Avaya Aura® System Manager Overview and Specification

Release 7.1.3
Issue 5
October 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Contents

Chapter 1: Introduction

Purpose

This document describes tested characteristics and capabilities of System Manager, including feature descriptions, interoperability, performance specifications, security, and licensing requirements.

This document is intended for anyone who wants to gain a high-level understanding of System Manager features, functions, capacities, and limitations within the context of solutions and verified reference configurations.

Change history

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

Issue	Date	Summary of changes
5	October 2018	For Release 7.1.3, updated the Trust Management on page 51 section.
4	May 2018	For Release 7.1.3, added the following section: • New in System Manager Release 7.1.3 on page 8 • Virtual machine report on page 37 • Security hardening options on page 37 For Release 7.1.3, updated the Appliance Virtualization Platform overview on page 40 section.
3	December 2017	For Release 7.1.2, added the following section: • New in System Manager Release 7.1.2 on page 9
2	August 2017	For Release 7.1.1, added the following sections: • New in System Manager Release 7.1.1 on page 11 • Avaya Aura on Kernel-based Virtual Machine overview on page 45
1	May 2017	Release 7.1 document.

Chapter 2: System Manager Overview

System Manager overview

Avaya Aura® System Manager is a central management system that provides a set of shared management services and a common console. All shared and element specific management for Avaya Aura® applications that System Manager supports is done from the common console. System Manager provides the following key capabilities:

- Centralized software management solution to support deployments, migrations, upgrades, and updates to the suite of Avaya Aura® applications
- Avoid duplicate data entry through shared management services
- Centralized access to all Avaya Aura® applications through a browser-based Avaya management console with single sign on
- Optimize IT skill sets with consistency of management functions across Avaya solutions
- Integration with enterprise IT infrastructure, such as identity management, authentication, authorization, security, and enterprise directory

You can download System Manager from the Avaya Support website at http://support.avaya.com or order the System Manager software DVD.

Related links

New in System Manager Release 7.1.3 on page 8
New in System Manager Release 7.1.2 on page 9
New in System Manager Release 7.1.1 on page 11
New in System Manager Release 7.1 on page 11

New in System Manager Release 7.1.3

Avaya Aura® System Manager Release 7.1.3 supports the following new features and enhancements:

- System Manager supports cluster level alarms.
- For the 9641SIP template type, an **Attendant** check box is available:
  - On the New/Edit/View/Duplicate User Profile pages in the CM Endpoint Profile section.
  - On **General Options** tab on the New/Edit/View/Duplicate/ Endpoint, Global Endpoint Change, and New Endpoint Template pages.

If you select the **Attendant** check box, you can administer the endpoint as an attendant.

- For the SIP template type, the **SIP URI** field is available:
  - On the New/Edit/View/Duplicate User Profile pages in the CM Endpoint Profile section.
  - On the New/Edit/View/ Hunt Group page.
- Bulk import and export of **Endpoints**, **Coverage Paths**, and **Hunt Groups** using System Manager. For adding, deleting and updating **Endpoints**, **Coverage Paths**, and **Hunt Groups** in bulk, you can download a pre-loaded excel **<Excel template file name>.xlsx** file from **More Actions** > **Download Excel Template** on the following pages:
  - For Endpoints: **Elements** > **Communication Manager** > **Endpoints** > **Manage Endpoints** page
  - For Coverage Path: **Elements** > **Communication Manager** > **Coverage** > **Coverage Path** page
  - For Hunt Group: **Elements** > **Communication Manager** > **Groups** > **Hunt Group** page
- Using the **`securityHardeningOptions`** command, you can enable or disable one or more than one security hardening options. The security hardening options that you can:
  - Enable are selinux, audit, fips, aide, TLSv1, TLSv1.1, and TLSv1.2.
  - Disable are selinux, audit, and aide.
- Using the `/swlibrary/reports/generate_report.sh` script, you can generate the report of virtual machines that are installed on the Appliance Virtualization Platform host.
- Using **More Actions** > **Snapshot Manager** on the **Hosts** tab, you can delete the virtual machine snapshots that are running on the Appliance Virtualization Platform host.
- Avaya Technician Certificate-based Authentication and **Avaya Technician Access Level** are not supported.

Related links

System Manager overview on page 8

New in System Manager Release 7.1.2

Avaya Aura® System Manager Release 7.1.2 supports the following new features and enhancements:

- Management of trunk group by using System Manager enhanced editor. Using the enhanced editor, you can:
  - Add, edit, view, and delete trunk group.
  - Schedule the addition and deletion of trunk group for a specific time.
  - Assign permissions to add, edit, view, and delete the trunk group for a user.
- Bulk import and export of Vector Directory Numbers (VDNs) using System Manager. For adding, deleting and updating VDNs in bulk, you can download a pre-loaded excel

`VdnData.xlsx` file from **More Actions** > **Download Excel Template** on the **Elements** > **Communication Manager** > **Call Center** > **Vector Directory Number** page.

- Export of the added, updated, or deleted user-related data for the specific delta period. You can export the delta users from **More Actions** > **Export Delta Users** on the **Users** > **User Management** page.
- Migration of the System Platform-based system and elements to Appliance Virtualization Platform remotely by:
  - Using the **Migrate With AVP Install** check box through System Manager Solution Deployment Manager.
  - Importing the `AVP_Bulk import spread sheet.xlsx` spreadsheet through System Manager Solution Deployment Manager.
- System Manager Solution Deployment Manager automates the migration of Communication Manager LSPs to Release 7.1.2.
  - Communication Manager LSPs from Release 6.x Templates: Simplex Survivable Remote and Survivable Remote. This can include Communication Manager, Utility Services, or Branch Session Manager.
  - Communication Manager Release 5.2.1 bare Metal on S8300D

  Hardware Supported: S8300D, S8300E, and Common Server (1, 2 and 3) when configured as an LSP
- New System Manager Solution Deployment Manager capabilities:
  - Bulk Provisioning File (Excel): ability to import configuration parameters in bulk for upgrading or migrating to Appliance Virtualization Platform remotely.
  - Appliance Virtualization Platform upgrade integrated into the functions: Software Library, Analyze, Pre-upgrade checks, Logging, and RBAC.
- Configuration of WebLM Server that hosts the Appliance Virtualization Platform Release 7.1.2 license file. To fetch the license file for the Appliance Virtualization Platform host, you can configure the WebLM Server details under **More Actions** > **WebLM Configuration** on the **Hosts** tab.
- While updating the Appliance Virtualization Platform host, you must accept the End User License Agreement.
- Remote access of System Manager Web console and Command Line Interface by using EASG Login credentials for Avaya Technician.

Related links

System Manager overview on page 8

New in System Manager Release 7.1.1

Avaya Aura® System Manager Release 7.1.1 supports the following new features and enhancements:

- Management of hunt group by using System Manager enhanced editor. Using the enhanced editor, you can:
  - Add, edit, view, and delete hunt group.
  - Schedule the addition and deletion of hunt group for a specific time.
- Assign permissions to add, edit, view, and delete the hunt group and attributes of hunt group for a user. You can also specify the extension range for adding hunt group extensions.
- If Platform Service Controller (PSC) is configured to facilitate the SSO authentication service to a vCenter, then you can provide the IP or FQDN of PSC at the time of adding a vCenter to Solution Deployment Manager.
- For generating the kickstart file for the Appliance Virtualization Platform installation, the **Confirm Password** field is added on the Generate AVP Kickstart page.

Related links

System Manager overview on page 8

New in System Manager Release 7.1

Avaya Aura® System Manager Release 7.1 supports the following new features and enhancements:

- From System Manager Release 7.1, the root user account is disabled. You must log in with the administrator privilege account that you create during deployment or upgrade of System Manager. You can use the same account for performing various operations on System Manager.
- Security profiles to enable hardened security modes:
  - Standard Grade Hardening
  - Commercial Grade Hardening
  - Military Grade Hardening
- Support for IPv6 addresses with dual stack.
- The System Manager system that has security hardening enabled, displays the login warning banner message.
- Authentication based on certificate to facilitate password-less login for System Manager user interface and CLI access.
- System Manager backup encryption based using a global password.

- Audit logging configuration to notify the System Manager administrator and perform the configured action in certain cases:
    - Audit failure
    - 75% occupation of audit partition
    - 90% occupation of audit partition
- Prerequisite for enabling and configuring Geographic Redundancy:
    1. Adding the primary System Manager server as Certificate Revocation List (CRL) in the secondary System Manager server.
    2. Adding trusted certificate of primary System Manager server to secondary System Manager server.
- Enhancements to Upgrade Management in System Manager:
    - Upgrade rollback option for System Manager instance those are present on the same host.
    - OVA, Data migration, and Service or Feature Pack file selection from **URL**, **S/W Library**, or **Browse**.
- When upgrading System Manager through CLI, you can use the different network parameters to configure the new system. However, the virtual FQDN (vFQDN) must be same on the new system as you recorded on the existing system.

  While restoring backup on the new system, you must use the same network and system parameters of the old system from which you have taken the backup. This is applicable for both regular backup/restore and cold standby procedures.
- Support for Remote Syslog server details configuration in System Manager:
    - Adding, editing, and deleting Syslog receiver configuration.
    - Viewing and pushing the virtual machine system log to the configured Syslog server.
- Regeneration of Symmetric and Asymmetric data protection keys in case of outdated or compromised keys.
- OVA signing to digitally sign OVAs to ensure the file integrity.
- Validation of file format during operations, such as uploading certificates, upgrades, and bulk importing users. System Manager filters uploaded files based on the file extension and mime type or bytes in the file.
- Using System Manager Web console, create kickstart file to install Avaya Virtualization Platform.
- For generating the new license file, the value of **Primary Host ID** is now 14 characters.

Related links

System Manager overview on page 8
Third-party certificate support on page 13
Audit Logging on page 13
Geographic Redundancy configuration prerequisites on page 13
IPv6 Support on page 13

Dual stack support on page 14

Enhanced Access Security Gateway (EASG) overview on page 14

Third-party certificate support

With support for third-party certificates, you can use third-party signed certificates in System Manager. A Certificate Signing Request (CSR) needs to be generated and shared with the third-party.

After the third party signs the CSR, the certificate is valid. Third-party certificates can be used for application on Avaya Virtualization Platform. These certificates can also be used for certificate—based and common access card-based authentications.

Related links

New in System Manager Release 7.1 on page 11

Audit Logging

Using the audit logging configuration in System Manager 7.1, the system can notify the System Manager administrator and perform the configured action during one or all of the following events:

- Audit failure
- 75% occupation of audit partition
- 90% occupation of audit partition

Related links

New in System Manager Release 7.1 on page 11

Geographic Redundancy configuration prerequisites

With System Manager 7.1, the System Manager administrator must perform the following in sequence before enabling and configuring Geographic Redundancy:

1. Adding the primary System Manager server as Certificate Revocation List (CRL) in the secondary System Manager server.
2. Adding trusted certificate of primary System Manager server to secondary System Manager server.

Related links

New in System Manager Release 7.1 on page 11

IPv6 Support

In Release 7.1, System Manager supports IPv6 addresses with dual stack capabilities. System Manager administrator can configure IPv6 addresses for features such as Geographic Redundancy, Certificates with IPv6 address, System Upgrade, and Discovery of network elements.

Related links

New in System Manager Release 7.1 on page 11

Dual stack support

System Manager 7.1 now supports dual stack, which involves nodes that are capable of handling both IPv4 and IPv6 addresses simultaneously. For applications with management interface over both IPv4 and IPv6, System Manager will support only IPv4 addresses until explicitly reconfigured to support IPv6 addresses.

Related links

New in System Manager Release 7.1 on page 11

Enhanced Access Security Gateway (EASG) overview

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

Related links

New in System Manager Release 7.1 on page 11

Feature description

Overview

The following sections provide a brief description of the functionality of the feature that System Manager provides in support for various Avaya products. For detailed information on the services available for a specific Avaya product, see the interoperability table in the *System Manager 7.x Product Offer Definition* on the Avaya Support website at http://support.avaya.com.

Related links

New in System Manager Release 7.1 on page 11

Common console

The common console is a common management interface for managing various applications in System Manager. The common console is a framework for the aggregation of management presentation views. The common console framework supports dynamic extendibility and contraction as you add or remove management applications. You can use the Web management console in a variety of scenarios ranging from product-specific management to suite management. The different scenarios can leverage the common look-and-feel, common components, and the behavior.

Related links

New in System Manager Release 7.1 on page 11

Solution Deployment Manager

Solution Deployment Manager overview

Solution Deployment Manager is a centralized software management solution in System Manager that provides deployments, upgrades, migrations, and updates to Avaya Aura® applications.

Solution Deployment Manager supports the operations on customer Virtualized Environment and Avaya Aura® Virtualized Appliance model.

Solution Deployment Manager provides the combined capabilities that Software Management, Avaya Virtual Application Manager, and System Platform provided in earlier releases.

From Release 7.1 and later, Solution Deployment Manager supports migration of Virtualized Environment-based 6.x and 7.0.x applications to Release 7.1 and later in customer Virtualized Environment.

Release 7.0 and later supports a standalone version of Solution Deployment Manager, the Solution Deployment Manager client. For more information, see *Using the Solution Deployment Manager client*.

System Manager is the primary management solution for Avaya Aura® Release 7.0 and later applications.

System Manager with Solution Deployment Manager runs on:

- Avaya Aura® Virtualized Appliance: Contains a server, Appliance Virtualization Platform, and Avaya Aura® application OVA. Appliance Virtualization Platform includes a VMware ESXi 6.0 hypervisor.

  From Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.
- Customer-provided Virtualized Environment solution: Avaya Aura® applications are deployed on customer-provided, VMware® certified hardware.

With Solution Deployment Manager, you can perform the following operations in Virtualized Environment and Avaya Aura® Virtualized Appliance models:

- Deploy Avaya Aura® applications.
- Upgrade and migrate Avaya Aura® applications.
- Download Avaya Aura® applications.
- Install service packs, feature packs, and software patches for the following Avaya Aura® applications:
  - Communication Manager and associated devices, such as gateways, media modules, and TN boards.
  - Session Manager
  - Branch Session Manager
  - Utility Services
  - Appliance Virtualization Platform, the ESXi host that is running on the Avaya Aura® Virtualized Appliance.

The upgrade process from Solution Deployment Manager involves the following key tasks:

- Discover the Avaya Aura® applications.
- Refresh applications and associated devices, and download the necessary software components.
- Run the preupgrade check to ensure successful upgrade environment.
- Upgrade Avaya Aura® applications.

- Install software patch, service pack, or feature pack on Avaya Aura® applications.

For more information about the setup of the Solution Deployment Manager functionality that is part of System Manager 7.x, see *Avaya Aura® System Manager Solution Deployment Manager Job-Aid*.

Related links

New in System Manager Release 7.1 on page 11

Capability comparison between System Manager Solution Deployment Manager and the Solution Deployment Manager client

Centralized Solution Deployment Manager	Solution Deployment Manager client
Manage virtual machine lifecycle	Manage virtual machine lifecycle
Deploy Avaya Aura® applications	Deploy Avaya Aura® applications
Deploy hypervisor patches only for Appliance Virtualization Platform	Deploy hypervisor patches only for Appliance Virtualization Platform
Upgrade Avaya Aura® applications Release 7.x supports upgrades from Linux-based or System Platform-based to Virtualized Environment or Appliance Virtualization Platform. Release 7.1 and later supports Virtualized Environment to Virtualized Environment upgrades.	Upgrade System Platform-based System Manager
Install software patches for Avaya Aura® applications excluding System Manager application	Install System Manager patches
Discover Avaya Aura® applications	Deploy System Manager
Analyze Avaya Aura® applications	-
Create and use the software library	-

Related links

New in System Manager Release 7.1 on page 11

Solution Deployment Manager client

For the initial System Manager deployment or when System Manager is inaccessible, you can use the Solution Deployment Manager client. The client can reside on the computer of the technician. The Solution Deployment Manager client provides the functionality to install the OVAs on an Avaya-provided server or customer-provided Virtualized Environment.

A technician can gain access to the user interface of the Solution Deployment Manager client from the web browser.

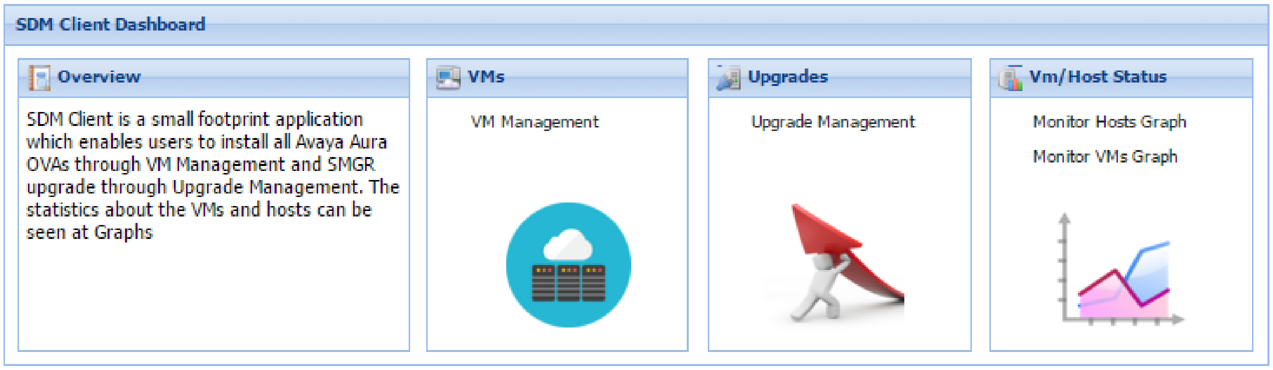
Use the Solution Deployment Manager client to:

- Deploy System Manager and Avaya Aura® applications on Avaya appliances and Virtualized Environment.
- Upgrade System Platform-based System Manager.
- Upgrade Virtualized Environment-based System Manager from Release 7.0.x to Release 7.1 and later.

- Install System Manager software patches, service packs, and feature packs.
- Configure Remote Syslog Profile.
- Create Appliance Virtualization Platform Kickstart file.
- Install Appliance Virtualization Platform patches.
- Restart and shutdown the Appliance Virtualization Platform host.
- Start, stop, and restart a virtual machine.
- Change the footprint of Avaya Aura® applications that support dynamic resizing. For example, Session Manager and Avaya Breeze™.

Note:

You can deploy or upgrade the System Manager virtual machine only by using the Solution Deployment Manager client.



SDM Client is a small footprint application which enables users to install all Avaya Aura OVAs through VM Management and SMGR upgrade through Upgrade Management. The statistics about the VMs and hosts can be seen at Graphs

Figure 1: Solution Deployment Manager client dashboard

Related links

[New in System Manager Release 7.1](#) on page 11
[Solution Deployment Manager client capabilities](#) on page 17

Solution Deployment Manager client capabilities

The Solution Deployment Manager client provides the following capabilities and functionality:

- Runs on the technician computer on the following operating systems:
  - Windows 7, 64-bit Professional or Enterprise
  - Windows 8.1, 64-bit Professional or Enterprise
  - Windows 10, 64-bit Professional or Enterprise
- Supports the same web browsers as System Manager.
- Provides the user interface with similar look and feel as the central Solution Deployment Manager in System Manager.
- Supports deploying the System Manager OVA. The Solution Deployment Manager client is the only option to deploy System Manager.

- Supports Flexible footprint feature. The size of the virtual resources depends on the capacity requirements of the Avaya Aura® applications.
- Defines the physical location, Appliance Virtualization Platform or ESXi host, and discovers virtual machines that are required for application deployments and virtual machine life cycle management.
- Manages lifecycle of the OVA applications that are deployed on the ESXi host. The lifecycle includes start, stop, reset virtual machines, and establishing trust for virtual machines.
- Deploys the Avaya Aura® applications that can be deployed from the central Solution Deployment Manager for Avaya Aura® Virtualized Appliance and customer Virtualized Environment. You can deploy one application at a time.
- Configures application and networking parameters required for application deployments.
- Supports the local computer or an HTTP URL to select the application OVA file for deployment. You do not need access to PLDS.
- Supports changing the hypervisor network parameters, such as, IP Address, Netmask, Gateway, DNS, and NTP on Appliance Virtualization Platform.
- Supports installing patches for the hypervisor on Appliance Virtualization Platform.
- Supports installing software patches, service packs, and feature packs only for System Manager.

  Note:

  > To install the patch on a System Manager virtual machine, the Solution Deployment Manager client must be on the same version as of patch. For example, if you are deploying the patch for System Manager Release 7.1.1, you must use the Solution Deployment Manager client Release 7.1.1.

  Avaya Aura® applications must use centralized Solution Deployment Manager from System Manager to install software patches, service packs, and feature packs or the application Command Line Interface or Web pages.
- Configure Remote Syslog Profile.
- Create Appliance Virtualization Platform Kickstart file.

Related links

Solution Deployment Manager client on page 16

Solution Deployment Manager

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

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

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3

- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8
- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

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

- Linux-based Communication Manager 5.x and the associated devices, such as Gateways, TN boards, and media modules.

  Note:

  In bare metal Linux-based deployments, the applications are directly installed on the server and not as a virtual machine.
- Hardware-based Session Manager 6.x
- System Platform-based Communication Manager
  - Duplex CM Main / Survivable Core with Communication Manager
  - Simplex CM Main / Survivable Core with Communication Manager, Communication Manager Messaging, and Utility Services
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded CM Main with Communication Manager, Communication Manager Messaging, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
- System Platform-based Branch Session Manager
  - Simplex Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services
  - Embedded Survivable Remote with Communication Manager, Branch Session Manager, and Utility Services

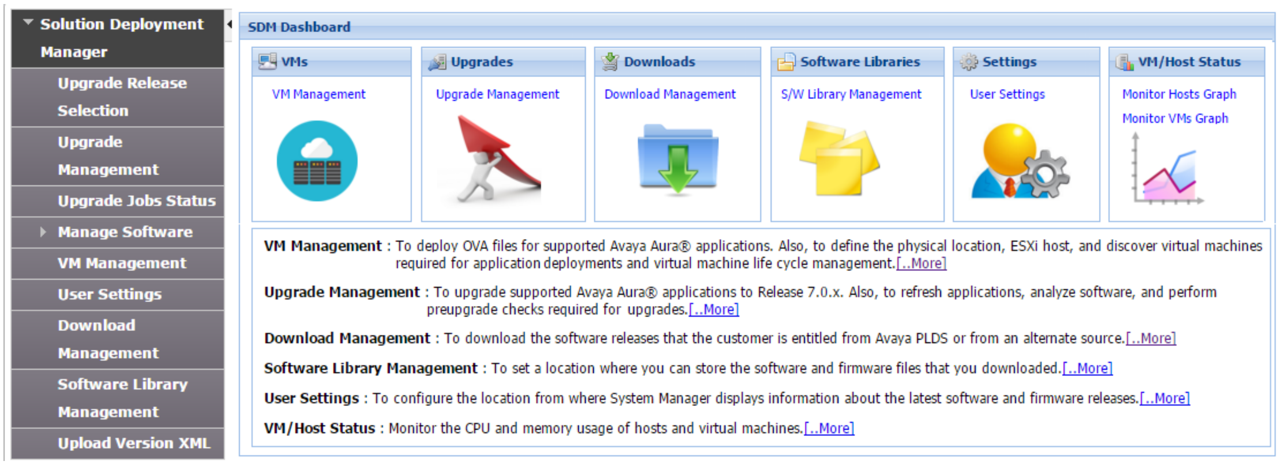
Note:

However, you must manually migrate Services virtual machine that is part of the template.

The centralized deployment and upgrade process provide better support to customers who want to upgrade their systems to Avaya Aura® Release 7.1.3. The process reduces the upgrade time and error rate.

Solution Deployment Manager dashboard

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



VM Management : To deploy OVA files for supported Avaya Aura® applications. Also, to define the physical location, ESXi host, and discover virtual machines required for application deployments and virtual machine life cycle management.[..More]

Upgrade Management : To upgrade supported Avaya Aura® applications to Release 7.0.x. Also, to refresh applications, analyze software, and perform preupgrade checks required for upgrades.[..More]

Download Management : To download the software releases that the customer is entitled from Avaya PLDS or from an alternate source.[..More]

Software Library Management : To set a location where you can store the software and firmware files that you downloaded.[..More]

User Settings : To configure the location from where System Manager displays information about the latest software and firmware releases.[..More]

VM/Host Status : Monitor the CPU and memory usage of hosts and virtual machines.[..More]

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 7.0** or **6.3.8** as the target upgrade. Release 7.1.3 is the default upgrade target.
- **Manage Software**: To analyze, download, and upgrade the IP Office, Unified Communications Module (UCM) and IP Office Application Server firmware. Also, you can view the status of the firmware upgrade process.
- **VM Management**: To deploy OVA files for the supported Avaya Aura® application.
    - Configure Remote Syslog Profile.
    - Generate the Appliance Virtualization Platform Kickstart file.
- **Upgrade Management**: To upgrade Communication Manager that includes TN boards, media gateways and media modules, Session Manager, Communication Manager Messaging, Utility Services, Branch Session Manager, WebLM to Release 7.1.3.
- **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 `version.xml` file to perform upgrades.

Related links

[New in System Manager Release 7.1](#) on page 11

Automated upgrades and migrations of Avaya Aura® applications

From System Manager Release 7.1.3, several Avaya Aura® applications support an automated migration path that the central System Manager Solution Deployment Manager facilitates. The migration process includes situations such as:

- Changing the server, operating system, and the hypervisor.
- Creating a backup and restoring a backup in addition to the normal upgrade process for the application.

The following are the objectives of the Avaya Aura® automated upgrade and migration:

- Move from a manual step-by-step procedure that is performed on the application server to an automated migration procedure on a centralized System Manager.
- Eliminate the time spent in waiting for each migration step to an automated sequencing of tasks with the application migration events automatically running in the background.
- Move from multiple manual tasks that require human intervention and assessment that might be error prone to reliable integrated checks that assess and confirm migration readiness.

Release 7.1.3 and later support automated migrations for:

- System Platform-based Communication Manager Release 6.x and Branch Session Manager Release 6.x
- Linux-based Session Manager Release 6.x and Communication Manager Release 5.2.1

The automated migration functionality applies to the appliance offer provided by Avaya and the customer-provided Virtualized Environment solution.

Related links

[New in System Manager Release 7.1](#) on page 11

Supported servers

In the Avaya Aura® Virtualized Appliance model, Solution Deployment Manager supports the following servers for deployments and upgrades to Release 7.0 and later:

- Dell™ PowerEdge™ R610
- HP ProLiant DL360 G7
- Dell™ PowerEdge™ R620
- HP ProLiant DL360p G8
- Dell™ PowerEdge™ R630
- HP ProLiant DL360 G9

For fresh installations, use Dell™ PowerEdge™ R630 or HP ProLiant DL360 G9.

Related links

[New in System Manager Release 7.1](#) on page 11

Out of Band Management in System Manager

Out of Band Management is two physically or logically separated network connections or both that connects to a private management network of the customer. The network connection provides secure management and administration of Avaya products. With Out of Band Management, you can separate the management network and data network traffic to System Manager.

System Manager provides the following network interfaces:

- The regular eth0 interface that was present in releases earlier than System Manager Release 7.1.3, is called the Management interface or Out of Band Management interface. The IP address is called as the Management IP address. The Management interface is mandatory for configuration.

  The following are the examples of System Manager Management network traffic:

  - Database replication with Session Manager
  - Element management. For example, Session Manager, Communication Manager, and Avaya Breeze™.
  - User management
  - Solution deployment, upgrades, and software patch install
- If Out of Band Management is enabled, then the public interface is configured with Public IP address and used for the nonmanagement traffic. This is an optional configuration.

  The following are the examples of System Manager nonmanagement or public network traffic:

  - End-user self-provisioning
  - Client devices getting certificates through SCEP
  - Tenant Management

Out of Band Management configuration persists across System Manager upgrades, updates, and restarts.

For configuring Out of Band Management in System Manager, System Manager must be installed on an Appliance Virtualization Platform host that is configured with Out of Band Management. Out of Band Management is enabled during the deployment of Appliance Virtualization Platform.

Note:

Once OOBM is enabled on System Manager, public interface eth1 is no longer reachable using ping command from other systems that are present in a public network. However, System Manager can reach other systems on a public interface.

Out of Band Management in a Geographic Redundancy setup

When you configure Geographic Redundancy, provide Management network details only. Validation fails if you configure Geographic Redundancy with Public network details. In Geographic Redundancy setup, you do not disable or enable Out of Band Management on both primary and secondary System Manager virtual machine. You can enable Out of Band

Management on the primary System Manager virtual machine and disable Out of Band Management on the secondary System Manager virtual machine, and vice versa.

Restoring System Manager backup

While restoring backup on System Manager with different Out of Band Management network details, the restore operation fails at validation phase.

Tenant Management on Out of Band Management-enabled System Manager

By default, the Multi Tenancy feature is disabled on System Manager when Out of Band Management is enabled. You must enable Multi Tenancy on Out of Band Management-enabled System Manager for the Tenant Management administrator to manage tenant users.

Related links

New in System Manager Release 7.1 on page 11

Geographic Redundancy

The System Manager Geographic Redundancy service replicates the Avaya Aura® element support for two geographically distant System Manager sites with separate subnetworks and across a WAN so that the System Manager management services can change from one site to another when one of the sites or servers fails. The System Manager Geographic Redundancy sites are set up in pairs with each site in a System Manager standalone or System Manager HA configuration. You can designate one server from the pair as the primary System Manager server and the other as the secondary System Manager server.

In normal operation also called sunny-day scenario, the primary System Manager provides all element administration and automatically replicates the administrative changes made on the primary System Manager server to the secondary System Manager server on a batch transaction basis. The secondary System Manager functions in the warm standby mode or the read-only mode and provides a subset of System Manager services, such as the System Manager Geographic Redundancy status or statistics, Inventory, and Authentication and Authorization.

In the event of catastrophic failure or split network, also called rainy-day scenario, you can activate the System Manager server that you designated as secondary to assume full management of all supported Avaya Aura® elements. The elements that support the Active-Standby mode include Avaya Aura® Session Manager and Avaya Aura® Communication Manager. Geographic Redundancy-unaware elements might require manual intervention to gain services from the secondary System Manager server that is active.

The primary and the secondary System Manager servers can be in active mode in the split network scenarios.

After deactivation of the secondary System Manager server, the system administrator selects the database of the primary or the secondary System Manager server as the master database. The System Manager feature provides tools to select the database. After the database recovery and replication, the System Manager Geographic Redundancy servers revert to the normal operation mode, Active-Standby.

Related links

New in System Manager Release 7.1 on page 11

Data Replication Service

Data Replication Service (DRS) replicates data stored on the System Manager server to other element nodes or the slave nodes. DRS uses and extends SymmetricDS as the underlying mechanism for data replication.

SymmetricDS is an asynchronous data replication software that supports multiple subscribers and bi-directional synchronization. SymmetricDS uses Web and database technologies to replicate tables between relational databases in near real time. The system provides several filters while recording the data, extracting the data that has to be replicated to a slave node, and loading the data on the slave node.

Databases provide unique transaction IDs to rows that are committed as a single transaction. SymmetricDS stores the transaction ID along with the data that changed, so that it can play back the transaction at the destination node exactly the way it happened. This means that the target database maintains the same integrity as the source.

DRS provides a mechanism wherein elements can specify their data requirements in an XML document. On the basis of the XML document, DRS creates database triggers on the specified application tables and captures the database events for delivery to other element nodes. The client nodes then fetch these database events.

Data replication happens in two distinct phases:

- Full-sync. This is the initial replication phase, wherein whatever data the replica node requests is replicated to the client node.
- Regular-sync. This is the phase after full-sync, wherein subsequent change events are replicated to the replica node.

DRS supports the following modes of replication:

- Replication in Repair mode. In the repair mode, DRS replicates all of the requested data from the master database to the database of the replica node. Repair should only be necessary if there is a post-install failure of DRS.
- Automatic synchronization mode. After the database of the replica node is loaded with the requested data, the subsequent synchronizations of the master database and the replica database occur automatically. DRS replicates only the data that has been updated since the last replication. Automatic synchronization is a scheduled activity and occurs after each fixed interval of time as set in the configuration files.

The data from the master database is sent to the replica node in batches. DRS creates replication batches whenever the data in the master database is added, modified, and deleted.

Using DRS, you can:

- View replica nodes in a replica group.
- Repair the replica nodes that are not synchronized. The repair action replicates the required data from System Manager.

Related links

New in System Manager Release 7.1 on page 11

Manage users, public contacts, and shared address

Manage users

User Management (UPM) is a shared service that supports a logically centralized data store. Applications can gain access to the data store using System Manager Web Console and obtain the user information that applications need. Administrators or end users do not need to provide user information for each application.

UPM uses data synchronization to achieve a single-point user administration. UPM synchronizes a user data event that is generated at the application level with the central user space and other connected applications. If an enterprise directory is connected, then UPM maintains synchronization at the enterprise level. UPM adapts to the changes that occur in the enterprise directory, specifically additions, deletions, and modifications.

Manage public contacts

As an administrator, you can define public contacts of users in System Manager for an enterprise. You can share the public contacts with all the users in System Manager.

Manage shared address

You can manage the shared address of the users in the enterprise. All users in the enterprise share the common addresses. As an administrator, you can create a new shared address, modify, and delete an existing shared address.

Related links

New in System Manager Release 7.1 on page 11

Fault management

The Fault management service presents the status of alarms, traps, and notifications received by System Manager and System Manager components, and the other elements that are integrated with the System Manager SAL agent. The Fault management service maps events to alarms and tracks the state of alarms. Using the Fault Management service, you can acknowledge and clear alarms.

The Alarm management service provides a central point for receiving alarms that System Manager and other components generate. The Alarm management service supports alarm monitoring, acknowledgement, configuration, clearing, and retiring. You can also browse System Manager for historical alarm events.

Related links

New in System Manager Release 7.1 on page 11

Logging service

The Logging service provides configuration capabilities and overall management of logs. The Logging service receives and stores log events and harvests file-based logs or local database logs. The log viewer is integrated with the common console to provide consistent presentation of log messages for System Manager and the adopters.

The log viewer displays a list of logs where you can view the details of each log, search for logs, and filter specific logs. The log details include information about the event that generates the log, the severity level of the log. You can search logs based on search conditions and set filters to view logs that match the filter criteria.

Related links

New in System Manager Release 7.1 on page 11

Log Harvester

The Log Harvester service manages the retrieval, archival, and analysis of harvested log files stored in hosts or elements on which Serviceability Agent is enabled. The Serviceability Agent harvests the logs and sends the harvested logs to the Logging service through HTTPS. The logging service identifies a successful harvest request related to a harvest profile, 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 computer or on 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.

Related links

New in System Manager Release 7.1 on page 11

Scheduler

The Scheduler service provides a generic job scheduling service for System Manager and the adopting products. The Scheduler service provides an interface to execute a task on demand or on a periodic basis. You can schedule a job to generate an output immediately or set the frequency of the task execution to run on a periodic basis. You can modify the frequency for a periodic job schedule any time. After you define a task or a job, System Manager creates instances of the task, monitors the execution of the task, and updates the status of the task.

Scheduled jobs can be of three types: system scheduled, admin scheduled, and on-demand.

Related links

New in System Manager Release 7.1 on page 11

Bulk import and export

In System Manager, you can bulk import and export user profiles and global settings. To import data in bulk, you must provide an XML file or an Excel file as input file. System Manager validates any file that you upload during the bulk import operation.

System Manager filters uploaded files based on file extension and mime type or bytes in the file.

The system exports the data to an XML file and an Excel file. The System Manager database stores the imported user profiles and global settings data.

You can import and export the following user attributes in bulk:

- Identity data
- Communication profile set
- Handles

- Communication profiles

  The supported communication profiles are CM Endpoint, CM Agent, Messaging, Session Manager, CS 1000 Endpoint, CallPilot Messaging, Conferencing, IP Office, Presence, Avaya Breeze™, Work Assignment, Officelinx, Avaya Equinox profile.

You can import and export the following global settings attributes in bulk:

- Public Contact Lists
- Shared Addresses
- Default access control list (ACLs)

❗ **Important:**

System Manager does not support import and export of roles in bulk.

Related links

New in System Manager Release 7.1 on page 11

Bulk import and export using the Excel file

In System Manager, you can import and export user profiles in bulk by using an Excel file and an XML file. To import data in bulk, provide an XML file or an Excel file as input that System Manager supports. When you export the data from the System Manager web console, the system exports the data to an XML file and an Excel file that System Manager supports.

Microsoft Office Excel 2007 and later support bulk import and export in the `.xlsx` format. You can download the Excel file from the User Management page.

Import and export in bulk by using the Excel template provides the following features:

- Supports the following types of user information:
  - Basic. The identity attributes of the user that include user provisioning rule name for the user, the tenant, and organization hierarchy details
  - Profile Set. Entries for all communication profile sets for all users

    The Profile Set sheet contains an entry for each communication profile set for a user. The user must set only one communication profile set as true for a user in the **Is Default** column. The value true indicates that the communication profile set of the user is default
  - Handle. The communication address of the user
  - Session Manager profile
  - Avaya Breeze™ profile
  - CM Endpoint profile with all attributes of the station communication profile
  - CM Agent profile with all attributes.
  - Messaging profile
  - Officelinx profile
  - CallPilot profile
  - IP Office Endpoint profile

    - CS 1000 Endpoint profile
    - Presence profile
    - Conferencing profile
    - Work Assignment profile
    - Avaya Equinox profile
- Supports more than one communication profile set.
- Supports the creation, updation, and deletion of the user using the same Excel file. However, you can perform one operation at a time.
- For updation, supports only the partial merge operation.

  Bulk import and export by using Excel does not support complete or partial replace of the user for imports in bulk.

Bulk import and export by using Excel supports a subset of user attributes that XML supports. For example, Excel does not support user contacts, address, and roles.

The Excel file

The sample Excel file contains the sample data of some key attributes of the user. The Excel file provides a description of header fields. When you download the Excel template from the User Management page, the values remain blank. To use the Excel file, export some users for reference in an Excel file.

The login name in the **Basic** worksheet is the key attribute that you use to link the user records in other worksheets.

The login name of the user and the profile set name in the **Profile Set** worksheet are used as key to link to the user records in other worksheets for that user profile.

- Although you can edit the header fields in the Excel template, do not change any details of any headers in the worksheets. The import or export might fail if you change the details of the header.
- Do not change the column position in the Excel file or change the structure of the Excel template.
- Do not sort the data in worksheets.

CM Endpoint communication profile

The Excel file contains all attributes for the CM station endpoint profile that are spread in different worksheets. The parent sheet provides a link to the same user profile record in the child worksheet. The link points to the first record in the child sheet if the user profile contains multiple records in the child worksheet.

Related links

New in System Manager Release 7.1 on page 11

Multi Tenancy

Using the Multi Tenancy feature, customers, also known as tenants, can share the same instance of the application, while allowing the tenants to manage users to fit the customer needs as if the application runs on a dedicated environment.

You can manage Multi Tenancy from System Manager web console. System Manager supports the following capabilities:

- View, create, edit, copy, and delete the tenant.
- View, create, edit, and delete tenant administrators for a tenant.
- View, create, edit, and delete the organization hierarchy of the tenant.
- View the tenant hierarchy on the Tenant Management page and User Management page.
- View the tenant associated with a user.
- Create and edit the user associated with a tenant from the User Management page.

System Manager provides a tenant administration dashboard that requires administrator credentials.

By default, the Multi Tenancy feature is disabled. You have to manually enable the Multi Tenancy feature. After enabling the Multi Tenancy feature, you cannot disable the feature.

System Manager supports a maximum of 250 tenant partitions as part of System Manager Multi Tenant Management.

Related links

New in System Manager Release 7.1 on page 11

User provisioning rule

The administrator can create rules called user provisioning rules. When the administrator creates a user by using the user provisioning rule, the system displays the default values, the communication addresses, and the communication profiles that are defined in the rule. The administrator need to provide minimal user information.

The administrator can provision the user by using the user provisioning rules from the System Manager web console, Web services, directory synchronization, and bulk import services. You can assign only one user provisioning rule to a user.

System Manager supports creating, editing, duplicating, and deleting the user provisioning rule. You can use the User Management link on the System Manager web console to associate the user provisioning rule with users while creating and editing users.

Related links

New in System Manager Release 7.1 on page 11

Virtualized Environment footprint flexibility

Virtualized Environment applications provide a fixed profile based on the maximum capacity requirements. Based on the number of supported users, System Manager offers a flexible footprint profile for customers who do not require the maximum capacity.

The customer can configure VMware CPU and RAM of the System Manager virtual machine based on the following capacity size categories:

- Profile 1, SMGR Profile 1 Max User 35K, supports 35,000 users.

- Profile 2, SMGR Profile 2 Max User 250K, supports 250,000 users.

System Manager Multi Tenancy feature does not support Profile 2.

Related links

[New in System Manager Release 7.1](#) on page 11
[System Manager footprint hardware resource matrix](#) on page 30

System Manager footprint hardware resource matrix

The following table describes the resource requirements to support different profiles for System Manager in Avaya-Appliance offer and customer Virtualized Environment.

Table 1: Avaya Appliance Virtualization Platform

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
Virtual RAM	9 GB	12 GB	18 GB
Virtual Hard Disk	105 GB	105 GB	250 GB
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager
Common Server R1 support	Yes	No	No
Common Server R2 and R3 support	Yes	Yes	Yes

Table 2: Customer Virtualized Environment

VMware resource	Profile-1	Profile-2	Profile-3
vCPU Reserved	4	6	8
Minimum vCPU Speed	2290 MHz	2290 MHz	2290 MHz
CPU reservation	9160 MHz	13740 MHz	18320 MHz
Virtual RAM	9 GB	12 GB	18 GB
Memory reservation	9126 MB	12288 MB	18432 MB
Virtual Hard Disk	105 GB	105 GB	250 GB
Shared NICs	1	1	1
Number of users	Up to 35000 with up to 35 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 250 Branch Session Manager and 12 Session Manager	>35000 to 250000 with up to 500 Branch Session Manager and 28 Session Manager

Related links

[Virtualized Environment footprint flexibility](#) on page 29

Configuration management

Configuration management provides a configuration repository for System Manager services. Configuration management is responsible for storing configuration data, also called as profiles, for System Manager services and notifying the services of configuration changes.

You can view and edit a profile of a service using Configuration management.

Related links

New in System Manager Release 7.1 on page 11

Element management

Inventory maintains a repository that records elements deployed on System Manager, including their runtime relationships. An element in the Inventory refers to a single or clustered instance of a managed element. Inventory provides a mechanism for creating, modifying, searching, and deleting elements and the access point information from the repository. Inventory retrieves information about elements that are added or deleted from the repository.

Inventory integrates the adopting products with the common console of System Manager. Through Inventory, element type can provide a link that can redirect to the Web page of the element manager. System Manager Web Console displays the links for only specific element types.

Inventory supports the creation and updation of application systems by importing data from an XML file. You can import elements only through the Web console.

Related links

New in System Manager Release 7.1 on page 11

Group management

Group and Lookup Service (GLS) is a shared service that provides group administration and lookup service for managed resources. GLS encapsulates the mechanisms for creating, changing, searching, and deleting groups and group memberships. Use GLS to group resources in ways that work best for the business, such as organizing resources by location, organization, and function.

On the System Manager web console, with GLS, you can assign different roles to administrators and allow administrators to perform only limited tasks on group of resources. For example, you can create a user group so that only an authorized user can manage the user group.

GLS supports group administration for the following common resources:

- Shared across elements, such as roles and users
- Unshared element-specific resources

GLS contains a repository of groups and memberships from System Manager and other applications that use the GLS service. GLS synchronizes the resources with other Avaya applications and services that manage these resources. GLS maintains resource IDs and their group memberships. With GLS, you can search for one or more resources based on their attribute values and get resource attributes for one or more resources.

With GLS, you can perform the following operations:

- Create groups.
- View and change groups.
- Create duplicate groups by copying properties of existing groups.
- Move groups across hierarchies.
- Assign and remove resources for groups.
- Delete groups.
- Synchronize groups.

As a shared service, GLS reduces the time and effort involved by defining reusable groups of managed resources that more than one application or service requires. For example, you can use the group of resources to assign permissions through Role Based Access Control (RBAC).

Related links

New in System Manager Release 7.1 on page 11

License management

System Manager provides Web-based license manager (WebLM) to centrally manage licenses for one or more Avaya software products for your organization. All Avaya applications that use WebLM for license management use WebLM that System Manager provides instead of WebLM on System Platform.

System Manager WebLM supports the Centralized licensing feature for Avaya Aura® Communication Manager.

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

Related links

New in System Manager Release 7.1 on page 11

System Manager Communication Manager capabilities overview

System Manager provides a common, central administration of some IP Telephony products. With the central administration feature, you can consolidate the key capabilities of Integrated Management administration products with other Avaya Management tools on a common software platform. With System Manager, you can administer Avaya Aura® Communication Manager, Communication Manager Messaging, Avaya Aura® Messaging, and Modular Messaging. The following sections provide some features of System Manager.

Managing Communication Manager objects

System Manager displays a collection of Communication Manager objects under **Communication Manager**. With System Manager, you can add, edit, view, or delete objects through Communication Manager.

Endpoint management

Using endpoint management you can create and manage endpoint objects and add, change, remove, and view endpoint data.

Template management

Using Templates, you can specify specific parameters of an endpoint or a subscriber once and reuse the template for subsequent tasks of adding endpoints or subscribers. You can use default templates or add your own custom templates.

The two categories of templates are: default templates and user-defined templates. You cannot edit or delete the default templates. However, you can modify or remove user-defined templates at any time.

Subscriber management

Using Subscriber Management, you can manage, add, change, remove, and view subscriber data. Subscriber management supports Avaya Aura® Messaging, Communication Manager Messaging, and Modular Messaging objects.

Discovery Management

You can discover specific devices within the network using the Discovery Management capability of System Manager. You can also manage the Simple Network Management Protocol (SNMP) access parameters used for the discovery process. Device discovery discovers your network, including subnets and nodes.

Element Cut Through

Using the Element Cut-Through link, you can gain access to the Communication Manager cut through the Element Cut-Through page. As an administrator, you have permission to gain access to the Communication Manager cut through.

Related links

New in System Manager Release 7.1 on page 11

Granular role-based access control

With the Granular role-based access control feature, you can restrict access to Communication Manager resources, such as gateways and servers, and objects on resources, such as Agent Login ID.

Based on the role that a user has, System Manager supports range permissions along with the operation permissions assigned to the user. You can assign permissions or a combination of permissions to users. The permissions include adding, editing, deleting, and duplicating objects. For example, if you assign a range of 1000:4000 and define permissions for Add, Edit, and Delete operations, the user can create, edit, and delete extensions within the range of 1000:4000.

The default value in the specific **Range** field is asterisk (*). If you retain this value, the user has access to the entire defined range.

You can define range-level granular permissions for the following Communication Manager objects:

- Endpoints

- Agent Login ID
- Announcement
- Audio Group
- Best Service Routing Pickup Group
- Holiday Table
- Variables
- Vector
- Vector Directory Number (VDN)
- Vector Routing Table
- Service Hours Table
- Coverage Answer Group
- Coverage Path
- Coverage Remote
- Coverage Time-of-Day
- Group-Page
- Hunt-Group
- Intercom Group
- Pickup Group
- Terminating Extension Group
- Route-Pattern
- Class of Restriction (COR)

Related links

New in System Manager Release 7.1 on page 11

Communication Manager feature concurrency enhancements

- Improve navigation speed on User management and Endpoint management webpages on System Manager.
- Feature concurrency with new Communication Manager and SIP Phone features:
  - Service observing from SIP Phone support, new **sip-sobsv** button and **listen-only** sub-field within the **sip-sobsv** button available
  - VOA Repeat or Interrupt for SIP CC Phone support, new **voa-repeat** button available
  - Add or Remove Agent Skill from SIP Phone support, new **add-rem-skill** button available
  - Auxiliary Agents Considered Idle support, new **AUX Agent Considered Idle** field to administer on the Agent LoginId object
  - Forced Agent Logout from Auxiliary Work by Aux Reason Code Support, new fields available

  - Streaming Music-on-Hold from an external source, such as cloud, new **LiveStreamSource** field available
  - Hunt Position Busy Button support, new **hntpos-bsy** button available.

Related links

New in System Manager Release 7.1 on page 11

Certification validation

With System Manager Solution Deployment Manager and Solution Deployment Manager client, you can establish a certificate-based TLS connection between the Solution Deployment Manager service and a host that is running Avaya Aura® 7.x applications. This provides secure communications between System Manager Solution Deployment Manager or the Solution Deployment Manager client and Appliance Virtualization Platform or ESXi hosts or vCenter.

The certificate-based sessions apply to the Avaya Aura® Virtualized Appliance offer using host self-signed certificates and the customer-provided Virtualization Environment using host self-signed or third-party certificates.

You can check the following with certificate-based TLS sessions:

- Certificate valid dates
- Origin of Certificate Authority
- Chain of Trust
- CRL or OCSP state

  Note:

  Only System Manager Release 7.1 and later supports **OCSP**. Other elements of Avaya Aura® Suite do not support **OCSP**.

- Log Certificate Validation Events

Solution Deployment Manager checks the certificate status of hosts. If the certificate is incorrect, Solution Deployment Manager does not connect to the host.

For the correct certificate:

- The fully qualified domain or IP address of the host to which you are connecting must match the value in the certificate SAN or the certificate Common Name and the certificate must be in date.
- Appliance Virtualization Platform and VMware ESXi hosts do not automatically regenerate their certificates when host details such as IP address or hostname and domain changes. The certificate might become incorrect for the host.

If the certificate is incorrect:

- For the Appliance Virtualization Platform host, Solution Deployment Manager regenerates the certificate on the host and then uses the corrected certificate for the connection.
- For the VMware ESXi host or vCenter, the system denies connection. The customer must update or correct the certificate on the host or vCenter.

  For more information about updating the certificate, see “Updating the certificate on the ESXi host from VMware”.

Note:

Solution Deployment Manager:

- Validates certificate of vCenter
- Validates the certificates when a virtual machine is deployed or upgraded on vCenter managed hosts

With Solution Deployment Manager, you can only accept certificate while adding vCenter. If a certificate changes, the system gives a warning that the certificate does not match the certificate in the trust store on Solution Deployment Manager. You must get a new certificate, accept the certificate as valid, and save the certificate on the system.

To validate certificates, you can open the web page of the host. The system displays the existing certificate and you can match the details.

Related links

New in System Manager Release 7.1 on page 11

Bulk import and export enhancements

System Manager provides the following bulk import and export enhancements:

- An option to export user data by using Excel or XML files.
- Time zone field for Avaya Aura® Messaging subscribers.

  The value must be in the standardized name format. For example, America/Phoenix. Otherwise, the system sets the Avaya Aura® Messaging subscriber time zone to the System Manager server time zone.

Related links

New in System Manager Release 7.1 on page 11

Avaya Aura® Device Services element

System Manager supports Avaya Aura® Device Services as an element.

With Avaya Aura® Device Services, clients and endpoints can store centrally and retrieve data such as configuration and deployment data. You can manage the data from any device.

Avaya Aura® Device Services supports the following services for devices:

- Contact Services: The service provides the following end user-focused services that are centrally located:
  - Directory Service: Manages your contacts from any of your devices. Performs an enterprise search of existing sources of contacts such as System Manager through PPM, and exchange local contacts, enterprise directory.

    Only a provisioned user can use Contact Services.
  - User Service: Sets and retrieves information such as your preferred names, picture, and other preferences.

  - Picture Service: Supports creating (overrides default enterprise), deleting, and updating a picture of user and provides a centralized, firewall-friendly interface to present picture URLs in the contact information or search results.
- Notification Service: Provides a common infrastructure for a client or endpoint to subscribe to receive events from a number of service resources with a single connection.
- Dynamic Configuration Service: Provides discovery of configuration settings to UC Clients that can be customized on a global, group, individual or platform basis. This simplifies the configuration process of users, and skips manual configuration and makes ready for use. Clients only need to only provide identity information such as email address or Windows userid and enterprise credentials.
- Web Deployment Service: Supports publishing and deploying UC client updates for end users.

Related links

New in System Manager Release 7.1 on page 11

Virtual machine report

With System Manager Release 7.1.3 and later, you can generate a report of virtual machines that are installed on the Appliance Virtualization Platform host.

The script to generate the virtual machine report is in the `/swlibrary/reports/generate_report.sh` folder.

Important:

If you run the report generation script when an upgrade is in progress on System Manager, the upgrade might fail.

Related links

New in System Manager Release 7.1 on page 11

Security hardening options

System Manager provides the following security hardening options:

- selinux
- audit
- fips
- aide
- TLSv1, TLSv1.1, and TLSv1.2

You can enable or disable one or more security hardening options. While you can enable all the options, you can only disable selinux, audit, and aide.

Related links

New in System Manager Release 7.1 on page 11

Security features

OVA Signing

OVA signing is a new security feature where OVA files are digitally signed to ensure file integrity. The system will verify the digital signature of the OVA, feature pack, and service pack before deploying, upgrading, and patching operation.

Related links

New in System Manager Release 7.1 on page 11

Security hardening

Using the security hardening feature, you can enable or disable military grade hardening or commercial grade hardening for System Manager. Enabling military grade hardening in System Manager enables commercial grade hardening by default.

It also facilitates a system with higher security and restricts unauthorized access and changes to the system settings.

Related links

New in System Manager Release 7.1 on page 11

Certificate-based authentication

With System Manager 7.1, you can disable the password-based login and configure the certificate-based authentication for system login.

The certificates for this authentication can be issued by System Manager as the certificate authority or by a third-party certificate authority.

To authenticate the user, the system provides the option to retrieve only the selected fields from the certificate.

Related links

New in System Manager Release 7.1 on page 11

Backup encryption

With System Manager 7.1, you can encrypt system backups using a password. Encrypted backups of a military grade hardened system can be restored to a matching type of hardened system: military grade, commercial grade, and standard.

Encrypted backups of a commercial grade hardened system can be restored only on a commercial grade hardened system or a standard hardened system. Likewise, encrypted backups of standard hardened system can be restored only on a standard hardened system.

Related links

New in System Manager Release 7.1 on page 11

Chapter 3: Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized offers

Avaya Aura® Release 7.0 and later supports the following two Avaya virtualization offers based on VMware:

- Avaya Aura® Virtualized Appliance (VA): Avaya-provided server, Avaya Aura® Appliance Virtualization Platform, based on the customized OEM version of VMware® ESXi 6.0.
- Avaya Aura® Virtualized Environment (VE): Customer-provided VMware infrastructure

The virtualization offers provide the following benefits:

- Simplifies IT management using common software administration and maintenance.
- Requires fewer servers and racks which reduces the footprint.
- Lowers power consumption and cooling requirements.
- Enables capital equipment cost savings.
- Lowers operational expenses.
- Uses standard operating procedures for both Avaya and non-Avaya products.
- Deploys Avaya Aura® virtual products in a virtualized environment on Avaya provided servers or customer-specified servers and hardware.
- Business can scale rapidly to accommodate growth and to respond to changing business requirements.

Avaya Aura® Virtualized Appliance overview

Avaya Aura® Virtualized Appliance is a turnkey solution. Avaya provides the hardware, all the software including the VMware hypervisor and might also offer the customer support of the setup. Virtualized Appliance offer is different from Avaya Aura® Virtualized Environment, where Avaya provides the Avaya Aura® application software and the customer provides and supports the VMware hypervisor and the hardware on which the hypervisor runs.

Deployment considerations

- Deployment on the Appliance Virtualization Platform server is performed from the System Manager Solution Deployment Manager or the Solution Deployment Manager standalone Windows client.
- Avaya provides the servers, Appliance Virtualization Platform, which includes the VMware ESXi hypervisor.

Appliance Virtualization Platform overview

From Release 7.0, Avaya uses the VMware®-based Avaya Aura® Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya Aura® Virtualized Appliance offer.

Avaya Aura® Virtualized Appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, Dell™ PowerEdge™ R630, HP ProLiant DL360 G7, HP ProLiant DL360p G8, and HP ProLiant DL360 G9
- S8300D and S8300E

  Note:

  With WebLM Release 7.x, you cannot deploy WebLM on S8300D Server or S8300E Server running on Appliance Virtualization Platform.

Note:

The introduction of Spectre and Meltdown fixes with the Avaya Aura® Release 7.1.3 has an impact on S8300D scalability performances. A Survivable Remote configuration for Communication Manager LSP and Branch Session Manager with the Spectre and Meltdown fixes enabled can only support 200 users with up to 500 BHCC traffic.

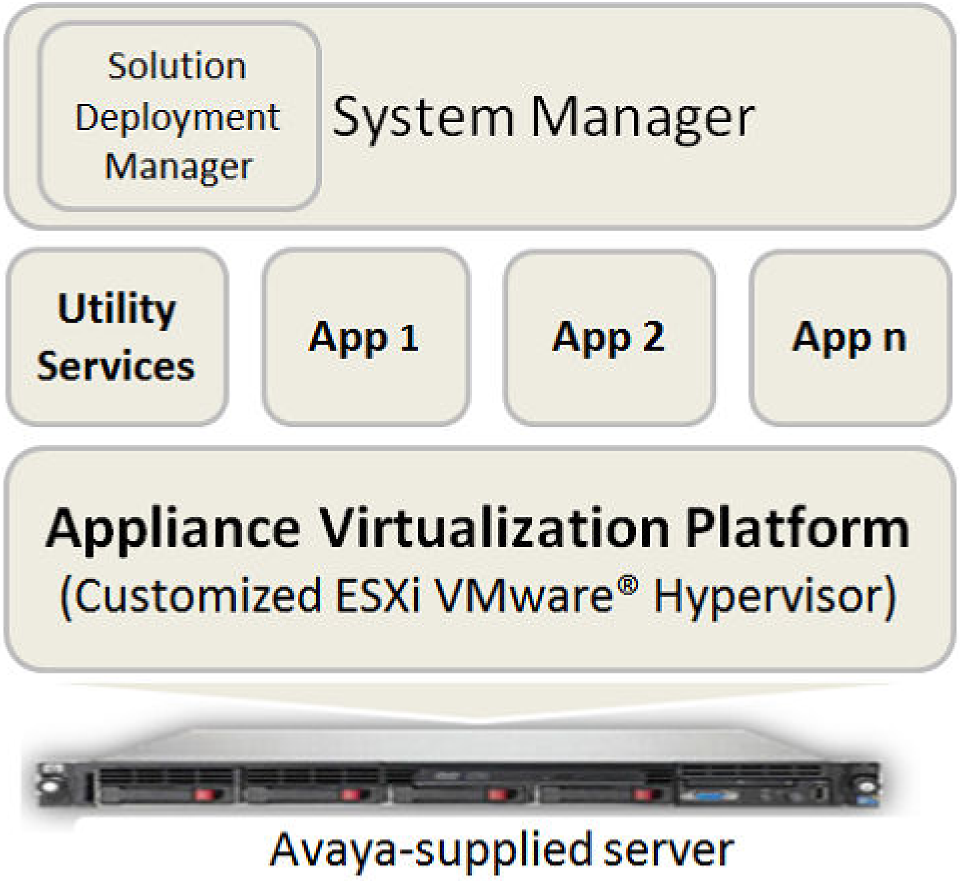
Since the Spectre and Meltdown fixes are enabled by default, consider configuration changes to upgrade to the Release 7.1.3.

Consider the following options if the higher capacity is required from the S8300D:

- Disable Spectre and Meltdown fixes on S8300D. This allows the S8300D to deliver the same level of capacity as in the Avaya Aura® Release 7.1.2 and before.
- Upgrade the embedded server to the latest S8300E model if disabling fixes on the S8300D is not viable.

For more information about Spectre and Meltdown fixes included in Avaya Aura® Release 7.1.3, see PSN020346u on the Avaya Support site at: https://downloads.avaya.com/css/P8/documents/101048606.

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 6.0. With Appliance Virtualization Platform, customers can run any combination of supported applications on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements.


Solution Deployment Manager
System Manager
Utility Services
App 1
App 2
App n
Appliance Virtualization Platform
(Customized ESXi VMware® Hypervisor)
Avaya-supplied server

From Avaya Aura® Release 7.0 and later, Appliance Virtualization Platform replaces System Platform.

You can deploy the following applications on Appliance Virtualization Platform:

- Utility Services 7.1.3
- System Manager 7.1.3
- Session Manager 7.1.3
- Branch Session Manager 7.1.3
- Communication Manager 7.1.3
- Application Enablement Services 7.1.3
- WebLM 7.1.3
- Avaya Breeze™ 3.3.x with Presence Services
- SAL 3.0
- Communication Manager Messaging 7.0
- Avaya Aura® Messaging 7.0
- Avaya Aura® Device Services 7.1.2
- Avaya Aura® Media Server 7.8

- Avaya Equinox 9.1
- Avaya Proactive Contact 5.1.2

  For more information about installing Avaya Proactive Contact and administering Appliance Virtualization Platform with Avaya Proactive Contact, see the Avaya Proactive Contact documentation.

✱ **Note:**

For deploying Avaya Aura® applications on Appliance Virtualization Platform only use Solution Deployment Manager.

Avaya Aura® Virtualized Environment overview

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

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

✱ **Note:**

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

- server and host
- reservations and configuration values

Deployment considerations

Avaya Pod Fx for Enterprise Communications

Avaya Pod Fx for Enterprise Communications is an alternative deployment option for Avaya Aura® Virtualized Environment applications.

Avaya Pod Fx is a full-stack turnkey solution that combines storage arrays from EMC, virtualization software from VMware, and networking, management, and real-time applications from Avaya.

Avaya Pod Fx accelerates deployment of Avaya Aura® applications and simplifies IT operations.

Documentation

The following table lists the Avaya Pod Fx for Enterprise Communications documents. These documents are available on the Avaya support website at http://support.avaya.com.

Title	Description
Avaya Pod Fx for Enterprise Communications – Technical Solutions Guide	Provides an overview of the solution, specifications, and components that Avaya Pod Fx for Enterprise Communications integrates.
Avaya Pod Fx for Enterprise Communications – Pod Orchestration Suite User Guide	Provides an overview of the Avaya Pod Orchestration Suite (POS). The POS contains the applications which orchestrate, manage, and monitor the Avaya Pod Fx. This guide explains how to access and use the applications in the POS management suite.
Avaya Pod Fx for Enterprise Communications – Locating the latest product documentation	Identifies the Avaya Pod Fx customer documentation. Also includes the documentation for the Avaya and non-Avaya products that are included in the Avaya Pod Fx solution.
Avaya Pod Fx for Enterprise Communications – Release Notes	Describes fixed and known issues for Avaya Pod Fx. This document does not describe issues associated with each component in the Avaya Pod Fx. For information on the specific components, see the component Release Notes.

Avaya Aura® virtualized software

Software delivery

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

- The application software and operating system.
- Preinstalled VMware tools.
- Preset configuration details for:
  - RAM and CPU reservations and storage requirements
  - Network Interface Card (NIC)

Note:

The customer provides the servers and the VMware® infrastructure, that includes VMware® licenses.

Patches and upgrades

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

Important:

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

Performance and capacities

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

Caution:

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

Avaya Aura® on Amazon Web Services overview

Amazon Web Services (AWS) is a cloud services platform that enables enterprises to securely run applications on the virtual cloud. The key components of AWS are Amazon Elastic Compute Cloud (EC2) and Amazon Simple Storage Service (S3).

Supporting the Avaya applications on the AWS Infrastructure as a service (IaaS) platform provides the following benefits:

- Minimizes the capital expenditure (CAPEX) on infrastructure. The customers can move from CAPEX to operational expense (OPEX).
- Reduces the maintenance cost of running the data centers.
- Provides a common platform for deploying the applications.
- Provides a flexible environment to accommodate the changing business requirements of customers.

You can deploy the following Avaya Aura® applications on Amazon Web Services:

- Avaya Aura® System Manager
- Avaya Aura® Session Manager
- Avaya Aura® Communication Manager
- Avaya Aura® Utility Services
- Avaya WebLM
- Presence Services using Avaya Breeze™
- Avaya Session Border Controller for Enterprise

- Avaya Aura® Device Services
- Avaya Aura® Application Enablement Services (Software only)
- Avaya Aura® Media Server (Software only)
- Avaya Diagnostic Server (Software only)

The supported Avaya Aura® AWS applications can also be deployed on-premises.

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

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

Avaya Aura® on Kernel-based Virtual Machine overview

Kernel-based Virtual Machine (KVM) is a virtualization infrastructure for the Linux kernel that turns the Linux kernel into a hypervisor. You can remotely access the hypervisor to deploy applications on the KVM host.

KVM virtualization solution is:

- Cost effective for the customers.
- Performance reliable and highly scalable.
- Secure as it uses the advanced security features of SELinux.
- Open source software that can be customized as per the changing business requirements of the customers.

You can deploy the following Avaya Aura® applications on KVM:

- Avaya Aura® System Manager Release 7.1.3
- Avaya WebLM Release 7.1.3
- Avaya Aura® Session Manager Release 7.1.3
- Avaya Aura® Communication Manager Release 7.1.3
- Avaya Aura® Utility Services Release 7.1.3

  Note:

  Utility Services 7.1.1 and later requires the Utility Services 7.1 KVM image.
- Avaya Aura® Application Enablement Services Release 7.1.3
- Avaya Aura® Media Server Release 7.8 SP5 (Software only)
- Avaya Diagnostic Server Release 3.0 (Software only)

- Avaya Session Border Controller for Enterprise Release 7.2

Chapter 4: Interoperability

Product compatibility

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

Chapter 5: Licensing requirements

Licensing requirements

When you place an order for the following products using the Avaya Solution Designer, you can include a new System Manager or an upgrade of System Manager as an entitlement:

- New Communication Manager, Session Manager, or CS 1000
- Upgrade of Communication Manager, Session Manager, or CS 1000

Additionally, you can add the System Manager DVD and the System Manager server to the order.

Chapter 6: Performance specifications

Capability and scalability specification

The table provides the maximum capacities supported for each element type.

Note:

Because only one System Manager is available with each Avaya Aura® deployment, the solution number is not the sum of all supported elements listed in the table.

Capacity	Maximum limit	Notes
Administrator logins	250	
Simultaneous logins	50	
Total administered endpoints of all types	250,000	The total number of endpoints are defined in Home/Elements/ Communication Manager/ Endpoints / Manage Endpoints Endpoint page in System Manager.
Total administered users defined in the System Manager database	250,000	The total number of administered users with an Identity is configured in System Manager, and might not have a communication profile defined. Users are defined in the Home/ Users/Manage Users Users page System Manager.
Messaging mailboxes	250,000	
Contacts per user	250	
Public contacts	1000	
Personal contact lists per user	1	
Members in a personal contact list	250	
Groups	300	
Members in a group	400	
Elements	25,000	

Table continues…

Capacity	Maximum limit	Notes
Communication Manager and/or CS 1000	500	Capacity counts against the total number of elements.
Session Managers	28	
Branch Session Manager	500	
IP Office	2000	To support central licensing of 2,000 IP Office 9.x, local WebLM licensing servers that are slaved to System Manager licensing are required. See the IP Office 9.x product offer and System Manager WebLM for details.
IP Office Unified Communication Module (UCM) or Application servers as part of Branch deployments	2000	
Roles	200	
Roles per user	20	
Licensing clients	1000	
Concurrent License requests per WebLM	300	
license requests during any 9 minute window per WebLM	50,000	
Local WebLM	22	
Trust management clients	2500	
Tenants (System Manager Multi Tenant)	250	

Geographic Redundancy

System Manager Geographic Redundancy service replicates Avaya Aura® application support for two geographically distant System Manager sites with separate subnetworks and across a WAN. You can change the System Manager management services from one site to another when one of the sites or servers fails. System Manager Geographic Redundancy sites are set up in pairs. From the server pair, one is designated as the primary System Manager server and the other is designated as the secondary System Manager server.

Chapter 7: Security

Security specification

As the management console for some of the Avaya products, System Manager must be resilient to attacks that might cause service disruption, malfunction, or unauthorized access or modification of the data. System Manager as part of the Avaya Aura® solution must be protected from security threats such as the following:

- Unauthorized access or modification of data
- Theft of data
- Denial of Service (DoS) attacks
- Viruses and Worms
- Web-based attacks that includes Cross-Site Scripting and Cross-Site Forgery

For information about security-related considerations, features, and services for System Manager, see *System Manager Release 6.3 Security Guide* available on the Avaya Support website at https://support.avaya.com/security.

Related links

Trust Management on page 51

Trust Management

System Manager uses Trust Management to provision and manage certificates of various applications, servers, and devices thereby enabling a secure, inter-element communication. Trust Management provides Identity (Server) and Trusted (Root/CA) certificates that applications can use to establish mutually authenticated TLS sessions.

System Manager uses a third-party open source application as a Certificate Authority, Enterprise Java Beans Certificate Authority (EJBCA), to issue Identity and Trusted certificates to applications through Simple Certificate Enrollment Protocol (SCEP). However, it does not issue certificates to the endpoints.

For information about getting the endpoint certificates, see the endpoint specific documentation on the Avaya Support website.

Related links

Security specification on page 51

External authentication

You can configure System Manager to authenticate administrative users using external authentication services, such as an enterprise directory, Kerberos, or a RADIUS server. An administrative account is provisioned within System Manager during installation for initial access.

System Manager supports the following authentication authorities:

- Local users
- External RADIUS users
- External LDAP users
- External Security Assertion Markup Language (SAML) users

The authentication scheme policy determines the order in which you can use the authentication authorities. The authentication servers policy controls the settings for the external SAML, LDAP, RADIUS and KERBEROS servers.

Related links

SAML authentication on page 52

SAML authentication

For enterprise level Single Sign On, System Manager provides Security Assertion Markup Language (SAML) authentication. System Manager uses SAML implementation version 2.0 of OpenAM Release 9.5.4 to provide SAML based authentication with external Identity Providers. System Manager uses Web Browser Single Sign On profile of SAML authentication.

Related links

External authentication on page 52

Role Based Access Control

In System Manager, you require appropriate permissions to perform a task. The administrator grants permissions to users by assigning appropriate roles. Role Based Access Control (RBAC) in System Manager supports the following types of roles:

- Built-in
- Custom

With these roles, you can gain access to various elements with specific permission mappings.

Built-in roles are default roles that authorize users to perform common administrative tasks. You can assign built-in roles to users, but you cannot delete roles or change permission mappings in the built-in roles.

You can perform LDAP synchronization of Active Directory administrator roles with System Manager administrator roles. The capability includes system roles and custom roles on System Manager.

Note:

Granular RBAC is not supported for managing Equinox Conferencing, Web Gateway, and Work Assignment elements by creating custom roles.

Port utilization

System Manager 7.1.3 Port Matrix lists all the ports and protocols that System Manager uses. Avaya Direct, Business Partners, and customers can find the port matrix document at http://support.avaya.com/security. On the webpage, select the Avaya Product Port Matrix Documents link, and click the System Manager 7.1.3 Port Matrix document.

You can gain access to the port matrix document only after you log in to the Avaya Support site by using the valid support site credentials.

Chapter 8: Resources

Documentation

The following table lists the documents related to System Manager. Download the documents from the Avaya Support website at http://support.avaya.com.

Title	Description	Audience
Implementation		
Installing the Dell™ PowerEdge™ R620 server	Install the Dell™ PowerEdge™ R620 server.	Implementation personnel
Installing the HP ProLiant DL360p G8 server	Install the HP ProLiant DL360p G8 server.	Implementation personnel
Deploying Avaya Aura® System Manager	Deploy the Avaya Aura® System Manager virtual machine.	Implementation personnel
Administration		
Administering Avaya Aura® System Manager	Perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators
Maintenance and Troubleshooting		
Upgrading Avaya Aura® System Manager	Upgrade the Avaya Aura® System Manager virtual application to Release 7.1.2.	System administrators and IT personnel
Troubleshooting Avaya Aura® System Manager	Perform maintenance and troubleshooting tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators and IT personnel
Maintaining and Troubleshooting the Dell™ PowerEdge™ R620 server	Maintaining and troubleshooting the Dell™ PowerEdge™ R620 Server	System administrators and IT personnel
Maintaining and Troubleshooting the HP ProLiant DL360p G8 server	Maintaining and troubleshooting the HP ProLiant DL360p G8 Server.	System administrators and IT personnel

Related links

Finding documents on the Avaya Support website on page 55

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Related links

Documentation on page 54

Training

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

Course code	Course title	Type
2007V/W	What is New in Avaya Aura® Release 7.1.3	AvayaLive™ Engage Theory
2008V/W	What is New in Avaya Aura® Application Enablement Services 7.0	AvayaLive™ Engage Theory
2009V/W	What is New in Avaya Aura® Communication Manager 7.0	AvayaLive™ Engage Theory
2010V/W	What is New in Avaya Aura® Presence Services 7.0	AvayaLive™ Engage Theory
2011/V/W	What is New in Avaya Aura® Session Manager Release 7.1.3 and Avaya Aura® System Manager Release 7.1.3	AvayaLive™ Engage Theory
2012V	Migrating and Upgrading to Avaya Aura® Platform 7.0	AvayaLive™ Engage Theory

Table continues…

Course code	Course title	Type
2013V	Avaya Aura® Release 7.1.3 Solution Management	AvayaLive™ Engage Theory
1A00234E	Avaya Aura® Fundamental Technology	AvayaLive™ Engage Theory
1A00236E	Knowledge Access: Avaya Aura® Session Manager and Avaya Aura® System Manager Fundamentals	AvayaLive™ Engage Theory
5U00106W	Avaya Aura® System Manager Overview	WBT Level 1
4U00040E	Knowledge Access: Avaya Aura® Session Manager and System Manager Implementation	ALE License
5U00050E	Knowledge Access: Avaya Aura® Session Manager and System Manager Support	ALE License
5U00095V	Avaya Aura® System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 1
5U00097I	Avaya Aura® Session Manager and System Manager Implementation, Administration, Maintenance, and Troubleshooting	vILT+Lab Level 2
3102	Avaya Aura® Session Manager and System Manager Implementation and Maintenance Exam	Exam (Questions)
5U00103W	Avaya Aura® System Manager 6.2 Delta Overview	WBT Level 1

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

  Note:

  Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 57

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.

4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 57

Glossary

Active-standby (Auto)	Active-Active: The elements leverage the services of the primary and the secondary System Manager servers. The system functions in this mode when the enterprise network splits.
Active-standby (Manual)	Active-Standby: The elements communicate with the active System Manager server. The mode is also called Active-Standby Auto. In the normal operation scenario, the primary System Manager server is active and the secondary System Manager server is in the standby mode. The primary System Manager server continues to manage elements until the primary System Manager server becomes unavailable. If the primary System Manager server fails and the administrator activates the secondary System Manager server, the elements automatically switch to the secondary System Manager server.
Elements	An element is an instance of an Avaya Aura® network entity managed by System Manager, for example, a Session Manager server or a Communication Manager server.
Geographic Redundancy-aware element	An element that supports Geographic Redundancy, such as Avaya Aura® Session Manager Release 6.3.
Geographic Redundancy-unaware element	An element that does not support Geographic Redundancy, such as Avaya Aura® Session Manager release earlier than 6.3.
Primary System Manager server	The first or the master System Manager server in a Geographic Redundancy setup that serves all system management requests.
Secondary System Manager server	The System Manager server that functions as a backup to the primary System Manager server in a Geographic Redundancy setup. The secondary System Manager server provides the full System Manager functionality when the system fails to connect to the primary System Manager server.

Index