Deploying and Updating Avaya Aura® Media Server Appliance 7.7 FP1

Release 7.7 FP1
Issue 4
April 2017

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.

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.

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.

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.

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.

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. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

- Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.
- Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.
- Database License (DL). End User may install and use each copy or an Instance of the Software on one Server or on

multiple Servers provided that each of the Servers on which the Software is installed communicates with no more than one Instance of the same database.

- CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya's prior consent and payment of an upgrade fee.
- Named User License (NU). You may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.
- Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

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 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.

How to Get Help

For additional support telephone numbers, go to the Avaya support Website: http://www.avaya.com/support. If you are:

- Within the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the appropriate link for the type of support that you need.
- Outside the United States, click the Escalation Contacts link that is located under the Support Tools heading. Then click the International Services link that includes telephone numbers for the international Centers of Excellence.

Providing Telecommunications Security

Telecommunications security (of voice, data, and/or video communications) is the prevention of any type of intrusion to (that is, either unauthorized or malicious access to or use of) your company's telecommunications equipment by some party.

Your company's "telecommunications equipment" includes both this Avaya product and any other voice/data/video equipment that could be accessed via this Avaya product (that is, "networked equipment").

An "outside party" is anyone who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf. Whereas, a "malicious party" is anyone (including someone who may be otherwise authorized) who accesses your telecommunications equipment with either malicious or mischievous intent.

Such intrusions may be either to/through synchronous (time-multiplexed and/or circuit-based), or asynchronous (character-, message-, or packet-based) equipment, or interfaces for reasons of:

- Utilization (of capabilities special to the accessed equipment)
- Theft (such as, of intellectual property, financial assets, or toll facility access)
- Eavesdropping (privacy invasions to humans)
- Mischief (troubling, but apparently innocuous, tampering)
- Harm (such as harmful tampering, data loss or alteration, regardless of motive or intent)

Be aware that there may be a risk of unauthorized intrusions associated with your system and/or its networked equipment. Also realize that, if such an intrusion should occur, it could result in a variety of losses to your company (including but not limited to, human/data privacy, intellectual property, material assets, financial resources, labor costs, and/or legal costs).

Responsibility for Your Company's Telecommunications Security

The final responsibility for securing both this system and its networked equipment rests with you - Avaya's customer system administrator, your telecommunications peers, and your managers. Base the fulfillment of your responsibility on acquired knowledge and resources from a variety of sources including but not limited to:

- Installation documents
- System administration documents
- Security documents
- Hardware-/software-based security tools
- Shared information between you and your peers
- Telecommunications security experts

To prevent intrusions to your telecommunications equipment, you and your peers should carefully program and configure:

- Your Avaya-provided telecommunications systems and their interfaces
- Your Avaya-provided software applications, as well as their underlying hardware/software platforms and interfaces
- Any other equipment networked to your Avaya products

TCP/IP Facilities

Customers may experience differences in product performance, reliability and security depending upon network configurations/design and topologies, even when the product performs as warranted.

Product Safety Standards

This product complies with and conforms to the following international Product Safety standards as applicable:

- IEC 60950-1 latest edition, including all relevant national deviations as listed in the IECEE Bulletin—Product Category OFF: IT and Office Equipment.

- CAN/CSA-C22.2 No. 60950-1 / UL 60950-1 latest edition.

This product may contain Class 1 laser devices.

- Class 1 Laser Product
- Luokan 1 Laserlaite
- Klass 1 Laser Apparat

Electromagnetic Compatibility (EMC) Standards

This product complies with and conforms to the following international EMC standards, as applicable:

- CISPR 22, including all national standards based on CISPR 22.
- CISPR 24, including all national standards based on CISPR 24.
- IEC 61000-3-2 and IEC 61000-3-3.

Avaya Inc. is not responsible for any radio or television interference caused by unauthorized modifications of this equipment or the substitution or attachment of connecting cables and equipment other than those specified by Avaya Inc. The correction of interference caused by such unauthorized modifications, substitution or attachment will be the responsibility of the user. Pursuant to Part 15 of the Federal Communications Commission (FCC) Rules, the user is cautioned that changes or modifications not expressly approved by Avaya Inc. could void the user's authority to operate this equipment.

Federal Communications Commission Part 15 Statement:

For a Class A digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

For a Class B digital device or peripheral:

Note:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Equipment With Direct Inward Dialing ("DID"):

Allowing this equipment to be operated in such a manner as to not provide proper answer supervision is a violation of Part 68 of the FCC's rules.

Proper Answer Supervision is when:

1. This equipment returns answer supervision to the public switched telephone network (PSTN) when DID calls are:
   - answered by the called station,
   - answered by the attendant,
   - routed to a recorded announcement that can be administered by the customer premises equipment (CPE) user
   - routed to a dial prompt
2. This equipment returns answer supervision signals on all (DID) calls forwarded back to the PSTN.

Permissible exceptions are:

- A call is unanswered
- A busy tone is received
- A reorder tone is received

Avaya attests that this registered equipment is capable of providing users access to interstate providers of operator services through the use of access codes. Modification of this equipment by call aggregators to block access dialing codes is a violation of the Telephone Operator Consumers Act of 1990.

Automatic Dialers:

When programming emergency numbers and (or) making test calls to emergency numbers:

- Remain on the line and briefly explain to the dispatcher the reason for the call.
- Perform such activities in the off-peak hours, such as early morning or late evenings.

Toll Restriction and least Cost Routing Equipment:

The software contained in this equipment to allow user access to the network must be upgraded to recognize newly established network area codes and exchange codes as they are placed into service.

Failure to upgrade the premises systems or peripheral equipment to recognize the new codes as they are established will restrict the customer and the customer's employees from gaining access to the network and to these codes.

For equipment approved prior to July 23, 2001:

This equipment complies with Part 68 of the FCC rules. On either the rear or inside the front cover of this equipment is a label that contains, among other information, the FCC registration number, and ringer equivalence number (REN) for this equipment. If requested, this information must be provided to the telephone company.

For equipment approved after July 23, 2001:

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the Administrative Council on Terminal Attachments (ACTA). On the rear of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXX. If requested, this number must be provided to the telephone company.

The REN is used to determine the quantity of devices that may be connected to the telephone line. Excessive RENs on the telephone line may result in devices not ringing in response to an incoming call. In most, but not all areas, the sum of RENs should not exceed 5.0.

L'indice d'équivalence de la sonnerie (IES) sert à indiquer le nombre maximal de terminaux qui peuvent être raccordés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque de dispositifs, à la seule condition que la somme d'indices d'équivalence de la sonnerie de tous les dispositifs n'excède pas cinq.

To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2001, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXX. The digits represented by ## are the REN

without a decimal point (for example, 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.

Means of Connection:

Connection of this equipment to the telephone network is shown in the following table:

Manufacturer's Port Identifier	FIC Code	SOC/ REN/ A.S. Code	Network Jacks
Off premises station	OL13C	9.0F	RJ2GX, RJ21X, RJ11C
DID trunk	02RV2.T	AS.2	RJ2GX, RJ21X, RJ11C
CO trunk	02GS2	0.3A	RJ21X, RJ11C
	02LS2	0.3A	RJ21X, RJ11C
Tie trunk	TL31M	9.0F	RJ2GX
Basic Rate Interface	02IS5	6.0F, 6.0Y	RJ49C
1.544 digital interface	04DU9.BN	6.0F	RJ48C, RJ48M
	04DU9.1KN	6.0F	RJ48C, RJ48M
	04DU9.1SN	6.0F	RJ48C, RJ48M
120A4 channel service unit	04DU9.DN	6.0Y	RJ48C

If this equipment causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice is not practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens, the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with this equipment, for repair or warranty information, please contact the Technical Service Center at 1-800-242- 2121 or contact your local Avaya representative. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.

A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.

Installation and Repairs

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to certified equipment should be coordinated by a representative designated by the supplier. It is recommended that repairs be performed by Avaya certified technicians.

FCC Part 68 Supplier's Declarations of Conformity

Avaya Inc. in the United States of America hereby certifies that the equipment described in this document and bearing a TIA TSB-168 label identification number complies with the FCC's Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments (ACTA) adopted technical criteria.

Avaya further asserts that Avaya handset-equipped terminal equipment described in this document complies with Paragraph 68.316 of the FCC Rules and Regulations defining Hearing Aid Compatibility and is deemed compatible with hearing aids.

Copies of SDoCs signed by the Responsible Party in the U. S. can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

Canadian Conformity Information

This Class A (or B) digital apparatus complies with Canadian ICES-003.

Cet appareil numérique de la classe A (ou B) est conforme à la norme NMB-003 du Canada.

This product meets the applicable Industry Canada technical specifications/Le présent materiel est conforme aux specifications techniques applicables d'Industrie Canada.

European Union Declarations of Conformity

CE

Avaya Inc. declares that the equipment specified in this document bearing the "CE" (Conformité Europeénne) mark conforms to the European Union Radio and Telecommunications Terminal Equipment Directive (1999/5/EC), including the Electromagnetic Compatibility Directive (2004/108/EC) and Low Voltage Directive (2006/95/EC).

Copies of these Declarations of Conformity (DoCs) can be obtained by contacting your local sales representative and are available on the following Web site: http://support.avaya.com/DoC.

European Union Battery Directive

Avaya Inc. supports European Union Battery Directive 2006/66/EC. Certain Avaya Inc. products contain lithium batteries. These batteries are not customer or field replaceable parts. Do not disassemble. Batteries may pose a hazard if mishandled.

Japan

The power cord set included in the shipment or associated with the product is meant to be used with the said product only. Do not use the cord set for any other purpose. Any non-recommended usage could lead to hazardous incidents like fire disaster, electric shock, and faulty operation.

本製品に同梱または付属している電源コードセットは、本製品専用です。本製品以外の製品ならびに他の用途で使用しないでください。火災、感電、故障の原因となります。

If this is a Class A device:

This is a Class A product based on the standard of the Voluntary Control Council for Interference by Information Technology Equipment (VCCI). If this equipment is used in a domestic environment, radio disturbance may occur, in which case, the user may be required to take corrective actions.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

If this is a Class B device:

This is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If this is used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

この装置は，情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラス Ｂ 情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。取扱説明書に従って正しい取り扱いをして下さい。

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1: Introduction

Purpose

Use this document when you are working with the Avaya Aura® Media Server (MS) 7.7 FP1 and later appliance. This document contains the procedures for:

- Deploying and updating Avaya Aura® Media Server 7.7 appliances on the Avaya Appliance Virtualization Platform (AVP).
- Deploying, upgrading, and updating Avaya Aura® Media Server 7.7 appliances in the VMware® Virtualized Environment.
- Upgrading, updating, and reinstalling Avaya Aura® Media Server 7.7 appliances on Avaya Common Servers.

Important:

Avaya also provides a non-appliance, software-only, application version of Avaya Aura® Media Server which is installed on servers that you provide. For non-appliance installation, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

Administrators of the appliance version of Avaya Aura® Media Server 7.7 prior to Feature Pack 1 (FP1) must use this document. This document is intended for people who install, upgrade, and troubleshoot Avaya Aura® Media Server 7.7 FP1 and later appliances.

Avaya Aura® Media Server FP1 is identified as follows:

- During initial physical or virtual appliance deployment, the version is 7.7.0.334_A15 or later.
- After the media server is deployed, the software layers are managed separately. For FP1, the Application layer is 7.7.0.334 or later, and the System layer is 7.7.0.19 or later.

Administrators of the appliance version of Avaya Aura® Media Server 7.7 must use this document before referring to any other Avaya Aura® Media Server 7.7 documents.

Administrators of non-appliance versions of Avaya Aura® Media Server 7.7 must not use this document.

Warranty

Avaya provides a 90-day limited warranty on the Avaya Aura® MS software. For detailed terms and conditions, see the sales agreement or other applicable documentation. Additionally, for the standard warranty description of Avaya and the details of support, see **Help & Policies** > **Policies & Legal** > **Maintenance and Warranty Information** on the Avaya Support website at http://support.avaya.com.

For additional information, see **Help & Policies** > **Policies & Legal** > **License Terms**.

For more details on the hardware maintenance for supported products, see http://portal.avaya.com/ptlWeb/services/SV0452.

Chapter 2: Overview

About the Avaya Aura® MS 7.7 appliance

The Avaya Aura® MS 7.7 appliance is a software appliance that combines the Avaya Aura® MS 7.7 software and an optimized Linux® operating system in a single and integrated package.

A deployed Avaya Aura® MS 7.7 appliance includes the following:

- Avaya Aura® MS 7.7 software
- Avaya Aura® MS Element Manager (EM)
- Security-hardened Linux® operating system
- Pre-configured support accounts

There are two types of Avaya Aura® MS 7.7 appliances:

- Virtual appliances: Avaya Aura® MS 7.7 appliances on the Appliance Virtualization Platform or VMware® virtualized environment.
- Physical appliances: Avaya Aura® MS 7.7 appliances on Avaya Common Servers.

Note:

This document contains the procedures for all types of appliances. Ensure that you use the procedures that are appropriate for your appliance type.

Important:

Avaya also provides a non-appliance, software-only, application version of Avaya Aura® Media Server which is installed on servers that you provide. For non-appliance installations, see *Installing and Updating Avaya Aura® Media Server Application on Customer Supplied Hardware and OS*.

New in this release

Virtual Appliance on Avaya Appliance Virtualization Platform

In addition to Avaya Aura® MS 7.7 appliances on VMware® Virtualized Environment, Avaya Aura® MS 7.7 appliances are also supported on Avaya Appliance Virtualization Platform (AVP) as virtual appliances.

Note:

You can deploy and delete an Avaya Aura® MS VM using Solution Deployment Manager (SDM), but you cannot use SDM to update, patch, or manage Avaya Aura® MS. Instead, manage Avaya Aura® MS using the update, backup, and restore procedures in this document.

Related links

Deploying in the Avaya AVP virtualized environment on page 14

Physical Appliance on Avaya Common Server

In addition to virtual appliances, Avaya Aura® MS 7.7 appliances are also available on Avaya Common Servers as physical appliances.

Related links

Deploying the Avaya Aura MS physical appliance on page 32

System layer updates

The underlying operating system and other software that forms the required operational environment for Avaya Aura® MS appliances can be updated.

Easier updates (FP1)

Avaya Aura® MS 7.7 Feature Pack 1 (FP1) provides Element Manager tasks to install and manage software updates. In earlier releases you were required to use commands in a Linux® shell to install and manage software updates. With, Feature Pack 1, you can use a browser to upload updates. All uploaded updates are installed by using Element Manager (EM).

The Linux® shell commands previously used to install and manage software updates are deprecated in FP1. These commands refer to the new `installUpdate` command when you attempt to use them.

Configuration profiles (FP1)

Avaya Aura® MS 7.7 Feature Pack 1 (FP1) adds configuration profile options at the time of virtual machine deployment. The following profiles are available in Avaya Aura® MS 7.7 FP1:

Profile	Configuration
Profile 1	4 vCPUs, 4.5 GB Memory, 50 GB vDisk
Profile 2	4 vCPUs, 4.5 GB Memory, 250 GB vDisk
Profile 3	8 vCPUs, 8 GB Memory, 50 GB vDisk
Profile 4	8 vCPUs, 8 GB Memory, 250 GB vDisk
Demo Profile	2 vCPUs, 2 GB Memory, 50 GB vDisk

Chapter 3: Deploying in the Avaya AVP virtualized environment

System requirements

Appliance Virtualization Platform (AVP) is a customized OEM version of VMware® ESXi 5.5 or ESXi 6.0. Avaya uses the VMware® based AVP to provide virtualization for Avaya Aura® applications in Avaya appliance offerings.

The Avaya Aura® MS appliance is deployed using Solution Deployment Manager (SDM). You can use a Windows®-based SDM Client or SDM in System Manager to deploy a VM.

AVP does not support VMware® management tools, such as vCenter and vSphere Client for VM management. You must use Solution Deployment Manager to deploy and manage the Avaya Aura® MS VM.

The AVP host must meet the following system requirements:

AVP host resource	Requirement
CPU	The core processor speed must be at least 2294 MHz. The total number of AVP host vCPUs cannot exceed the total number of physical CPUs. Configuration profile 1 and 2 require 4 vCPUs. Configuration profile 3 and 4 require 8 vCPUs.
Memory	Configuration profile 1 and 2 require 4608 MB of memory. Configuration profile 3 and 4 require 8192 MB of memory.
Disk space	Configuration profile 1 and 3 require 52 GB of AVP datastore. Configuration profile 2 and 4 require 250 GB of AVP datastore.
Network bandwidth	A dedicated pair of 1 Gbps network interfaces must be available in a teamed, failover configuration.

Ensure that the required network interfaces are connected before deploying the OVA. The AVP and Utility Services IP addresses are available on NIC 1. Media server network interfaces are selected at the time of deployment and use a free network interface controller starting with NIC 4.

Avaya Aura® MS does not support out of band management. Out of band management must remain disabled on the AVP host.

SDM deploys Avaya Aura® MS with the correct CPU, memory settings and reservations to ensure correct operation. These VM parameters must not be altered. VMware® management tools must not be used to alter VM parameters or to configure the following vSphere features, which are not supported for Avaya Aura® MS appliances:

- vMotion for running VMs
- Storage vMotion
- High Availability
- Fault tolerance
- Distributed Resource Scheduler (DRS)
- Distributed Power Management (DPM)
- VM snapshots, which adversely impact the VM disk and CPU performance

Best practice recommendations

Use the following best practices to deploy the Avaya Aura® MS appliance in the Appliance Virtualization Platform enviroment.

- All physical servers that can host a VM must have the same CPU, memory, and networking specifications.
- Do not modify the CPU or memory reservations that are set for Avaya Aura® MS OVA.
- Physical CPUs on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with Avaya Aura® MS. A physical CPU refers to a physical CPU core and not to a hyper-thread. For example, the total number of vCPUs across all VMs on an AVP host that has 12 physical cores with 24 hyper-threads, must not exceed 12.

  Note:

  This recommendation prevents CPU oversubscription. Therefore, the CPU reservation of the media server VM effectively enforces the minimum CPU core speed of the underlying hardware. The VM fails to start if the underlying hardware does not meet the core speed requirements.
- For maximum system performance, ensure that the energy savings features are disabled or that the maximum performance settings are enabled in the server BIOS.
- Deploy media server OVAs using the centralized Solution Deployment Manager in System Manager. Use the SDM Client on a Windows® computer to deploy OVAs only when SDM in System Manager is not available.
- Old media server backup files must be removed to maintain free space on the system.

Choosing a Solution Deployment Manager

About this task

The Avaya Aura® MS appliance is deployed on AVP using Solution Deployment Manager.

Note:

You can deploy and delete an Avaya Aura® MS VM using SDM, but you cannot use SDM to update, patch, or manage Avaya Aura® MS. Instead, manage Avaya Aura® MS using the update, backup, and restore procedures in this document.

Avaya provides the following Solution Deployment Manager options:

- Centralized Solution Deployment Manager in System Manager.
- Solution Deployment Manager Client (SDM Client) for Windows® computers.

To learn about the capabilities of each option and to install the Avaya Solution Deployment Manager client, see *Migrating and Installing Avaya Appliance Virtualization Platform*.

Avaya recommends using System Manager Solution Deployment Manager unless System Manager is unavailable.

Next steps

Obtain the Avaya Aura® MS OVA file.

Obtaining Avaya Aura® MS OVA

About this task

You can download Avaya Aura® MS OVA from the Avaya Product Licensing and Delivery System (Avaya PLDS) at https://plds.avaya.com.

You can also order DVDs containing the OVA using the following details:

- Material ID: 700512735
- Material Description: AAMS R7 MEDIA DVD - OVA
- DVD Label: Avaya Aura® Media Server 7.7 Virtual Appliance for AVP and VMware®

Next steps

Deploy the OVA file using vSphere Client.

Adding the OVA file to a software library

About this task

Use this task to upload an Avaya Aura® MS OVA file when you are using Solution Deployment Manager (SDM) in System Manager to deploy the VM. Alternatively, you can use the SDM Client application, which you download and install on your Windows® computer.

You must transfer an Avaya Aura® MS OVA file to System Manager before you can deploy the OVA file using SDM. The OVA file must be added to a software library on the system. OVA files are staged on System Manager and then a library that you specify pulls the staged file in from the staging area. The OVA file is available for deployment after it is in a software library.

Note:

You can deploy and delete an Avaya Aura® MS VM using SDM, but you cannot use SDM to update, patch, or manage Avaya Aura® MS. Instead, manage Avaya Aura® MS using the update, backup, and restore procedures in this document.

Procedure

1. Transfer the OVA file to System Manager by using the sftp file transfer tool, or another similar tool.

   The file must be stored in the `/swlibrary/staging/sync`.
2. Log in to the Avaya Aura® System Manager web console.
3. Navigate to **Services** > **Solution Deployment Manager** > **Software Library Management**.
4. Select the required software library.
5. Click **Manage Files**.
6. In the **Sync Files from directory**, select the checkbox next to the name of the required OVA file.
7. Enter the checksum of the OVA file in the **MD5 Checksum** field.
8. In the **Software Library** field, select a local System Manager library.
9. In the **Product Family** field, select **Avaya Aura Media Server**.
10. In the **Device Type** field, select **OVA**.
11. In the **Software Type** field, select **OVA**.
12. Click **Sync**.

    Wait for the upload to complete.
13. **(Optional)** Perform the following steps to view the uploaded file in the software library:
    a. Navigate to **Services** > **Software Library Management**.
    b. Select the checkbox next to the name of the library containing the OVA.
    c. Click **Manage Files**.

       The uploaded OVA file is listed in the **Software Library File** section.

Next steps

Deploy the OVA file using Solution Deployment Manager.

Deploying the OVA file by using Solution Deployment Manager

About this task

Use this task to deploy Avaya Aura® MS virtual appliances on Avaya Appliance Virtualization Platform system using Solution Deployment Manager.

Before you begin

- If you are not able to use SDM in System Manager, then install Avaya SDM Client on your Windows® workstation.
- Upload the Avaya Aura® MS 7.7 OVA file to an SDM software library or to your Windows® workstation if you are using Avaya SDM Client.
- Obtain the following network configuration settings for the new VM. These settings can be from an existing system if you are redeploying the Avaya Aura® MS OVA file.
  - Hostname
  - IP address
  - Netmask
  - Gateway IP address
  - Network domain
  - IP address of the DNS servers
  - IP address of the NTP servers
- Ensure that the required network interfaces are connected before deploying the OVA. The AVP and Utility Services IP addresses are available on NIC 1. Media server network interfaces are selected at the time of deployment and use a free network interface controller starting with NIC 4.
- NIC 1 is the connection for AVP and Utility Services management. The NIC you choose for the media server traffic and management during deployment must be on the same subnet as NIC1.
- To determine the current NIC configuration on the system and to make changes to the NIC configuration, see the “Network” chapter in *Migrating and Installing Avaya Appliance Virtualization Platform*.
- If you are redeploying an Avaya Aura® MS VM appliance, ensure that you remove the current Avaya Aura® MS VM from SDM.

Procedure

1. To gain access to the **SDM Dashboard**, log in to System Manager and navigate to **Services** > **Solution Deployment Manager** or launch the Avaya SDM Client on your Windows® computer.

2. Click **VM Management**.
3. Navigate the **VM Management Tree** and click the name of the required AVP host.
4. On the **Virtual Machines** tab, click **New**.

   The system displays **VM Deployment** window.
5. In the **Select Location and Host** section, select the required data stored from the **Data Store** drop-down menu.
6. Click **Next**.
7. In the **Deploy OVA** section, set **Select Software Library** to the library that contains the required OVA file.
8. In the **Deploy OVA** section, select the required Avaya Aura® MS OVA file:
   - If you are using SDM in System Manager, set the **Select OVAs** field to the required OVA file.
   - If you are using SDM Client, select options in the **Deploy OVA** section that locate the required OVA file. Click **Submit** if required.
9. In the **Deploy OVA** section, select the required deployment configuration profile in the **Flexi Footprint** field.

   See application documentation for the recommended system profile.
10. Click **Next**.
11. On the **Configuration Parameters** tab, type a name for the new VM in the **VM Name** field.
12. In the **Network Settings** section on the **Configuration Parameters** tab, enter the required network settings, as follows:
    a. Enter an IP address for the media server in the **Media Server IP address** field. The IP address you enter must be on the same subnet as AVP and Utility Services.
    b. Enter a hostname for the VM in the **Short Hostname** field.
    c. Enter the **Network domain, Media Server netmask, Default gateway,** and **DNS Servers** as required for your network.
13. In the **System Time Settings** section, on the **Configuration Parameters** tab, enter the optional time settings.
14. In the **Customer Login Settings** section, on the **Configuration Parameters**, enter a **Login Name** and **Password** for your customer account.
15. On the **Network Parameters** tab, in the **AMS Public** field, select an NIC for Avaya Aura® MS. The NIC you select must be on the same subnet as AVP and Utility Services.
16. Click **Deploy**.

    The system displays the end user license agreement.
17. Read the license agreement and click **Accept**.
18. To monitor the status of the deployment, click on the **Virtual Machines** tab.

19. **(Optional)** To monitor individual steps of the deployment process, click **Status Details** in the **Current Action Status** column for the VM you are deploying.

Chapter 4: Deploying in the VMware® virtualized environment

System requirements

The Avaya Aura® MS appliance is deployed using a vSphere client connected to a vCenter or directly to a standalone ESXi host. You can deploy an Avaya Aura® MS 7.7 appliance in an ESXi 5.1, ESXi 5.5 or ESXi 6.0 vSphere system.

The ESXi host must meet the following system requirements:

ESXi host resource	Requirement
CPU	The core processor speed must be at least 2294 MHz. The total number of ESXi host vCPUs cannot exceed the total number of physical CPUs. Configuration profile 1 and 2 require 4 vCPUs. Configuration profile 3 and 4 require 8 vCPUs.
Memory	Configuration profile 1 and 2 require 4608 MB of memory. Configuration profile 3 and 4 require 8192 MB of memory.
Disk space	Configuration profile 1 and 3 require 52 GB of ESXI datastore. Configuration profile 2 and 4 require 250 GB of ESXI datastore.
Network bandwidth	A dedicated pair of 1 Gbps network interfaces must be available in a teamed, failover configuration. Alternatively, 1 Gbps of dedicated bandwidth on a pair of 10 Gbps network interfaces must be available in a teamed, failover configuration.

The following vSphere features are not supported and must not be configured for Avaya Aura® MS appliances:

- vMotion for running VMs
- Storage vMotion
- High Availability
- Fault tolerance
- Distributed Resource Scheduler (DRS)
- Distributed Power Management (DPM)
- VM snapshots, which adversely impact the VM disk and CPU performance

Best practice recommendations

Use the following best practices to deploy the Avaya Aura® MS appliance in the VMware® virtualized environment:

- All physical servers that can host a VM must have the same CPU, memory, and networking specifications.
- Do not modify the CPU or memory reservations that are set for Avaya Aura® MS OVA.
- Physical CPUs on the host must not be oversubscribed with respect to vCPU count across all VMs that share the host with Avaya Aura® MS. A physical CPU refers to a physical CPU core and not to a hyper-thread. For example, the total number of vCPUs across all VMs on an ESXi host that has 12 physical cores with 24 hyper-threads, must not exceed 12.

  Note:

  This recommendation prevents CPU oversubscription. Therefore, the CPU reservation of the media server VM effectively enforces the minimum CPU core speed of the underlying hardware. The VM fails to start if the underlying hardware does not meet the core speed requirements.
- For maximum system performance, ensure that the energy savings features are disabled or that the maximum performance settings are enabled in the server BIOS.
- When deploying the OVA file, select **Thick Provision Lazy Zeroed** option for the VM virtual disks.
- If the physical network interfaces on the ESXi host are 10 Gbps interfaces, then NetIOC and traffic shaping must be performed. NetIOC and traffic shaping must allocate 1 Gbps of network bandwidth for the Avaya Aura® MS VM.
- Old media server backup files must be removed to maintain free space on the system.

Obtaining Avaya Aura® MS OVA

About this task

You can download Avaya Aura® MS OVA from the Avaya Product Licensing and Delivery System (Avaya PLDS) at https://plds.avaya.com.

You can also order DVDs containing the OVA using the following details:

- Material ID: 700512735
- Material Description: AAMS R7 MEDIA DVD - OVA
- DVD Label: Avaya Aura® Media Server 7.7 Virtual Appliance for AVP and VMware®

Next steps

Deploy the OVA file using vSphere Client.

Deploying the OVA file by using vSphere Client

Before you begin

- Install the vSphere Client Windows application on the workstation. Alternatively, follow the procedure to use vSphere web client.
- Obtain the Avaya Aura® MS 7.7 OVA file and save it on the workstation where you will run vSphere Client to configure the new VM.
- Obtain the following networking configuration settings for the new VM. These settings can be from an existing system if you are redeploying the Avaya Aura® MS OVA file.
  - Hostname
  - IP address
  - Netmask
  - Gateway IP address
  - Network domain
  - IP address of the DNS servers
  - IP address of the NTP servers
- Ensure that you turn off the current Avaya Aura® MS VM appliance.

Procedure

1. Log in to the VMware® host by using the vSphere Client Windows application provided by VMware®.
2. Navigate to **Home** > **Inventory** > **Hosts and Clusters**.
3. Expand the inventory tree of hosts and clusters to locate and select the target deployment host.
4. From the menu, click **File** > **Deploy OVF Template**.
5. To locate the required Avaya Aura® MS OVA file, click **Browse**. Select the required file and click **Open**.
6. Review the file selection and click **Next**.
7. Confirm the properties of the OVA file that you selected on the OVF Template Details page, and click **Next**.
8. To accept the End User License Agreement, click **Accept**, and click **Next**.
9. Enter a name for the new Avaya Aura® MS VM, and click **Next**.
10. Select the required deployment configuration profile in the **Configuration** field, and click **Next**.

    See application documentation for the recommended system profile.

Important:

The VM disk size is always 50 GB when using VMware® deployment tools. Only the Avaya AVP deployment tools automatically extend the default disk size above the 50 GB default size. To manually extend the disk size above 50 GB, use standard VMware® procedures to edit the virtual hardware settings of a deployed VM.

11. Select the required datastore for the new VM from the list, and click **Next**.
12. Select the **Thick Provision Lazy Zeroed** disk format option, and click **Next**.
13. Select the required destination network, and click **Next**.
14. Configure the details for the new VM on the **Properties** page, and click **Next**.
15. On the **Ready to Complete** page, verify the options.
    a. If the values are incorrect, click **Back** to make changes
    b. Do not select the **Power on after deployment** option.
    c. If the values are correct, click **Finish**.

    Wait for the system to complete the deployment. The time taken to complete the deployment depends on the speed of the network connection and server.

    Tip:

    You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.
16. Locate the new VM in the inventory list, right-click on the VM entry in the list of the vSphere Client window, and click **Power** > **Power On**.
17. **(Optional)** To open a console window on your VM, right-click the VM entry in the inventory list and click **Open Console**.

    A console window displays the progress of the VM system initializing.
18. When the VM initialization is complete, you can log in by using the customer account that you set up earlier.
19. Perform the **Updating VMware® Tools** procedure.

Related links

Updating VMware® Tools on page 29

Deploying the OVA file by using vSphere web client

About this task

The steps in this procedure use the vSphere web client, which runs in a web browser. Alternatively, follow the procedure to use the vSphere Client, which is a Windows application you install on the workstation.

Before you begin

- Obtain the Avaya Aura® MS 7.7 OVA file. Save the file on the workstation where you will run vSphere web client to configure the new VM.
- Obtain the following networking configuration settings for the new VM. These settings can be from an existing system if you are redeploying Avaya Aura® MS OVA.
  - Hostname
  - IP address
  - Netmask
  - Gateway IP address
  - Network domain
  - IP address of the DNS servers
  - IP address of the NTP servers
- Ensure that you turn off the current Avaya Aura® MS VM appliance.

Procedure

1. Log in to the VMware® host by using the vSphere web client:

   `https://vCenterAddress:9443/vsphere-client`
2. In the vSphere Web Client navigator area on the left, click **vCenter**.
3. In **Inventory Trees**, click **Hosts and Clusters**.
4. Expand the inventory tree of hosts and clusters to locate and select the target deployment host.
5. From the menu, right-click the host and select **Deploy OVF Template**.
6. **(Optional)** If the **Client Integration Access Control** window pops up, click **Allow**.
7. For **1a Select source**, select **Local file**, and click **Browse**.
8. From the file filter drop-down menu in the lower right of the window, click **OVA Packages (*.ova)**.
9. Select the required Avaya Aura® MS OVA file, and click **Next**.
10. Confirm the properties of the OVA file that you selected on the **Review details** page, and click **Next**.
11. To accept the End User License Agreement, click **Accept** and **Next**.
12. Enter a name for the new Avaya Aura® MS VM, and click **Next**.
13. Select the required deployment configuration profile in the **Configuration** field, and click **Next**.

    See application documentation for the recommended system profile.

Important:

The VM disk size is always 50 GB when using VMware® deployment tools. Only the Avaya AVP deployment tools automatically extend the default disk size above the 50 GB default size. To manually extend the disk size above 50 GB, use standard VMware® procedures to edit the virtual hardware settings of a deployed VM.

14. Expand the tree under the vCenter server and select the required datacenter folder, and click **Next**.
15. Select **Thick Provision Lazy Zeroed** for the virtual disk format.
16. Select the required destination datastore, and click **Next**.
17. Select the required destination network, and click **Next**.
18. Expand **Network Settings** and configure the network details for the new VM on the Customize template page.
19. Expand **System Time Settings** and configure the time settings.
20. Expand **Customer Login Settings** and configure the account settings, click **Next**.
21. On the Ready to complete page, verify the options.
    a. If the values are incorrect, click **Back** to make changes.
    b. Do not select the **Power on after deployment** option.
    c. If the values are correct, click **Finish**.

    Wait for the system to complete deployment. The time that the system requires to complete the deployment depends on the speed of the network connection and server. The system displays the progress in **Recent Tasks** > **All**.

Tip:

You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.

22. Click the refresh arrow () located to the left of your login ID at the top of the vSphere web client page.

    The system updates the inventory list and displays the new VM.
23. Select the new VM in the inventory list of the vSphere web client window and click the **Summary** tab.
24. Select **Power On** from the **Actions** menu.
25. **(Optional)** To open a console page on your VM, click **Launch Console** on the **Summary** tab.

    A console window displays the progress of the VM system initializing.
26. When the VM initialization is complete, you can log in by using the customer account that you set up earlier.
27. Perform the Updating VMware® Tools procedure.

Related links

Updating VMware® Tools on page 29

Deploying the OVA file without using vCenter

Before you begin

- Install the vSphere Client Windows application on the workstation.
- Obtain the Avaya Aura® MS 7.7 OVA file. Save the file on the workstation where you will run vSphere Client to configure the new VM.
- Obtain the following network configuration settings for the new VM. These settings can be from an existing system if you are redeploying Avaya Aura® MS OVA.
  - Hostname
  - IP address
  - Netmask
  - Gateway IP address
  - Network domain
  - IP address of the DNS servers
  - IP address of the NTP servers
- Ensure that you turn off the current Avaya Aura® MS appliance.

Procedure

1. Log in to the VMware® host using the vSphere Client Windows application provided by VMware®.
2. Navigate to **Home** > **Inventory**, and select the target deployment host in the inventory list.
3. From the menu, click **File** > **Deploy OVF Template**.
4. To locate the required Avaya Aura® MS OVA file, click **Browse**. Select the required file and click **Open**.
5. Review the file selection and click **Next**.
6. Review the OVF template details, and click **Next**.
7. To accept the End User License Agreement, click **Accept** and **Next**.
8. Enter a name for the new Avaya Aura® MS VM, and click **Next**.
9. Select the required deployment configuration profile in the **Configuration** field, and click **Next**.

   See application documentation for the recommended system profile.

Important:

The VM disk size is always 50 GB when using VMware® deployment tools. Only the Avaya AVP deployment tools automatically extend the default disk size above the 50 GB default size. To manually extend the disk size above 50 GB, use standard VMware® procedures to edit the virtual hardware settings of a deployed VM.

10. Select the **Thick Provision Lazy Zeroed** disk format option, and click **Next**.
11. Select the required destination network, and click **Next**.
12. On the **Ready to Complete** page, verify the options.
    a. If the values are incorrect, click **Back** to make changes.
    b. Do not select the **Power on after deployment** option.
    c. If the values are correct, click **Finish**.
    d. Wait for the system to complete the deployment. The time required to complete the deployment depends on the speed of the network connection and server.
13. Locate and right-click the new VM in the inventory list of the vSphere Client window, and click **Power** > **Power On**.
14. Immediately open a console window on the VM.
    a. Right-click the VM entry in the inventory list.
    b. Click **Open Console**.

    A console window displays the progress of the VM system.
15. Double-click the console window to establish keyboard focus in the console.
16. Read the End User License Agreement. Use the spacebar to scroll through the text. Type `yes` to accept the agreement and proceed.
17. After the VM system initialization is complete, you are prompted to configure the VM. Type `Y` to proceed.
18. Enter the network settings, date, time, and customer account information for the server. For **Enable static route**, use the default value of `N`.

    Tip:

    You can alter the configuration settings later by running the **`netSetup`** command in a Linux® shell.
19. Perform the Updating VMware® Tools procedure.

Related links

Updating VMware® Tools on page 29

Updating VMware® Tools

About this task

Perform the following procedure to update the version of VMware® Tools to the version required by the ESXi host.

Note:

Do not update VMware® Tools when Avaya Aura® MS is deployed on AVP.

Before you begin

- Perform updates during scheduled maintenance times.
- Ensure that the VM is running.
- Ensure that there is no traffic on Avaya Aura® MS.
- Back up the system.

  In case of unforeseen problems during the update, you can redeploy the appliance and use the backup to restore the system to the current configuration.
- Ensure that you apply the tool updates to one node at a time in a cluster configuration while the other nodes in the cluster maintain service.

Procedure

1. Determine if you need to update the VMware® tools.

   If the **VMware Tools** field on the **Summary** tab indicates **(Out-of-date)** then update VMware® Tools.

   If you are using vSphere Web Client:

   a. Click **Interactive Upgrade**.
   b. Select **Interactive upgrade**.
   c. Click **Upgrade**.

      Monitor the **Recent Tasks** section of vSphere Web Client page. Wait for the **Initiated VMware Tools Installer Mount** task to be complete. A green checkmark indicates that the task is complete.

   If you are using vSphere Client:

   a. Select the VM from the list of VMs.
   b. Right-click the VM and select **Guest** > **Install/Upgrade VMware Tools**.
   c. Select **Interactive Tools Upgrade** and click **OK**.

      Monitor the **Recent Tasks** section of vSphere Client and wait for the **Initiated VMware Tools Installer Mount** task to complete.

2. Using the customer login credentials, open a Linux® shell and run the following command to update VMware® Tools:

   ```
   updateVMwareTools
   ```

3. Review the important messages displayed by the tool.
4. Type `Y` and press `Enter` to update VMware® Tools.

   After the tool update is complete, the VM is automatically restarted to apply the changes.

   Note:

   If vSphere Client displays a question about a locked CD-ROM door, accept the default answer **No** and click **OK** to continue.

   Important:

   The update is complete after a few minutes. Do not interrupt the update by typing `Control+C` or by using any other method that ends the `updateVMwareTools` process while it is running. Interrupting the VMware® tools update can leave the tools in an inoperable state, requiring reinstallation. The VM also becomes unstable requiring you to redeploy the VM.
5. After the restart is complete, verify that the VMware® Tools update is successful.

Result

The **VMware Tools** field on the **Summary** tab for the VM indicates **(Current)** after a successful update. If you are using vSphere Web Client, refresh the web page to update the display with the latest status

Chapter 5: Deploying Avaya Common Server physical appliances

System requirements

Avaya Aura® MS physical appliances shipped with the appliance software already installed on Avaya Common Server platforms. The appliances are ready for customer network configuration when deployed. The following appliances are available:

Material ID	Avaya Common Server Description
380841	R220XL SERVER AAMS STANDARD
382929	DL360G9 SERVER AAMS LARGE
383553	R630 SERVER AAMS LARGE

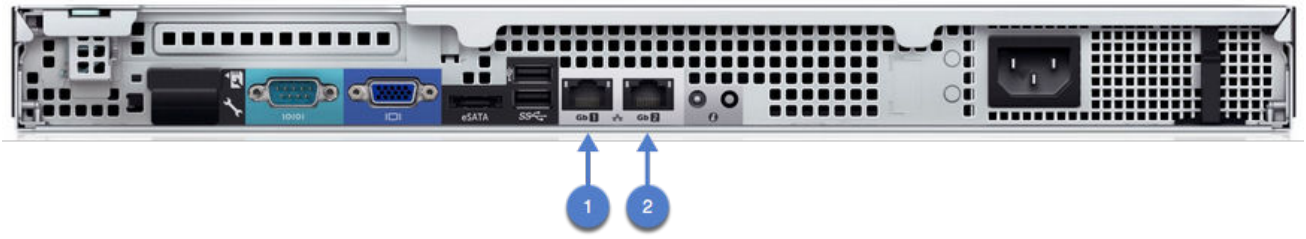
The required BIOS settings are configured by Avaya prior to delivery.

Two network interfaces are required to support Linux® channel bonding for high availability. Network cables must be plugged in to both active network interface ports.

Use the diagrams in the following sections to identify the active network interface ports on each server.

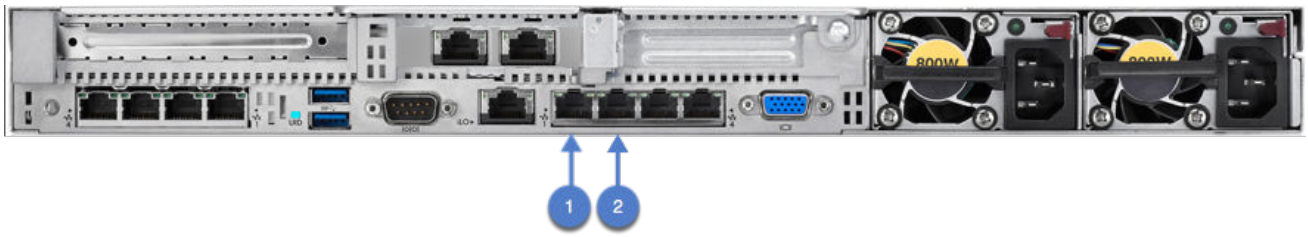
Dell R220XL active network ports

Plug Ethernet cables into the Ethernet ports labeled as 1 and 2 in the diagram. The ports on the R220XL chassis are read from left to right and are labeled 1 and 2.



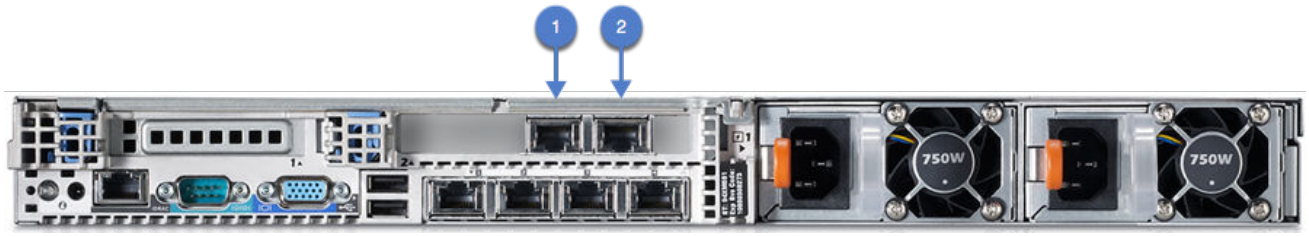
HP DL360G9 active network ports

Plug Ethernet cables into the Ethernet ports labeled as 1 and 2 in the diagram. The corresponding ports on the DL360G9 chassis are labeled as 1 and 2 in the bottom row of Ethernet ports. The bottom row of ports is read from left to right and is labeled 1 through 4.



Dell R630 active network ports

Plug Ethernet cables into the Ethernet ports labeled as 1 and 2 in the diagram. The corresponding ports on the Dell R630 chassis are labeled as 0 and 1 in the top row of Ethernet ports. The top row of ports is read from left to right, and is labeled 0 through 1.



Deploying the Avaya Aura® MS physical appliance

About this task

New Avaya Aura® MS appliances are shipped with the appliance software already installed and are ready to be deployed in the customer network.

The system automatically enters the customer configuration procedure when it starts for the first time after deployment.

Perform the following procedure to configure the Avaya Aura® MS appliance at the customer site.

Before you begin

Obtain the following network and server information:

- Hostname
- IP address

- Netmask
- Gateway IP address
- Network domain
- IP/FQDN of the primary NTP server
- NTP daemon
- IP address of the NTP servers

Procedure

1. Install one of the supported Avaya Common Server hardware platforms and plug in the network and power cables.
2. Turn on the Avaya Aura® MS appliance server.
3. Press `Y`, and then press `Enter` to start the configuration procedure.

   The system displays the instructions to configure the system time.

   Note:

   If `N` is provided as the response, then the server is automatically turned off. Configuration takes place the next time that the server is turned on.
4. Press `Enter` to continue.
5. When prompted, enter the network parameters, date, time, and customer account information for the server.

   Tip:

   You can alter the configuration settings later by running the `netSetup` command in a Linux® shell.
6. Verify the network configuration values in the response summary.

   If required, press `U` to update a value before proceeding.
7. Press `C` and then press `Enter` to continue.

   The system applies the network configuration and displays a prompt to configure the customer login ID.
8. Enter a login ID to use for the customer account and press `Enter`.
9. Press `C` and then press `Enter` to continue.

   The system displays the set password prompt.
10. Enter a password for the login ID to use for the customer account and press `Enter`.
11. Type the password again to confirm and press `Enter`.

    The server configuration is complete. After several seconds, system initialization is complete and the system displays the login prompt.

Obtaining physical appliance recovery software

New Avaya Aura® MS 7.7 appliances are shipped with the appliance software already installed. Avaya Aura® MS appliance software is only required to support the field replacement procedure, for example, disk replacement.

You can download Avaya Aura® MS recovery software from the Avaya Product Licensing and Delivery System (Avaya PLDS) at https://plds.avaya.com.

You can also order DVDs containing the recovery software using the following details:

- Material ID: 700512734
- Material Description: AAMS R7 MEDIA DVD – Bare Metal
- DVD Label: Avaya Aura® Media Server 7.7 FP1 server Appliance Installer/Recovery DVD.

Next Steps:

Reinstall the Avaya Aura® MS physical appliance.

Reinstalling the Avaya Aura® MS physical appliance

About this task

New Avaya Aura® MS appliances are shipped with the appliance software already installed. The Avaya Aura® MS appliance software is reinstalled only to support field replacement procedures, for example, disk replacement.

Important:

All data is lost when you reinstall Avaya Aura® MS appliance.

Perform the following procedure to format the system disk and reinstall Avaya Aura® MS appliance.

Before you begin

- Obtain the Avaya Aura® MS physical appliance software installation DVD.
- The power to the server must be on so that the disc tray can be opened.

Procedure

1. Open the system disc tray, insert the Avaya Aura® MS appliance installation disc, and close the disc tray.
2. Restart the server by using one of the following methods:
   - Press `Control+Alt+Delete` on your keyboard, and select **Restart**.
   - Type `reboot` in a Linux® shell.
   - Press the power button to turn the server off and then press the power button again to turn it back on.
   - Press the reset button until the server restarts.

The system restarts from the installation disc. After several minutes, the system displays the Avaya Aura® Media Server welcome screen.

Tip:

The welcome screen displays the appliance build number, a list of detected network interfaces, and a list of attached storage devices with their sizes. Review this information for accuracy to verify whether these characteristics are as expected.

3. Press `Y` to proceed with the installation.

   The system installs the operating system, ejects the disc tray, and automatically reboots. The system automatically installs Avaya Aura® MS after the reboot. After several minutes, the system displays the installation result.

   Note:

   When you type `N` in response to the confirmation prompt, then the installation is cancelled and the server is automatically turned off. The installation can be restarted later.

4. Press `Enter` to turn off the server.

   The system turns off and is ready to be configured the next time that the server is turned on.

   Note:

   The next time the server is turned on, the system confirms that a configuration must be performed. If `N` is provided as the response, then the server is immediately turned off. This procedure is useful for verifying that the system successfully starts. Use the `Y` response only when the system is ready to be configured.

Next steps

Deploy the Avaya Aura® MS physical appliance.

Chapter 6: Signing in to the Avaya Aura® MS appliance

Element Manager

Element Manager (EM) is a web-based administration tool that facilitates the operation, administration, and maintenance (OAM) of Avaya Aura® MS.

For more information and detailed procedures about using Avaya Aura® MS EM and configuring your browser to use Avaya Aura® MS EM, see *Implementing and Administering Avaya Aura® Media Server 7.7*.

Accessing Avaya Aura® MS EM

About this task

Use this procedure to gain access to EM on the Avaya Aura® MS appliance. You need EM to perform some procedures mentioned in this document.

Procedure

1. In a web browser, type the following URL:

   `https://serverIP:8443/em`

   where, *serverIP* is the address of Avaya Aura® MS. For example,

   `https://10.60.86.209:8443/em`

2. Sign in to Avaya Aura® MS EM by using the customer account username and password.

   The customer account is created during the initial power-up configuration procedure.

Accessing Linux® shells

You must gain access to Linux® shells to perform some of the procedures in this document. Use Secure Shell (SSH) to access the Linux® command-line on the Avaya Aura® MS appliance. Use the

customer account or support account credentials for SSH log in. The customer account is created during customer server configuration of the Avaya Aura® MS appliance.

The system supports a maximum of five simultaneous logins for each user account. The system rejects additional SSH and Putty sessions when five sessions are already logged in.

Note:

To protect the system, the customer account does not have root privileges. Avaya has added some root privileges to the customer account using Linux® sudoer aliases. Enable Avaya support access and contact Avaya support if additional privileges are required.

Enabling Avaya support access

About this task

You can enable one of several pre-defined service accounts on the system so that Avaya Support Engineers can remotely access the system. Access to the service accounts requires a one-time set-up of the Avaya Access Security Gateway (ASG) authentication system. ASG employs a challenge and response protocol to confirm the validity of the Avaya support personnel accessing the system.

Perform the following procedure to install an authentication file and enable secure access for Avaya Support Engineers.

Before you begin

Obtain the Avaya Aura® MS authentication file from Avaya.

Procedure

1. Log in to a Linux® shell by using the customer account.

   The customer account is created during the deployment procedure.

2. Transfer the authentication file to the home directory of the customer account. Use the `sftp` file transfer tool, or another similar tool to transfer the file.

   Note:

   If you are using a remote-file-transfer client like WinSCP or FileZilla to upload the authentication file to the system then you must provide the customer account credentials to the tool.

3. Enable ASG by using the authentication file that you uploaded with the following command:

   ```
   loadpwd -f -l AuthFile.xml
   ```

Chapter 7: Configuration

Configuring Avaya Aura® MS

To configure Avaya Aura® MS, enable additional capabilities, and create clusters, see *Implementing and Administering Avaya Aura® Media Server 7.7*.

Chapter 8: Network configuration

Updating the network configuration

About this task

Server networking information can be updated by using the `netSetup` command in a Linux® shell. The `netSetup` command guides you through the process of updating the following settings:

- Time zone and UTC
- Date and time
- Hostname
- IP address
- Netmask
- Gateway address
- Domain name
- Static route (virtual appliance only)
- Up to three DNS server IP addresses
- Up to three NTP server IP addresses

Before you begin

Stop Avaya Aura® MS before changing the network configuration. See *Implementing and Administering Avaya Aura® Media Server 7.7*.

Procedure

1. Log in to a Linux® shell using the customer account.
2. Type the following command:

   `netSetup`

   Follow the on screen prompts to update the network settings.

   Accept the system-determined default value for the **Enable static route** prompt. **Enable static route** has a default value of `Y` for Avaya Appliance Virtualization Platform systems. When you press `Enter` with a value of `Y`, the system displays prompts that allow you to reconfigure the Utility Services static route. All other virtual appliance installations must use the default value of `N` for **Enable static route**.

3. Perform the following steps if you changed the IP addresses or hostname.
   a. Navigate to **EM** > **System Configuration** > **Network Settings** > **IP Interface Assignment**.
   b. **IP Interface Assignment** fields show errors, due to the IP address change. Select valid IP addresses from the drop-down menus for each field showing **Invalid**.
   c. If you are using security certificates with information dependent on FQDN or other server specific information, create new certificates. To update the certificates navigate to **EM** > **Security Certificate Management**.
   d. If this server is a member of a load sharing cluster or High Availability cluster, then navigate to **EM** > **Cluster Configuration** > **Server Designation**.

      On each server, ensure that the IP address you just changed is updated.
   e. If this server is a primary server of a master cluster, then replication clusters that point to the master cluster must be updated with the new address of this server.

      On the primary node in each replication cluster, navigate to **EM** > **Cluster Configuration** > **Replication Settings** > **Master Cluster Primary Node Address**.

   For more information on configuring each item, see *Implementing and Administering Avaya Aura® Media Server 7.7*.
4. You must restart the server. Use one of the following methods to restart the server:
   - Press `Control+Alt+Delete` on your keyboard, and select **Restart**.
   - Type `reboot` in a Linux® shell.
   - Press the power button to turn the server off and then press the power button again to turn it back on.
   - Press the reset button until the server restarts.

Chapter 9: Backup and restore

Performing a backup

About this task

Perform the following procedure to create a backup of the system configuration and application content. For more information about backup and restore, see *Implementing and Administering Avaya Aura® Media Server* 7.7.

Procedure

1. To backup Avaya Aura® MS data, navigate to **EM** > **Tools** > **Backup and Restore** > **Backup Tasks**.
2. Create or select an existing backup task that includes System Configuration and Application Content backup types.
3. Click **Run Now**.
4. To monitor the Backup and Restore History Log, navigate to **EM** > **Tools** > **Backup and Restore** > **History Log**.

   After the backup is complete, the log shows a completed backup task entry.
5. If you are using an FTP or SFTP backup destination, ensure that the backup files are saved to their required location.

   There is one file for each backup type for a total of two backup files.
6. If you are using a local backup destination and about to perform an upgrade or redeploy of the Avaya Aura® Media Server (MS) appliance, you must move the backup files to a safe location by performing the following steps:
   a. Log in to a Linux® shell using the customer account.
   b. Change to the public directory by using the `cdpub` alias or the following command:

      ```
      cd /opt/avaya/app/pub
      ```
   c. List the backups available on the local system by using the following command:

      ```
      bkupFile -list
      ```
   d. Move the recent configuration and application data backups from the local backup storage to the current directory by using the following commands:

      ```
      bkupFile -retrieve SystemConfiguration_backup.zip
      ```

      ```
      bkupFile -retrieve ApplicationContent_backup.zip
      ```

e. Save both backup files in a safe location by using the `sftp` file transfer tool, or another similar tool, to transfer the files off the server.

f. After you confirm the files are saved in a safe location, you can delete the backup files from the current directory to free disk space.

Uploading and restoring backup files

About this task

Use this procedure to upload backup files to Avaya Aura® MS appliance.

Procedure

1. Perform the EM web browser-based upload task.

   See Uploading a backup file for a restore in *Implementing and Administering Avaya Aura® Media Server 7.7*.

2. Perform the EM task to restore data using a backup saved in the default local backup destination.

   See Restoring from the local destination in *Implementing and Administering Avaya Aura® Media Server 7.7*.

Related links

Alternate procedure for uploading and restoring large backup files on page 42

Alternate procedure for uploading and restoring large backup files

About this task

Use this procedure if you encounter errors when using EM to upload backup files to Avaya Aura® MS appliance. Many browsers have a 2 GB limit on file upload. Perform the following procedure to upload backup files larger than 2 GB to the local backup destination.

Procedure

1. Log in to a Linux® shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:

   `cd /opt/avaya/app/pub`.

3. Transfer the configuration and application data backups to the system by pulling them with the `sftp` file transfer tool, or another similar tool.

4. Move the configuration and application data backups from the current directory into the local backup storage by using the following commands:

   ```
   bkupFile -insert SystemConfiguration_backup.zip
   ```

   ```
   bkupFile -insert ApplicationContent_backup.zip
   ```

5. Confirm the backup files are available on the local system by typing the following command:

   ```
   bkupFile -list
   ```

6. Perform the EM task to restore data using a backup saved in the local backup destination.

   For information about restoring from the local destination, see *Implementing and Administering Avaya Aura® Media Server* 7.7.

Chapter 10: Updates

Viewing the installed version and updates

About this task

Perform the following procedure to display information about the currently installed software.

Procedure

1. Log in to Avaya Aura® MS EM by using the customer account username and password.
2. Display the installed software by navigating to **EM** > **Tools** > **Manage Software** > **Inventory**.

   EM displays the currently installed software versions for the application and system layers.
3. Display details about the last installed update by navigating to **EM** > **Tools** > **Manage Software** > **History**.

   EM displays the last installed updates for the application and system layers. Only official updates are listed.

Related links

Accessing Avaya Aura MS EM on page 36

Uploading media server updates

About this task

The Avaya Aura® MS application and system software updates are versioned and delivered separately. Uploading the software updates makes them available for installation.

Perform the following procedure to upload each required software update to Avaya Aura® MS.

Procedure

1. Navigate to **EM** > **Tools** > **Manage Software** > **Updates**.
2. To select the software update to upload, click **Browse**.

   The selected file must be an official Avaya Aura® MS update package in ISO format.
3. Click **Upload**.

   The browser shows a progress spinner while the system uploads the file.

When the upload completes the system displays the license agreement.

4. Read the license agreement and click **Accept**.

   The browser shows a progress spinner while the system verifies the integrity and authenticity of the update.

   The system displays the details of the update including the filename of the uploaded file.

5. Use the chevron buttons to expand (⌄) and collapse (⌃) additional details about the update.

Next steps

Repeat this procedure for each required update.

Install the update.

Related links

Uploading media server updates using a Linux® shell on page 45
Unable to upload updates on page 58
Installing an update on page 46
Deleting an uploaded update on page 46

Uploading media server updates using a Linux® shell

About this task

The Avaya Aura® MS application and system software updates are versioned and delivered separately. Uploading the software updates makes them available for installation.

Perform the following procedure to upload each required software update to Avaya Aura® MS.

Procedure

1. Log in to a Linux® shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:

   ```
   cd /opt/avaya/app/pub
   ```

3. Transfer the update package to the `pub` directory. You can use the `sftp` file transfer tool, or another similar tool, to transfer the file. The file must be an official update from Avaya in ISO format.

   Tip:

   After you upload the update to one server, you can copy the update to other local servers. This is faster than transferring the file multiple times from a workstation that may be on another network.

4. Run the following command to stage the software:

   ```
   stageUpdate -stage -f softwareUpdate.iso
   ```

Next steps

Repeat this procedure for each required update.

Install the update.

Related links

Installing an update on page 46
Deleting an uploaded update on page 46

Deleting an uploaded update

About this task

Perform the following procedure to remove an update that has been uploaded to the media server but not yet installed.

Procedure

1. To view the uploaded updates, navigate to **EM** > **Tool** > **Manage Software** > **Updates**.
2. To delete an update click **Delete** next to the update.

   The system immediately deletes the update.

Installing an update

About this task

Perform the following procedure to update the media server to the latest software release when Avaya Aura® MS 7.7 is already on FP1 or later.

Important:

If Avaya Aura® MS 7.7 is on a version earlier than Application layer 7.7.0.334_A15 and System layer 7.7.0.19, then you must use the Updating to FP1 on page 48 procedure instead of using this procedure.

Before you begin

Before applying media server updates, ensure that you:

- Upload an update by using the Uploading media server updates task. You can upload an update prior to the scheduled maintenance time for installing an update, to avoid delays during the maintenance time.
- Back up the system. In case of unforeseen problems during the update installation, you can use the backup to restore the system to the current configuration.
- Apply the updates to one node at a time in a cluster configuration, while the other nodes in the cluster maintain service. For High Availability clusters, see Managing media server changes for 1+1 High Availability clusters on page 50.

- Perform updates during scheduled maintenance times.

Procedure

1. To prevent new sessions from starting on the system, navigate to **EM** > **System Status** > **Element Status** and select **More Actions** > **Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

   Wait for the active sessions to end. The media server automatically changes to the Locked state after all the sessions have ended.

   Perform the following steps if you want to continue before the active sessions end:

   a. Manually lock Avaya Aura® MS, by navigating to **EM** > **System Status** > **Element Status** and clicking **More Actions** > **Lock**. Locking the media server also ends any remaining sessions.

   b. Click **Confirm**.
4. To install the uploaded updates, navigate to **EM** > **Tools** > **Manage Software** > **Updates** and click **Install Updates...**
5. Click **Confirm**.

   The browser shows a progress spinner while the update is installed.

   The update is complete when you can log in to EM.
6. Navigate to **EM** > **Tools** > **Manage Software** > **History**.
7. Verify that the expected versions are displayed.
8. Use the chevron buttons (⌄⌄) to expand the details about each update.
9. Verfify that each listed update component indicates **(Installed)**.
10. Select **EM** > **System Status** > **Element Status** > **More Actions** > **Unlock**.
11. Click **Confirm**.
12. Check for any service-impacting alarms and perform an appropriate test of the system.

    For example, place a call to the application.

Related links

Uploading media server updates on page 44
Managing media server changes for 1+1 High Availability clusters on page 50
Updating to FP1 on page 48

Updating to FP1

About this task

Perform the following one-time procedure to update Avaya Aura® MS with no feature packs to the latest software release with FP1 or later.

Avaya Aura® MS 7.7 FP1 provides a new, easier to use software update procedure. After you update the media server to FP1 or later, see Installing an update on page 46 to install updates.

Before you begin

Before applying media server updates:

- Upload both the media server and system later updates.
- Back up the system. In case of unforeseen problems during the update installation, you can use the backup to restore the system to the current configuration.
- Apply the updates to one node at a time in a cluster configuration while the other nodes in the cluster maintain service. For High Availability clusters, see Managing media server changes for 1+1 High Availability clusters on page 50.
- Perform updates during scheduled maintenance times.

Procedure

1. To prevent new sessions from starting on the system, navigate to **EM** > **System Status** > **Element Status** and select **More Actions** > **Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

   Wait for the active sessions to end. The media server automatically changes to the Locked state after all the sessions have ended.

   Perform the following steps if you want to continue before the active sessions end:

   a. Manually lock Avaya Aura® MS, by navigating to **EM** > **System Status** > **Element Status** and clicking **More Actions** > **Lock**. Locking the media server also ends any remaining sessions.

   b. Click **Confirm**.
4. Close all open Linux® shells that are connected to Avaya Aura® MS.
5. Using the customer login credentials, log in to a new Linux® shell and run the following command to install the Avaya Aura® MS software update: `installUpdate`.

   Note:

   The system reports the `installUpdate` command as not found if you do not use a new Linux® shell.
6. Type `yes` to start the installation.

   The system displays the following message:

```
Proceeding...
Update installation scheduled successfully
```

Within one minute, the system begins to install the updates and performs several reboots to apply the changes.

The update takes less than 15 minutes. The update is complete when you can login to EM.

7. Verify that the required software is installed by navigating to **EM** > **Tools** > **Manage Software** > **Inventory**.
8. To view the details of the most recently installed updates navigate to **EM** > **Tools** > **Manage Software** > **History**.

   EM displays a page indicating the date each update was installed and details describing the content of the update.
9. Use the chevron buttons (⌄) to expand the details about each update.
10. Verify that each listed update component indicates **(Installed)**.
11. To verify the media server is started, select **EM** > **System Status** > **Element Status**.
12. Select **EM** > **System Status** > **Element Status** > **More Actions** > **Unlock**.
13. Click **Confirm**.
14. Check for any service-impacting alarms and perform an appropriate test of the system. For example, place a call to the application.

Related links

Uploading media server updates on page 44
Managing media server changes for 1+1 High Availability clusters on page 50

Removing an installed update

About this task

The update removal procedure removes service packs, feature packs and update revisions from the system.

If you follow this procedure, you do not have to re-configure or re-provision the system. All system configuration and application content data are preserved.

Remove updates during scheduled maintenance times.

Perform the following procedure to remove an installed update from your system.

Before you begin

Before proceeding with the software removal, ensure that you:

- Use Element Manager to upload the previously installed software version so that you can reinstall the earlier software. You cannot install a version older than the original factory version installed on the appliance.

- Back up the system.

  In case of unforeseen problems during the update removal, you can use the backup to restore the system to the current configuration.

- Remove updates one node at a time in a cluster configuration. The other nodes in the cluster maintain service. For High Availability clusters, see Managing media server changes for 1+1 High Availability clusters on page 50.

Procedure

1. To remove the currently installed update and roll back to an earlier update, you must first upload the required earlier update to the media server. See Uploading media server updates on page 44.
2. To install the earlier update, see Installing an update on page 46.

Related links

Uploading media server updates on page 44
Installing an update on page 46

Managing media server changes for 1+1 High Availability clusters

About this task

Use this procedure to install or remove a media server update in High Availability clusters. Changes are applied as follows, to prevent loss of service:

1. Apply or remove the update for the standby server.
2. After activating the updated standby server, apply or remove the update for the other server.

Before you begin

If you are updating both the system layer and the Avaya Aura® MS software, then update the system layer software first.

Procedure

1. Navigate to **EM** > **Element Status** on each server and determine which server has the **High Availability State** of Standby or Active.
2. To lock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and select the **Local High Availability State Lock** check box.
3. Click **Save**.
4. Click **Confirm**.
5. To install or remove an update for the standby server, go to Step 4 of the procedure for Installing an update on page 46 or Updating to FP1 on page 48, as appropriate.

Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.

6. To unlock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and clear the **Local High Availability State Lock** check box.
7. Click **Save**.
8. Click **Confirm**.
9. To put the active server in the standby state, navigate to **EM** > **Element Status** and select **Failover** from the **More Actions** drop-down menu.
10. Click **Confirm**.

    The active server is now the standby server.
11. To lock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and select the **Local High Availability State Lock** check box.
12. Click **Save**.
13. Click **Confirm**.
14. To install or remove an update for the standby server, go to Step 4 of the procedure for Installing an update on page 46 or Updating to FP1 on page 48, as appropriate.
15. Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.
16. To unlock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and clear the **Local High Availability State Lock** check box.
17. Click **Save**.
18. Click **Confirm**.

Related links

Installing an update on page 46
Updating to FP1 on page 48

Chapter 11: Upgrade from a previous release

Upgrade overview

You can upgrade a system from Avaya MS 7.6 to Avaya Aura® MS 7.7 by deploying the Avaya Aura® MS 7.7 appliance. You can transfer the configuration and application data to the new system using backups of the Avaya MS 7.6 system with the Avaya Aura® MS 7.7 upgrade tool.

Perform upgrades only during the maintenance window or at an off peak-usage time.

The upgrade procedures set the operational state of the media server to Pending Lock. The purpose of placing the media server in the Pending Lock state is to ensure that the system does not start any new sessions. After all the sessions on the server have ended, the server can be upgraded without disruption to any users.

When you are ready to upgrade the server, the operational state is set to Locked, which ends any remaining active sessions.

If the media server is set to Pending Lock before the upgrade maintenance window, then the system ends a minimum number of user sessions, if any.

Upgrading to Avaya Aura® MS 7.7

About this task

A standalone media server that is not part of a cluster is referred to as a simplex media server. Each media server appliance, whether simplex or part of a cluster, is upgraded as follows:

- Back up the configuration and application data.
- End active sessions by setting the server through a progression of Pending Lock, Lock, and Stopped states.
- Shutdown the Avaya MS 7.6 appliance.
- Deploy the Avaya Aura® MS appliance.
- Use the Avaya Aura® MS upgrade tool to restore and upgrade preserved Avaya MS 7.6 configuration and application data.
- Verify the system is functional and that there are no unexpected alarms.

Before you begin

- If you are upgrading a server that is a member of a cluster, ensure that you are performing this task as part of one of a cluster upgrade procedures before continuing. Ensure that you start at the correct step in the following procedure, as specified by the cluster upgrade procedure.
- Ensure that the current media server is on release 7.6. You can check the installed software version on the EM Home page or by navigating to **EM** > **System Status** > **Element Status** > **Installed Software Packages**.
- Create Avaya MS 7.6 backups. Avaya MS 7.6 configuration and application data backups are required to preserve the data through the upgrade process and if a rollback to Avaya MS 7.6 is required.

Procedure

1. To prevent new sessions from starting on the system, navigate to **EM** > **System Status** > **Element Status** and select **More Actions** > **Pending Lock**.
2. Click **Confirm**.
3. Check for active sessions on the server by navigating to **EM** > **System Status** > **Monitoring** > **Active Sessions**.

   Wait for the active sessions to end. The media server automatically changes to the Locked state after all the sessions have ended.

4. Perform the following steps if you want to continue before the active sessions end:
   a. Manually lock Avaya Aura® MS, by navigating to **EM** > **System Status** > **Element Status** and clicking **More Actions** > **Lock**.

      Locking the media server also ends any remaining sessions.

   b. Click **Confirm**.
5. After the system ends all the sessions, stop Avaya Aura® MS by navigating to **EM** > **System Status** > **Element Status** and clicking **Stop**.
6. Click **Confirm**.
7. You must use the same hostname and server IP address information on the new system.
8. Perform the following steps to collect the current network configuration of the server:
   a. Log in to a Linux® shell using the customer account and type the following command:

      `netSetup`

   b. Press `Enter` or `C` followed by `Enter` to advance through each configuration item. Take note of the current values and save them to use when setting up the new system. Do not alter any values.

   c. When the system prompts you to verify responses, press `A` and press `Enter` to exit the tool.
9. Before proceeding, ensure that you have system configuration and application content backups saved off of the server.

Backup files are used to upgrade the current data. All data is lost if you do not have a backup of your Avaya MS 7.6 data.

10. Shutdown the server.
11. Use an appropriate appliance deployment procedure to install Avaya Aura® MS 7.7 on the system.

    You must configure the new system with the network setup data you saved from the Avaya MS 7.6 system. During the Avaya Aura® MS 7.7 appliance deployment you configure the customer login credentials. You can also perform the procedures for enabling Avaya support access and updating VMware® tools.
12. After the deployment is complete, log in to the new Avaya Aura® MS EM.

    If security alert dialog boxes appear in the browser, accept the new security conditions to proceed.
13. To stop Avaya Aura® MS, navigate to **EM** > **System Status** > **Element Status** and click **Stop**.
14. Click **Confirm**.
15. Log in to a Linux® shell using the customer account.
16. Change to the public directory by using the `cdpub` alias or the following command:

    ```
    cd /opt/avaya/app/pub
    ```
17. Transfer the two backup files to the system. You can use the `sftp` file transfer tool, or another similar tool, to transfer the files to the `pub` directory.
18. Use the upgrade tool to upgrade the system configuration data by running the following command:

    ```
    amsupgrade SystemConfigBackupFilename.zip
    ```

    Important:

    - Restore the system configuration data before restoring the application data to ensure that the application data is restored to the configured location.
    - Backup data is not portable from one server to another. If you need to replace a server, you must configure the server with the same installation path, IP address, and hostname so that the data is compatible with the server configuration.
19. Press `Y` to stop all Avaya Aura® MS services when prompted.

    The tool upgrades the data.
20. Use the upgrade tool to upgrade the application content data by running the following command:

    ```
    amsupgrade AppContentBackupFilename.zip
    ```
21. Press `Y` to stop all Avaya Aura® MS services when prompted.

    The tool upgrades the data.

Note:

The time required to complete the application content upgrade depends on the amount of application data in the backup file.

22. The VoiceXML application interpreter is disabled by default. If you are using VXML applications, then you must perform the following steps to activate VXML functionality.
    a. Navigate to **EM** > **System Configuration** > **Server Profile**.
    b. Select the additional application interpreters required.
    c. Click **Save**.
23. To start Avaya Aura® MS, navigate to **EM** > **System Status** > **Element Status** and click **Start**.
24. Click **Confirm**.
25. Check for any service-impacting alarms and perform an appropriate test for the system. For example, place a call to the application.

Important:

Running the upgrade tool, as recommended in this procedure, ensures that the system configuration parameters and all application data is upgraded and ready to use. However, there are new and updated system configuration options in this release that are not automatically configured. To ensure that the new options are configured properly, see *Implementing and Administering Avaya Aura® Media Server* 7.7. Many systems may not need any additional configuration.

Upgrading 1+1 High Availability clusters

About this task

When you upgrade one server at a time, 1+1 High Availability clusters provide continuous access to services during upgrades. You can do this by first upgrading the standby server. After activating the upgraded standby server, then you upgrade the other server.

Procedure

1. Navigate to **EM** > **Element Status** on each server and determine which server has the **High Availability State** of Standby or Active.
2. To lock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and select the **Local High Availability State Lock** checkbox.
3. Click **Save**.
4. Click **Confirm**.
5. To upgrade the standby server, see Step 6 of Upgrading to Avaya Aura® MS.

Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.

6. To unlock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and clear the **Local High Availability State Lock** checkbox.
7. Click **Save**.
8. Click **Confirm**.
9. To put the active server in the standby state, navigate to **EM** > **Element Status** and select **Failover** from the **More Actions** drop-down menu.
10. Click **Confirm**.

    The active server is now the standby server.
11. To lock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and select the **Local High Availability State Lock** checkbox.
12. Click **Save**.
13. Click **Confirm**.
14. To upgrade the standby server, see Step 6 of Upgrading to Avaya Aura® MS 7.7.

    Wait for any alarms to clear as the server returns to service and synchronizes the active sessions with the other server.
15. To unlock the state on the active server, navigate to **EM** > **Cluster Configuration** > **High Availability** and clear the **Local High Availability State Lock** checkbox.
16. Click **Save**.
17. Click **Confirm**.

Related links

Upgrading to Avaya Aura MS 7.7 on page 52

Upgrading N+1 load sharing clusters

About this task

Load sharing media server clusters can provide continuous access to services during upgrades, when you upgrade one server at a time.

The Primary and Secondary nodes in the cluster require special consideration during the upgrade, since these nodes have master Content Store components on them serving the data needs of the entire cluster. To provide continuous content access, either the Primary or Secondary server must remain in service during the upgrade. Standard nodes can only connect to Primary or Secondary servers on the same software release. To ensure that the Standard nodes have a connection to a Primary or Secondary server on the same release during the cluster upgrade, the Primary is upgraded first and the Secondary server is upgraded last.

Use this procedure to upgrade N+1 load sharing clusters.

Procedure

1. To upgrade the Primary server, see *Upgrading to Avaya Aura® MS 7.7*.

   Wait for any alarms to clear as the server returns to service after the upgrade.
2. To upgrade each Standard server, see *Upgrading to Avaya Aura® MS 7.7*.

   Wait for any alarms to clear as the server returns to service after the upgrade.
3. To upgrade the Secondary server, see *Upgrading to Avaya Aura® MS 7.7*.
4. Verify the success of the installation.

   Check for any service-impacting alarms and perform a test of the system. For example, place a call to an application, and verify all the nodes in the cluster receive calls.

Related links

Upgrading to Avaya Aura MS 7.7 on page 52

Rollback to 7.6

About this task

Rolling back the system restores the system to the pre-upgrade state by reinstalling the previous release of Avaya MS. You might need to roll back the system if:

- Functionality in the new version is not compatible with other components of your solution.
- The upgrade process encountered an error and did not complete successfully.
- An unsupported upgrade path ended the upgrade process.
- The upgrade tool could not read the backup data file.
- You stopped the upgrade during the procedure.

Procedure

1. Turn off the Avaya Aura® MS 7.7 FP1 appliance.
2. Use one of the following methods to restore the Avaya MS 7.6 appliance:
   - If you still have the Avaya MS 7.6 VM, turn it on to return it to service.
   - If you no longer have the Avaya MS 7.6 VM, then deploy Avaya MS 7.6 again. Use the backup files to restore the system configuration and application data after it is deployed. For Avaya MS 7.6 appliance procedures, see *Deploying and Updating Avaya Media Server using VMware in the Virtualized Environment*.

Chapter 12: Troubleshooting the Avaya Aura® MS appliance

Overview

This chapter contains troubleshooting information specific to an Avaya Aura® MS appliance deployment. For general Avaya Aura® MS troubleshooting, see the “Troubleshooting” chapter in *Implementing and Administering Avaya Aura® Media Server* 7.7

Unable to upload files larger than 2 GB

You can encounter errors when using EM to upload large backup files to the Avaya Aura® MS appliance. Many browsers have a 2 GB limit on file upload.

Proposed Solutions

- Use the latest versions of the Chrome or Firefox browsers. These browsers support file uploads greater than 2 GB.
- Use an alternate upload procedure listed in the “Related links” section.

Related links

Unable to upload updates on page 58
Alternate procedure for uploading and restoring large backup files on page 42

Unable to upload updates

If there is a situation where you cannot use your browser, EM, Avaya Aura® MS is not installed, or there is a software incompatibility preventing you from uploading new software, you can use an alternate upload procedure.

Proposed Solution

1. Log in to a Linux® shell using the customer account.
2. Change to the public directory by using the `cdpub` alias or the following command:

```
cd /opt/avaya/app/pub
```

3. Transfer the update package to the pub directory. You can use the `sftp` file transfer tool, or another similar tool, to transfer the file. The file must be an official update from Avaya in ISO format.
4. Run the following command to stage the software:

   ```
   stageUpdate -stage -f softwareUpdate.iso
   ```

5. Now that the software is staged, you can complete the installation following the appropriate task to apply Avaya Aura® MS or system updates.

Backup or restore tasks fail

The system requires temporary work space to create and restore backup archives of the application content. The work space required is equal to two times amount of data stored in the media server. For example, a system which will contain 2 GB of data in the Content Store, the `/opt/avaya/app` volume must be provisioned with at least 6 GB of space. This equates to 2 GB of stored data and 4 GB of required free workspace for backup and restore operations. Old backup files should be removed to maintain free space on the system.

Perform the following procedure to ensure there is enough free disk space on the volume for a backup or restore.

Proposed Solution

1. Log in to a Linux® shell using the customer account.
2. Display the available disk space on the system by issuing the following command:

   ```
   df -h
   ```

3. Note the amount of space in the **Avail** column of the output for the line containing `/opt/avaya/app` in the **Mounted on** column.

   For example, in the following example output, the available space is 47 GB.

   ```
   Filesystem                    Size  Used Avail Use% Mounted on
   /dev/mapper/storage_vg-root1  3.9G  943M  2.7G  26% /
   tmpfs                         2.0G  1.5M  2.0G   1% /dev/shm
   /dev/sda1                     4.0G  171M  3.6G   5% /boot
   /dev/mapper/storage_vg-home   2.9G  4.6M  2.8G   1% /home
   /dev/mapper/storage_vg-app     51G  1.3G   47G   3% /opt/avaya/app
   /dev/mapper/storage_vg-var1   5.8G  383M  5.2G   7% /var
   ```

4. Remove old backup files and other unnecessary files to create the required space. Perform the following steps to remove backup files:
   a. Use the following command to list the current backup files:

      ```
      bkupFile -list
      ```

   b. Remove a backup file with the following commands:

      ```
      bkupFile -retrieve filename
      ```

      ```
      rm filename
      ```

Resetting locked login accounts

If you are unable to log in to the system, the account might be locked.

The system locks the customer account after four failed login attempts.

The system supports a maximum of five simultaneous logins per user account. The system rejects additional SSH, SCP, and Putty sessions when the five sessions are already logged in.

Proposed Solution

1. Close unused sessions if the maximum number of sessions has been exceeded.
2. Before you log in again, wait for about 20 minutes for the system to reset the locked account.
3. Contact Avaya support if the problem persists.

   Avaya support personnel with root access can reset accounts that get locked as a result of too many failed log in attempts.

Restarting or shutting down from Linux® shell

Some maintenance tasks and configuration procedures require you to restart or shutdown the server. Use the following commands in a Linux® shell to restart or gracefully power-off the server.

Proposed Solution

- To restart the server, type the following command in a Linux® shell:

  ```
  reboot
  ```

- To power-off the server with graceful shutdown, type the following command in a Linux® shell:

  ```
  shutdown –h now
  ```

Chapter 13: Related resources

Documentation

See the following related documents at http://support.avaya.com.

Title	Use this document to:	Audience
Implementing and Administering Avaya Aura® Media Server 7.7	Configure and administer Avaya Aura® Media Server	System administrators and implementation engineers
Migrating and Installing		
Migrating and Installing Avaya Appliance Virtualization Platform Release 7.0	Learn about Solution Deployment Manager options. Install and configure Avaya SDM Client.	System administrators and implementation engineers
Deploying Avaya Aura® applications from Avaya Aura® System Manager	Deploy Avaya Aura® applications by using Solution Deployment Manager.	System administrators and implementation engineers
Using		
Using Web Services on Avaya Aura® Media Server 7.7	Develop web services to provision and manage Avaya Aura® Media Server	Avaya Professional Services and application developers

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. You can also request an agent to connect you to a support team if a problem requires more expertise.

Index

S

T

U

V

W