Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300

Release 5.1.x
Issue 11
March 2025

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya 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 the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

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

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

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, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

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

Third Party Components

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

Service Provider

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document provides installation procedures and information for Avaya Solutions Platform S8300 or ASP S8300 (Avaya-Supplied ESXi 7.0) Release 5.1.x.

This document is intended for the professional who is involved in installation and support activities for ASP S8300 (Avaya-Supplied ESXi 7.0) Release 5.1.x.

Change history

Issue	Date	Summary of changes
11	March 2025	Updated Chapter 9 note referencing release notes and upgrade paths to highlight unique R5.1.0.6 update.
10	August 2024	Updated Chapter 6 to reflect the following licensing changes in Release 5.1.0.5: • All NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. • A unique foundations license key will be provided on a label on the ASP S8300 HDD/SSD.
9	April 2024	• Updated Resources section to reflect 5.1.0.4. • Provided clarification for NIC port type.
8	January 2024	• Replaced the diagram with a new one in Default mode configuration in ASP S8300 on page 46. • Updated the information about Port Group and replaced the diagram in OOBM mode configuration in ASP S8300 on page 47. • Added a note in OOBM configuration on ASP S8300 on page 48. • Replaced `asp_oobm_v2.sh` with `asp_oobm_v3.sh` across the document.

Table continues…

Issue	Date	Summary of changes
		- Added a note in Configuring OOBM on Avaya Solutions Platform S8300 after deploying VMs on page 50 and Disabling OOBM on Avaya Solutions Platform S8300 on page 54.
7	December 2023	Added the following sections: - LED behavior when upgrading from Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release on page 16. - Reconfiguring the vmk0 IP address after enabling OOBM in Avaya Solutions Platform S8300 on page 52. - Reconfiguring the vmk0 IP address after disabling OOBM in Avaya Solutions Platform S8300 on page 56. Updated the following sections: - Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 30. - Configuring SNMP v2c on an ESXi 7.0 host on page 34. - Configuring SNMP v3 on an ESXi 7.0 host on page 37. - OOBM configuration on ASP S8300 on page 48. - Configuring OOBM on Avaya Solutions Platform S8300 before deploying VMs on page 48. - Configuring OOBM on Avaya Solutions Platform S8300 after deploying VMs on page 50. - Disabling OOBM on Avaya Solutions Platform S8300 on page 54. - Powering Virtual Machines ON after disabling OOBM on the host on page 57. - Upgrading Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release on page 60. - Restoring the VMware ESXi Configuration on page 64.
6	September 2023	Updated the following sections: - Avaya Solutions Platform S8300 installation checklist for fresh install/remaster on page 22. - Installing Avaya Solutions Platform S8300 on page 26. - Configuring network parameters on page 28. - Configuring NTP server using vSphere client on page 29. - Verifying Avaya Solutions Platform S8300 software release and ESXi version on page 44.
5	July 2023	Updated the command to set the FQDN of the ESXi host in Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 30.

Table continues…

Issue	Date	Summary of changes
4	February 2023	Updated the "LED Behavior on the Avaya Solutions Platform S8300 server" section.
3	January 2023	Added new chapter "Upgrading Avaya Solutions Platform S8300".
2	October 2022	Updated the OOBM script. Updated the information related to preloaded/prelicensed Avaya Solutions Platform S8300. Added SNMP information.
1	March 2022	Release 5.1

Prerequisites

Before installing or migrating Avaya Solutions Platform S8300, ensure that you have the following knowledge, skills, and tools.

Knowledge

- Linux® Operating System
- VMware ESXi
- Appliance Virtualization Platform (recommended)

Skills

To administer the System Manager web console, Solution Deployment Manager (SDM) Client, and Avaya Solutions Platform S8300 Release 5.1.x.

S8300E server

The Avaya Solutions Platform S8300 Release 5.1.x is only supported on an S8300E server and not in the earlier versions of the S8300 server such as S8300C and S8300D. The S8300E server is based on an Intel Dual Core 2.0 GHz Ivy Bridge processor. The S8300E has 16GB of DDR RAM. Depending on the age of the board, storage capacity may range from 320GB to 1TB HDD, or a 480 GB SSD. The S8300E server is certified as VMware ready.

Chapter 2: Avaya Solutions Platform S8300 overview

ASP S8300 is Avaya's Integration with ESXi 7.0 preloaded and provisioned with a Foundation version license.

Note:

- ASP S8300 utilizes VMware vSphere ESXi 7.0 with a Foundation license. Avaya does not permit or support the repurposing of Servers that deviate from their original integrated configuration.
- On ASP S8300, VMware vSphere 7.0 is installed and a "Foundation" license key is assigned.
- Initial shipments of the ASP S8300 Release 5.1.x servers will ship blank and will need to have Release 5.1 software and the license key installed. At a future date, new shipments will be preloaded with Release 5.1.x and prelicensed. Even when the server is prelicensed, the ESXi 7.0 Foundation License on PLDS must be activated prior to completing the implementation.

What's New in Avaya Solutions Platform Release 5.1.x

For details on individual 5.1.0.x releases, reference the *Avaya Solutions Platform S8300 Release Notes.*

- Avaya Aura® Release 10.1 is supported on Avaya Solutions Platform S8300 Release 5.1.x and Avaya Solutions Platform 130 Release 5.0 and Release 5.1.x.

  Note:

  After migrating from Avaya Aura® Appliance Virtualization Platform Release 8.1.x on an S8300E to Avaya Solutions Platform S8300 Release 5.1.x, Avaya Aura® Release 8.1.x applications are still running on Avaya Solutions Platform S8300 Release 5.1.x. Prolonged running in this type of mixed configuration is not supported. Avaya recommends running in a mixed configuration only as long as necessary to support application upgrades. If an issue is identified on an Avaya Aura® 8.1.x application running on Avaya Solutions Platform S8300 Release 5.1.x, Avaya will require an upgrade of the Avaya Aura® solution to Release 10.1.

- With the introduction of Avaya Solutions Platform 5.x and Avaya Aura$^{®}$ 10.1, AVP/AVPU goes end of sale. Last supported AVP/AVPU release is Avaya Aura$^{®}$ 8.1.3.x. AVP and AVPU are not supported with Avaya Aura$^{®}$ 10.1.
- EASG is supported starting with Avaya Solutions Platform Release 5.1
- A new directory (`/opt/avaya/etc/`) is created with both the Avaya Solutions Platform S8300 zip upgrade file and the Avaya Solutions Platform S8300 ISO install file. The Avaya Tools VIB will create this directory.
- The Avaya Solutions Platform S8300 Release 5.1.x has the Avaya Tools VIB, which replaces the functionality of `Avaya-Config-v1` script file in the Avaya Solutions Platform 130 Release 4.0 and Release 5.0
    - In Avaya Solutions Platform 130 Release 4.0 and Release 5.0, the `Avaya-Config-v1` script file configured the services port and had to be copied to the shell and manually applied.
    - In Avaya Solutions Platform Release 5.1.x, this is no longer necessary. The Avaya Tools VIB is a part of the Avaya Solutions Platform S8300 Release 5.1.x ISO and zip files.
- The Avaya Solutions Platform S8300 Release 5.1.x ISO for fresh install, recovery or catastrophic/forklift migrations includes the Avaya Tools VIB.
    - The Avaya EASG VIB must be downloaded separately from PLDS and copied to the shell, and manually applied after the ISO is installed.
- The Avaya Solutions Platform S8300 Release 5.1.x upgrade zip file contains the Avaya Tools VIB and the Avaya EASG VIB, thus no need to download the Avaya EASG VIB from PLDS.
    - The Avaya Solutions Platform S8300 Release 5.1.x zip file is used for upgrades only.
- From Avaya Solutions Platform Release 5.1 onwards, **Autostart** is enabled and the **Autostart start delay** and **stop delay** fields are set to **0**.
- Reference to the latest Avaya Solutions Platform 130 Release Notes available on https://support.avaya.com for detailed information about each specific release.
- New shipments of the Avaya Solutions Platform S8300 Release 5.1.x servers will initially ship blank and will need to have the Release 5.1.x software installed and the license key installed. At a future date, new shipments will be preloaded with Release 5.1.x and prelicensed.

S8300E server specification

The following table lists the S8300E server components and their respective specification:

S8300E components	Specification
CPU	Intel B925C based on Ivy Bridge processor
CPU frequency	2.0
Physical cores	2
Virtual cores	4

Table continues…

S8300E components	Specification
Supports HyperThreading	Yes
RAM Type	DDR3
RAM Size	16GB
Maximum RAM Size	16GB
HDD Type	SATA2
Storage	HDD/SSD
Capacity	320GB, 500GB, and 1TB HDD and 480GB SSD
NIC port type	1 GbE (internal connection to Gateway backplane, limited to 100Mbps)
Number of LAN ports	3
USB	2
Number of USB ports	3

On S8300E, the public network of virtual machines (VM Network) is assigned to vmnic1 and the vmnic1 is connected through the G4x0 gateway backplane. The internal connection to the G4X0 backplane is limited to 100Mbps. The LAN port on the G4x0 Gateway is assigned to the public interface of the virtual machines. The management interface of the hypervisor (Management Network) is assigned to vmnic1 and the vmnic1 is connected through the backplane of the G4x0 similar to the VM network.

S8300E server LEDs

The S8300E faceplate provides the following interfaces:

- Services Ethernet port with link status and activity LEDs.
- Ethernet LAN port for future use.
- Three USB 2.0 ports.
- Four LEDs:
    - Alarm (**ALM**)
    - Application up (**APP**)
    - Active (**ACT**)
    - **OK TO REMOVE**
- **SHUT DOWN** button.

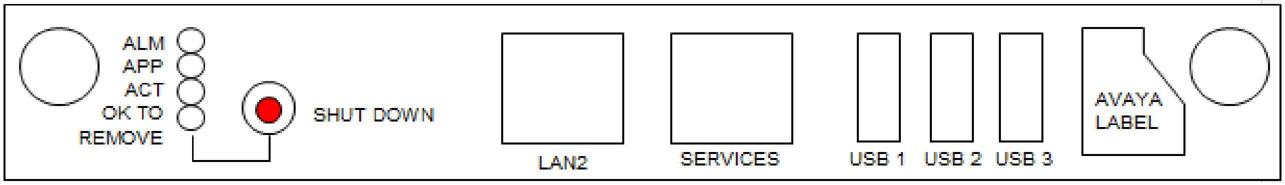


Figure 1: S8300E server

LED Behavior on the Avaya Solutions Platform S8300 server

The following table lists all LED types, colors and their respective behaviors:

LED type	Color	Behavior
ALM LED	Red	• on within first 30 seconds and starts to blink when ASP S8300 boots • on when the Communication Manager (CM) deployed on the ASP S8300 system displays a major alarm • maintains current status when ASP S8300 shutdown is in progress • off when ASP S8300 shutdown completes using shutdown button on the front plate of S8300, Web client or command line • on when the CM Survivable Remote / local survivable processor (LSP) VM is deployed on the ASP S8300, it registers with the media gateway and the CM Survivable Remote / LSP becomes active. • off when the CM Survivable Remote / LSP VM is deployed on the ASP S8300 and the CM Survivable Remote / LSP is not active.

Table continues…

LED type	Color	Behavior
APP LED	Green	• on when CM is deployed on ASP S8300 and CM processes are up • off when CM is deployed on ASP S8300 and CM processes are down • maintains current status when ASP S8300 shutdown is in progress • off when ASP S8300 shutdown completes using shutdown button on the front plate of S8300
ACT LED	Yellow	• on when a media gateway registers with CM running on ASP S8300 • on when a CM Survivable Remote / LSP VM registers with CM running on ASP S8300 • off when the media gateway and the CM Survivable Remote / LSP VM does not register with CM running on ASP S8300 • maintains current status when ASP S8300 shutdown is in progress • off when ASP S8300 shutdown completes using shutdown button on the front plate of S8300
OK TO REMOVE LED	Green	• on when ASP S8300 shutdown completes using shutdown button on the front plate of S8300E, ASP S8300 SSH command line, or ESXi web client • blinks when ASP S8300 shutdown is in progress after pressing shutdown button on the front plate of S8300E • does not blink when ASP S8300 shutdown is in progress using ASP S8300 SSH command line • does not blink when ASP S8300 shutdown is in progress using ESXi web client • off when ASP S8300 is powered on completely

LED behavior during Boot, Installation, Migration, and Upgradation of Avaya Solutions Platform S8300

LED behavior when Avaya Solutions Platform S8300 boots

This section is applicable to preloaded/prelicensed Avaya Solutions Platform S8300.

The Avaya Solutions Platform S8300 takes approximately 2 to 3 minutes to boot. When ASP S8300 boots, APP LED, ACT LED and OK TO REMOVE LED are off, but ALM LED turns on for approximately 30 seconds and starts to blink. Before the boot completes, the LED lights turn on and off sequentially in the following order - ALM LED -> APP LED -> ACT LED -> OK TO REMOVE LED. Each LED turns on and off within 1 second, and the process takes approximately 4 to 5 seconds to complete. However, ALM LED turns on and off within 1 second and ALM LED continues to blink for a few more seconds. After the LED sequence turns on and off in the above order, all LEDs turn off automatically. You can now connect to the ASP S8300.

LED behavior when performing fresh installation of Avaya Solutions Platform S8300

The following steps describe LEDs behavior sequentially when you start the fresh installation of the Avaya Solutions Platform S8300:

For more information about starting the fresh installation of the ASP S8300, see Installing Avaya Solutions Platform S8300 on page 26.

1. When the fresh installation starts, APP LED, ACT LED, and OK TO REMOVE LED are off, but ALM LED turns on for approximately 30 seconds.
2. After ALM LED turns on, it starts to blink. The LED on the DVD drive also blinks to indicate that the DVD is being read.
3. After a few minutes (approximately 3 to 4 minutes), the DVD disc is read, and the installation process is complete. The LED on the DVD drive turns off. The ALM LED continues to blink for the next few minutes (approximately 7 to 8 minutes) and ALM LED turns off.
4. After some time (approximately 3 to 4 minutes), the DVD drive automatically ejects the DVD, and the ASP S8300 starts to reboot. The ALM LED turns on for approximately 30 seconds and blinks to indicate that the ASP S8300 is starting to boot.
5. After a few minutes (approximately 2 to 3 minutes), along with ALM LED, other LEDs turn on and off sequentially in the following order - ALM LED -> APP LED -> ACT LED -> OK TO REMOVE LED. Each LED turns on and off within 1 second, and the process takes approximately 4 to 5 seconds to complete. However, ALM LED turns on and off within 1 second and ALM LED continues to blink for a few more seconds. After the LED sequence turns on and off in the above order, all LEDs turn off automatically. You can now connect to the ASP S8300.

LED behavior when migrating from Avaya Virtualization Platform 8.1.x to Avaya Solutions Platform S8300

The LED behavior when migrating from AVP 8.1.x to ASP S8300 is similar to the LED behavior when ASP S8300 boots as described in LED behavior when Avaya Solutions Platform S8300 boots on page 14.

When the AVP migration starts, all LEDs keep the current status. After the upgrade to ASP is initiated, and the server starts to reboot, the APP LED, ACT LED and OK TO REMOVE LED are off and then the ALM LED turns on for approximately 30 seconds and begins to blink. After approximately 2 to 3 minutes, in addition to the ALM LED, other LEDs turn on and off sequentially in the following order:

ALM LED -> APP LED -> ACT LED -> OK TO REMOVE LED

After that, all LEDs turn off automatically. You can now connect to the ASP S8300.

For more information about AVP migrating to ASP S8300, see Migrating from Avaya Virtualization Platform 8.1.x to Avaya Solutions Platform S8300 section in the *Migrating from Avaya Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300* publication.

LED behavior when upgrading from Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release

The LED behavior when upgrading from ASP S8300 5.1.0.x to a later ASP S8300 5.1.0.x release is similar to the LED behavior when ASP S8300 boots, as described in LED behavior when Avaya Solutions Platform S8300 boots on page 14.

When the ASP S8300 upgrade starts, all LEDs keep the current status. After the upgrade begins and the server starts to reboot, the APP, ACT, and OK TO REMOVE LEDs turn off, and the ALM LED turns on for approximately 30 seconds and starts blinking.

After approximately 2 to 3 minutes, in addition to the ALM LED, other LEDs turn on and off sequentially in the following order:

ALM LED -> APP LED -> ACT LED -> OK TO REMOVE LED

After that, all LEDs turn off automatically. You can now connect to the ASP S8300.

For more information about upgrading from ASP S8300 5.1.0.x to a later ASP S8300 5.1.0.x release, see Upgrading Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release on page 60.

S8300E server environmental specifications

Name	Minimum specification
Operating temperature	5 °C to 40 °C
Operating relative humidity	10% to 90% noncondensing humidity
Operating altitude	300 m to 3048 m above sea level

Chapter 3: Registration

Overview

In order to receive support from Avaya Services, Avaya Customers and Avaya Channel Partners must have their end user product information in the HealthCheck tool.

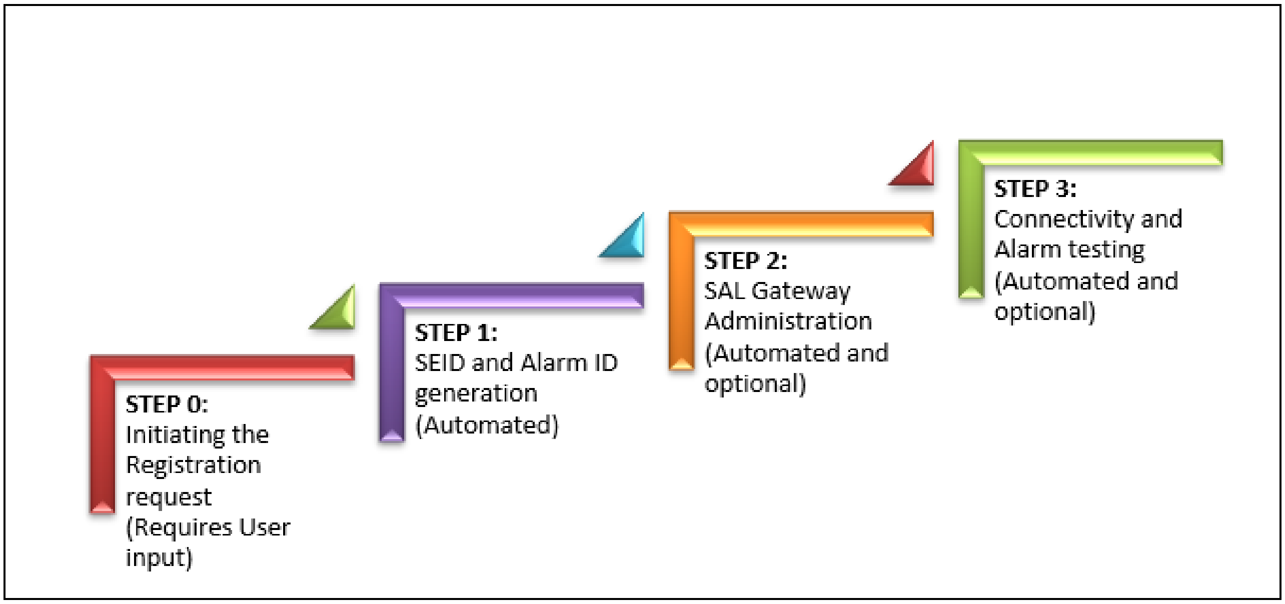
The install base creation, final record validation, and equipment moves are still in global registration tool (GRT), but if you do a Technical Onboarding (TOB) you'll be redirected to the HealthCheck Tool. The SAP order with the new S8300E material codes must be placed prior to using the Healthcheck tool. The SAP order will automatically populate Assets under the GRT install base creation.

End user product install base is a prerequisite for services support of S8300E. Registration establishes accurate inventory, test SAL connectivity, alarm configuration (if necessary), and ensures proper on-boarding of customers into all levels of Avaya support.

General information on registration can be found at https://support.avaya.com/registration.

HealthCheck tool registration process

HealthCheck tool registration feature initiates Technical Onboarding that can be divided into four steps. Only the first step has to be completed by the user manually. The other three steps are automated and completed by Avaya backend.


STEP 0:
Initiating the Registration request (Requires User input)
STEP 1:
SEID and Alarm ID generation (Automated)
STEP 2:
SAL Gateway Administration (Automated and optional)
STEP 3:
Connectivity and Alarm testing (Automated and optional)

- An Avaya user initiates the product registration request from the HealthCheck Tool.
- HealthCheck submits the registration request to Avaya backend where SEID and Alarm ID for the device is generated.
- HealthCheck portal verifies if the user has opted for SAL Administration and if the provided details are correct. SAL Administration request is then forward to SAL Gateway.
- HealthCheck portal verifies if Alarm testing is enabled and forwards the request to Avaya backend.
- HealthCheck Tool sends an email to the user once the request is submitted, and the request is completed with a link of the Status page on the HealthCheck Tool UI.

Registering a new device

About this task

Use this task to register and onboard a new Avaya device. For more information, refer to *HealthCheck Tool Registration Feature Description* on https://support.avaya.com/.

If the customer install base record is not automatically created, then it needs to be done manually by performing the following steps:

Before you begin

Ensure that you have the following:

- An SSO account with a valid user ID and password registered with Avaya to login.
- A Location ID (FL Number) of the device that you want to register.

Note:

- US Sold To (functional location) location number format: 000XXXXXXX (000 + 7 digits or can be 00 + 8 digits as well).
- Outside of US (Rest of the World) FL# (Ship To) location number: 00XXXXXXXX (always 00 + 8 digits).

- The install base of the device that needs to be onboarded must be created in Siebel.

Note:

Secure Access Link Registration (also called technical onboarding) requires a verified customer install base and FL or Sold to.

- Ensure you have your IP address and host names for the ESXi host.

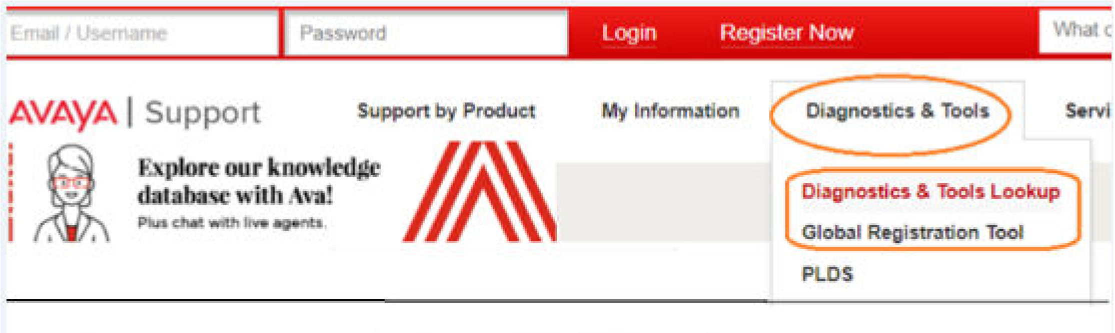
  The ESXi Host IP address is linked with the ESXi host.

- The SAP order with the new S8300E material codes must be in customer install base record prior to using the Healthcheck tool.

  The SAP order will automatically populate Assets under the GRT install base Creation. The ASP S8300E new material codes are the following: 700515840 S8300E PRELOADED TAA or 700515841 S8300E PRELOADED. Login to the GRT install base and verify that the S8300E hardware has been added.

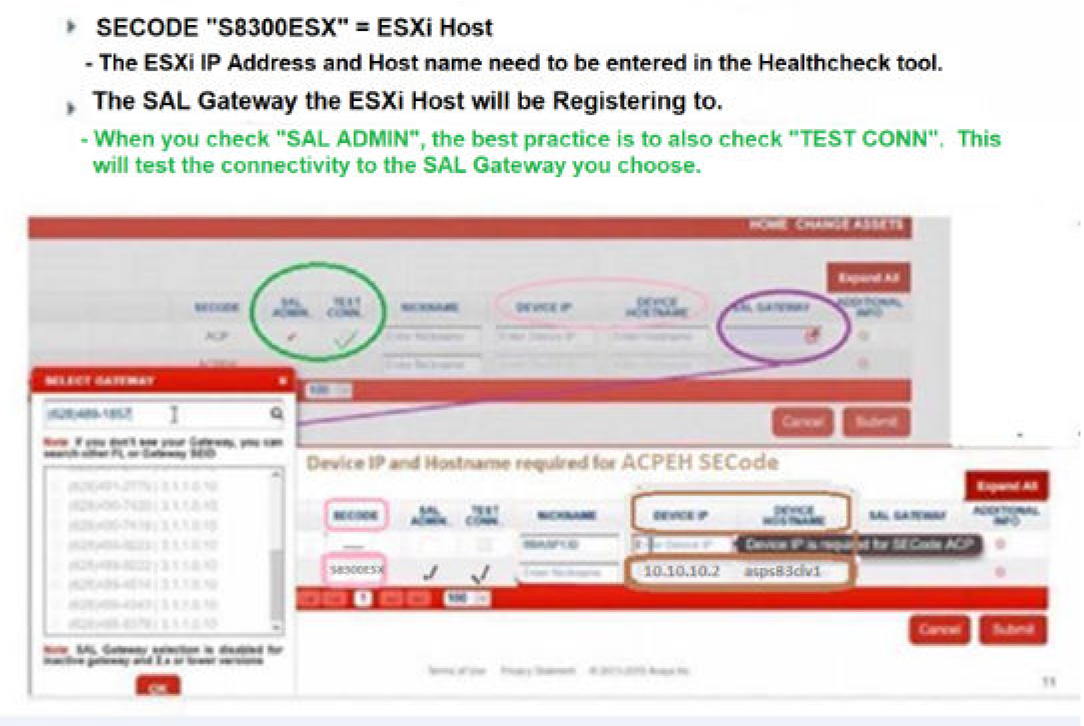
Procedure

1. Log on to https://support.avaya.com/.
2. On the Home page, click **Diagnostic & Tools**.
3. Click **Diagnostic & Tools Lookup**.



4. Click **Diagnostics and Healthcheck**.
5. Click **Healthcheck**.
6. Click **Load Consolidated Dashboard**.
7. Enter the details in the **Location/Installation ID** field.
8. Click **Unregistered Assets**.
9. Find Avaya Solutions Platform S8300 asset and enter the quantity in the **Location ID** field. Click **Register**.

10. Enter the details in the **S8300ESX** and **SAL Gateway** fields for the ASP S8300E.



- SECODE "S8300ESX" = ESXi Host
  - The ESXi IP Address and Host name need to be entered in the Healthcheck tool.
- The SAL Gateway the ESXi Host will be Registering to.
  - When you check "SAL ADMIN", the best practice is to also check "TEST CONN". This will test the connectivity to the SAL Gateway you choose.

Device IP and Hostname required for ACPEH SECode

SECODE	SAL ADMIN	TEST CONN	NICKNAME	DEVICE IP	DEVICE HOSTNAME	SAL GATEWAY	ADDITIONAL INFO
S8300ESX	✓	✓	Enter Nickname	10.10.10.2	asps83dlv1		

Device IP is required for SECode ACP

11. Click **Submit**.
12. Click **Submit** again to confirm.

    You will receive an email with the Registration status.

Registration request status

HealthCheck portal sends an email notification to the user when the request is submitted and when the request is completed. This email contains the current progress of the registration request, details of the devices, and a link to the Registration Summary page of HealthCheck Tool UI.

For more information, see *HealthCheck Tool Registration Feature Description* on https://downloads.avaya.com/css/P8/documents/101067434

Technical Onboarding Process

Technical Onboarding comprises of the following:

- SAL Gateway Administration: After a new device is registered with valid SEID and Alarm ID, it must be added to a SAL Gateway as a Managed element. This is required in case of errors or issues so that Avaya Service engineers receive the alarm and request remote access to your device to troubleshoot them.
- Connectivity and Alarm Testing: In case of failure or issues with your device and device connectivity, an alarm is generated and sent to Avaya backend. Connectivity and Alarm Testing ensures that the alarm generated by the device reaches the Avaya service team for troubleshooting.

These steps are optional while you register a new device, but Avaya recommends you to complete these steps at the earliest.

If you fail to complete these steps while registering the device, you can still come back and complete the TOB process with the HealthCheck tool.

To administer an already registered device or to complete the Connectivity and Alarm Test, see Using HealthCheck Tool KB article.

Registering device after S8300E migrates from AVP to ESXi

About this task

A TOB is required for device registration after the S8300E server migrates from AVP to ESXi. Following are the TOB recommendations:

Before you begin

Complete upgrade in Avaya PLDS website with material code 412787.

Procedure

1. Use the new tracking code (415291) for TOB.
2. Offboard AVP / System Platform SEIDs from SAL Gateway, associated with the following material codes: 700508924 or 700508955.
3. TOB S8300E with new tracking code (415291 - S8300E UPG TO ESXI TRK) to get S8300ESX – ESXi SEID (new SE code).

   Note:

   Use specific material codes for onboard application and deployment respectively.

Chapter 4: Installing Avaya Solutions Platform S8300

Overview

This chapter covers steps for the following scenarios:

- ASP S8300 ships blank and/or remaster of ASP S8300.
- ASP S8300 ships preloaded/prelicensed.

Avaya Solutions Platform S8300 installation checklist for fresh install/remaster

Use the following checklist for installing Avaya Solutions Platform S8300 Release 5.1.x.

No.	Task	Description	✔
1	Generate the Avaya Solutions Platform S8300 kickstart file. The kickstart file name must remain aspks.cfg and the contents of the generated aspks.cfg file must never be modified.	Generating the Avaya Solutions Platform S8300 kickstart file on page 24	
2	Configure the Avaya Solutions Platform S8300 USB stick. Get USB Flash stick in the FAT32 format.	Configuring the ASP S8300 USB stick on page 25	
3	From the Avaya PLDS website (https://plds.avaya.com/), download the `asp-s8300-5.1.0.x.0-xx.iso` installation file and burn it in the DVD. Reference PCN2145S for details on the ASP S8300 releases and associated PLDS ids.	This step is to indicate that the installation file `asp-s8300-5.1.0.x.0-xx.iso` is available in the Avaya PLDS website.	
4	Install Avaya Solutions Platform S8300.	Installing Avaya Solutions Platform S8300 on page 26	

Table continues…

No.	Task	Description	✔
5	Configure and verify network parameters.	Configuring network parameters on page 28	
6	Configure NTP server.	NTP server configuration on page 28	
7	Regenerate ASP S8300 self-signed certificate	Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 30	
8	Install the EASG VIBs.	Installing the Avaya EASG VIB on page 31	
9	Install ESXI 7.0 License file.	Chapter 6: Installing ESXi 7.0 License file on page 41	
10	Perform the post-installation verification.	Chapter 7: Post-installation verification on page 44	
11	Configure Securing Network Configuration (OOBM) if necessary.	Chapter 8: Securing Network Configuration on page 45	

Checklist for installing preloaded/prelicensed ASP S8300

Use the following checklist for installing Avaya Solutions Platform S8300 (Avaya-Supplied ESXi 7.0) Release 5.1.x.

No.	Task	Description	✔
1	Verify that Avaya Solutions Platform S8300 has the latest Avaya certified ESXi 7.0 build. Refer to PCN 2145S for details. If necessary, update to the latest available as noted in PCN 2145S and downloadable from PLDS.	In ESXi shell, run the **`vmware -vl`** command to verify the build.	
2	Configure IP address, Subnet Mask, Default Gateway, Domain, DNS and Naming with the customer information.	Configuring network parameters on page 28	
3	Configure NTP server	NTP server configuration on page 28	
4	Regenerate ASP S8300 self-signed certificate	Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 30	
5	Perform the post-installation verification.	Chapter 7: Post-installation verification on page 44	
6	Configure Securing Network Configuration (OOBM) if necessary.	Chapter 8: Securing Network Configuration on page 45	

Generating the Avaya Solutions Platform S8300 kickstart file

About this task

This procedure is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Generate the kickstart file for the fresh installation of Avaya Solutions Platform S8300.

Note:

To generate the `aspks.cfg` file for the S8300E server, use Solution Deployment Manager Release 10.1.x.

- For System Manager Solution Deployment Manager, use Release 10.1 HF GA patch `System_Manager_R10.1.0.0_HF_101014254.bin` or latest software version.

  For information about latest released software information, see https://support.avaya.com. Download the latest software from the Avaya PLDS website.

- For Solution Deployment Manager Client, use Release 10.1 HF GA client `Avaya_SDMClient_win64_10.1.0.0.0337789_4.zip` or latest software version.

  For information about latest released software information, see https://support.avaya.com. Download the latest software from the Avaya PLDS website.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Kickstart Generation**.
3. On Create AVP/ASP Kickstart, select **ASP S8300 5.1**.
4. In Generate Kickstart for, select **Fresh Installation**.
5. Enter the appropriate information in the fields.

   For information, see “Create ASP S8300 Kickstart field descriptions”.
6. Click **Generate Kickstart File**.

   Solution Deployment Manager prompts you to save the generated kickstart file on your local computer.

   For Avaya Solutions Platform S8300 Release 5.1 and later, the kickstart file name must be `aspks.cfg` and the contents of the generated aspks.cfg file must never be manually edited or modified.

Create ASP Kickstart field descriptions

This section is not required for preloaded or prelicensed Avaya Solutions Platform S8300.

Name	Description
Choose AVP/ASP Version	The field to select the Avaya Solutions Platform S8300 host. For Avaya Solutions Platform S8300, the option is **ASP S8300 5.1**.
Generate Kickstart for	The field to select the option for generating the Avaya Solutions Platform S8300 kickstart file. Use the **Fresh Installation** option to generate the kickstart file for installing Avaya Solutions Platform S8300 Release 5.1 and later. ✱ **Note:** Do not use the **Upgrade** option, it is for future use only.
ASP Management IPv4 Address	The IPv4 address is used to access Avaya Solutions Platform S8300 through SSH.
ASP IPv4 Netmask	The IPv4 subnet mask for the Avaya Solutions Platform S8300 host.
ASP Gateway IPv4 Address	The IPv4 address of the customer default gateway on the network. Must be on the same network as the Host IP address.
ASP Hostname	The hostname for the Avaya Solutions Platform S8300 host. The hostname: • Can contain alphanumeric characters and hyphen • Can start with an alphabetic or numeric character • Must contain at least 1 alphabetic character • Must end in an alphanumeric character • Must contain 1 to 63 characters
Main IPv4 DNS Server	The DNS Server IPv4 address for the Avaya Solutions Platform S8300 host.

Button	Description
Generate Kickstart File	Generates the Avaya Solutions Platform S8300 kickstart file and prompts you to save the file on your local computer.

✱ **Note:**

FQDN is used to add host to SDM.

Configuring the ASP S8300 USB stick

About this task

This procedure is not required for preloaded/prelicensed ASP S8300.

Before you begin

The USB must be in a FAT 32 format file.

Procedure

1. Generate the ASP S8300 kickstart file by using Solution Deployment Manager.
2. Save a copy of `aspks.cfg` on the USB stick.

Next steps

Install ASP S8300.

Installing Avaya Solutions Platform S8300

About this task

This procedure is not required for preloaded/prelicensed ASP S8300.

Before you begin

- Download and burn the ASP S8300E R5.1.x ISO to a DVD.
- Create an `aspks.cfg` file with the appropriate password and IP information using SMGR SDM or SDM client 10.1 or later.
- The kickstart file name must remain aspks.cfg and the contents of the generated aspks.cfg file must never be modified.
- Copy the `aspks.cfg` file to a USB stick. The USB stick must be in the FAT32 format.
- Ensure that a backup file of all applications residing on the S8300 are saved on a different server.

Note:

To deploy the ASP S8300 server while connected to the customer network, ensure that the IP address used for ASP S8300 is not in use by another system. If the configured IP address is already in use on the network during installation, the installation process stops. You must remove the duplicate IP address and restart the deployment.

Procedure

1. To install ASP S8300 on S8300E, insert the external Avaya-approved USB DVD reader in the USB1 port, if you use a locally sourced external power supply for the Avaya approved USB DVD reader. Otherwise, use the Avaya approved USB DVD reader that requires a Y cable and will utilize two USB ports (USB1 and USB2) to ensure availability of sufficient power.

   Note:

   The only supported USB DVD drives are Digistor DIG-72032, Digistor DIG73322, and comcode 700406267.

2. Insert a USB stick with the `aspks.cfg` file on it in the next available USB port of the S8300E.

3. Insert the S8300E into slot v1 of the G4x0 Branch Gateway to start the installation process. If already inserted, pull the S8300E and re-insert into slot v1 of the G4x0 Branch Gateway to initiate installation.

   The Alarm LED blinks to indicate the start of the installation process.

   ⚠ **Warning:**

   When ASP S8300 is installed, all existing data on the server is lost.

   The system installs the ASP S8300 and automatically ejects DVD. The installation process takes about 20 minutes to complete.

4. After the system ejects DVD and the LEDs are off, remove the external USB DVD drive and USB stick from ASP S8300.

5. Using an SSH client, connect to the server through the eth1 services port using the following network parameters on your local PC:

   - IP address: 192.11.13.5
   - Netmask: 255.255.255.252
   - Gateway: 192.11.13.6

   The SSH client must use UTF-8 and TLS 1.2. Alternatively, you can connect to the public network address configured during the installation from a computer on the customer network.

   You can access the ASP S8300 host with IP address: 192.11.13.6

6. Log in to ASP S8300 as *root* and provide the default password *ACP130_pw*

   The ASP S8300 displays the End user license agreement (EULA) screen.

7. Read the EULA and type `Y` to accept the terms.

   You can press any key to read EULA and use the space bar to scroll down.

8. Log into ESXi host and configure host name and domain name.

9. Install a valid license file on the ASP S8300 host.

   For more information on installing a valid license file on the ASP S8300 host, see Installing ESXi 7.0 License file on the ASP S8300 host on page 41

10. Regenerate the self-signed certificate using the FQDN.

    See Regenerating ASP S8300 self-signed certificate with FQDN using the command line interface on page 30.

Next steps

Configure and verify network parameters.

Configuring network parameters

Procedure

1. Open a browser and navigate to https://192.11.13.6/ui.

   Note:

   Connect your laptop to the **SERVICES** port to use the 192.11.13.6 IP address.

2. Log in using the Avaya Solutions Platform S8300 credentials.
3. Navigate to **Networking** > **VMkernel NICs**.
4. Click **vmk0** > **Edit Settings**.
5. Enter the ESXi host IP address and subnet mask in the IPv4 settings and click **Save**.
6. Navigate to **Networking** > **TCP/IP Stack**.
7. Click **Default TCP/IP Stack** > **Edit Settings**.
8. Enter the Hostname, Domain name, Primary and Secondary DNS servers, Search Domain, IPv4 default gateway and click **Save**.
9. Open an SSH connection and run the following commands:
   - `cat /etc/hosts`: To validate hostname and FQDN.
   - `esxcli network ip interface ipv4 get`: To validate IP address and subnet mask.

Next steps

Configure the NTP server.

NTP server configuration

Network Time Protocol (NTP) server configuration is required for both preloaded/prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

The NTP server can be configured using CLI commands or the vSphere client.

Configuring NTP server using CLI commands

Procedure

1. Use a PuTTY client SSH to connect to Avaya Solutions Platform S8300 using the ASP Management IP address or using 192.11.13.6.

Note:

Connect your laptop to SERVICES port to use the 192.11.13.6 IP address.

2. Run `vi /etc/ntp.conf` to edit the NTP configuration file.
3. Press **i** to switch to insert mode and type the following IP address: `server <ntp_server_ipv4_or_ipv6_address>`.

   Replace <ntp_server_ipv4_or_ipv6_address> with IPv4 or IPv6 address of your NTP server.

   Note:

   To configure multiple NTP servers, you can add the NTP servers on separate lines with their respective IP addresses, similar to the following example:

   ```
   server <ntp_address1>
   server <ntp_address2>
   ```

4. Press the **ESC** key to exit insert mode. Save the file and press **:wq** to exit.
5. Run `/etc/init.d/ntpd start` to start the ntpd service.

Configuring NTP server using vSphere client

Procedure

1. Open a browser and navigate to https://ASP-host-IP/ui or https://192.11.13.6/ui.

   Note:

   Connect your laptop to the SERVICES port to use the 192.11.13.6 IP address.

2. Log in using the Avaya Solutions Platform S8300 credentials.
3. In the **Host** tab, on the **Navigator** menu, go to **Manage**.
4. Click the **System** menu.
5. Navigate to **Time & date** > **Edit NTP Settings**.
6. In the dialog box, click the **Use Network Time Protocol (enable NTP client)** radio button.
7. In the **NTP service startup policy** menu, select **Start and stop with host**.
8. In the **NTP servers** text box, enter the IP address of the NTP server.

   Note:

   To configure multiple NTP servers, separate IP addresses with commas.

9. Click **Save**.
10. Click the **Services** menu.

11. Search for **ntpd** and click on it to highlight **ntpd**.
12. Press **Start** to start the service.

Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface

About this task

This procedure is required for both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

Before adding an Avaya Solutions Platform S8300 host, to regenerate the Avaya Solutions Platform S8300 self-signed certificate with FQDN, perform the following steps:

For information about adding an Avaya Solutions Platform S8300 host, see Adding an Avaya Solutions Platform S8300 Release host on page 32.

Procedure

1. Log in to the Avaya Solutions Platform S8300 command line interface.
2. To change the FQDN, type the following command:

   ```
   esxcli system hostname set --fqdn=server.abc.com
   ```

   Here, *server.abc.com* is the FQDN of the ESXi host.

   For more information, see Changing the host name on the VMware documentation website.
3. To regenerate the self-signed certificate, do the following:
   a. Enable SSH on the ESXi host, then put the ESXi host into the maintenance mode.

   b. SSH to the ESXi host and use the following commands to take backups of the current certificate file and private key file.

   ```
   cd /etc/vmware/ssl
   mv rui.crt rui.crt.bkp
   mv rui.key rui.key.bkp
   ```

   c. To regenerate a new certificate, type the following command:

   ```
   /sbin/generate-certificates
   ```

   Verify that the new certificate file and private key file are generated.

   d. To restart the ESXi Server management agent, reboot the host.

   The ESXi host generates a new self-signed certificate.

   For more information, see Generating new self-signed certificates for the ESXi host.

Network ports of ASP S8300

When ASP S8300 installs the connection through the branch gateway, Ethernet ports are assigned to the public interface of virtual machines. When ASP S8300 installs the connection through the branch gateway backplane, the LAN port on the G4x0 Gateway is assigned to the public interface of virtual machines.

Installing the Avaya EASG VIB

About this task

This procedure is not required for preloaded/prelicensed ASP S8300.

After installing ASP S8300, install the Avaya EASG VIB using the `AVA-avaya-easg_1.0-2_19246618.zip` file.

Note:

Download `AVA-avaya-easg_1.0-2_19246618.zip` file from Avaya PLDS website.

Procedure

1. Log in to the ASP S8300 command line interface.
2. Copy `AVA-avaya-easg_1.0-2_19246618.zip` file to the `/vmfs/volumes/datastore1` directory.
3. Run the following command to install the EASG VIB:

   ```
   esxcli software vib install -d /vmfs/volumes/datastore1/<name of EASG zip>
   ```

4. Run the **`EASGStatus`** command to ensure successful installation.

   Output:

   ```
   EASG is enabled
   ```

Chapter 5: Administering ASP S8300

Adding an Avaya Solutions Platform S8300 Release host

About this task

This procedure is required for both preloaded or prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to add an Avaya Solutions Platform S8300 Release 5.1.x host. You can associate an Avaya Solutions Platform S8300 Release 5.1.x and later host with an existing location.

Before you begin

- If Appliance Virtualization Platform that was migrated to Avaya Solutions Platform S8300 Release 5.1.x is available in Solution Deployment Manager on the **Platforms** tab, remove that Appliance Virtualization Platform and add the Avaya Solutions Platform S8300 Release 5.1.x host.
- Regenerate the self-signed certificate using the FQDN.

  See "Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface”.
- If you are connected to the Avaya Solutions Platform S8300 host through the services port using the SDM client, perform the following:
  1. Edit the `C:\Windows\System32\Drivers\etc\hosts` file in your laptop to add the IP Address and FQDN of the host.
  2. Add the host in the format 192.11.13.6 <*changed FQDNname*>

     For example: `192.11.13.6 esxihost6.hostdomain.com`
- Add Avaya Solutions Platform S8300 host to an existing location or associate it with a new location.
- Install a valid license file on the Avaya Solutions Platform S8300 host.

Procedure

1. To add an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, choose one of the following:
   - For System Manager SDM, on the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
   - For SDM client, on the **SDM Client** web console, click **Application Management**.

2. In **Application Management Tree**, select an existing location or add a new location.
3. On the **Platforms** tab, in the Platforms for Selected Location <location name> section, click **Add**.
4. In the New Platform section, do the following:
    a. Provide details of Platform name, Platform FQDN, username, and password.

       For Avaya Solutions Platform S8300 deployment, you can also provide the root username.

    b. In **Platform Type**, select **ASP 130/S8300**.
5. Click **Save**.

   The Avaya Solutions Platform S8300 certificate is updated based on the platform FQDN.

After adding an Avaya Solutions Platform S8300 host using System Manager SDM or SDM client, perform the following:

6. Deploy the required virtual machines.
7. In the Certificate dialog box, click **Accept Certificate**.

   System Manager generates the certificate and adds the Avaya Solutions Platform S8300 host.

   In the **Application Management Tree**, System Manager displays the new host in the specified location and discovers applications.
8. To view the discovered application details, such as name and version, establish trust between the application and System Manager doing the following:
    a. On the **Applications** tab, in the Applications for Selected Location <location name> section, select the required application.
    b. Click **More Actions** > **Re-establish connection**.
    c. Click **More Actions** > **Refresh App**.
9. On the **Platforms** tab, select the required platform and click **Refresh**.

Next steps

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

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

Related links

Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface on page 30

Enabling and disabling SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager

About this task

This procedure is applicable to both preloaded/prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Use this procedure to enable SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager.

Note:

After installing Avaya Solutions Platform S8300, SSH is enabled automatically. The only time this procedure is necessary is if the ASP SSH enable/disable shell script is executed or if SSH is disabled manually from the ESXi embedded host client or via Solution Deployment Manager.

Procedure

1. On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In **Application Management Tree**, select a location.
3. Select the required host.
4. To enable SSH, do the following:
    a. Click **More Actions** > **SSH** > **Enable SSH**.
    b. In the Confirm dialog box, in **Time (in minutes)**, type the time after which the system times out the SSH connection.

       The range is 10 minutes through 120 minutes.
    c. Click **Ok**.

       Solution Deployment Manager displays `enabled` in the **SSH status** column.
5. To disable SSH, click **More Actions** > **SSH** > **Disable SSH**.

   Solution Deployment Manager displays `disabled` in the **SSH status** column.

Configuring SNMP on an ESXi 7.0 host

Configuring SNMP v2c on an ESXi 7.0 host

About this task

This section provides instructions on how to configure SNMP on the Avaya Solutions Platform S8300 server. The Avaya Secure Access Link (SAL) Gateway, as an SNMP trap receiver, can support SNMP v1, v2c and v3. Some trap receivers may only support SNMP v2 and other may require SNMP v3. The ESXi host can support SNMP v2c and v3 simultaneously, if needed.

Note:

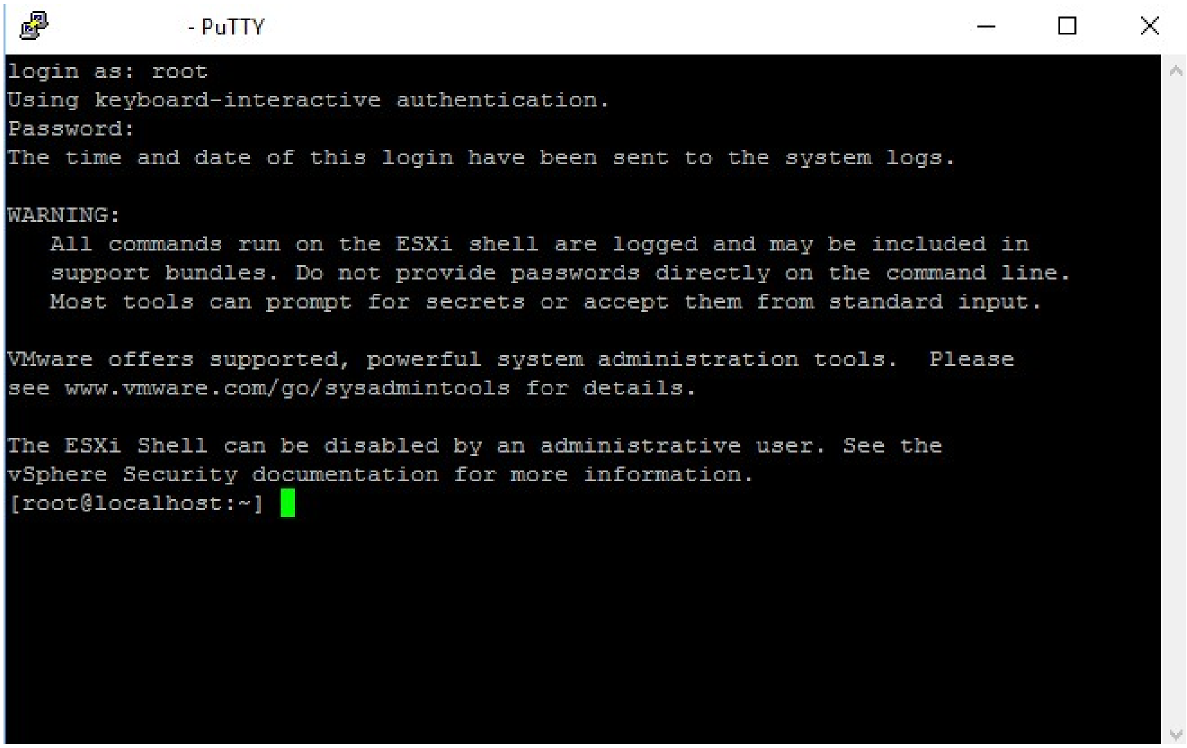
Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Note:

The SSH functionality must be enabled on ESXi. The Avaya installation guidelines direct administrators to enable SSH, so this should not be an issue. If, however, SSH is not enabled, refer to Enabling and disabling SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager on page 34 to enable SSH.

Procedure

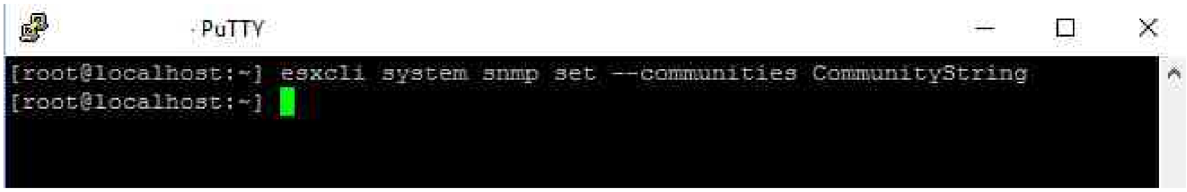
1. From a Putty session, via SSH, access the ESXi host. Authenticate using the existing ***root*** credentials.



```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@localhost:~]
```

2. Type the following command to set the community string to be exchanged between the ESXi host and the trap receiver(s):

```
esxcli system snmp set --communities <community string>
```



```
[root@localhost:~] esxcli system snmp set --communities CommunityString
[root@localhost:~]
```

3. Administer the trap receivers:

   ```
   esxcli system snmp set --targets <SAL_GW_IP_ADDRESS>@<port#>/<community>
   ```

   Example with multiple targets, separated by a comma:

   ```
   esxcli system snmp set --targets 10.1.1.1@162/avaya123,10.1.1.2@162/avaya123
   ```

   Note:

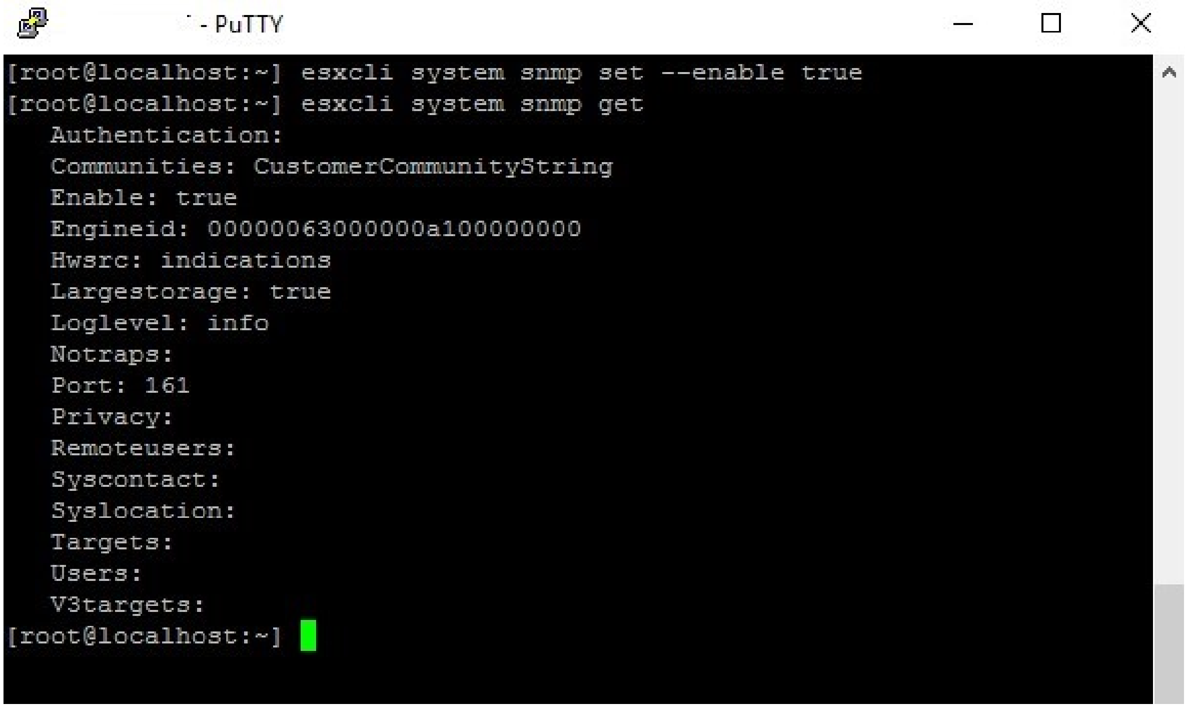
   - Port 162 is the standard and default SNMP port for receiving traps, but any port number can be assigned as long as it is matched at both send/receive devices.
   - Up to three trap destinations can be administered and must be separated by commas with no subsequent space.
   - If sending traps to a System Manager server, the default port that the System Manager uses for trap reception is port 10162.

4. Enable/Disable SNMP on the host using the following command:

   ```
   esxcli system snmp set --enable true (to enable)
   esxcli system snmp set --enable false (to disable)
   ```

5. Confirm the settings with the following command:

   ```
   esxcli system snmp get
   ```

   ```
   [root@localhost:~] esxcli system snmp set --enable true
   [root@localhost:~] esxcli system snmp get
      Authentication:
      Communities: CustomerCommunityString
      Enable: true
      Engineid: 00000063000000a100000000
      Hwsrc: indications
      Largestorage: true
      Loglevel: info
      Notraps:
      Port: 161
      Privacy:
      Remoteusers:
      Syscontact:
      Syslocation:
      Targets:
      Users:
      V3targets:
   [root@localhost:~]
   ```

6. Run the following command to send a test trap and confirm that the administered destination(s) is/are sent SNMP notifications:

   ```
   esxcli system snmp test
   ```

Note:

The trap sent to the trap receiver(s) may not cause a warning/alarm state change for the ESXi host being administered. The trap will likely be an Informational message variety trap, communicating the ability for the ESXi device to transfer SNMP packets with the administered receiver(s).

7. Use the following command, if you want to remove the SNMP configuration:

   ```
   esxcli system snmp set -reset
   ```

Configuring SNMP v3 on an ESXi 7.0 host

About this task

The SNMP v3 setting is available on ESXi. This section provides steps on configuring the more secure option of SNMP v3.

Note:

Avaya recommends the more secure SNMPv3 protocol be implemented. Use of SNMPv2 may result in security scans reporting vulnerabilities.

Note:

The SSH functionality must be enabled on ESXi. The Avaya installation guidelines direct administrators to enable SSH, so this should not be an issue. If, however, SSH is not enabled, refer to Enabling and disabling SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager on page 34 to enable SSH.

Note:

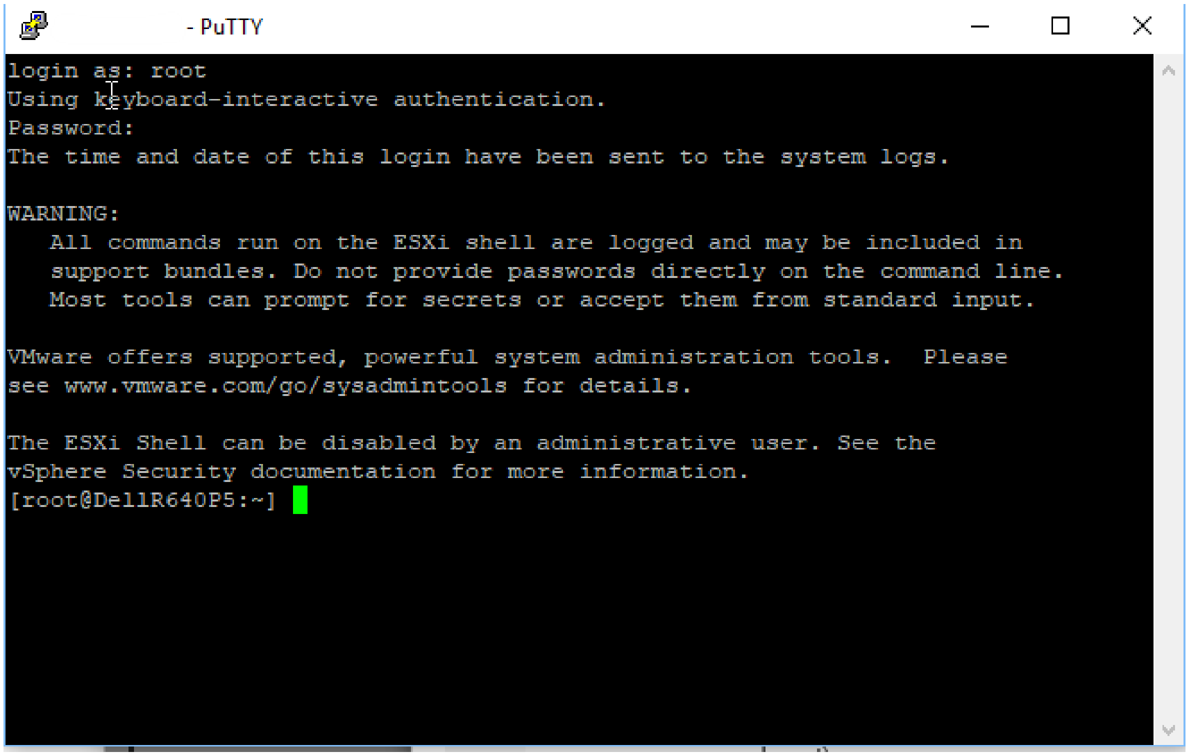
The SAL Gateway does not support Engine ID info exchange; configuring that function has been omitted from this section. For details on creating/supporting Engine ID with other NMS devices, please refer to the following VMware KB article: https://docs.vmware.com/en/VMware-vSphere/7.0/com.vmware.vsphere.monitoring.doc/GUID-4AF8AA5F-D652-4080-B984-B36A25456A4B.html.

Note:

Starting with ESXi 7.0, MD5 is no longer a supported authenticated method and it has been deprecated due to known weakness on its algorithm. SHA-1 cryptographic hashing algorithm will be deprecated in a future release of vSphere too.

Procedure

1. From a Putty session, via SSH, access the ESXi host. Authenticate using the existing ***root*** credentials.



- PuTTY

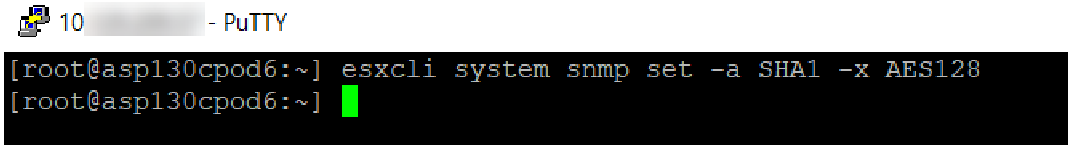
```
login as: root
Using keyboard-interactive authentication.
Password:
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@DellR640P5:~]
```

2. Set the *authorization* and *privacy protocols* in ESXi.

```
esxcli system snmp set -a SHA1 -x AES128
```

Note:

Syntax is case sensitive.

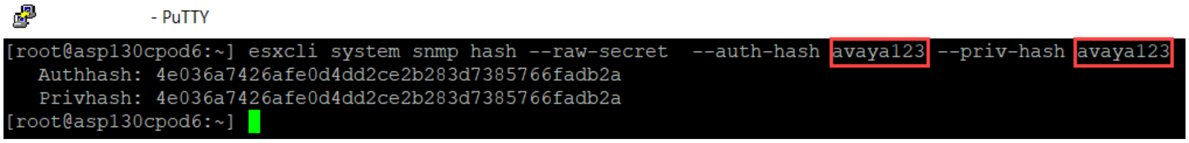


10 [redacted] - PuTTY

```
[root@asp130cpod6:~] esxcli system snmp set -a SHA1 -x AES128
[root@asp130cpod6:~]
```

3. Generate hash values for the privacy and authentication settings.

```
esxcli system snmp hash --raw-secret --auth-hash <authentication password> --priv-hash <privacy password>
```



- PuTTY

```
[root@asp130cpod6:~] esxcli system snmp hash --raw-secret  --auth-hash avaya123 --priv-hash avaya123
   Authhash: 4e036a7426afe0d4dd2ce2b283d7385766fadb2a
   Privhash: 4e036a7426afe0d4dd2ce2b283d7385766fadb2a
[root@asp130cpod6:~]
```

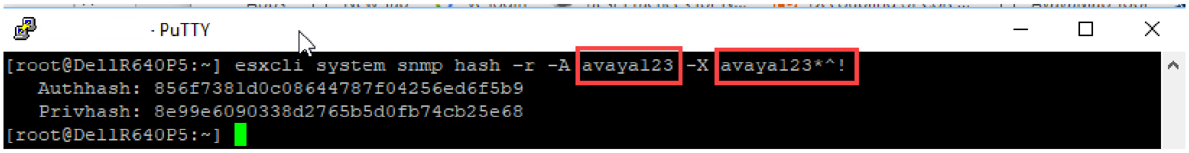
A shorthand method of typing this same command is available:

```
esxcli system snmp hash -r -A <authentication password> -X <privacy password>
```

In the example above, the same avaya123 was used for the authentication and privacy users. This resulted in the same hash key being generated for **Authhash** and **Privhash**. This method is secure and acceptable.

If even more layers of secure handshake keys are required/desired, unique hash keys foreach element may be generated by selecting unique user secrets for the authentication and privacy elements.

In the example below, the use of unique user secrets, *avaya123* and *avaya123*^!*, produces a unique hash output for each element.



```
[root@DellR640P5:~] esxcli system snmp hash -r -A avaya123 -X avaya123*^!
   Authhash: 856f7381d0c08644787f04256ed6f5b9
   Privhash: 8e99e6090338d2765b5d0fb74cb25e68
[root@DellR640P5:~]
```

Passwords for ESXi 7.0 must be a minimum of 7 characters long and less than 40 characters.

Characters recommended:

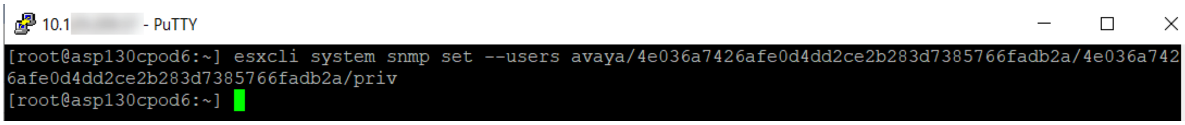
- Lower case and capital letters
- Numbers
- !@ # $ % ^ *

4. Using the hash output values, create a user that will query the SNMP service. The following command will be typed as a line (continuous) command.

```
esxcli system snmp set --users <userid>/authentication hash/privacy hash/model
```

Note:

model is one of (none|auth|priv).



```
[root@asp130cpod6:~] esxcli system snmp set --users avaya/4e036a7426afe0d4dd2ce2b283d7385766fadb2a/4e036a742
6afe0d4dd2ce2b283d7385766fadb2a/priv
[root@asp130cpod6:~]
```

In this example, the user is administered as *avaya*. Any user name may be created with a minimum of the same 8 characters that are applied to the hash key secret.

The security option of *priv* provides authentication based on HMAC-MD5 algorithms and AES encryption.

5. Set the SNMP trap receiver(s) for the ESXi host alarms.

```
esxcli system snmp set --v3targets <Receiver IP Address>@162/userid/security-
level/message-type
```

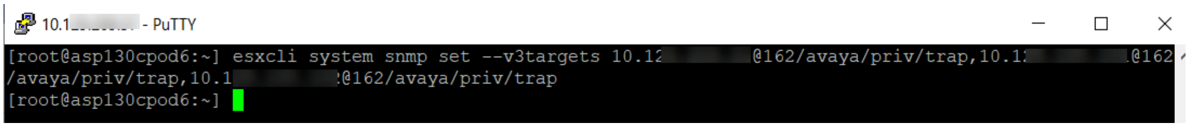
The parameters of the command are as follow

Security-Level: The level of authentication and privacy you have configured. Use *auth* if you have configured authentication only, *priv* if you have configured both authentication and privacy, and *none* if you have configured neither.

Message-type: The type of the messages received by the management system. Use *trap* or *inform*.

Note:

- Port 162 is the standard and default SNMP port for receiving traps, but any port number can be assigned as long as it is matched at both send/receive devices.
- Up to three trap destinations can be administered and must be separated by commas with no subsequent space.



10.1[redacted] - PuTTY

```
[root@asp130cpod6:~] esxcli system snmp set --v3targets 10.12[redacted]@162/avaya/priv/trap,10.1[redacted]@162
/avaya/priv/trap,10.1[redacted]@162/avaya/priv/trap
[root@asp130cpod6:~]
```

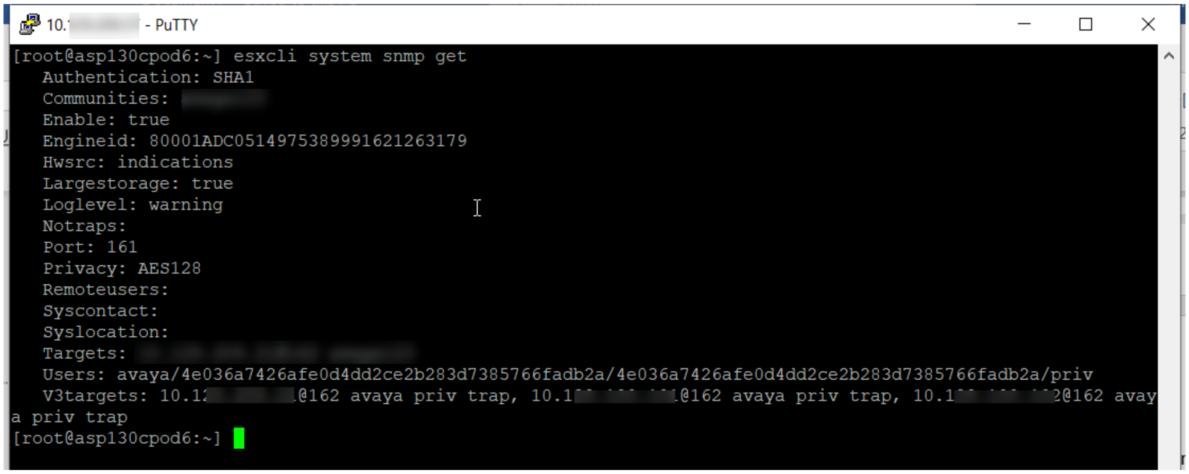
6. Enable SNMP service.

```
esxcli system snmp set --enable true  (to enable)
```

```
esxcli system snmp set --enable false (to disable)
```

7. Review the configuration you have just administered for SNMPv3.

```
esxcli system snmp get
```



10.1[redacted] - PuTTY

```
[root@asp130cpod6:~] esxcli system snmp get
   Authentication: SHA1
   Communities: [redacted]
   Enable: true
   Engineid: 80001ADC0514975389991621263179
   Hwsrc: indications
   Largestorage: true
   Loglevel: warning
   Notraps:
   Port: 161
   Privacy: AES128
   Remoteusers:
   Syscontact:
   Syslocation:
   Targets: [redacted]
   Users: avaya/4e036a7426afe0d4dd2ce2b283d7385766fadb2a/4e036a7426afe0d4dd2ce2b283d7385766fadb2a/priv
   V3targets: 10.12[redacted]@162 avaya priv trap, 10.1[redacted]@162 avaya priv trap, 10.1[redacted]@162 avay
a priv trap
[root@asp130cpod6:~]
```

8. Once the far end trap receiver has also been configured for SNMPv3, run the following command to send a test trap and confirm that the administered destination(s) is/are sent SNMP notifications:

```
esxcli system snmp test
```

9. Use the following command, if you want to remove the SNMP configuration.

```
esxcli system snmp set --reset
```

Chapter 6: Installing ESXi 7.0 License file

✱ **Note:**

Due to changes in our third-party vendor agreement, all NEW orders for ASP 5.1.x will no longer have the ESXi license key posted in PLDS. A unique standard license key will be provided on a label on the ASP 130 server lid. In the event of a server replacement, the server lid with the ESXi license key must be moved to the new replacement server. Existing ASP 130 servers with a license obtained from PLDS are **not** impacted by this change, only new orders shipped from Avaya's Integrator and warehouses. Existing inventory that was previously sold to Distributors and Partners and is present in their supply chain, will still have the old key. Only when they replenish stock with new orders, post the cutover, will the change take place. *Target cutover is tentatively scheduled for early-mid August, 2024, subject to change. Ensure you are signed up for e-notification.*

Installing ESXi 7.0 License file on the ASP S8300 host

About this task

This procedure is not required for preloaded/prelicensed ASP S8300. However, for a preloaded/prelicensed S8300 the ESXi 7.0 Foundation License on PLDS must be activated by the implementor prior to completing the implementation.

Before you begin

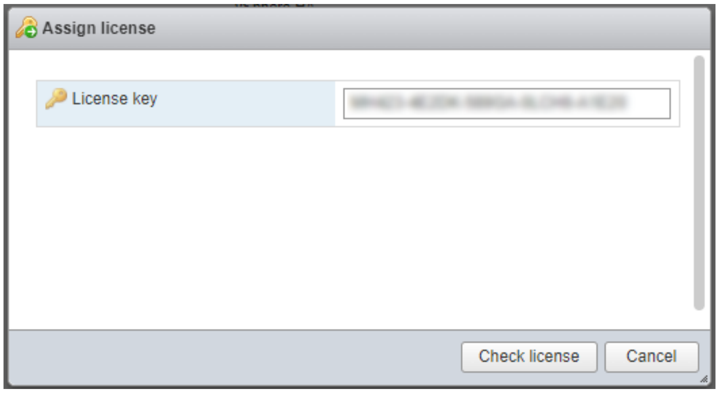
- ASP S8300 with a newly installed or upgraded ESXi 7.0 that is NOT a preloaded/prelicensed board from Avaya's integrator.
- Activate the ESXi 7.0 Foundation License on PLDS and then download the ESXi 7.0 license key from the Avaya PLDS website.
- One ESXi key is required for each ASP S8300.
- Ensure to copy the license key from Avaya PLDS for each host.

✱ **Note:**

VMware has equipped Avaya with a unique Avaya license key for ASP servers that enables Avaya to use one key for ASP S8300 ESXi 7.0 customer licensing. However, Avaya must maintain records that show individual entitlements for each server that the key is applied to. Each ASP S8300 running ESXi 7.0 or greater must be associated with an LAC in PLDS. It is possible that one LAC can have multiple quantities for ASP S8300 licenses, if multiple quantities are ordered.

Procedure

1. Log in to the ESXi host at `https://[IP Address of host]/ui`.
2. In the left pane, click **Host** to expand the **Host** menu.
3. Click **Manage**.
4. In the right pane, navigate to **Licensing** tab and click **Assign license**.
5. In the **Assign license** dialog box, paste the license key downloaded from PLDS.
6. Click **Check license**.

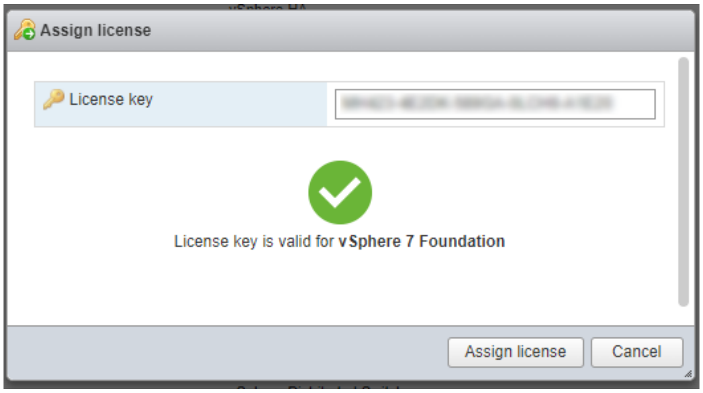
   License key [redacted]

7. A pop-up dialog box displays the following message:

   ```
   License key is valid for vSphere 7 Foundation
   ```

   Verify that the license key is valid for vSphere 7 Foundation. Only a Foundation license is valid on the ASP S8300.

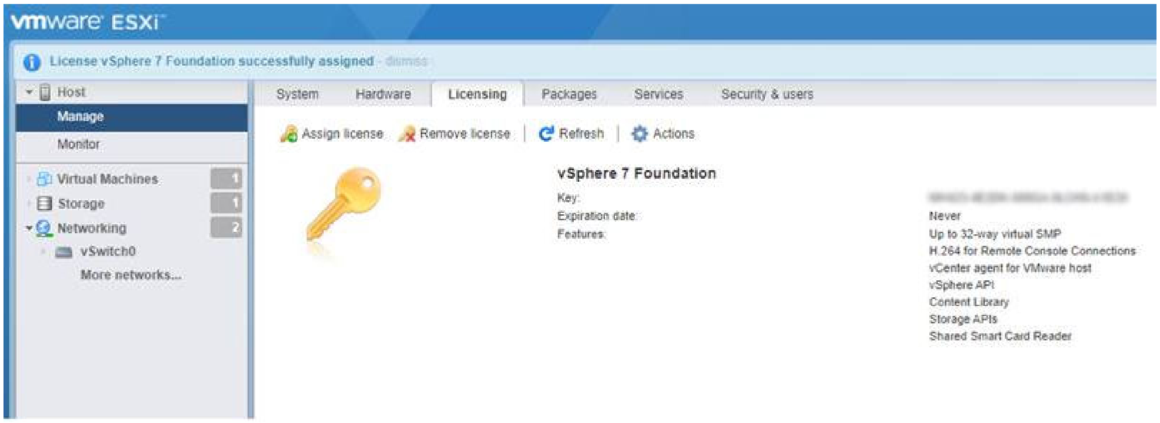
8. Click **Assign license** to confirm.

   License key [redacted]

   License key is valid for **vSphere 7 Foundation**

   The **Licensing** tab displays the updated ESXi 7.0 license.



License vSphere 7 Foundation successfully assigned - dismiss

vSphere 7 Foundation

Key: [redacted]

Expiration date: Never

Features: Up to 32-way virtual SMP
H.264 for Remote Console Connections
vCenter agent for VMware host
vSphere API
Content Library
Storage APIs
Shared Smart Card Reader

Chapter 7: Post-installation verification

Verifying Avaya Solutions Platform S8300 software release and ESXi version

About this task

This procedure is applicable to both preloaded/prelicensed Avaya Solutions Platform S8300 and fresh install on Avaya Solutions Platform S8300.

Note:

Preloaded/prelicensed ASP S8300s may not contain the latest Avaya certified ESXi release. It is the responsibility of the installer to ensure that the latest Avaya certified ESXi release is installed prior to handoff to customer.

The versions shown below are examples. Always verify the version information against the relevant upgrade bundle that was utilized.

Procedure

1. Log in to the ESXi host by using a *Secure Shell (SSH)* client, such as PuTTY (Not provide by Avaya).
2. Authenticate using the existing *root* credentials.
3. To verify the Avaya Solutions Platform S8300 software release, type the **`cat /opt/avaya/etc/avaya-asp.version`** command and press **Enter**.

   Example output:

   ```
   ASP Release 5.1
   ```

4. To verify the ESXi version, type the **`vmware -vl`** command or the **`esxcli system version get`** command.

   Example output after you type the **`vmware -vl`** command and press **Enter**:

   ```
   VMware ESXi 7.0.2 build-18538813
   VMware ESXi 7.0 Update 2
   ```

   Example output after you type the **`esxcli system version get`** command and press **Enter**:

   ```
   Product: VMware ESXi
   Version: 7.0.2
   Build: Releasebuild-18538813
   Update: 2
   Patch: 25
   ```

Chapter 8: Securing Network Configuration on ASP S8300

Overview

This section is applicable to both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

The Out of Band Management (OOBM) network configuration separates management traffic of the hypervisor and virtual machines through a secure private network, separated from rest of the customer network. The OOBM network configuration permits restricted access only to System Administrators.

By default, the Avaya Solutions Platform S8300 supports both public and management traffic over the same network interface. On S8300E, the public network of virtual machines (VM Network) is assigned to vmnic1 and the vmnic1 is connected through the G4x0 gateway backplane. The LAN port on the G4x0 Gateway is assigned to the public interface of the virtual machines. The management interface of the hypervisor (Management Network) is assigned to vmnic1 and the vmnic1 is connected through the backplane of the G4x0 similar to the VM network.

S8300E ports

The S8300E server has 3 NIC ports - NIC port, Server NIC port, and OS VMNIC port.

The Server NIC ports numbering starts from 1 and refers to the external physical NIC ports. The OS VMNIC ports numbering starts from 0 and refers to the NIC ports from the operating system.

NIC port	Server NIC port	OS VMNIC port	Server NIC port location
First NIC port	Server NIC 1	VMNIC0 or SERVICES	Front of S8300 labeled Services.
Second NIC port	Server NIC 2	VMNIC1	Internal connection to Gateway backplane, limited to 100Mbps (VMs use this connection).
Third NIC port	Server NIC 3	VMNIC2 or LAN2	Front of S8300 labeled LAN2 (dedicated for OOBM only).

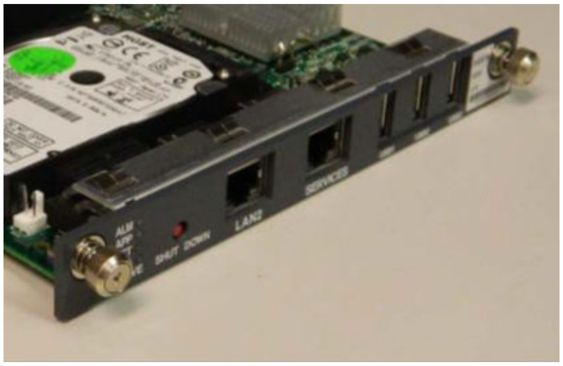


Figure 2: The S8300E server faceplate displaying vmnic2 (LAN2) port and vmnic0 (SERVICES) port

Default mode configuration in ASP S8300

The Avaya Solutions Platform S8300 installs on the S8300E server with the following networking configuration:

- The management traffic of the hypervisor and the management and public traffic of the virtual machines are directed through **vSwitch0** with uplink **vmnic1**, so all IP addresses are on the same network.
- The **SERVICES** port traffic is directed through **vSwitch1** with uplink **vmnic0**.
- The **vmnic2** or LAN2 port on the faceplate of S8300E is not used in the default mode configuration.

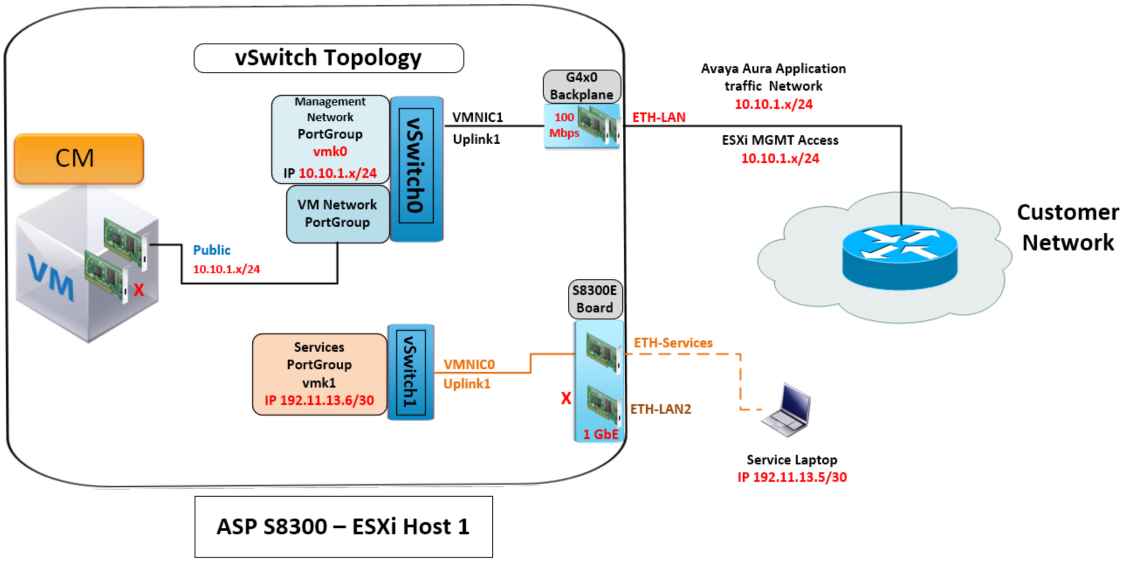


Figure 3: Default mode configuration

OOBM mode configuration in ASP S8300

The Avaya Solutions Platform S8300 network configuration changes after you enable the OOBM network using the following steps:

- A new virtual switch **vSwitch2** is created with **vmnic2** uplink (LAN2 on S8300E faceplate).
- The VM Network Port Group remains on **vSwitch0**. However, the Host **Management Network** Port Group label is changed to **OOB Management Network**, and along with the VMkernel “**vmk0**”, these get moved to the newly created **vSwitch2**. When the script completes its job, the user must change the IP address of the VMKernel “vmk0” to an available IP within the Customer Out of band Management Network to regain access to the host via its new OOBM interface.
- A new portgroup **Out of Band Management** is created and added to **vSwitch2**. This is used for Out of Band management traffic of the VMs.
- The ports on **vSwitch2** are addressed on the same network, which is the customer OOBM network and this network is separated from other customer networks, such as **vSwitch0**.
- **vSwitch2** and **vmnic2** separates the OOBM network physically from other customer networks.
- The management traffic of the hypervisor and the virtual machines is directed through **vSwitch2** with uplink **vmnic2**.
- The **SERVICES** port traffic is directed through **vSwitch1** with uplink **vmnic0**.

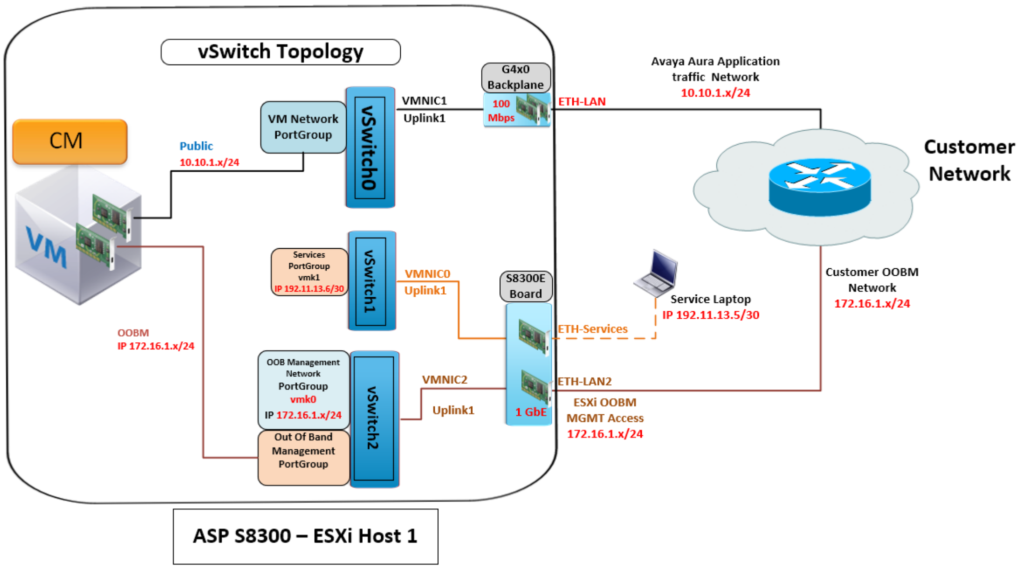


Figure 4: OOBM mode configuration

OOBM configuration on ASP S8300

You can configure OOBM on ASP S8300 during both of the following processes:

- Before VM deployment on the ASP S8300 host. For example, fresh installations.
- After VM deployment on the ASP S8300 host. For example, after fresh installed ASP, hosts migrated from AVP 8.1.X to ASP S8300 and hosts upgraded from ASP S8300 5.1.0.x to a later ASP S8300 5.1.0.x release.

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

Configuring OOBM on Avaya Solutions Platform S8300 before deploying VMs

About this task

OOBM can be configured only through a **SERVICES** port connection to the host. Use the following procedure to configure OOBM on Avaya Solutions Platform S8300 before deploying VMs.

Important:

Plan OOBM configuration activity only during the maintenance window as it involves network outage thereby resulting in downtime of hosts.

Before you begin

- A secure private network separated from rest of the customer network MUST be available for IP addressing. It is recommended that only System Administrators have access to this network. Connect the LAN cable to **LAN2** port of the S8300E.
- Ensure you have one available IP address from the customer's OOBM network.
- To deploy VMs after enabling OOBM on the host, have a System Manager SDM in the same OOBM network, so that the host can be added to the SDM. If you use SDM client on your laptop, then connect to the host through the **SERVICES** port and deploy VMs accordingly.
- Get a copy of `asp_oobm_v3.sh` shell script.

  Note:

  The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.
- For OOBM specific settings on the deployed VMs, see application-specific documentation.

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

Procedure

1. Connect your laptop to **SERVICES** port and configure IP address.
2. Using a SSH client, log in to 192.11.13.6 IP address.
3. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
4. Copy the `asp_oobm_v3.sh` shell script to ASP filesystem at the `/` path.
5. Type `chmod +x asp_oobm_v3.sh` and press **Enter** to grant execute permissions to the shell script.
6. Type `sh asp_oobm_v3.sh` and press **Enter** to view the shell script syntax usage.

   The console displays the following output:

   ```
   Command to configure Out of Band Management on ASP
   Management interfaces will be set to vmnic2
   Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
   Management configuration

   WARNING: Contact to the host may be lost due to the movement of ASP host
   management connection.
   Please make sure you are connected to the host via Services Port before
   proceeding with OOBM configuration
   ```
7. Type `sh asp_oobm_v3.sh enable` and press **Enter** to view the shell script syntax usage.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge configuring OOBM on the host.
8. Type `y` and press **Enter** to acknowledge.

   ```
   Performing pre-config checks...
   SUCCESS: Hardware Supported for ASP OOBM Configuration
   SUCCESS: Platform is ASP, OOBM can be configured

   pre-config checks succeeded...

   WARNING: Contact to the host may be lost due to movement of ASP host management
   connection. Please make sure you are connected to the host via Services Port. Are
   you sure you want to enable Out of Band Management? (Y)es/(N)o: y

   Initiated the process of enabling Out of Band Management on the host
   ```

   The script proceeds to shut down the VMs similar to the following output:

   ```
   Shutting down all the guest VMs deployed on this host

   All guest VMs shut down
   Host has no VMs deployed
   ```

```
Out of Band Management is now enabled on the host
Please change adapter settings of VMs and power on VMs from browser
```

9. There are no VMs deployed now, so ignore the following message:

   ```
   Please change adapter settings of VMs and power on VMs from browser
   ```

   OOBM is enabled on the host.

   Note:

   During deployment of OVA from SMGR SDM or SDM client, select the **Out of Band Management** portgroup for the VM ethernet interface to connect to the OOBM network.

Next steps

Proceed with VM deployment. For information on VM deployment, see Configuring network adapter setting to Out of Band Management on page 53.

Configuring OOBM on Avaya Solutions Platform S8300 after deploying VMs

About this task

Use the following procedure to configure OOBM on Avaya Solutions Platform S8300 after deploying VMs or after migrating from Avaya Virtualization Platform 8.1.x to Avaya Solutions Platform S8300.

Before you begin

- A secure private network separated from rest of the customer network MUST be available for IP addressing. It is recommended that only System Administrators have access to this network.

  Connect the LAN cable to **LAN2** port of the S8300E.

- Ensure you have one available IP address from the customer's OOBM network.
- Get a copy of `asp_oobm_v3.sh` shell script.

  Note:

  The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.

- For OOBM specific settings on the deployed VMs, see application-specific documentation.

  Note:

  Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

Procedure

1. Connect your laptop to **SERVICES** port and configure services port IP address for technician's laptop.
2. Using a SSH client, log into 192.11.13.6 IP address.
3. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
4. Copy the `asp_oobm_v3.sh` shell script to ASP filesystem at the `/` path.
5. Type `chmod +x asp_oobm_v3.sh` and press **Enter** to grant execute permissions to the shell script.
6. Type `sh asp_oobm_v3.sh` and press **Enter** to view the shell script syntax usage.

   The console displays the following output:

   ```
   Command to configure Out of Band Management on ASP
   Management interfaces will be set to vmnic2
   Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
   Management configuration

   WARNING: Contact to the host may be lost due to the movement of ASP host
   management connection.
   Please make sure you are connected to the host via Services Port before
   proceeding with OOBM configuration
   ```
7. Type `sh asp_oobm_v3.sh enable` and press **Enter** to enable OOBM on the host.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge configuring OOBM on the host.
8. Type `y` and press **Enter** to acknowledge.

   ```
   Performing pre-config checks...

   SUCCESS: Hardware Supported for ASP OOBM Configuration
   SUCCESS: Platform is ASP, OOBM can be configured

   pre-config checks succeeded...

   WARNING: Contact to the host may be lost due to the movement of ASP host
   management connection. Please make sure you are connected to the host via
   Services Port. Are
   you sure you want to enable Out of Band Management? (Y)es/(N)o: y

   Initiated the process of enabling Out of Band management on the host
   ```

   The script proceeds to shut down VMs similar to the following output:

   ```
   Shutting down all the guest VMs deployed on this host
   Shutting down server id: 4
   Waiting for 20 seconds for serverid: 4 to shut down, attempt: 1
   Waiting for 20 seconds for serverid: 4 to shut down, attempt: 2
   serverid: 4 is off
   Shutting down server id: 5
   Waiting for 20 seconds for serverid: 5 to shut down, attempt: 1
   ```

```
serverid: 5 is off
Shutting down server id: 6
Waiting for 20 seconds for serverid: 6 to shut down, attempt: 1
serverid: 6 is off
Out of Band Management is now enabled on the host

Please change adapter settings of VMs and power on VMs from browser
```

OOBM is enabled on the host.

Next steps

Proceed to change the vmk0 IP address settings after enabling OOBM on ASP S8300. For information on reconfiguring the vmk0 IP address, see Reconfiguring the vmk0 IP address after enabling OOBM in Avaya Solutions Platform S8300 on page 52.

Reconfiguring the vmk0 IP address after enabling OOBM in Avaya Solutions Platform S8300

About this task

When enabling OOBM in Avaya Solutions Platform S8300 servers, the VMkernel vmk0 is migrated from vSwitch0 (former in-band Management connection) to vSwitch2 to become part of the Customer OOBM network and provide Out of Band Management access to the ESXi host. Therefore, the vmk0 IP address must be re-configured to accommodate this change.

Before you begin

- Connect your laptop to the **SERVICES** port.
- Ensure you have one available IP address from the customer's OOBM network.

Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
2. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
3. Navigate to **Networking** > **VMkernel NICs**.
4. Click **vmk0** > **Edit settings**.
5. If required, expand the IPv4 settings view.
6. In the **Address** field, type the new IP address to be set that is part of the customer out of band management network.

   For example, `172.16.1.10`
7. In the **Subnet mask** field, enter the subnet mask to be set that is part of the customer out of band management network.

   For example, `255.255.255.0`
8. Click **Save**.

9. Navigate to **Networking** > **TCP/IP stacks**.
10. Click **Default TCP/IP stack** > **Edit settings**.
11. In the **IPv4 gateway** field, enter the default gateway to be set that is part of the customer out of band management network.

    For example, `10.10.1.1`
12. Click **Save**.

Next steps

Proceed with changing the network adapter settings and enabling OOBM on the VMs. For information on changing the network adapter settings, see Configuring network adapter setting to Out of Band Management on page 53.

Configuring network adapter setting to Out of Band Management

About this task

The VMs are in power OFF state after running the `asp_oobm_v3.sh` shell script as a part of configuring OOBM in the Avaya Solutions Platform S8300. Before powering VMs to the ON state, you need to configure the **Network Adapter** setting to **Out of Band Management**.

Before you begin

Connect your laptop to the **SERVICES** port.

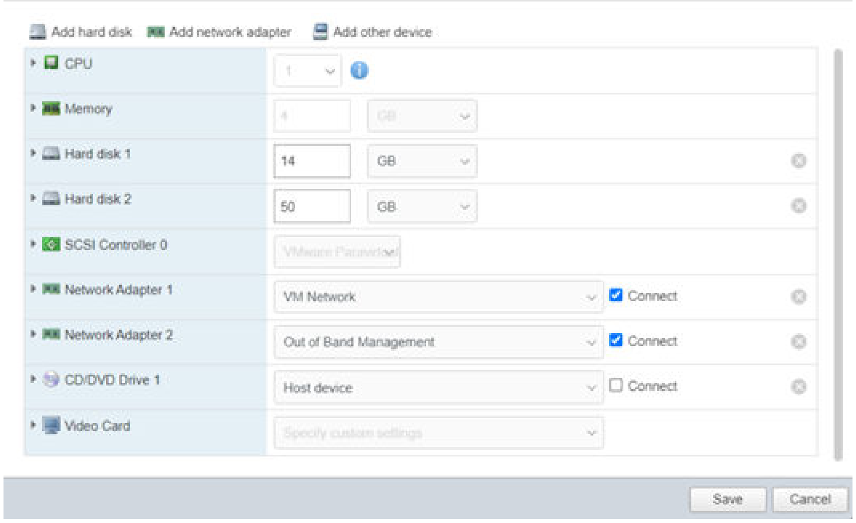
Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
2. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
3. Select a VM and navigate to **Actions** > **Edit Settings**.
4. In the **Edit Settings** dialog box, change the **Network Adapter** setting to **Out of Band Management** on the network adpater that will be used for OOBM. The setting change connects the OOBM ethernet interface of the VM to the OOBM Network.

   Important:

   Perform this step for all VMs and follow application specific documentation to fully enable OOBM for each VM.

   For example, the following Communication Manager VM screenshot displays the **Network Adapter 2** or eth1 interface that supports OOBM configuration. This is because the **Network Adapter 2** setting is changed to **Out of Band Management** portgroup. Additional OOBM configuration is required on the CM SMI to complete the OOBM configuration for CM. Refer to respective guides of all products to configure OOBM network for the respective products.



CPU	1		
Memory	4	GB	
Hard disk 1	14	GB	
Hard disk 2	50	GB	
SCSI Controller 0	VMware Paravirtual		
Network Adapter 1	VM Network		☑ Connect
Network Adapter 2	Out of Band Management		☑ Connect
CD/DVD Drive 1	Host device		□ Connect
Video Card	Specify custom settings		

5. After configuring the Network Adapters of all VMs to **Out of Band Management** portgroup you can power ON all the VMs.

   Access management interface of all VMs and host from OOBM network.

   Note:

   During deployment of OVA from System Manager SDM or SDM client, select the **Out of Band Management** portgroup for the VM ethernet interface to connect to the OOBM network. Refer to respective guides of all products to configure OOBM for the respective products.

Disabling OOBM on Avaya Solutions Platform S8300

About this task

The following procedure configures in-band management again on the host.

Important:

- Reconfigure in-band management on the VMs before disabling OOBM on the host.
- Test Public network access to the host before attempting to configure an application.

Note:

Unless otherwise stated by Avaya, DO NOT change the default Port Group labels for virtual machine traffic and ESXi management services traffic that are created during the ESXi installation, as this may impact integration with other Avaya applications and scripts.

Procedure

1. Connect your laptop to **SERVICES** port and configure services port IP address for technician's laptop.
2. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
3. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
4. Select a VM and navigate to **Actions** > **Edit Settings**.
5. In the **Edit Settings** dialog box, change the **Network Adapter** setting from **Out of Band Management** to **VM Network**. The setting change connects the Ethernet interface of VM from OOBM Network back to customer's public network.

   Important:

   Perform this step for all VMs.
6. Using a SSH client, copy the `asp_oobm_v3.sh` shell script to ASP filesystem at the `/` path.

   The OOBM script filename used in the document and screenshots are representative and might change as new versions of the script are provided. Refer to the PCN and Release Notes to ensure you obtain the latest script from PLDS.
7. Type `chmod +x asp_oobm_v3.sh` and press **Enter** to grant execute permissions to the shell script.
8. Type `sh asp_oobm_v3.sh` and press **Enter** to view the shell script syntax usage.

   The console displays the following output:

   ```
   Command to configure Out of Band Management on ASP
   Management interfaces will be set to vmnic2
   Usage: sh asp_oobm_v3.sh enable/disable - to put/remove the host into Out of Band
   Management configuration

   WARNING: Contact to the host may be lost due to the movement of ASP host
   management connection.
   Please make sure you are connected to the host via Services Port before
   proceeding with OOBM configuration
   ```
9. Type `sh asp_oobm_v3.sh disable` and press **Enter** to disable OOBM on the host.

   The script performs a few pre-configuration checks. If the pre-configuration checks result in a pass, the script prompts you to acknowledge disabling OOBM on the host.
10. Type `y` and press **Enter** to acknowledge.

    ```
    Performing pre-config checks...

    SUCCESS: Hardware Supported for ASP OOBM Configuration
    SUCCESS: Platform is ASP, OOBM can be configured

    pre-config checks succeeded...
    ```

```
WARNING: Contact to the host may be lost due to the movement of ASP host
management connection. Please make sure you are connected to the host via
Services Port. Are
you sure you want to disable Out of Band Management? (Y)es/(N)o: y

Initiated the process of disabling Out of Band management on the host
```

The script proceeds to shut down the VMs similar to the following output:

```
Shutting down all the guest VMs deployed on this host
Shutting down server id: 4
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 1
Waiting for 20 seconds for serverid: 4 to shut down, attempt: 2
serverid: 4 is off
Shutting down server id: 5
Waiting for 20 seconds for serverid: 5 to shut down, attempt: 1
serverid: 5 is off
Shutting down server id: 6
Waiting for 20 seconds for serverid: 6 to shut down, attempt: 1
serverid: 6 is off
Out of Band Management is now disabled on the host

Please change adapter settings of VMs and power on VMs from browser
```

OOBM is disabled on the host.

Next steps

Proceed to change the vmk0 IP address settings after disabling OOBM on ASP S8300. For information on reconfiguring the vmk0 IP address, see Reconfiguring the vmk0 IP address after disabling OOBM in Avaya Solutions Platform S8300 on page 56.

Reconfiguring the vmk0 IP address after disabling OOBM in Avaya Solutions Platform S8300

About this task

When disabling OOBM in Avaya Solutions Platform S8300 servers, the VMkernel vmk0 is migrated from vSwitch2 (former Out of Band Management connection) to vSwitch0 to become part of the Public network and provide in-band management access to the ESXi host. Therefore, the vmk0 IP address must be re-configured to accommodate this change.

Before you begin

- Connect your laptop to the **SERVICES** port.
- Ensure you have one available IP address from the public network.

Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.

2. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
3. Navigate to **Networking** > **VMkernel NICs**.
4. Click **vmk0** > **Edit settings**.
5. If required, expand the IPv4 settings view.
6. In the **Address** field, type the new IP address to be set that is part of the public network.
7. In the **Subnet mask** field, enter the subnet mask to be set that is part of the public network.
8. Click **Save**.
9. Navigate to **Networking** > **TCP/IP stacks**.
10. Click **Default TCP/IP stack** > **Edit settings**.
11. In the **IPv4 gateway** field, enter the default gateway to be set that is part of the public network.
12. Click **Save**.
13. Disconnect the LAN cable from the **LAN2** port.

Next steps

Proceed to turn VMs ON. For information on turning VMs to the ON state, see Powering Virtual Machines ON after disabling OOBM on the host on page 57.

Powering Virtual Machines ON after disabling OOBM on the host

About this task

The VMs are in power OFF state after running the `asp_oobm_v3.sh` shell script as a part of disabling OOBM in the Avaya Solutions Platform S8300. Before powering VMs to the ON state, check if **Network Adapter** is set to **VM Network**.

Before you begin

Connect your laptop to the **SERVICES** port.

Procedure

1. Open a web browser and go to https://192.11.13.6/ui to open the vSphere HTML client.
2. In the username field, type `root` and in the password field, type `ACP130_pw` or the password you configured for the root account.
3. Select a VM and navigate to **Actions** > **Edit Settings**.
4. In the **Edit Settings** dialog box, verify if **Network Adapter** is set to **VM Network**.

Important:

Perform this step for all VMs.

5. Power ON all VMs.

   Access the management interface of all VMs and the ESXi host from the customer's network to verify connectivity/access.

Chapter 9: Upgrading Avaya Solutions Platform S8300

Upgrading Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release

About this task

This chapter covers steps on upgrading the ASP S8300 from an earlier 5.1.0.x release to a later 5.1.0.x release.

Before you begin

Important:

Refer to the latest Avaya Solutions Platform S8300 Release Notes for supported upgrade paths. This is imperative for the ASP 5.1.0.6 release as it is based on an express patch from VMware/Broadcom and therefore is NOT cumulative. It must only be applied to ASP R5.1.0.5.

Ensure that:

- Current ASP S8300 is on an official Avaya certified ASP S8300 5.1.0.x load.
- ESXi license is a valid vSPhere 7 Foundation License (reference Chapter 6 for details on Licensing).
- Download the appropriate offline bundle zip file that will be utilized for the upgrade. Reference PCN2145S for details on the ASP S8300 releases and associated PLDS ids for the zip file.

  For example, if you are at ASP S8300 R 5.1 and want to upgrade to R5.1.0.1. Download *upgrade-asp-s8300-5.1.0.1.0-08.zip* (Download ID:ASP000000105) from PLDS.

Important Notes/Considerations

- During the update process, the ESXi host will try to shut down all Virtual Machines (VMs). If any VM fails to shut down, it will be forced to shut down.
- The host will enter maintenance mode after all VMs are shut down.
- The upgrade process includes a dry run and requires user input.

- After a successful upgrade, the host will exit out of maintenance mode and reboot.
- If unsuccessful, the host will only exit out of maintenance mode.
- All the Avaya vibs are removed and reinstalled during the upgrade process.
- Upon successful upgrade of ASP, all the Virtual Machines will AutoStart after reboot.
- The EASG vib will be installed during the upgrade process (if it was not previously present).
- If the ASP S8300 5.1.x was originally migrated from AVP 8.1.x, the persistent storage directory will be */vmfs/volumes/server-local-disk/*.
- If the ASP S8300 5.1.x was a new server (not migrated from AVP), the persistent storage directory will be */vmfs/volumes/datastore1/*.
- Post install recommendation – remove the offline zip file copied into persistent storage.

Upgrading Avaya Solutions Platform S8300 5.1.0.x to a later 5.1.0.x release

The procedures documented below utilize ASP S8300 5.1.0.2 as an example and the persistent storage directory will be *datastore1* as is seen on a new ASP S8300.

Procedure

1. Backup all Virtual Machines running on the host and ensure the backups are stored off of the host.
2. Start an SSH session to the ASP S8300.
3. Log in to the Avaya Solutions Platform S8300 command line interface (CLI).
4. Copy the appropriate offline bundle zip file as documented in PCN2145S to persistent storage of the host. The file MUST be copied directly into persistent storage, either */vmfs/volumes/server-local-disk* or */vmfs/volumes/datastore1*. Do not create a separate directory as the dry run will fail.

   For example, to upgrade to ASP S8300 5.1.0.2 from an earlier ASP S8300 5.1.0.x release, use offline bundle zip file: *upgrade-asp-s8300-5.1.0.2.0-04.zip*
5. Change directories to the location (persistent storage) of where you copied the offline bundle zip file.

   ```
   cd /vmfs/volumes/datastore1/
   ```
6. To ununzip the bundle, type the following command and press Enter.

   ```
   unzip <bundle-name>
   ```

   Example:

   ```
   unzip upgrade-asp-s8300-5.1.0.2.0-04.zip
   ```
7. Verify the following two files are present.
   - aspupdate.sh

- avaya-asp-[5.1.0.x.0-0x].zip
    - Example for ASP S8300 5.1.0.2: *avaya-asp-5.1.0.2.0-04.zip*

8. Run the shell script by providing the complete path to the location of the *avaya-asp-[5.1.0.x.0-0x].zip* file. For example, to upgrade from an earlier ASP S8300 5.1.0.x release to ASP S8300 5.1.0.2:

```
/vmfs/volumes/datastore1/aspudate.sh
      /vmfs/volumes/datastore1/avaya-asp-5.1.0.2.0-04.zip
```

9. Enter "Y" to confirm that the application backups have been taken. The system will proceed with the upgrade process.
10. The upgrade process will first perform a dry run.
11. If the dry run is not successful, the host will exit maintenance mode but the VMs will not autostart and will need to be manually started. Review the logs located in the persistent storage directory under the *upgradelogs* directory, for example:

```
/vmfs/volumes/datastore1/upgradelogs
```

12. After the dry run for the upgrade is successful, the actual upgrade commences.
13. The user should see a successful upgrade message similar to the following:

```
ASP 5.1.0.2.0 patch installation
        complete
```

14. The server will exist from maintenance mode and the ASP S8300 host will reboot.
15. After the reboot, login to the ASP S8300 embedded host client UI and ssh into the CLI to confirm the version upgrade is displayed. Reference Chapter 7 for details on how to verify the version information.
16. Post install recommendation – remove the offline zip file (and associated extracted files) from persistent storage.

Chapter 10: Maintaining Avaya Solutions Platform S8300

S8300E server component maintenance

This section is applicable to both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

There are no Field Replaceable Units (FRUs) on an S8300E server. The entire S8300E must be replaced.

For Gateway and Media Module maintenance information, refer to G450 Branch Gateway or G430 Branch Gateway on https://support.avaya.com/.

Configuration of S8300E server with G430 Branch Gateway/G450 Branch Gateway

G430 Branch Gateway/G450 Branch Gateway comprises a VoIP engine, an optional WAN router, and an Ethernet LAN connectivity. G430 Branch Gateway/G450 Branch Gateway supports IP telephones, digital telephones, and analog devices, such as modems, fax machines, and telephones. Communication Manager runs on the S8300E server to provide call control services to G430 Branch Gateway/G450 Branch Gateway.

Verifying heartbeat between S8300E and G430 Branch Gateway/G450 Branch Gateway

Procedure

1. Run **`ping 169.254.1.11`** or **`traceroute 169.254.1.11`** to check if gateway's backplane LAN private IP is reachable.
2. Run `/etc/init.d/hbmond status` to verify if `hbmond` is running. The output `hbmond is running` indicates that it is running.

3. Run `cat /etc/cajun` to check and view if board details are correctly populated.

   The following is a sample output when S8300E is seated into the *v1* slot of Media Gateway:

   ```
   cajun_slot=1
   cajun_fw_vintage=1
   cajun_board_suffix=E
   cajun_board_serial_number=<serial number of S8300>
   ```

   Check if the serial number of S8300E displayed on the screen <serial number of S8300> matches with the serial number on the faceplate of the S8300E.

4. Log in to Media gateway and run **`show mm v1`**

   The following is a sample output when S8300E is seated into the *v1* slot of the Media Gateway:

   ```
   MEDIA MODULE DESCRIPTION: v1
   -------------------------------------------------
   Type             : ICC
   Description      : S8300 Media Module
   Serial Number    : <serial number of S8300>
   HW Vintage       : 1
   HW Suffix        : E
   FW Version       : 0
   No. of ports     : 2
   Faults           : No Fault Messages
   ```

   Check if the serial number of S8300 displayed on the screen <serial number of S8300> matches with the serial number on the faceplate of the S8300E.

ASP S8300 host backup and restore

Applications deployed on the ASP S8300 host should be backed up to a remote storage device.

Backing up the VMware ESXi Configuration

About this task

Note:

This procedure assumes that *no DHCP* was used for assigning IP addresses to the ASP S8300 host, that it is still in the same configuration originally deployed and shipped by Avaya.

You need to have a current backup of the VMware ESXi host configuration data in case a server fails and needs to be replaced. Use the procedure in this section to back up the VMware ESXi host configuration using the ESXi command line.

Note:

For additional information and procedures, see VMware Knowledge Base article 2042141: https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042141.

The following is a list of some of the key ESXi items and configurations that are backed up during the procedure:

- ESXi host details (Hostname, IP address, FQDN, domain)
- Network configurations (vSwitches, VMkernel’s, Port groups, NIC teaming, tagging)
- Certificates (self-signed and third-party)
- Licensing
- Enabled services (SSH, Shell)
- User accounts and credentials for access (DCUI, root, custom accounts)
- List of VM’s configured for AutoStart
- Logs and log file directory locations
- The /etc/hosts file contents
- TLS/SSL protocols enabled/disabled

Procedure

1. Log in to the ESXi host by using a Secure Shell (SSH) client e.g., PuTTY.
2. Authenticate using the existing *root* credentials or *sroot* EASG if enabled.
3. Use the command **`vim-cmd hostsvc/firmware/backup_config`** to back up the ESXi host configuration.

   A URL will be displayed in the command line similar to the following example:

   ```
   http://*/downloads/52c08d7e-3f2a-6156ec7c-8f9cb8f77911/
   configBundle-esxi1.sv.avaya.com.tgz
   ```

4. Copy and paste the URL into a browser and in place of the `*` in the URL enter the ESXi host IP or FQDN. Press **Enter**.

   Example:

   ```
   http://<IP address or FQDN of ESXi
   host>/downloads/52c08d7e-3f2a-6156ec7c- 8f9cb8f77911/configBundle-
   esxi1.sv.avaya.com.tgz
   ```

   Note:

   The backup will automatically be downloaded to the local laptop as soon as you press **enter**.

Restoring the VMware ESXi Configuration

About this task

Use the procedures in this section to restore ESXi host configuration in case of server failure or replacement through the ESXi command line.

Note:

When restoring configuration data, the build number of the ESXi host must match the build number of the host backup file and UUID (can be obtained using the command "**`esxcfg-info -u`**") of the host should match the UUID of the host on backup file.

For additional information and procedures, see VMware Knowledge Base article 2042141:

https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2042141.

Before you begin

- The ESXi host network settings will be required to be configured first in order to access the ESXi host to run the restore procedure. See Configuring network parameters on page 28.
- Enable SSH access on the ESXi host. See Enabling and disabling SSH on Avaya Solutions Platform S8300 Release 5.1.x from Solution Deployment Manager on page 34.
- The `configBundle-HostFQDN.tgz` backup file should be renamed as `configBundle.tgz` before initiating the restore command. If not changed the restore command will fail.

Procedure

1. Connect to the ESXi host using SSH with PuTTY.
2. Log in using the local administrative credentials.
3. Use the command `vim-cmd hostsvc/maintenance_mode_enter` to put the host into Maintenance Mode.
4. Use WinSCP to copy the backup configuration file to the `/tmp` directory on the host.

   Important:

   Using the command in the next step reboots the host after completion. You will not be warned or asked to defer the reboot.
5. Use the command `vim-cmd hostsvc/firmware/restore_config /tmp/configBundle.tgz` to restore the configuration.
6. The server will automatically reboot to restore the ESXi configuration from the backup after command completion.
7. Once the server is back online, if not done automatically, use the command `vim-cmd hostsvc/maintenance_mode_exit` to exit the host from Maintenance Mode.

   All configuration data including the vSwitches/VMkernels/Licensing is restored.

Chapter 11: Avaya Solutions Platform S8300 component MIBs and OIDs

Avaya Solutions Platform S8300 component MIBs and OIDs

This section is applicable to both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

The following links contain the MIBs and OIDs provided by vendors for using third-party monitoring tools:

VMware ESXi 7.0:

- SNMP MIB module file download: https://kb.vmware.com/s/article/1013445
- Determining the MIB module listing, name and type of an SNMP OID: https://kb.vmware.com/s/article/2054359

This information is provided for reference only.

Chapter 12: Troubleshooting Avaya Solutions Platform S8300

Overview

This section is applicable to both preloaded/prelicensed ASP S8300 and fresh install on ASP S8300.

Performing server recovery, software remastering or catastrophic migration

About this task

Use the following procedure to perform software remastering.

⚠ **Warning:**

All information will be lost from the S8300E. If performing a catastrophic migration from AVP on S8300 to ASP S8300, make sure to save a copy of the AVP IP and naming information/ conventions.

All application data should be backed up to a remote storage device. This data will be required for a seamless recovery.

Before you begin

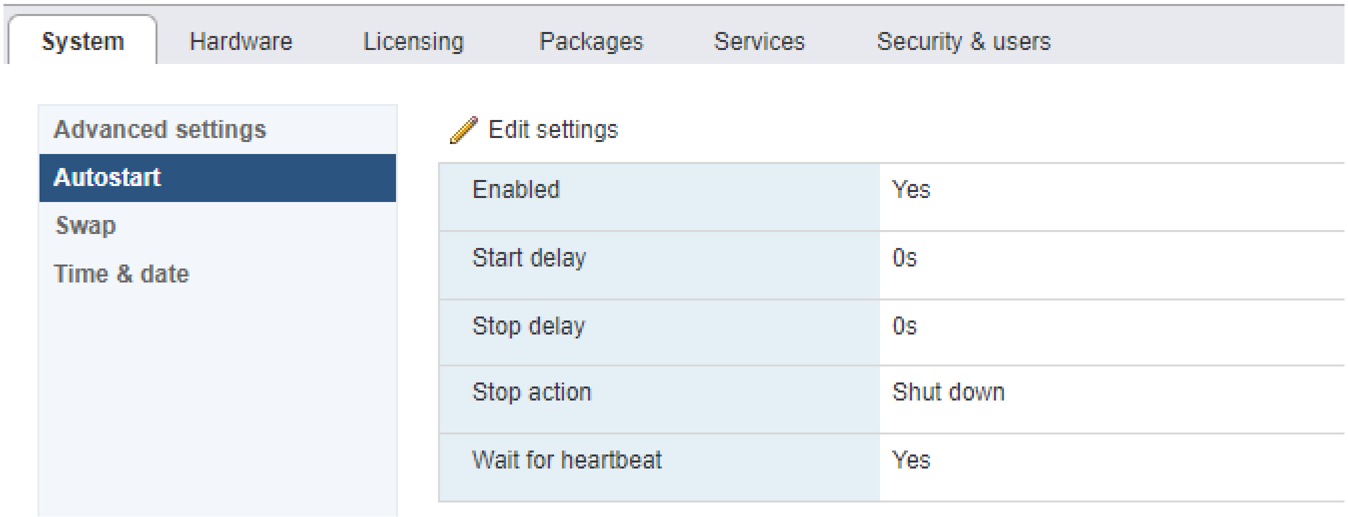
- Configure `aspks.cfg` file utilizing the SDM Client and save to the USB stick.
- The kickstart file name must remain `aspks.cfg` and the contents of the generated `aspks.cfg` file must never be modified.
- Ensure you have an Avaya certified external USB DVD Reader.
- Ensure that the appropriate ASP S8300 ISO file is downloaded and burned to a DVD.
- If access to the S8300E is still possible, ensure all applications deployed on the S8300E are backed up and stored on a remote storage device, ready for restoration.

Procedure

1. Power G430/G450 on the S8300E should NOT be inserted at this point.
2. Connect the External USB DVD Reader and the USB stick (containing the aspks.cfg file) to the S8300.

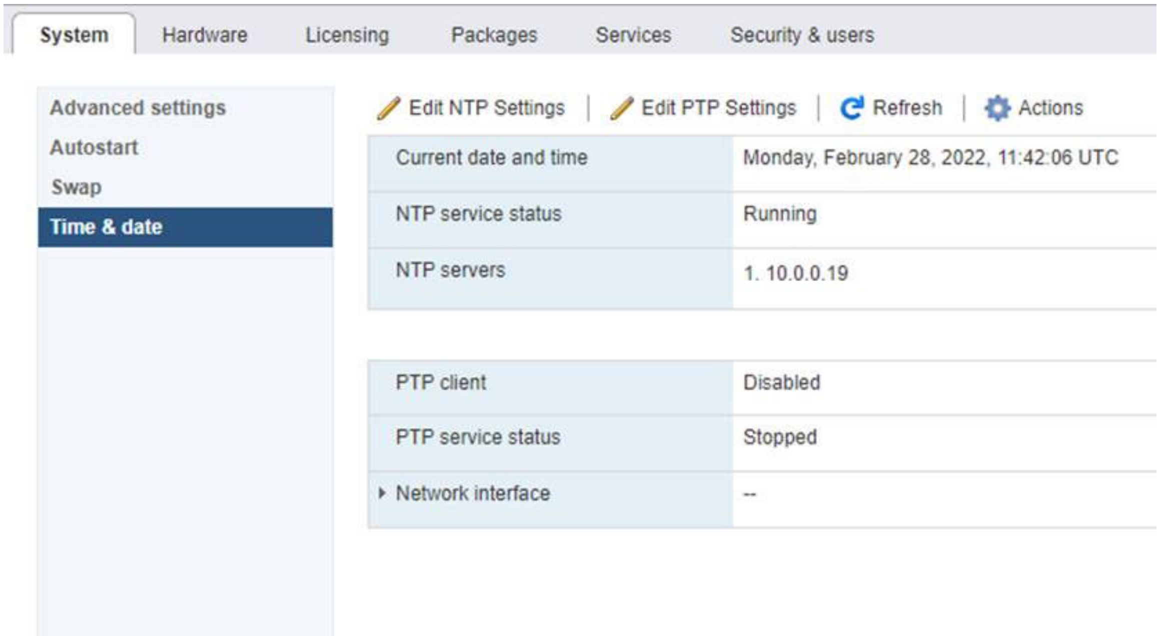
3. Insert S8300E into G430/G450 gateway.
    a. The Alarm LED blinks to indicate the start of the installation process.
    b. The system installs the ASP S8300 and automatically ejects DVD.
    c. After the system ejects DVD and the LEDs are off, remove the External DVD Reader and USB stick from ASP S8300.
    d. The installation process takes about 20 minutes to complete.
4. Using an SSH client, connect to the server through the Services Port by using the following network parameters on your local PC:
    - IP address: 192.11.13.5
    - Netmask: 255.255.255.252
    - Gateway: 192.11.13.6
5. Login with `root` username and `ACP130_pw` as default password.
6. Run the **`vmware -vl`** command to verify if ESXi 7.0.x was installed.
7. Click the https://192.11.13.6/ui link to open a web browser.
8. Type `root` for username and `ACP130_pw` for password.
9. Self-signed certificate must be regenerated. Refer to the “Regenerating Avaya Solutions Platform S8300 self-signed certificate with FQDN using the command line interface” section in “Chapter 4: Installing Avaya Solutions Platform S8300”. All steps must be performed.
10. Load ESXi 7.0 license.

    For more information on loading ESXi 7.0 license, see Installing ESXi 7.0 License file on the ASP S8300 host on page 41.
11. Navigate to **Host** > **Manage** > **System** and verify if **Autostart** is enabled. If it is not, enable **Autostart**.



Enabled	Yes
Start delay	0s
Stop delay	0s
Stop action	Shut down
Wait for heartbeat	Yes

12. Navigate to **Time & date** and verify if time and date are correct. If not, configure time and date.



Current date and time	Monday, February 28, 2022, 11:42:06 UTC
NTP service status	Running
NTP servers	1. 10.0.0.19

PTP client	Disabled
PTP service status	Stopped
▸ Network interface	--

13. Set values for NTP.

    For more information on configuring NTP, see NTP server configuration on page 28.

14. Deploy Communication Manager and Branch Session Manager OVAs.

    Note:

    OVAs may be deployed using SDM or the ESXi embedded host client.

    If deployed using the ESXi embedded host client, CM will not power up until the CPU settings are modified.

    To modify the CPU settings:

    a. Open a web page to the ESXi web interface on the ASP S8300 R5.1.x server.
    b. In the **navigator** > **virtual machines**, select the Communication Manager LSP VM.
    c. In the main window for the CM LSP VM, select **Actions** > **Edit Settings**.
    d. In the **Edit Settings** window, expand the CPU settings.
    e. In the **Reservation** parameter set the value to **None** in the drop-down menu.
    f. Select **Save** to update the settings.

    The CM VM can now be powered on.

15. After deploying the OVAs, if OVAs deployed via the ESXi embedded host client, launch VM Console from the ESXi UI and configure IP and naming information.

    For information on naming convention, refer to the SMI pages in Communication Manager documentation.

16. Perform Feature Pack/Service Pack/Security Service Pack/Patch Application and then Restore Backup.

    For more information on performing patch application and restoring backup, refer to application documentation on Communication Manager and Session Manager.

17. Deploy second application OVA and repeat process.

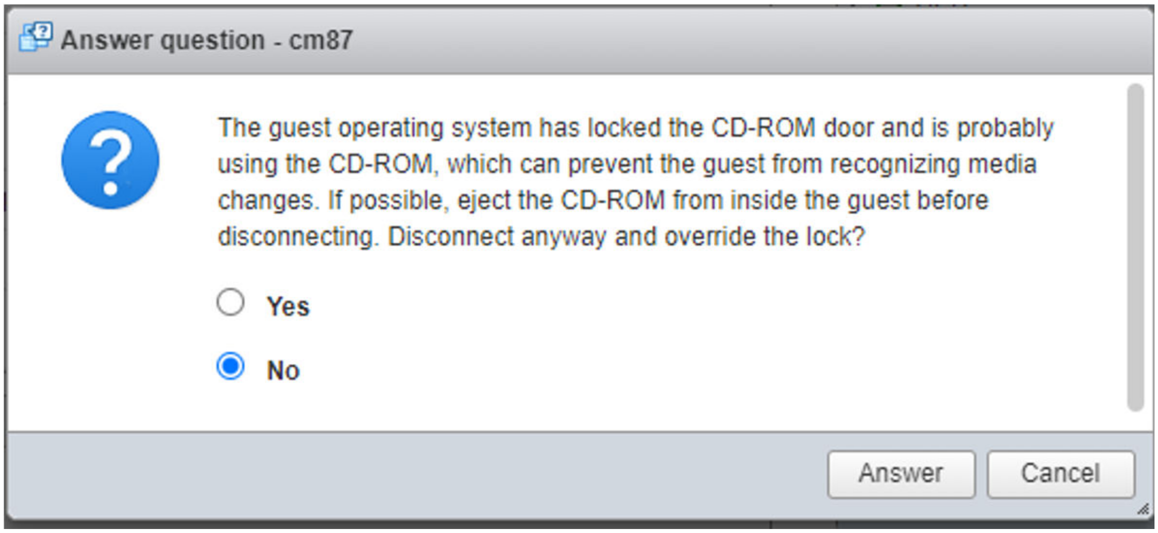
Preventing "Answer question dialog box" occurrence on the Avaya Solutions Platform S8300 web client

About this task

After you deploy VM on the Avaya Solutions Platform S8300 host, the VM automatically selects the **Connect at power on** setting. This selection results in the Avaya Solutions Platform S8300 host automatically connecting to the **CD/DVD Drive 1** of the VM after you perform one of the following procedures:

- Migrating from AVP to ASP S8300 with VM deployed on the AVP host because ASP S8300 is rebooted after migration.
- Rebooting ASP S8300.
- Shutting down and powering on VM.

The Avaya Solutions Platform S8300 host displays the **Answer question** dialog box only the first time when VM re-establishes trust with SDM after you perform one of the procedures listed above.



Answer question - cm87

The guest operating system has locked the CD-ROM door and is probably using the CD-ROM, which can prevent the guest from recognizing media changes. If possible, eject the CD-ROM from inside the guest before disconnecting. Disconnect anyway and override the lock?

○ Yes

● No

Do the following steps to prevent the **Answer question** dialog box occurrence:

Procedure

1. Select the virtual machine and click **Edit**.

2. In the **Edit settings** dialog box, navigate to **CD/DVD Drive 1** > **Status**.
3. Uncheck **Connect at power on**.
4. Click **Save**.

Server inaccessible

In some cases, an S8300E may become inaccessible. This can be identified with the OK-to-Remove LED blinking continuously.

Typically recovery requires a server reboot (reseat the S8300E). Within the following 8 to 10 minutes, the OK-to-Remove LED stops blinking and server undergoes a reboot automatically. After a further 5 to 6 mins if all LEDs are off, then the server is stabilized.

Troubleshooting S8300E inaccessible

Cause

S8300 card has been reseated without performing the graceful shutdown.

Best Practice

1. Before removing or reseating the S8300 card in the Branch Gateway, shut down the S8300 card by pressing the Shut Down button for 3 to 4 seconds.
2. Once OK TO REMOVE LED stops blinking and becomes stable, then reseat the S8300 into the Branch Gateway.

Troubleshooting using CLI commands

Troubleshooting gateway CLI command in S8300

The G450 and G430 gateway monitor the presence and sanity of the S8300 using a heartbeat on an internal Ethernet connection through the gateway backplane.

When you use the **`show mg list`** CLI command, one of the following messages or values are displayed when you check the status of the S8300 in slot *v1* :

- **`Not Installed`**

```
G450-001(super)# show mg list
SLOT   TYPE         CODE        SUFFIX  HW VINTAGE  FW VINTAGE
----   --------     ----------  ------  ----------  -----------
v1     -- Not Installed --
v2
```

  S8300 displays **`Not Installed`**, when the gateway does not detect a board. Possible causes are empty slot, S8300 not fully inserted, or faulty connectors.

- **Initializing/Faulted**

  ```
  G450-001(super)# show mg list
  SLOT   TYPE         CODE        SUFFIX  HW VINTAGE  FW VINTAGE
  ----   ---------    ----------  ------  ----------  -----------
  v1     -- Initializing --
  v2
  ```

  S8300 displays **Initializing/Faulted**, when the gateway detects a board, but it does not respond to ping. Possible causes are faulted board, vSwitch not setup correctly, software not loaded or not running.

- Board **SUFFIX** is **X** and **HW VINTAGE** is **0**

  ```
  G450-001(super)# show mg list
  SLOT   TYPE         CODE        SUFFIX  HW VINTAGE  FW VINTAGE
  ----   ---------    ----------  ------  ----------  -----------
  v1     S8300        ICC         X       0           0
  v2
  ```

  S8300 displays values for SUFFIX and HW VINTAGE as X and 0 respectively. This implies that the gateway can ping the S8300 on the internal VLAN, but the heartbeat is not present and the gateway did not receive the board suffix and Vintages. Possible causes are the S8300 is not fully initialized or the Avaya heartbeat software is not operational, but the ESXI vSwitch is setup correctly.

- Board **SUFFIX** is correct

  ```
  G450-001(super)# show mg list
  SLOT   TYPE         CODE        SUFFIX  HW VINTAGE  FW VINTAGE
  ----   ---------    ----------  ------  ----------  -----------
  v1     S8300        ICC         E       1           1
  v2
  ```

  S8300 displays correct suffix. This implies that the S8300 heartbeat is present and no issues are detected by the gateway.

Troubleshooting gateway log messages

You can view the syslog stored locally on the gateway using the **show logging file content** CLI command.

If the S8300 heartbeat stops, the gateway will reset the S8300 and log a message indicating that a **HARD RESET** and then a **SOFT RESET** was performed. There could also be **Unsupported Media Module** messages when the gateway has not identified the type of board in the slot.

```
<187>Dec 29 15:25:04 g450graf -NoTag: -NoUTC(0 0 0:14:20) 2021 350 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 carries out HARD RESET,
ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:24:11 g450graf -NoTag: -NoUTC(0 0 0:13:27) 2021 690 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
insertion 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:24:11 g450graf -NoTag: -NoUTC(0 0 0:13:27) 2021 690 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
extraction 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53

<187>Dec 29 15:22:05 g450graf -NoTag: -NoUTC(0 0 0:11:21) 2021 420 1
mediagateway.g450 | 0 MSY-TRPMAJNO[VOICE-Error: Unsupported Media Module
insertion 019V1, ID=e2a214cc8919d0e4ebf0620beb381a53
```

```
<187>Dec 29 15:19:43 g450graf -NoTag: -NoUTC(0 0 0:08:59) 2021 650 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 carries out SOFT RESET,
ID=e2a214cc8919d0e4ebf0620beb381a53
```

Gateway faults

You can generate and display faults or alarms when S8300 is not inserted into v1, using the **`set icc-monitoring enable`** CLI command and by setting the S8300 Monitoring status to **`Enabled`**. Set status to **`Disabled`** when you are not using the **`show faults`** feature.

```
g450graf-019(develop)# show icc-monitoring
Slot v1 S8300 Monitoring Status: Enabled
Done!
g450graf-019(develop)# show faults

CURRENTLY ACTIVE FAULTS
--------------------------------------------------------------------------
        + Expected S8300 in v1 not present, 01/13-16:14:24.00
```

When monitoring status is set to enabled, a log message is displayed similar to the following example, if the S8300 is not in service in the `show logging file content` output.

```
<187>Jan 21 16:14:24 g450graf -NoTag: -NoUTC(0 0 0:01:32) 2022 105 1
mediagateway.g450 | 0 ICC-TRPMAJNA[VOICE-Error: S8300 in slot v1 is NOT
INSERVICE, ID=e2a214cc8919d0e4ebf0620beb381a53
```

Chapter 13: Resources

Avaya Solutions Platform S8300 documentation

The following documents are available on Avaya support site at https://support.avaya.com/:

Title	Description
Installing, Maintaining, and Troubleshooting Avaya Solutions Platform S8300	Describes how to install, maintain, and troubleshoot Avaya Solutions Platform S8300.
Migrating from Appliance Virtualization Platform deployed on S8300 Server to Avaya Solutions Platform S8300	Describes migration procedure from AVP to Avaya Solutions Platform S8300.
Port Matrix for ASP S8300	This document provides a list of interfaces, TCP and UDP ports that hardware components and applications use for intra-connections and for inter-connections with external applications or devices.
Policies for technical support of the Avaya Solutions Platform (ASP) 130 and S8300E R5.1	This document and statements related to support are only with respect to Avaya Services support of the software and hardware of the Avaya Solutions Platform (ASP) 130 server and S8300E server based on supported and tested configurations.
Avaya Solutions Platform S8300 5.1.x Release Notes	Release Notes.
PCN2145S Avaya Solutions Platform S8300 5.1.x	This is a Product Correction Notice about the availability of Avaya Solutions Platform S8300 R5.1.x and Avaya's Customized Image of VMware ESXi 7.0.

Appliance Virtualization Platform documentation

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

Title	Description	Audience
Implementing		
Deploying Avaya Aura® Appliance Virtualization Platform	Deploy, configure, and administer Avaya Aura® Appliance Virtualization Platform.	Implementation personnel
Upgrading Avaya Aura® Appliance Virtualization Platform	Upgrade Avaya Aura® Appliance Virtualization Platform.	Implementation personnel
Administration		
Avaya Aura® Appliance Virtualization Platform and AVP Utilities Data Privacy Guidelines	Describes how to administer Avaya Aura® Appliance Virtualization Platform to fulfill Data Privacy requirements.	Implementation personnel, system administrator, service and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click 🔍 to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.

3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
10. Press **Enter**.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at https://documentation.avaya.com. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the Avaya Support website.

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.
- Click **Languages** (🌐) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.

- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** (➦) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (🔖). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

  You can do the following:

  - Create, rename, and delete a collection.
  - Set a collection as the default or favorite collection.
  - Save a PDF of the selected content in a collection and download it to your computer.
  - Share content in a collection with others through email.
  - Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

  - Enable **Email notifications** to receive email alerts.
  - Unwatch the selected content or all topics.
- Send feedback for a topic.

Support

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

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted..
3. Click **Product Support** > **Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Index