applies the patch.

3 8. To commit the Session Manager patch, type the command: `patchSM -c 10.2.0.0`

4 Perform this step when Session Manager is stable.

5 Session Manager commits the patch and removes the snapshot.

6 9. Check the patch installation and version using the command: `swversion`

7 10. After Session Manager upgrades successfully, on the Session Manager Dashboard page,
8 change **Service State** of the Session Manager server to **Accept New Service**.

Draft

Chapter 9: Upgrading Session Manager to Release 10.2.x on Software-only environment

Upgrade path for Software-only environment

You can migrate to Session Manager Release 10.2.x on Software-only environment from the following:

- Release 10.1.x on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 8.1.x on Appliance Virtualization Platform on Avaya-provided server, VMware/ KVM in customer-provided Virtualized Environment, AWS/ Google Cloud / Microsoft Azure on IaaS, or Software-only environment.
- Release 7.1.x on Appliance Virtualization Platform on Avaya provided server or on VMware in customer-provided Virtualized Environment or on AWS.

Upgrading Session Manager from Release 7.x, 8.x, or 10.1.x to Release 10.2.x on Software-only and IaaS

About this task

Use this procedure to upgrade Session Manager on Software-only and IaaS environments.

* Note:

- 18 Use this procedure to upgrade Avaya Aura® application Release 8.1.x on Nutanix to Avaya
- 19 Aura® application Release 10.2.x in the Software-only environment.

You must perform this procedure to get data migration tool certificates to avoid the loss of alarming and configuration data.

Before you begin

Back up the call history using User Data Storage. For more information, see *Administering Avaya Aura® Session Manager*.

Session Manager stores call logs only when the Centralized Call History is enabled.

Procedure

1. Log on to the on-premises Session Manager with the customer account.
2. Go to the customer's home directory. For example, `cd /home/cust`.
3. Download the latest version of the data migration utility to the local directory.
4. Run the `dmutility-10.2.0.0.xxxxxx.bin` utility.

```
$ bash dmutility-10.2.0.0.xxxxxx.bin
Verifying signature... [ OK ]
Checking integrity of install.sh [ OK ]
Checking integrity of sm_backup.sh [ OK ]
Checking integrity of cs_functions.sh [ OK ]
Mounted ISO image /tmp/tmp.GUqkp31591 to /iso
Removing any previous backup files
Backing up data
Moving backup file to the current directory
Data backup is complete.
Copy /home/cust/Session_Manager_backup.tgz to a remote server before shutting
down Session Manager.
```

5. Copy the backup file to a remote server.

Usually, the backup file is `/home/cust/Session_Manager_backup.tgz`. The `dmutility` displays the exact location of the backup file as an output.

6. Run the `shutdownSM` command to shutdown Session Manager.

```
$ shutdownSM
Note: It is strongly suggested that the Session Manager
be in Deny New Service state and that one waits for all
active calls to end before shutting down the server.
Active calls through this Session Manager will drop if
it remains down too long. New calls will immediately use
an alternate Session Manager (if available) once
this Session Manager is placed in the Deny New Service state.
Do you really want to continue? (y or n)
```

7. Deploy the Session Manager Release 10.2.x compatible application on your Software-only or IaaS environment.

For deploying the Session Manager application on Software-only or IaaS environment, see *Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment*.

8. Update the IP address of Session Manager (Asset/ SIP IP and Management IP) on the Routing and Inventory page of System Manager. For more information, see *Administering Avaya Aura® Session Manager*.
9. On the newly deployed Session Manager, copy the backup file to the customer's home directory.

10. Log on to the Session Manager with the customer account and run the **upgradeSM** command to run the restore utility.

```
$ upgradeSM Session_Manager_backup.tgz
Performing data migration
VSP_PROGRESS[[Starting restore]]VSP_PROGRESS
VSP_PROGRESS[[Stopping Session Manager]]VSP_PROGRESS
...
Trust Management Initialization started.
Trust Management Initialization with System Manager started.
Trust Management Initialization completed.
Upgrading saved certificates
Saving upgrade files to /opt/Avaya/prev-upgrade
Downloading System Manager root CA
Waiting for WebSphere components to startup...
Waiting for WebSphere components to startup...
...
Waiting for Management components to startup...
Waiting for Management components to startup...
Thu Apr 9 16:06:37 MDT 2015: DRS Replication registration succeeded
Please go to the System Manager Replication Page to check the synchronization
state
```

! Important:

- 22 If the backup host name is different than the target host name, the restore operation
- 23 fails because the certificates are associated with the host name. To avoid this issue,
- 24 ensure that the backup host name is the same as the restore host name.

11. On the System Manager web console, click **Elements > Session Manager > Dashboard**.
12. On the Session Manager Dashboard page, change **Service State** of the Session Manager server to **Deny New Service**.
13. Run the **patchSM <name of the *.bin file>** command to apply the Release 10.2.x patch (if applicable).
Go to the Session Manager Dashboard page and verify that both the **Data Replication** and **User Data Storage Status** columns display  green check marks.
14. On the Session Manager Dashboard page, change the **Service State** of the Session Manager server to **Accept New Service**.

Chapter 10: Post-upgrade verification

Post-upgrade checklist for Session Manager or Branch Session Manager

Use this checklist after upgrading Session Manager or Branch Session Manager to Release 10.2.x.

#	Task	Notes	✓
1	After the server reboots, log in to the server.	After the upgrade, log in with customer login name and password.	
2	If applicable, configure the Session Manager server in a System Manager Geographically Redundant environment.	See Configuring Session Manager in a geographically redundant environment on page 127.	
3	Type the swversion command and verify that the upgrade is completed successfully.	If the upgrade is not successful, contact Avaya Technical Support.	
5	Run the Session Manager server tests.	See Testing the Session Manager instance on page 127.	
6	Verify data replication between System Manager and Session Manager. The system synchronizes the data in about 15 minutes. Refresh the page as necessary.	See Verifying Data Replication on page 128.	
7	Verify the Security Module is active for the Session Manager server.	See Viewing Security Module status on page 129.	
8	If SIP monitoring is provisioned for Session Manager, verify the links are active for the Session Manager instance. The system updates the status in about 10 minutes. Refresh the page as necessary.	See Viewing Session Manager Entity Link Connection Status on page 130.	
9	Change Service State of the Session Manager or Branch Session Manager server to Accept New Service .	See Accepting new service on page 131.	
10	Make test calls to ensure the Session Manager server is processing calls properly.		

1 Configuring Session Manager in a System Manager geographically redundant environment

3 About this task

4 In a System Manager geographic redundant environment where the Primary System Manager is
5 down, perform this procedure after upgrading the Session Manager server.

6 Procedure

- 7 1. Log in as **craft** or customer to a console on the Session Manager server, or use SSH for
8 remote login.

* Note:

9 You can connect your laptop directly to the service port of the server.

- 10 2. Type the **changeMgmtIP** command, press **Enter**, and ensure that all fields are set
11 correctly.
- 12 3. Type the **dnat_failover.sh <SECONDARY_SMGR_IP>** command and press **Enter**.
- 13 4. Type the **initTM** command and press **Enter**.

14 Testing the Session Manager instance

15 Procedure

- 16 1. On the System Manager web console, under **Elements**, select **Session Manager >**
17 **System Tools > Maintenance Tests**.
- 18 2. In the **Select System Manager or a Session Manager to test** field, select the Session
19 Manager instance from the drop-down menu.
- 20 3. Select **Execute all Tests**.
- 21 4. Verify the **Test Result** field displays **Success**.

22 If any of the tests fail, see *Troubleshooting Avaya Aura® Session Manager* and *Maintaining*
23 *Avaya Aura® Session Manager*.

24 Installing the license file

25 Procedure

- 26 1. On the home page of the System Manager web console, click **Services > Licenses**.
- 27 2. In the navigation pane, click **Install license**.

3. Click **Browse** to specify the location of the Session Manager license file on your computer.
 4. Click **Accept the License Terms & Conditions**.
 5. Click **Install**.
- The System Manager web console displays Session Manager in the **Licensed products** section.

Verifying Data Replication

Procedure

1. On the System Manager web console, under **Services**, click **Replication**.
2. Verify the status for the appropriate replica group is **Synchronized**.
3. If the status for the replica group is not **Synchronized**, see [Troubleshooting Data Replication](#) on page 128.

Troubleshooting Data Replication

Procedure

1. On the home page of the System Manager Web console, under **Services**, click **Replication**.
2. If the status for the replica group is not **Synchronized**:
 - a. Select the affected replica group.
 - b. Click **View Replica Nodes**.
 - c. Verify that an instance exists in the replica group under **Replica Group Host Name**.
 - d. Select the appropriate instance under **Replica Group Host Name**.
 - e. Click **View Details**.
 - f. Under the Synchronization Statistics section, wait until the **Pending Batches** value is zero. Refresh the page as necessary by clicking **Refresh**.
3. If the **Pending Batches** value does not change to zero:
 - a. Click **Done**.
 - b. On the **Replica Group** page, click **Repair**.
 - c. Click **OK** in the dialog box.
4. Wait until the status of the replica group changes to **Synchronized**. Refresh the page as necessary.

Viewing the Security Module status

About this task

Use this procedure to view the security module status.

Possible causes for the security module status to be **Down** include:

- The security module might have recently been reset. A reset can take several minutes to complete.
- The security module might not have received security module configuration information from System Manager.

Procedure

1. On the System Manager web console, click **Elements > Session Manager**.
2. If the security module state of Session Manager does not display as **Up**:
 - a. Click the status text of the security module for Session Manager to display the Security Module Status page.
 - b. Verify that the IP address of Session Manager is correct.
 - c. Select the Session Manager instance.
 - d. Click **Synchronize**.
 - e. If the status remains **Down**, click **Reset**.



Warning:

- 18 Session Manager cannot process calls while the security module is being reset.

Related links

[Troubleshooting Security Module Sanity failure](#) on page 129

Troubleshooting Security Module Sanity failure

Procedure

1. On the System Manager Web Console, select **Elements > Session Manager > System Status > Security Module Status**.
2. Select **Refresh** to display the current status.
3. Verify that the **Status** for the indicated Session Manager is **Up**.
4. Verify that the IP address is correct.
5. If the status is selected as **Down**, reset the security module:
 - a. Select the appropriate Session Manager instance from the table.
 - b. Click **Reset**.



Warning:

- 1 Session Manager cannot process calls while the system resets the security
- 2 module.

6. Select **Refresh** to display the current status.

Related links

[Viewing the Security Module status](#) on page 129

Verifying the Enrollment Password status

Session Manager requires an Enrollment Password during the initial installation and deployment process. Enrolling a password establishes trust between System Manager and Session Manager. The Enrollment Password is also known as the **certificate enrollment password**.

If the Enrollment Password has expired, or if you do not know the password, do one of the following:

- Ask the customer for a password.
- Make up a password.

If **Time Remaining** is not zero, the password is valid. Verify that the time remaining is sufficient for the upgrade.

Procedure

1. On the home page of the System Manager web console, under **Services**, select **Security > Certificates > Enrollment Password**.
2. If the value of the **Time Remaining** field is zero, you need to reset the password:
 - a. In the **Password expires in** field, select a value from the drop-down menu for the time when the password must expire.
 - b. Enter a password in the **Password** field.
 - c. Re-enter the password in the **Confirm Password** field.
 - d. Make a note of the password for future reference.
 - e. Click **Commit**.

The system updates the **Time remaining** field.

Viewing the Session Manager entity link connection status

About this task

Use this procedure to view Session Manager entity link connection status.

*** Note:**

- 1 Entity Monitoring does not apply to a Branch Session Manager. The monitoring status of a
- 2 Branch Session Manager is always unknown (---).

3 An entity link consists of one or more physical connections between a Session Manager server
4 and a SIP entity. If all the connections are up, then the Entity Link status is **up**. If one or more
5 connections are down but at least one connection is up, the link status is **partially down**. If all the
6 connections are down, the Entity Link status is **down**.

7 On the Session Manager dashboard page, the number of down links and total links are shown in
8 the **Entity Monitoring** column. The values have the format **# of Down links / # of Total links**.

Procedure

1. On the System Manager web console, click **Elements > Session Manager**.
2. Under the **Entity Monitoring** column, red values indicate that at least one entity link is
down. Click the red values link to display the Session Manager Entity Link Connection
Status page.

The Session Manager Entity Link Connection Status page displays the details for each
link. If a link is down, the page displays a reason code.
3. To view the SIP Entity Link Monitoring Status Summary page, click **Summary View**.

Accepting new service

About this task

Use this procedure to change the state of a new service to accept.

*** Note:**

- 20 Even though Security Module displays the status as Up, the Security Module might take 5 to
- 21 10 minutes to begin routing calls.

Procedure

1. On the home page of the System Manager web console, click **Elements > Session
Manager > Dashboard**.
2. On the Session Manager Dashboard page, select the appropriate Session Manager or
Branch Session Manager instance in the **Session Manager Instances** table.
3. In the **Service State** field, click **Accept New Service**.
4. Click **Confirm**.

Enhanced Access Security Gateway

Session Manager supports Enhanced Access Security Gateway (EASG), an authentication interface that secures the system administration and logins on the system. EASG provides a secure method for Avaya services personnel to access the Avaya Aura® applications 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.

EASG uses a challenge and response protocol to confirm the validity of a user. This process reduces the opportunity for unauthorized access.

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

Checking EASG status

Before you begin

Log in to the application with the customer account.

Procedure

1. On the command line interface, type `EASGStatus`.
2. Press `Enter`.

The system displays one of the following:

- **EASG is enabled** — if EASG is enabled.
- **EASG is disabled** — if EASG is disabled.

Enabling and disabling EASG using CLI

About this task

Avaya recommends enabling EASG. 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 and allowing Avaya to resolve product issues in a timely manner. See the Avaya support site for additional information for registering products and establishing remote access and alarming.

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.

Before you begin

Log in to the application with the customer account.

Procedure

1. On the command line interface, do one of the following:

- To enable EASG, type `EASGManage --enableEASG`.
- To disable EASG, type `EASGManage --disableEASG`.

The system displays the message **Do you want to continue [yes/no] ?**

2. Type `yes` or `no`.

3. Press `Enter`.

Enabling and disabling EASG through System Manager

About this task

From the Session Manager Dashboard screen, you can enable or disable EASG for all supported users. To enable or disable EASG for individual users, you must use the command line interface. Enabling EASG globally through System Manager does not override the EASG disabled setting for individual users.

Procedure

1. On the System Manager web console, click **Elements** > **Session Manager**.

2. In the navigation pane, click **Dashboard**.

3. Click the **EASG** field.

4. Click one of the following:

- **Enable EASG.**
- **Disable EASG.**

5. Click **Confirm**.

EASGManage

Use **EASGManage** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

--enableEASG Enables Enhanced Access Security Gateway (EASG) authentication.

--disableEASG Disables EASG authentication.

--enable Enables EASG authentication only for the Avaya Services logins specified in the *user* variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter

- 1 what this setting reflects for an individual Avaya Services Login. EASG
- 2 supports only Avaya services logins, such as init, inads, and craft.
- 3 **--disable** 4 Disables EASG authentication only for the Avaya Services logins
- 5 specified in the *user* variable.
- 6 **--userStatus** 7 Displays the EASG status of the user specified in the *user* variable.
- 8 **--listUsers** 9 Lists the available EASG users.
- 10 **--f** 11 Forces the enable or disable action to run without prompts.
- 12 **--printDisableWarning** 13 Displays the warning message for disabling EASG on the system.
- 14 **--printEnableWarning** 15 Displays the warning message for enabling EASG on the system.

16 Loading and managing site certificate

17 About this task

18 Site certificates are used by the onsite technicians not having access to the Avaya network
 19 to generate a response to the Enhanced Access Security Gateway (EASG) challenge. The
 20 technician will generate and provide the site certificate to the customer. The customer must load
 21 this site certificate on each server (AVP Host) and virtual machine that the technician needs to
 22 access. Once this is done the technician can use EASG Site Manager to login with the EASG
 23 challenge. After the technician is done the customer can remove the site certificate from the server
 24 or they will be removed by the EASG software after the site certificate expires (~15 days later).

25 You can load a site certificate using `EASGSiteCertManage --add <pkcs7_file_path> .`
 26 You will need to specify a Site Authentication Factor (SAF). The SAF must be provided to
 27 the technician and is also used by EASG Site Manager to generate a response to the EASG
 28 challenge.

29 Before you begin

30 Customers must complete the following before loading and managing site certificates:

- 31 • Have a valid login and password.
- 32 • Use a tool such as WinSCP. Log in using a customer login, for example `cust`. Copy the
- 33 certificate to `/home/cust` directory (where `cust` is the customer directory).
- 34 • Use a 10 to 20 character Site Authentication Factor (SAF) for instance `12345abcwxyz`.
- 35 • Be familiar with CLI type shell commands.

36 Procedure

- 37 1. Log in to a Linux® shell by using the customer account.

38 The customer account is created during the deployment procedure.

- 39 2. To manage site certificates, type the following command:

```
40 [cust@host ~]$ EASGSiteCertManage --add johndoe.p7b
41 You are about to install this site certificate into your trusted repository:
42 Technician Name: johndoe
```

```

1      Expiration Date: Nov 10 17:02:15 2016 GMT
2      Do you want to continue [yes/no]? yes
3      Please enter a site authentication factor (SAF) for the technician to use
4      when getting access to your machine. The SAF is alphanumeric with at least 10
5      characters and no more than 20 characters.
6      Please enter your SAF: Site Authentication Factor
7      Please confirm your SAF: Site Authentication Factor
8      Site Certificate installed successfully.

```

Save the Site Authentication Factor to share with the technician once on site.

3. To display information about a site certificate, type the following command with the name of a valid site certificate:

```

12     [cust@host ~]$ EASGSiteCertManage --show johndoe.p7b
13     Subject:      CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
14     User Name:    johndoe
15     Expiration:   Nov 10 17:02:15 2016 GMT
16     Trust Chain:
17         1. O=Avaya, OU=IT, CN=AvayaITrootCA2
18         2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
19         3. O=Avaya LLC, OU=EASG, CN=EASG Intermediate CA
20         4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya LLC
21         5. CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC

```

4. To remove a site certificate, type the following command with the name of a valid site certificate:

```

24     [cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
25     Successfully removed Site Cert: johndoe.p7b

```

Alarming Configuration

* Note:

- Not all upgrade paths require alarming configuration. The upgrade checklists contain the alarm configuration step if the upgrade path requires alarming configuration.

Network Management Systems Destinations

The Session Manager serviceability agent can send SNMPv2c/v3 traps or informs for alarms to multiple destinations such as:

- SAL Gateway, mandatory trap destination
- System Manager trap listener
- Third-party NMS
- Avaya SIG server

SAL Gateway is a mandatory trap destination for traps sent to Avaya Services for system maintenance. SAL Gateway converts the traps to alarms and forwards the alarms to the Avaya Data Centre for ticketing purposes. Therefore, after you install or upgrade from release earlier than 6.2 to Session Manager Release 6.2 or later, you must configure the serviceability agent with SAL Gateway as a trap destination. You can configure the serviceability agent by using the

System Manager web console. You must also configure Session Manager as a managed device on SAL Gateway.

Optionally, you can configure any third-party Network Management Systems (NMS) as a trap destination. Based on customer requirements, Avaya technicians can also configure the Avaya SIG server as another trap destination.

For upgrades from Release 6.2 or later, the configuration of the serviceability agent persists through the Session Manager upgrade.

You can add an NMS destination using the System Manager web console. To add an NMS destination, you must create a target profile for the NMS destination and then attach the target profile to a serviceability agent. For more information on activating agents and attaching target profiles, see Managing Serviceability Agents in *Administering Avaya Aura® System Manager*.

Activating and managing the Session Manager serviceability agent

Use the System Manager web console to activate and manage the Session Manager serviceability agent. To add a Network Management System (NMS) destination, you first create a target profile for the NMS destination and then attach the target profile to a serviceability agent.

For more information on activating agents and attaching target profiles, see the SNMP Support chapter in *Administering Avaya Aura® Session Manager*.

For the Geographic Redundant system setup, administer both System Manager instances as targets for alarming.

Alarming configuration checklist

#	Action	Link/Notes	✓
1	Configure the Serviceability Agent for Session Manager.	See SNMP support for Session Manager in <i>Administering Avaya Aura® Session Manager</i> .	
2	Add Session Manager to the SAL Gateway.	Adding a Session Manager to the SAL Gateway on page 136.	
3	Generate a test alarm.	Generating a test alarm on page 138.	

Adding Session Manager to the SAL Gateway

About this task

Configure alarming and remote access for a Session Manager instance.

Do not perform this procedure if you are upgrading the Session Manager server that is already configured on a SAL Gateway.

Before you begin

Procedure

1. Log in to the System Platform Web console.
2. Click **Server Management > SAL Gateway Management**.
3. On the **SAL Gateway Management** page, click **Launch SAL Gateway Management Portal**.
4. When the SAL Gateway login page appears, enter the same user ID and password that you used to log in to the System Platform Web Console.
5. In the navigation pane of the SAL Gateway user interface, select **Secure Access Link Gateway > Managed Element**.
6. On the **Managed Element** page, click **Add new**.
7. Enter information in the following fields:
 - **Host Name:** Host Name of the Session Manager server.
 - **IP Address:** IP Address of the Session Manager server.
 - From the **Model** list, select **SessionMgr_x.x.x.x**.

The **Product** field is filled in automatically after you select the Session Manager.

 - **Solution element ID:** The Solution Element ID (SE ID) of Session Manager. The format of the ID is (NNN)NNN-NNNN where N is any digit from 0 to 9.
 - **Product ID:** The Product ID of Session Manager.
 - Select the **Provide remote access to this device** check box.
 - Select the **Transport alarms from this device** check box.

 **Important:**

 - 21 The SAL Gateway forwards alarms for this Session Manager only after you select
 - 22 the **Provide remote access to this device** and **Transport alarms from this**
 - 23 **device** check boxes.
8. Click **Add**.
9. Click **Apply** to apply the changes.
10. Restart the SAL Gateway for the configuration changes to take effect:
 - a. In the navigation pane of the SAL Gateway user interface, select **Administration > Apply Configuration Changes**.
 - b. Click **Apply** next to **Configuration Changes**.

The system restarts the SAL Gateway and updates the SAL Gateway with the new configuration values.

1 Generating a test alarm

2 About this task

3 Generate a test alarm to the targets assigned to the serviceability agent. These targets can
4 include:

- 5 • A SAL Gateway
- 6 The alarm is forwarded to ADC
- 7 • System Manager Trap Listener
- 8 • Third-party NMS
- 9 • Avaya SIG server

10 You can either run the **generateTestAlarmSM.sh** script using the Session Manager CLI, or you
11 can use the **Generate Test Alarm** button on the **Serviceability Agents** screen.

12 Procedure

- 13 1. If using the Session Manager CLI:
 - 14 a. Login to the Session Manager server.
 - 15 b. Run the Session Manager CLI command `generateTestAlarmSM.sh`.
- 16 2. If using the **Generate Test Alarm** button on the Serviceability Agents screen:
 - 17 a. On the System Manager web console, click **Services > Inventory > Manage**
18 **Serviceability Agents > Serviceability Agents**.
 - 19 b. Select a hostname from the list and click **Generate Test Alarm**.
- 20 3. To verify that the System Manager received the test alarm message, do one of the
21 following:
 - 22 a. On the System Manager web console, click **Services > Events > Alarms**.
 - 23 b. Check that the system displays the message **Test alarm for testing only, no**
24 **recovery action necessary** in the **Description** column.
- 25 4. If the serviceability agent is configured with other targets, verify that the other targets also
26 received the test alarm and also verify the clearing of the alarm.

* Note:

27 The test alarms are not generated when Session Manager is in Maintenance Mode.

Chapter 11: Resources

Session Manager documentation

The following table lists the documents related to Session Manager. Download the documents from the Avaya Support website at <https://support.avaya.com>.

Title	Description	Audience
Overview		
<i>Avaya Aura® Session Manager Overview and Specification</i>	Describes the key features of Session Manager.	System administrators
<i>Avaya Aura® Session Manager Security Design</i>	Describes the security considerations, features, and solutions for Session Manager.	Network administrators, services, and support personnel
Implementation		
<i>Deploying Avaya Aura® Session Manager and Avaya Aura® Branch Session Manager in Virtualized Environment</i>	Describes how to deploy the Session Manager virtual application in a virtualized environment.	Services and support personnel
<i>Deploying Avaya Aura® Session Manager in Software-Only and Infrastructure as a Service Environment</i>	Describes how to deploy the Session Manager in the Software-Only and Infrastructure as a Service (IaaS) environment.	Services and support personnel
<i>Routing Web Service API Programming Reference</i>	Describes how to use the System Manager Routing Web Service API for Session Manager.	Services and support personnel
<i>Avaya Aura® Session Manager Element Manager Web Service API Programming Reference</i>	Describes how to get programmatic access to Session Manager Dashboard and User Registration status data.	Services and support personnel
Administration		
<i>Administering Avaya Aura® Session Manager</i>	Describes the procedures to administer Session Manager using System Manager.	System administrators

Table continues...

Title	Description	Audience
<i>Avaya Aura® Session Manager Data Privacy Guidelines</i>	Describes how to administer Session Manager to fulfill Data Privacy requirements.	System administrators, Network administrators, services, and support personnel
Installation and upgrades		
<i>Upgrading Avaya Aura® Session Manager</i>	Describes the procedures to upgrade Session Manager to the latest software release.	Services and support personnel
Maintaining and Troubleshooting		
<i>Maintaining Avaya Aura® Session Manager</i>	Contains the procedures for maintaining Session Manager.	Services and support personnel
<i>Troubleshooting Avaya Aura® Session Manager</i>	Contains the procedures to troubleshoot Session Manager, resolve alarms, and replace hardware.	Services and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. (Optional) In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Accessing the port matrix document

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.

3. Click **Product Support > Documents**.
4. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
5. From the **Select Content Type** list, select one or both of the following options:
 - **Application & Technical Notes**
 - **Design, Development & System Mgt**

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

- 11 If the documentation you are looking for is not available on the Avaya Documentation Center,
- 12 you can find it on the [Avaya Support website](#).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** (🌐) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** (🔗) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (📁). You can add the topic and its subtopics or add the entire publication.

- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
 - Set a collection as the default or favorite collection.
 - Save a PDF of the selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
 - View and manage your watchlist by clicking **Watchlist** from the top menu with your name.
- You can do the following:
- Enable **Email notifications** to receive email alerts.
 - Unwatch the selected content or all topics.
- Send feedback for a topic.

Training

The following table contains courses that are available on <https://www.avaya-learning.com>. To search for the course, in the **Search** field, enter the course code and click **Go**.

New training courses are added periodically. Enter **Session Manager** in the **Search** field to display the inclusive list of courses related to Session Manager.

Course code	Course title
71201V	Integrating Avaya Aura® Core Components
72201V	Supporting Avaya Aura® Core Components
61131V	Administering Avaya Aura® System Manager

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 **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select 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 and do one of the following:
 - Enter a keyword or keywords 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 example, Contact Centers.

Note:

Videos are not available for all products.

Support

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

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.

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

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

- 5 1. Go to <https://support.avaya.com>.
- 6 2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when
7 prompted.
- 8 3. Click **Product Support > Products**.
- 9 4. In **Search Product**, start typing the product name and then select the appropriate product
10 from the list displayed.
- 11 5. Select the release number, if applicable.
- 12 6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: OS-level logins for Session Manager

The following is a list of logins that are created during the Session Manager software installation:

- **asset:** A login created during the installation of the Security Module software. By default, access to the system using this login is disabled.
- **csadmin:** Login used by the Solution Deployment Manager to manage Session Manager remotely.
- **cassandra:** Login used by the Cassandra application user
- **CDR_User:** A restricted shell login for the Call Detail Recording (CDR) feature. CDR collects call data from the Session Manager server. This login is restricted to sftp access only.
- **craft:** An Avaya services login to gain access to the system remotely for troubleshooting purposes.
- **customer:** A login that the **SMnetSetup** script creates. The default name of the *customer* login is **cust**. The customer must ensure the security of this login account. The *customer* login can run software tools which do not require root access on the Session Manager servers.
- **init:** An Avaya services login that accesses the system remotely for troubleshooting purposes.
- **jboss:** A login created for running the management jboss and is not a login account.
- **postgres:** A login created by the installation of the Session Manager software PostgreSQL database system. Access to the system using this login is disabled.
- **spirit:** A login created by the Secure Access Link remote alarming and remote access module for Avaya services.
- **sroot:** An Avaya services root permission login to gain access to the system remotely for troubleshooting purposes. You cannot gain access to the sroot login directly from a login prompt except on the server console.
- **wsuser:** A login created for running WebSphere. This login is not a login account.

Warning:

In Session Manager 8.1.x, Enhanced Access Security Gateway secures the following logins and prevents unauthorized access to the Session Manager servers by non-Avaya services personnel:

- **sroot**

- 1 • **init**
- 2 • **craft**

3 Using the customer login account, you can run most of the maintenance and troubleshooting
4 commands. You do not need root access for standard maintenance and support purposes. For
5 more information, see [PSN](#) (PSN003925U).

Draft

Appendix B: Upgrading RHEL

Upgrading RHEL 8.4 to RHEL 8.10 on OVA-based virtual machines

About this task

You can upgrade RHEL 8.4 to RHEL 8.10 using the following **av-upgrade-os** command. The **av-upgrade-os** command is available when Session Manager R10.2.1 is installed.

Before you begin

1. Install Session Manager R10.2.1.

To view the current version of Session Manager, run the following command: **swversion -s**.

2. Verify that **av-upgrade-os** command is available.

To verify if the **av-upgrade-os** command is available, run the following command: **which av-upgrade-os**

3. Verify the current version of RHEL on which Session Manager is running.

To view the current RHEL version, run any of the following commands:

- **cat /etc/redhat-release**
- **av-version**

4. Download Session Manager RHEL 8.10 Operating System bundle on Session Manager R10.2.1 virtual machine.

Procedure

1. Login to Session Manager CLI.

2. To upgrade from RHEL 8.4 to RHEL 8.10, run the following command: **av-upgrade-os <SM RHEL OS Bundle>**

For example, run **av-upgrade-os AV-SM10.2-RHEL8.10-OSUpdate-001.tar.bz2**

3. After successful upgrade to RHEL 8.10, the Session Manager virtual machine reboots.

4. Log in to Session Manager CLI.

5. To verify that RHEL 8.10 is upgraded successfully, run any of the following commands:

- **cat /etc/redhat-release**

1 • **av-version**

Draft

Appendix C: Product notifications

2

3 Avaya issues a product change notice (PCN) for a software update. A PCN accompanies a service
4 pack or patch that must be applied universally.

5 Avaya issues a product support notice (PSN) when there is a change in a product. A PSN provides
6 information such as a workaround for a known problem and steps to recover software.

7 Both of these types of notices alert you to important issues that directly impact Avaya products.

8 Viewing Product Correction Notices and Product Support 9 Notices

10 Procedure

- 11 1. Go to the Avaya Support website at <http://support.avaya.com>.
- 12 2. Enter your login credentials, if applicable.
- 13 3. On the top of the page, click **DOCUMENTS**.
- 14 4. In the **Enter your Product Here** field, enter the name of the product, then select the
15 product from the drop-down menu.
- 16 5. In the **Choose Release** field, select the specific release from the drop-down menu.
- 17 6. In the list of filters, select the **Product Correction Notices** and/or **Product Support**
18 **Notices** check box.

Note:

19 You can select multiple filters to search for different types of documents at one time.

- 20 7. Click **Enter**.

1 Registering for product notifications

* Note:

- 2 This procedure applies only to registered Avaya customers and business partners with an
- 3 SSO login.

4 Procedure

- 5 1. Go to the Avaya Support website at <http://support.avaya.com>.
- 6 2. Log in using your SSO credentials.
- 7 3. Click on the **MY PROFILE** link.
- 8 4. Click the highlighted **HI, <username>** tab.
- 9 5. Select **E Notifications** from the menu.
- 10 6. In the **Product Notifications** section:
 - 11 a. Click **Add More Products**.
 - 12 b. Select the appropriate product.
- 13 7. In the Product box that appears on your screen:
 - 14 a. Select the appropriate release or releases for which you want to receive notifications.
 - 15 b. Select which types of notifications you want to receive. For example, **Product**
 - 16 **Support Notices** and **Product Correction Notices (PCN)**.
 - 17 c. Click **Submit**.
- 18 8. If you want notifications for other products, select another product from the list and repeat
- 19 the above step.
- 20 9. Log out.

Appendix D: Archiving logs

The logs are located in various subdirectories on the Session Manager server. Running a log harvester on the Session Manager server, copies all the current logs, and archives them on the System Manager server for viewing at a later time, if necessary.

For more information about the log harvester and field descriptions, see *Administering Avaya Aura® System Manager*.

Log harvester

The log harvesting service manages the retrieval, archival, and analysis of the harvested log files stored in Serviceability Agent enabled hosts or elements. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging Service through HTTPS. With a successful harvest request related to a harvest profile, the logging service accepts the file segments, creates a well-defined file structure, and saves the request in the System Manager node.

You can harvest log files for one or more products of the same or different types running on the same or different computers. The system displays the list of file archives and respective profiles on the log harvesting user interface, and the status of each archive is available in the user interface table.

You can perform the following operations using the log harvesting service:

- Create a log harvesting profile to specify the products for which you want to harvest the logs.
- Submit the log harvesting request defined in a profile to the product.
- View the status of the log harvesting request.
- Store the harvested log files of a product in an archive file.
- View the harvested log files stored in the archive file.
- Download the harvested log files to a local computer.
- Search for a matching text in the harvested log files.

1 Accessing the Log Harvester service

2 Procedure

3 On the System Manager web console, click **Services > Events > Logs > Log Harvester**.

4 Creating a new log harvesting profile

5 To create a new log harvesting profile, you must specify:

- 6 • The host name of the server on which the product is running.
- 7 • The product name.
- 8 • The directories or log files.
- 9 • The filter text if you select one or more directories.

10 To harvest log files for products running on different servers, you must specify multiple filter
11 criteria.

12 Procedure

- 13 1. On the home page of the System Manager web console, under **Services**, click **Events >**
14 **Logs > Log Harvester**.
- 15 2. On the Log Harvest page, click **New**.
- 16 3. Enter the appropriate information in the **Profile Name** and **Profile Descriptions** fields.
- 17 4. Select the host name of the server, product, and directories or files from the respective
18 fields.
 - 19 • To select multiple directories or files from the respective drop-down menus, press **CTRL**
20 and click the directories or files.
 - 21 • To clear a selection, press **CTRL** and click the item.
 - 22 • To add another log harvesting request for a different product or for another instance of
23 the same product, click the plus sign (+).
- 24 5. If you select one or more directories, in the **File Name Filter** field, enter a text pattern for
25 the filter criteria.

26 During the harvesting operation, the system harvests only those files that match the filter
27 criteria.
- 28 6. Click **Save** to save the profile and the log harvesting requests in the profile.

29 Create New Profile field descriptions

30 Use this page to create a new log harvesting profile for harvesting log messages from the log files
31 for one or more products. The files can reside on one or more servers.

Name	Description
Profile Name	The name of the log harvesting profile.
Profile Description	A brief description of the profile. This is an optional field.
Host Name	The host name of the server on which products are installed.
Product	The products for which you can harvest logs.
Directories	A list of directories that contains the log files for the selected product.
Files	The log files that you can harvest for the selected product.
File Name Filter	The text on which to filter the log file names that display under the selected directory. For example: If you select the directory /a/b/c and enter com in the File Name Filter field, the harvest operation for this profile harvests the log files that are in the directory /a/b/c . The log files contain com in the file name. The field does not support wild cards.

Button	Description
+	Add another log harvesting request for a product.
–	Delete a log harvesting request for the product.
Commit	Commits the filter criteria for the selected directories.
Save Profile	Saves the new profile and settings for harvesting requests in the database.
Cancel Profile	Cancel the profile request.

1 Submitting a request for harvesting log files

2 About this task

3 Use this feature to submit a log harvesting request to one or more products running on the same
4 or different servers. After the request is successfully processed, the system on which the products
5 are installed returns the harvested log files specified in the request. When you select a profile and
6 click **Request**, the system generates a single request for all the requests contained in the profile.

7 Procedure

- 8 1. On the System Manager web console, click **Services > Events > Logs > Log Harvester**.
- 9 2. On the Log Harvester page, select a log harvesting profile, and click **Requests**.
- 10 3. On the Harvest Archives page, type the relevant information in the **Archive Name** and
11 **Archive Description** fields.

- 1 The system saves the harvested log files in the specified archive file.
- 2 4. Click **Run Profile** to send a request.
- 3 The table in the Harvest Criteria View section provides you the log harvesting request
- 4 status. If the execution status of the request is successful, the system creates a zip file
- 5 containing the harvested log files and saves the file in the specified location.

Draft

Appendix E: Virtual Machine Backup (clone) in ASP R6.0.x (KVM on RHEL 8.10)

Virtual Machine Backups (clone) as an alternative to snapshots

Avaya Aura® documentation refers to snapshots at the application level for various procedures. Snapshots apply to a VMware environment.

With the introduction of the alternative hypervisor in Avaya Solutions Platform R6.0.x (KVM on RHEL 8.10), RHEL 8.10 does not support snapshots and Linux does not support issues relating to the use of snapshots.

Virtual machine backup is a similar feature to snapshots. Virtual machine backups use the cloning feature. Use virtual machine backups in place of snapshots for ASP R6.0.x (KVM on RHEL 8.10).

You should only keep backups for a maximum 48 hours in order to ensure sufficient storage is available. You may need to remove them earlier.

Note:

The images and screenshots in this document are for illustration purposes only. The actual user interface may slightly vary due to updates and design changes.

Cloning a Virtual Machine on ASP R6.0.x (KVM on RHEL 8.10)

About this task

Use this procedure to create a clone for backup purposes.

Before you begin

- Ensure there is sufficient space to create the Virtual Machine Backup (clone). Clones are created as “thick provisioned” and require the same size as the virtual machine you are cloning.

- Refer to application documentation for guidelines on storage requirements for different application profiles.
- Shut down the virtual machine for which you are creating a backup (clone). This is a service impacting activity. Perform these steps within a customer-approved maintenance window.

*** Note:**

- 5 You must be root or use `sudo` with `custadm` account for CLI commands, and you must
6 enable Administrative access when using the Cockpit user interface.

*** Note:**

- 7 These clones must be created through the CLI as the Cockpit UI does not support the
8 necessary required options.

Procedure

1. Log in to the KVM Cockpit web console as `custadm` in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

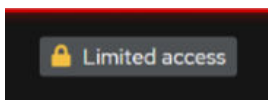


Figure 1: Limited access button

*** Note:**

- 16 You require administrator access in order to view virtual machines. Administrator
17 access is like root access. Ensure that you take care making updates.
3. In the Switch to administrative access window, enter the password for `custadm`.

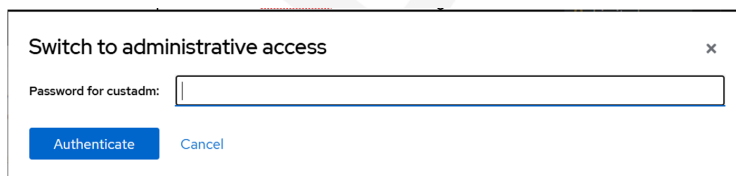
A light gray dialog box with a title bar that says 'Switch to administrative access' and a close button (X). Inside, there is a label 'Password for custadm:' followed by a text input field. Below the input field are two buttons: 'Authenticate' (blue) and 'Cancel' (light gray).

Figure 2: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

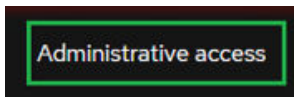


Figure 3: Administrative access button

4. Navigate to **System > Virtual Machines > Storage Pools**.

The Name `guest_images` is a label for `/var/lib/libvirt/images`. If you select `guest_images`, you can see additional information. If you select `Storage Volumes`, you can view all images in the `/var/lib/libvirt/images` directory.

5. Review the images and remove any of them that you no longer use.

Images that do not have a 'Used by' value are typically safe to remove.

6. Confirm that you have the necessary space for your clone.
7. Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Run the following command to obtain a list of all virtual machines:

```
sudo virsh list --all
```

Example output:

```
[custadm@asp130-r660xs-a3lp ~]# sudo virsh list --all
```

Id	Name	State
1	8HDD-RHEL-810-Fiotester2	running
2	8HDD-RHEL810-Fiotester1	running
-	8HDD-RHEL-810-Fiotester3	shut off
-	8HDD-RHEL-810-Fiotester3-Clone	shut off
-	8HDD-RHEL-810-Fiotester3-clone	shut off
-	Agent_Testing	shut off
-	Agent_Testing-Clone	shut off
-	Agent_Testing2	shut off
-	Agent_Testing3	shut off

In this example, the virtual machine `Agent_Testing3` is shut off state, ready for backup (clone).

9. Run the following command to backup (clone) the virtual machine. You must use the `nonsparse` option to ensure the clone is created as thick provisioned.

```
sudo virt-clone --original <Domain-to-be-cloned> --auto-clone --nonsparse
```

Example output:

```
sudo virt-clone --original Agent_Testing3 --auto-clone --nonsparse
Allocating 'RHEL810-agenttestvm3-fat-clone.qcow2' | 50 GB 00:01:06
Clone 'Agent_Testing3-clone1' created successfully.
```

This command creates a backup (clone) with default values. You can create a clone with any name for the virtual machine and QCOW2 labels by specifying a full path and using the following command:

```
sudo virt-clone --original <VM Domain> --name <Clone VM Label> --file /var/lib/libvirt/images/<VM Domain QCOW2 file name>.qcow2 --nonsparse
```

Example for single QCOW2 image:

```

1      sudo virt-clone --original RHEL810-fiotester1 --name RHEL810-
2      fiotester2 --file /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
3      --nonsparse

```

Example for multiple QCOW2 images:

```

5      sudo virt-clone --original Duplex_Active_974
6      --name Duplex_Active_974_CloneTest --file /var/lib/
7      libvirt/images/Duplex_Active_974_CloneTest_system.qcow2
8      --nonsparse --file /var/lib/libvirt/images/
9      Duplex_Active_974_CloneTest_Var_Disk.qcow2 --nonsparse

```

*** Note:**

10 Completion time varies depending on the size of original virtual machine disk.

11 Calculating space for the clone

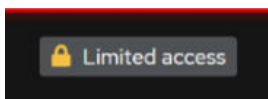
12 About this task

13 Use this procedure to figure out if you have the necessary space for the clone. This example
 14 refers to System Manager but the same information applies to all Avaya Aura® components.

15 You can use the Cockpit user interface to calculate this information. You can also use the
 16 Command Line Interface (CLI). The units of measure may differ. The Cockpit user interface (UI)
 17 uses International Electrotechnical Commission (IEC) values, such as Gibibyte. The CLI uses
 18 International System of Units (SI) values, such as Gigabyte.

19 Procedure

- 20 1. Log in to the KVM Cockpit web console as **custadm** in the following format: `https://<IP`
 21 `address or FQDN of KVM host>:9090`.
- 22 2. For administration actions, on the top-right of the window, click on the **Limited access**
 23 button.



24 **Figure 4: Limited access button**

*** Note:**

26 You require administrator access in order to view virtual machines. Administrator
 27 access is like root access. Ensure that you take care making updates.

- 28 3. In the Switch to administrative access window, enter the password for **custadm**.

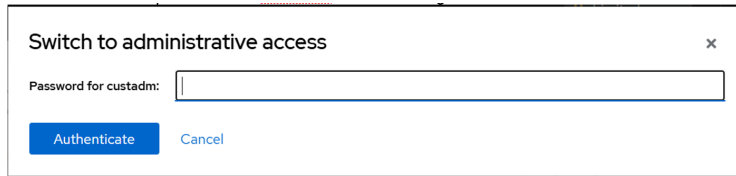


Figure 5: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

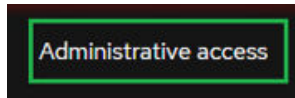


Figure 6: Administrative access button

4. Navigate to **System > Virtual Machines > Storage Pools**.
5. View the information on the **Storage Pools** screen.
6. Divide the amount of used and available space to get the percentage.

In this example, approximately 18% of the available storage is used ($579.51/3299 \sim 18\%$).

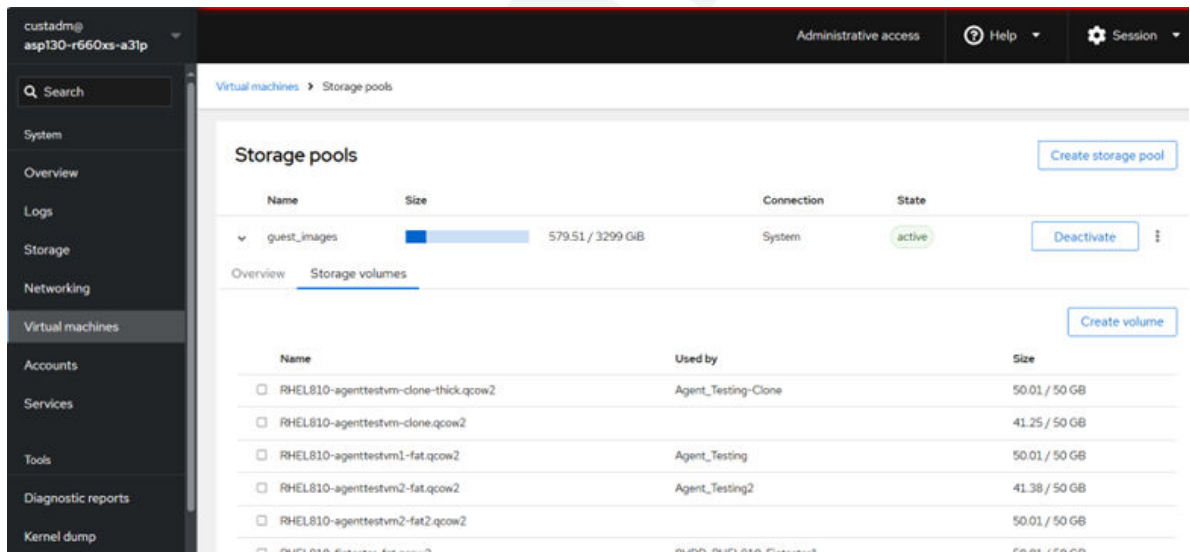


Figure 7: Example size

7. (Optional) Log in to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
8. Change the directory to `/var/lib/libvirt/images` and identify the available space.

In the example below, 18% of available storage is being used on the host.

Example output:

```
[custadm@asp130-r660xs-a31p ~]$ cd /var/lib/libvirt/images
[custadm@asp130-r660xs-a31p images]$ df -h .
```

1	Filesystem	Size	Used	Avail	Use%	Mounted on
2	dev/mapper/vg_system-lv_libvirt	3.3T	580G	2.7T	18%	/var/lib/libvirt

Validating a Virtual Machine Backup (clone)

Procedure

1. Login to the Avaya Solutions Platform R6.0.x Command Line Interface (CLI) as `custadm`.
2. Run the following command to validate the backup (clone):

```
sudo virsh list --all
```

Example output:

```
[custadm@asp130-r660xs-a3lp ~]# sudo virsh list --all
```

Id	Name	State
1	8HDD-RHEL-810-Fiotester2	running
2	8HDD-RHEL810-Fiotester1	running
-	8HDD-RHEL-810-Fiotester3	shut off
-	8HDD-RHEL-810-Fiotester3-Clone	shut off
-	8HDD-RHEL-810-Fiotester3-clone	shut off
-	Agent_Testing	shut off
-	Agent_Testing-Clone	shut off
-	Agent_Testing2	shut off
-	Agent_Testing3	shut off
-	Agent_Testing3-clone	shut off

In this example, the virtual machine `Agent_Testing3-clone` is the cloned virtual machine.

3. Confirm that the clone is thick provisioned by running the following command on the clone and ensuring that the virtual size is the same as the disk size:

```
cd /var/lib/libvirt/images
```

```
sudo qemu-img info <clone name>
```

Example output:

```
cd /var/lib/libvirt/images
```

```
sudo qemu-img info Agent_Testing3-clone.qcow2
```

```
image: Agent_Testing3-clone.qcow2
```

```
file format: qcow2
```

```
virtual size: 50 GiB (53687091200 bytes)
```

```
disk size: 50 GiB
```

```
cluster_size: 65536
```

```
Format specific information:
```

```
compat: 1.1
```

```

1      compression type: zlib
2      lazy refcounts: true
3      refcount bits: 16
4      corrupt: false
5      extended l2: false

```

4. Run the following command to ensure that the virtual machine is cloned with the same disk name that is provided during the backup (clone):

```
sudo virsh domblklist <cloned VM name>_8_1
```

For example, the output of the command appears as follows:

```
hda /var/lib/libvirt/images/RHEL810-fiotester2.qcow2
```

5. Log in to the KVM Cockpit web console as **custadm** in the following format: <https://<IP address or FQDN of KVM host>:9090>.
6. For administration actions, on the top-right of the window, click on the **Limited access** button.

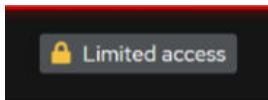


Figure 8: Limited access button

*** Note:**

- 17 You require administrator access in order to view virtual machines. Administrator
- 18 access is like root access. Ensure that you take care making updates.

7. In the Switch to administrative access window, enter the password for **custadm**.

Figure 9: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

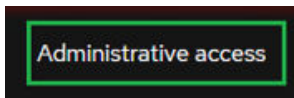


Figure 10: Administrative access button

8. Navigate to **System > Virtual Machines**.

9. View the cloned virtual machine in the virtual machines list.

Virtual machines			Filter by name	State	All	Import VM	Create VM
Name	Connection	State					
8HDD-RHEL-810-Fiorester2	System	Running	Shut down				
8HDD-RHEL-810-Fiorester3	System	Running	Shut down				
8HDD-RHEL810-Fiorester1	System	Running	Shut down				
Agent_Testing	System	Running	Shut down				
Agent_Testing2	System	Running	Shut down				
Agent_Testing3	Original	Shut off	Run				
Agent_Testing3-clone	Cloned VM	Shut off	Run				

Figure 11: Virtual machines list

Rolling back using the Virtual Machine Backup (clone)

About this task

If you experience a problem during an upgrade, you can roll back to a state using the cloned virtual machine.

Procedure

1. Log in to the KVM Cockpit web console as `custadm` in the following format: `https://<IP address or FQDN of KVM host>:9090`.
2. For administration actions, on the top-right of the window, click on the **Limited access** button.

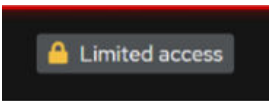


Figure 12: Limited access button

* Note:

- 15 You require administrator access in order to view virtual machines. Administrator
- 16 access is like root access. Ensure that you take care making updates.
3. In the Switch to administrative access window, enter the password for `custadm`.

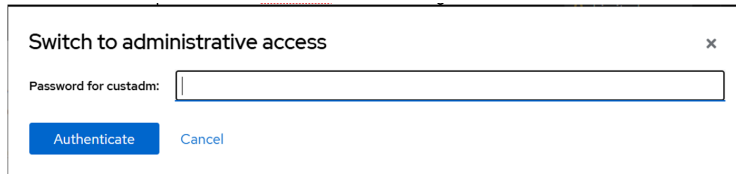


Figure 13: Switch to administrative access

The **Limited access** button on the top-right of the window changes to **Administrative access**.

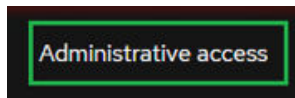


Figure 14: Administrative access button

4. Navigate to **System > Virtual Machines**.

5. Shut down the original virtual machine.

6. Rename the original virtual machine.

For example: `Virtual_Machine_Broken`

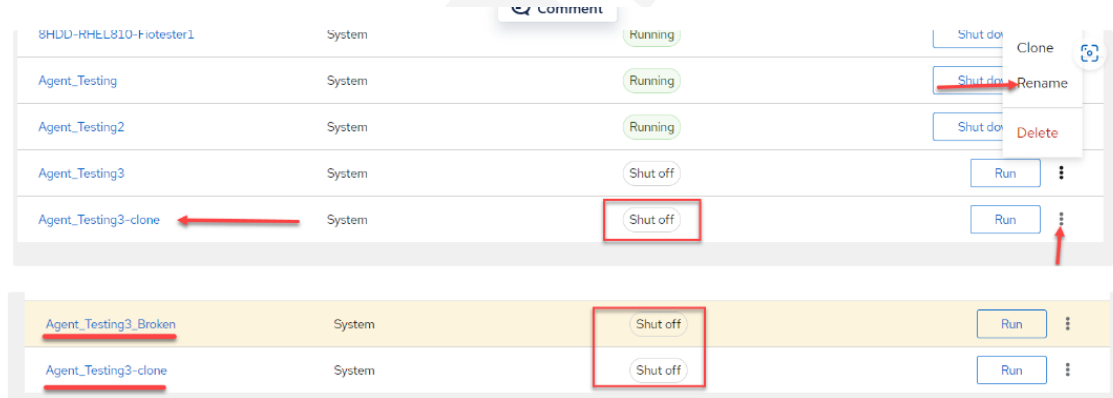


Figure 15: Roll back VM backup

7. While still in a power off state, edit the virtual machine clone Label to match the original virtual machine label. This ensures that the cloned virtual machine becomes the original virtual machine.

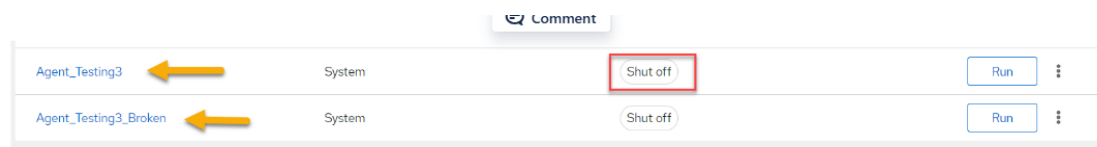


Figure 16: Edit Virtual Machine name

8. Configure the virtual machine that you renamed in step 5 to ensure the network interfaces and state match the broken virtual machine.

For example: `bridge0` and `state = up`

Comment

Type	Model type	MAC address	Source	State
bridge	virtio	52:54:00:b1:6f:b1	Bridge <code>bridge0</code>	up

Add network interface

Unplug Edit

Figure 17: Network interfaces

9. Power on the virtual machine that you renamed in step 5.

Comment

Agent_Testing3	System	Running	Shut down
Agent_Testing3_Broken	System	Shut off	Run

Figure 18: Power on

10. Delete any unused backups.

Appendix F: Security Service Pack

Avaya Aura® Security Service Packs overview

With Avaya Aura® Release 10.1.x, Avaya introduced a common version of Red Hat Enterprise Linux (RHEL) 8.4 or RHEL 8.10 to its Avaya Aura® platform. With the common versions of RHELs, Avaya has also changed how it provides and installs Security Service Packs (SSPs). Following Avaya Aura® applications support RHEL:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Application Enablement Services

* Note:

- Beginning with Communication Manager Release 10.1, security updates (Linux and Kernel) are provided in an SSP. There is no longer a separate Kernel Service Pack (KSP).
- Beginning with Application Enablement Services Release 10.1, Linux Security Updates (LSU) are now provided in an SSP. LSU is no longer available.

SSPs are cumulative for each release. The current SSP for a release includes the fixes from all previous SSPs for that release.

SSPs are applicable for Avaya Aura® Release 10.2.x running on:

- Avaya Solutions Platform 130 Release 5.1.x
- Avaya Solutions Platform S8300 Release 5.1 (For Communication Manager or Branch Session Manager)
- Avaya Solutions Platform 130 Release 6.0 (KVM on RHEL 8.10)
- Customer-provided VMware® certified hardware

* Note:

- SSPs are not applicable for Software-Only deployments.
- SSPs are applicable to Avaya Aura® OVA-based 10.2.x deployments.

SSP file format and command

File format of SSP is as follows:

```
AV-<product name><mainline release version>-RHEL<number>-SSP-<SSP #>-  
<build #>.tar.bz2
```

Where:

- **<product name>**: Name of the application.

For example:

<product name>	Application
CM	Communication Manager
SMGR	System Manager
SM	Session Manager
AES	Application Enablement Services

- **<Mainline release version>**: Mainline release version for the application. For example, 10.1.
- **RHEL <number>**: RHEL version used in the Avaya Aura® application. For example, RHEL 8.4 or RHEL 8.10.
- **SSP-<SSP #>**: A three-digit number that defines the SSP version. For example, the first SSP # is 001.
- **<build #>**: Build number associated with the SSP version. For example, AV-CM10.2-RHEL8.X-SSP-001-05.tar.bz2.

You can use the **av-update-os** command to install SSP and the **av-version** command to view the SSP version running on the application.

SSPs product change notice (PCN) reference

- For more information about Avaya Aura® System Manager 10.2.x SSP - S2 - Software, see PCN2163S.
- For more information about Avaya Aura® Session Manager 10.2.x SSP - S2 - Software, see PCN2161S.
- For more information about Avaya Aura® Communication Manager 10.2.x SSP - S2 - Software, see PCN2159S.
- For more information about Avaya Aura® Application Enablement Services 10.2.x SSP - S2 - Software, see PCN2165S.
- For more information about Avaya Aura® WebLM 10.2.x SSP - S2 - Software, see PCN2167S (For future use upon the release of Avaya Aura® WebLM R10.2.x.)

1 Glossary

2	Fully automated	6	
3	upgrade using	7	
4	Solution Deployment	8	
5	Manager	9	
		10	The fully automated upgrade process includes upgrading a product from earlier release to the latest release by using either Solution Deployment Manager Client or System Manager Solution Deployment Manager. In fully automated upgrade all subsequent steps are executed as a single process, including tasks such as backup, deploy, and post upgrade tasks such as applying patches or service packs.
		11	
		12	For fully automated upgrade using Solution Deployment Manager, the system does not allow to change the IP Address of the application.
		13	Alternatively, you can use the Migration using CLI method.
		14	
		15	To upgrade System Manager, use Solution Deployment Manager Client.
		16	To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.
		17	
18	Migration	19	
		20	The migration process includes changing the hypervisor or hardware while upgrading the application.
		21	
		22	• Migration using CLI: During migration, you need use the data migration utility.
		23	
		24	• Migration using SDM: Migration using Solution Deployment Manager is supported using same IP Address.
		25	For example, from AVP to VMware.
		26	To upgrade System Manager, use Solution Deployment Manager Client. To upgrade applications other than System Manager, use System Manager Solution Deployment Manager.
		27	
		28	
		29	If you want to migrate using different IP Address for the application, use the CLI method.
		30	
31	Update	32	
		33	The update process includes installing patches of an application. For example, security patches, hotfixes, service packs, and feature packs.
34	Upgrade using CLI	35	
		36	The upgrade process includes upgrading a product from earlier release to the latest release without the need to change the server hardware or hypervisor.
		37	

Index

A

accepting new service	131
access log harvesting	152
access to PLDS	43
accessing log harvest	152
accessing port matrix	140
Add Platform	66
adding	
Appliance Virtualization Platform host	60
AVP host	60
ESXi host	60
location	58
software-only platform	63
vCenter to SDM	72
adding ESXi host	60
adding location	58
adding location to host	74
adding NMS Destination	136
adding trusted certificates	46
adding vCenter to SDM	72
alarm configuration	
checklist	136
alarm test	138
analyze inventory	
SDM	51
Appliance Virtualization Platform	
restarting	65
shutdown	64
shutting down	64
application	
edit	67
re-establishing trust	69
restart	69
start	68
stop	68
Application management	57
applications	
preupgrade check	54
archiving logs	151
Avaya Aura application upgrade	101
Avaya Aura® application	
ESXi version	25
KVM version	26
supported servers	22
Avaya InSite Knowledge Base	143
Avaya Solutions Platform 130 Release 5.1 host	
adding	62
Avaya support website	143
avpshutdown.sh	64

B

backup and restore commands	50
Branch Session Manager	38
upgrade	17
Branch Session Manager upgrade	88 , 97
Branch Session Manager upgrade paths	15
browser requirements	37

C

Change IP FQDN	67
changes to platform support	8
Checking EASG status	132
checklist	
alarming configuration	136
clone	158
collection	
delete	141
edit	141
generating PDF	141
sharing content	141
common causes	
application deployment failure	70
Company ID	43
configuration data worksheet	
customer	21
configuring Session Manager	
geographically redundant environment	127
Configuring user settings	43
content	
publishing PDF output	141
searching	141
sharing	141
sort by last updated	141
watching for updates	141
creating	
log harvesting profile	152
creating a role in vCenter	71
creating software library	48
customer configuration data	21

D

data replication	128
default certificates	16
deleting	
location	58
deleting a location	58
deleting vCenter	74
deploy application	57
disabling EASG	132
document changes	9

document purpose	8	file download manager	53
documentation		filling	
Session Manager	139	bulk import spreadsheet	116
documentation center	141	bulk instances	116
finding content	141	finding content on documentation center	141
navigation	141	finding port matrix	140
documentation portal	141		
download software	49, 52, 66	G	
downloading bulk import spreadsheet	115	General Configuration Details	104
		generate an alarm	138
E		Get	
EASG	132	Company ID	43
disabling	132		
enabling	132	H	
EASGManage	133	hardware supported	
edit		System Manager	22
application	67		
edit application	67	I	
Edit Location	59	Import as PEM certificate	46
Edit Platform	66	Import from existing trusted certificates	46
Edit Upgrade Configuration	104	import from file	46
Element Configuration	104	Import using TLS	46
Edit vCenter	75	importing trusted certificates from file	46
editing		installed logins	145
location	58	installing	
vCenter	74	license file	127
editing the location	58	installing Session Manager or Branch Session Manager	
editing vCenter	74	software patches	121
element upgrade	101	installing software patches	121
elements		inventory	
refresh	51	refresh elements	51
enabling			
EASG	133	K	
enabling EASG	132	KB	
Enhanced Access Security Gateway	132	Support site	143
Enrollment Password status	130	KVM version	
Entity Link Connection Status	130	Avaya Aura® application	26
ESXi host			
adding	60	L	
restarting	65	latest software patches	27
ESXi version		license file	
Avaya Aura® application	25	installing	127
		Life cycle management	57
F		Loading and managing site certificate	134
field description		location	
User Settings	44	adding	58
field descriptions		deleting	58
Add Platform	66	editing	58
Edit Location	59	view	57
Edit Platform	66	log harvest; access	152
Map vCenter	75	Log Harvester	
New Location	59		
Preupgrade configuration	55		
Upgrade Configuration	103		
Upgrade Management	101		

Log Harvester (<i>continued</i>)		patchSM (<i>continued</i>)	
new profile field descriptions	152	status	120
log harvester overview	151	verify	120
log harvesting	151	PCN	27
log harvesting profile		PCN updates	149
creating	152	PCNs	
logins		viewing	149
installed	145	PLDS	
M		downloading software	48
managed element		PLDS access to Avaya	43
configuring in SAL Gateway	136	port matrix	140
Map vCenter	72 , 74 , 75	post upgrade checklist	
migrating		Branch Session Manager	126
Appliance Virtualization Platform deployed to Avaya		Session Manager upgrade	126
Solutions Platform S8300 5.1	91	preparing	
Appliance Virtualization Platform installed to Avaya		upgrade	50
Solutions Platform 5.0	93	prerequisites	
Appliance Virtualization Platform to Avaya Solutions		for upgrading application	9
Platform 5.0	94	Session Manager upgrade	20
Appliance Virtualization Platform to Avaya Solutions		preupgrade check	
Platform S8300 5.1	86	applications	54
Vmware to KVM	79 , 81	Preupgrade Configuration	54
migrating session manager and branch session manager		product notification enrollment	150
VMware to KVM	78	product notifications	
migration		e-notifications	150
Vmware to KVM	82 , 83	PSN	27
N		PSN updates	149
Network Management Systems Destinations	135	PSNs	
New Location	59	viewing	149
new service		R	
changing state to accept	131	re-establishing trust	
New vCenter	75	application	69
NMS		SDM elements	69
adding	136	Solution Deployment Manager elements	69
NMS destinations	135	re-establishing trust application	69
note		reestablish	
VM configuration details	79	connection	71
notifications	149	refresh elements in inventory	51
O		release notes for latest software patches	27
optional		removing	
upgrade sequence	30 , 33	Appliance Virtualization Platform host	65
P		Avaya Solutions Platform 130 host	65
patch information	27	ESXi host	65
patchSM		removing location from host	74
commit	120	removing vCenter	74
install	120	replication verification	128
remove	120	resources	
snapshot	120	server	24
		restart	
		application	69
		restart application from SDM	69
		restarting	
		Appliance Virtualization Platform	65
		ESXi host	65
		retrieve harvested log file	151

running maintenance tests [127](#)

S

SAL Gateway
 configuring a managed element [136](#)
SDM elements
 re-establishing trust [69](#)
 searching for content [141](#)
Security Module sanity failure
 troubleshooting [129](#)
Select Flexi Footprint [67](#)
servers supported [22](#)
Session Manager [38](#)
session manager backup
 VMware to KVM [84](#)
Session Manager upgrade [97](#)
 overview [13](#)
Session Manager upgrade paths [15](#)
sharing content [141](#)
shutdown
 Appliance Virtualization Platform [64](#)
shutting down
 AVP [64](#)
snapshot [121](#)
snapshots [155](#), [160](#), [162](#)
SNMP traps [135](#)
software
 download [49](#), [52](#), [66](#)
 software details [38](#)
 software library; add [48](#)
 software library; create [48](#)
 software patches [27](#), [121](#)
 software requirements [24](#)
Solution Deployment Manager [51](#)
 restart application [69](#)
 start application [68](#)
 stop application [68](#)
 supported applications [17](#)
Solution Deployment Manager elements
 re-establishing trust [69](#)
sort documents [141](#)
SSPs [165](#)
start
 application [68](#)
start application from SDM [68](#)
status
 Enrollment Password [130](#)
stop
 application [68](#)
stop application from SDM [68](#)
submitting a request for harvesting log files [153](#)
support [143](#)
supported browsers [37](#)
supported hardware and resources [24](#)
supported servers [22](#)
 Avaya Aura® application [22](#)

supported Session Manager upgrade paths [15](#)

T

testing
 Session Manager instance [127](#)
troubleshooting [128](#)
 Security Module sanity failure Alarms [129](#)
trusted certificates
 add [46](#)

U

upgrade
 alternate method [30](#)
 Branch Session Manager [17](#), [88](#), [97](#), [104](#)
 Session Manager [97](#), [104](#)
 VMware-based Session Manager Release 6.3.22 [100](#)
Upgrade Configuration
 field descriptions [103](#)
Upgrade Configuration Details [104](#)
Upgrade Management
 User Settings [44](#)
upgrade order
 Avaya Aura applications [27](#), [34](#)
 Avaya Aura platform [27](#), [34](#)
 Avaya components [27](#), [34](#)
 Avaya Components [27](#), [34](#)
upgrade path
 software-only [123](#)
upgrade paths
 Branch Session Manager [15](#)
 Session Manager [15](#)
upgrading
 Branch Session Manager instances in bulk [119](#)
Upgrading
 VMware ESXi version [56](#)
upgrading non-edge Branch Session Manager to edge
 Branch Session Manager [114](#)
upgrading Session Manager
 on AWS/GCN/Azure [123](#)
 on IaaS [123](#)
 software-only [123](#)
 using command-line interface [113](#)
 using data migration utility [111](#)
upgrading RHEL 8.4 to RHEL 8.10 [147](#)
User settings
 configure [43](#)
User Settings
 field description [44](#)

V

vCenter
 add [75](#)
 add location [74](#)

vCenter (<i>continued</i>)	
adding	72
deleting	74
edit	75
editing	74
field descriptions	75
manage	74
remove location	74
removing	74
unmanage	74
verify alarm configuration	138
verifying	
data replication	128
videos	142
view	
location	57
software version	33
survivable remote servers	33
view location	57
viewing	
Entity Link Connection Status	130
PCNs	149
PSNs	149
Security Module status	129
virtual machine backups	
creating	155
space	158
virtual machine backups (clone)	
definition	155
rolling back	162
validating	160
VM connection reestablish	71
VMware software requirements	24
 W	
watchlist	141