



Upgrading Avaya Solutions Platform 4200 Series using the Management Server Console

Release 4.1
Issue 3
May 2020

© 2018-2020, Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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](http://www.mpegla.com).

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Contents

Chapter 1: Introduction	7
Purpose.....	7
Product registration.....	7
Warranty.....	7
Chapter 2: New in this document	9
New in this document.....	9
Avaya Pod Fx upgrades to Avaya Solutions Platform 4200 series Release 4.1	9
Avaya Orchestrator.....	10
Chapter 3: MSC software and configuration	11
Management Server Console.....	11
Management Server Console software and configuration.....	11
Deploying Management Server Console.....	12
Connecting to the Management Server Console.....	22
Manual steps for changing the domain name in the MSC.....	22
Deleting Residual FQDN after changing DNS Suffix.....	27
Configuring Trusted Site on Internet Explorer	29
Configuring and licensing the Management Server Console.....	31
Windows Firewall (Optional).....	32
Configuring Windows 2016 MSC As NTP Client (Optional).....	32
Using Windows 2016 MSC as SFTP Server (Optional).....	36
Chapter 4: Upgrades	39
Upgrading Avaya Solutions Platform 4200 series.....	39
Supported upgrade paths.....	40
HPE Nimble supported upgrade paths.....	48
Determining licensing requirements.....	50
Checklist for upgrading and patching Avaya Solutions Platform 4200 series.....	50
Software and OVA repository.....	59
Download new software.....	60
Transferring files	60
File transfer options.....	61
Migrating to Avaya Orchestrator from POS applications.....	66
Disassociating VPFM from Applications and infrastructure components.....	67
Upgrading to VMware vCenter Server Appliance 6.5 Update 3b.....	70
Upgrading the HPE Qlogic driver.....	79
Using VUM to update ESXi hosts.....	80
Upgrading the switches.....	91
Upgrading storage devices.....	100
Upgrading server firmware.....	108
Upgrading PDU firmware.....	111

Upgrading ESXi Hosts manually using Command Line.....	113
Configuring Network Time Protocol.....	114
Deploying Avaya Diagnostic Server.....	118
Deleting VMware snapshots.....	121
Chapter 5: Resources	122
Resources.....	122
Documentation.....	122
Training.....	125
Avaya Mentor videos.....	125
Support.....	126

Chapter 1: Introduction

Purpose

This document provides information and tasks for using the Management Server Console for Avaya Solutions Platform 4200 series after the initial site installation and deployment. This document does not include optional or customized aspects of solution configurations, deployments, maintenance, or upgrades. This document is intended for Avaya Professional Services, Solution Integrators, certified technicians, and support personnel. The user of this document must be aware of the supported Avaya Solutions Platform 4200 series solution applications and the basic workings of VMware vSphere and Microsoft Windows Server.

Avaya Solutions Platform 4200 series was formerly called Avaya Converged Platform 4200, Avaya Pod Fx, and Avaya Collaboration Pod.

Product registration

To prevent service interruption, you must register your Avaya Solutions Platform products.

Following are the available methods for product registration:

- **Implementation as a service:** If Avaya Professional Services provided implementation services on site, Avaya Professional Services also performs product registration on your behalf.
- **Avaya Partner and Customer implementation:** For information about the step-by-step registration process, see the Avaya Classic Global Registration Process Help Document on the Avaya Product Support Registration page. The document ID is 100162279.

Product registration is a required element for effective Avaya customer support. You must follow the Partner and Customer Guidance in the Avaya Global Registration Process to help ensure the seamless support you have come to expect from Avaya.

Warranty

Avaya provides a limited warranty on its Hardware and Software (“Product(s)”).

Refer to your sales agreement to establish the terms of the limited warranty.

The standard warranty language for Avaya, 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: <http://support.avaya.com>.

 **Note:**

If you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Example

1. Go to the Avaya Support website at <http://support.avaya.com>.
2. In the Global search field, type `warranty`, to search the Avaya Knowledge Base for warranty topics.
The system displays a list of all warranty topics.
3. Click the relevant warranty topic.

Chapter 2: New in this document

New in this document

The following sections detail what is new in this document.

Avaya Pod Fx upgrades to Avaya Solutions Platform 4200 series Release 4.1

Preexisting Avaya Pod Fx platforms can upgrade to Avaya Solutions Platform 4200 series Release 4.1 software. For information on supported upgrade paths, see [Supported upgrade paths](#) on page 40.

 **Important:**

The Avaya Pod Utility Module has been removed from the Management Server Console software in Release 3.1. Perform upgrades using the procedures documented in *Upgrading Avaya Solutions Platform 4200 series using the Management Server Console Release 4.1*.

Avaya Solutions Platform 4200 series Release 4.1 upgrades must be performed by Avaya Professional Services, or by Avaya Solutions Platform 4200 series certified Business Partner. They must plan and prepare tasks before upgrading, such as downloading and transferring all the upgrade files required before starting any component upgrades.

To perform an Avaya Solutions Platform 4200 series Release 4.1 upgrade, update the following components to the Release 4.1 software baseline:

- HPE compute servers BIOS and firmware
- VMware vCenter and ESXi software
- Deploy Avaya Orchestrator
- Avaya network switches software and firmware
- EMC/HPE Nimble storage array software and firmware
- ServerTech Power Distribution Unit (PDU) firmware
- Remove Unisphere Remote and deploy Unisphere Central (only applicable for Avaya Solutions Platform with VNX5300)

 **Warning:**

Avaya Solutions Platform 4200 series Release 4.1 supports VMware release 6.5 and Avaya Aura[®] release 8.1. Before performing any upgrades, verify if your existing solution applications

are supported within these releases using the product compatibility matrix available at <https://secureservices.avaya.com/compatibility-matrix/menus/product.xhtml>.

You can upgrade ACM to the xCaaS 2.0 supported versions before performing an upgrade of the Avaya Pod Fx infrastructure to Avaya Solutions Platform 4200 series Release 4.1.

For more information about performing Avaya Solutions Platform 4200 series infrastructure upgrades, see [Upgrading Avaya Solutions Platform 4200 series](#) on page 39

It is recommended that you perform the Avaya Solutions Platform 4200 series Release 4.1 Configuration Design Review process in the event of an upgrade. This is recommended to validate the updated software line up for the applications does not require additional resources in the Avaya Solutions Platform 4200 series Release 4.1 such as additional storage or servers. To schedule a design review, email aspsales@avaya.com.

Avaya Orchestrator

The Avaya Orchestrator Release 1.5 is a visualization and management application which is used to monitor Avaya Solutions Platform 4200 series Release 4.1. Starting with Avaya Solutions Platform 4200 series Release 4.0, Avaya Orchestrator replaces the POD Orchestration Suite that is end-of-sale with the Avaya Pod Fx Release 3.1.

Avaya Orchestrator performs the following operations:

- Works in conjunction with the SAL Gateway to monitor and escalate product alarms and notifications across all the Avaya Solutions Platform 4200 series infrastructure hardware.
- Produces real-time and historical reporting tools for customized means to review solution state of health.
- Provides a single dashboard view for monitoring state of health of all Avaya Solutions Platform 4200 series racks, components, and services.
- Sends email notifications for product alarm escalations.
- Provides consistent proactive monitoring of all administered components.
- For the Avaya Orchestrator Release 1.5, software applications will continue to have alarms supported through the SAL gateway. Software alarm support will be available in a later release

For more information on Avaya Orchestrator, see *Configuring and Using Avaya Orchestrator*.

Chapter 3: MSC software and configuration

Management Server Console

The Management Server Console (MSC) is a Microsoft Windows 2016 Standard Edition server virtual machine provided on all Avaya Solutions Platform 4200 series. The MSC provides software and utilities to manage and upgrade the Avaya Solutions Platform 4200 series software and components.

! **Important:**

Ensure the Avaya Solutions Platform 4200 series has sufficient resources before deploying additional virtual machines or software components. Consult with a Solution Engineer to use the Avaya Configurator Tool (CTOOL) to calculate resource availability for the solution.

Software configuration

The MSC configuration includes:

- Microsoft Windows 2016 Standard Edition server
- VMware vSphere thick Client 6.0
- Mozilla Firefox
- Notepad++
- Wireshark
- WinSCP
- PuTTY
- DNS server enabled
- TFTP server
- SFTP Server

Management Server Console software and configuration

The following sections describe the Management Server Console (MSC) and installed software.

The Avaya Management Server Console is a Microsoft Windows Server 2016 Standard virtual appliance intended for use by Avaya professionals or co-delivery partners. Authorized

professionals can use the MSC for virtual appliance deployment, management, and upgrades of Avaya Solutions Platform 4200 series platforms.

Deploying Management Server Console

About this task

The following procedure describes the OVF deployment of Management Server Console (MSC).

Before you begin

- Download the new MSC OVA version **4.1.0.0.2** from PLDS and transfer the file into the current MSC, E: drive
- Ensure that you have one available IP address within the Management VLAN, whether or not you plan to reuse the IP address used by the existing MSC VM.

Procedure

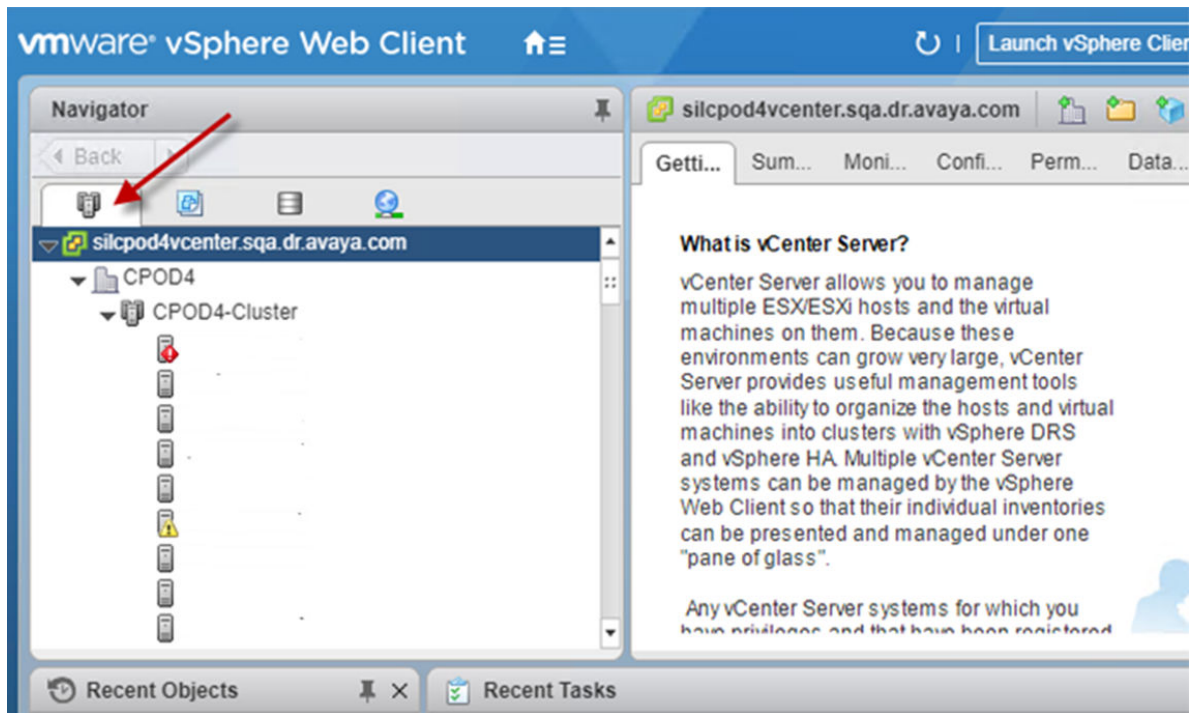
1. Use a Remote Desktop Connection (RDP) to access the existing Management Server Console and login using the Administrator credentials.
2. Open a web browser to connect to the vCenter web client.

 **Note:**

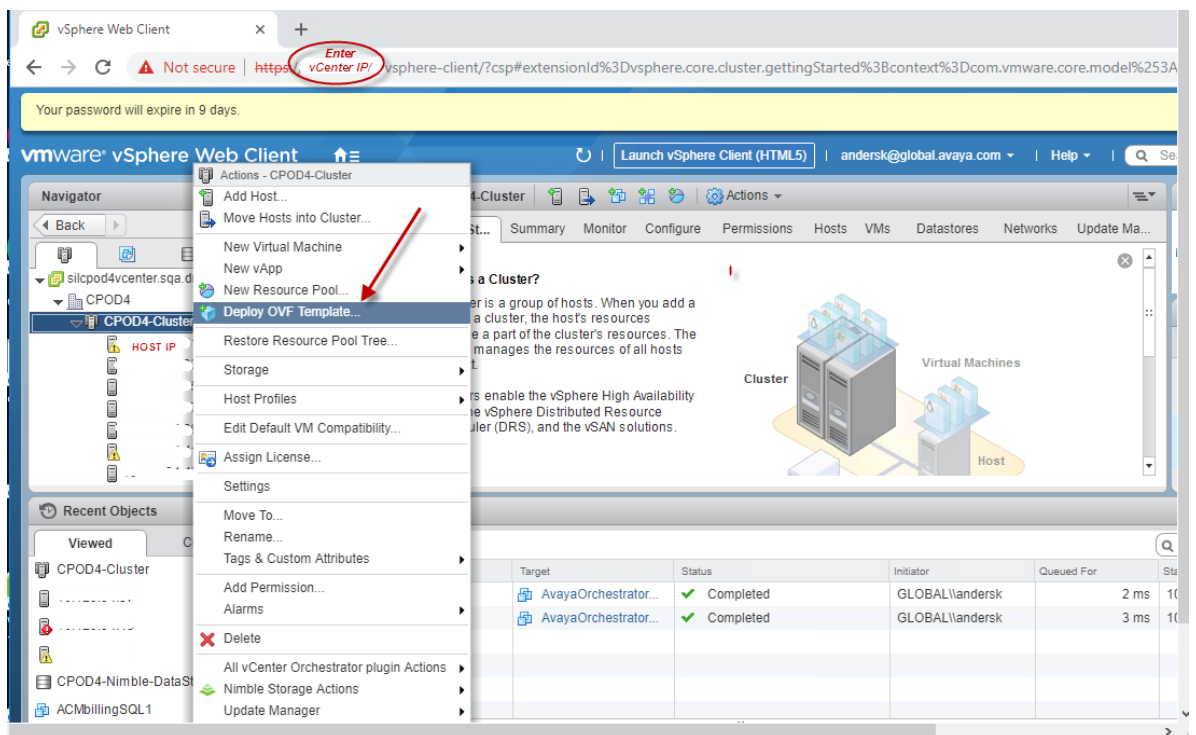
Ensure that you use Firefox browser when conducting OVF Deployments. Other browsers can cause the deployment to fail with random, multiple errors when the wizard tries to import the OVA or when the deployment is in progress.

3. Connect to administrator@vsphere.local account.

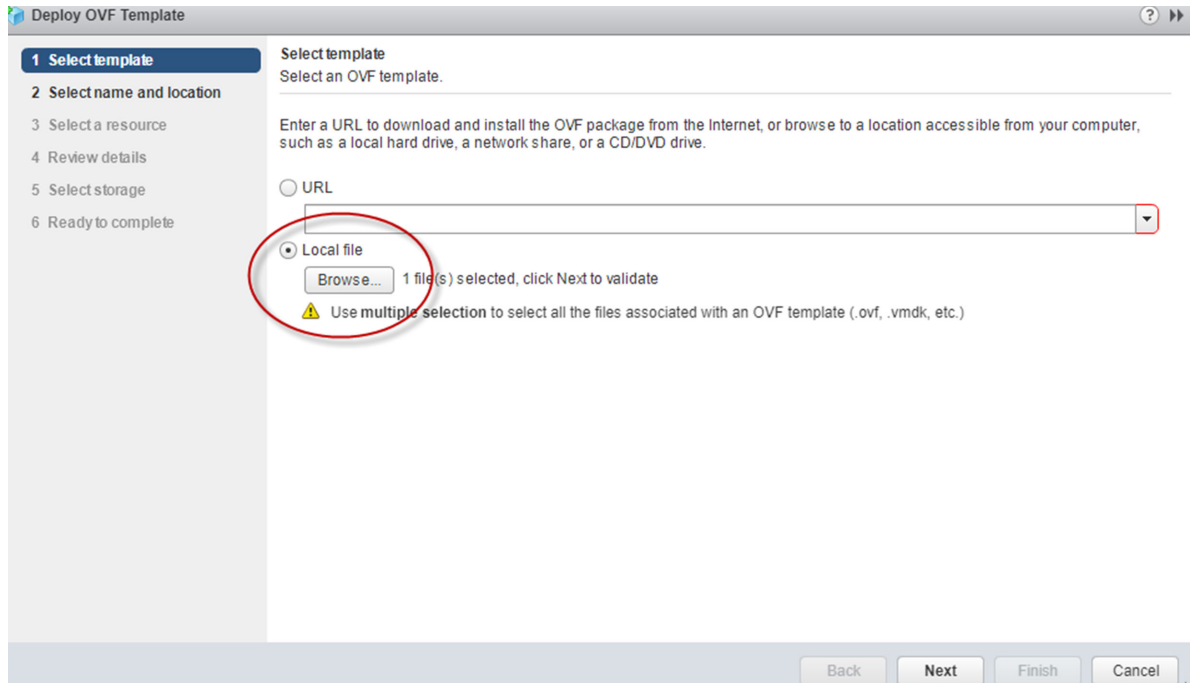
4. Select **Host and Clusters**.



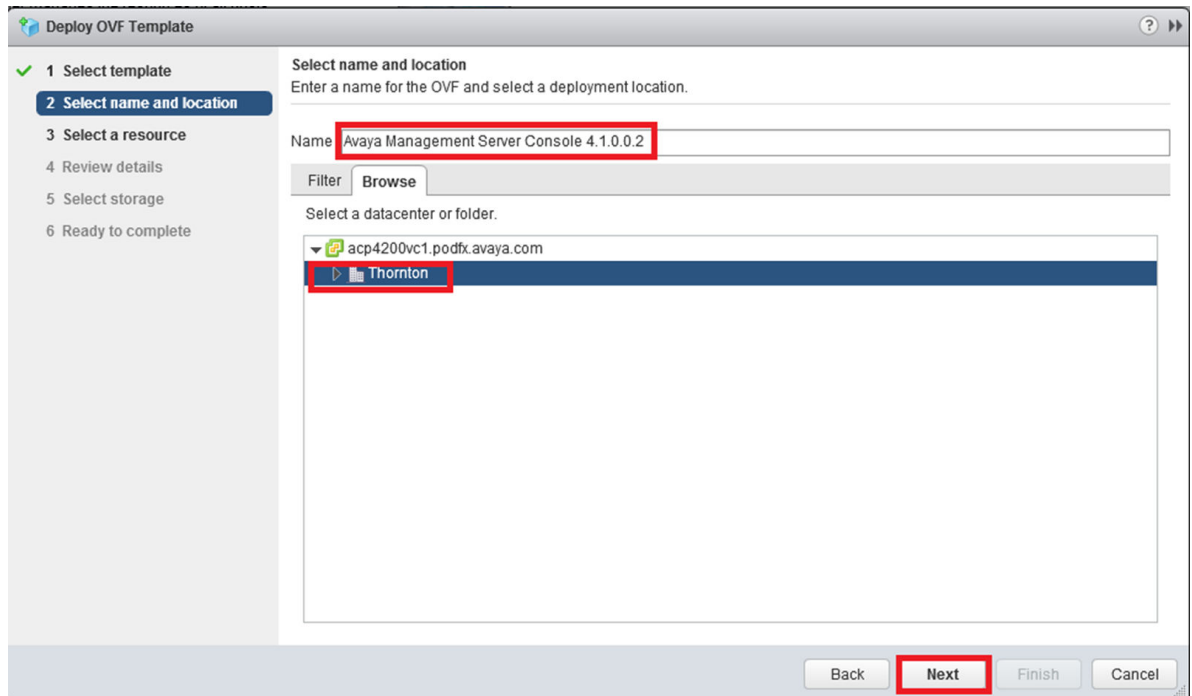
5. Right click the cluster where the application is deployed and select **Deploy OVF Template**.



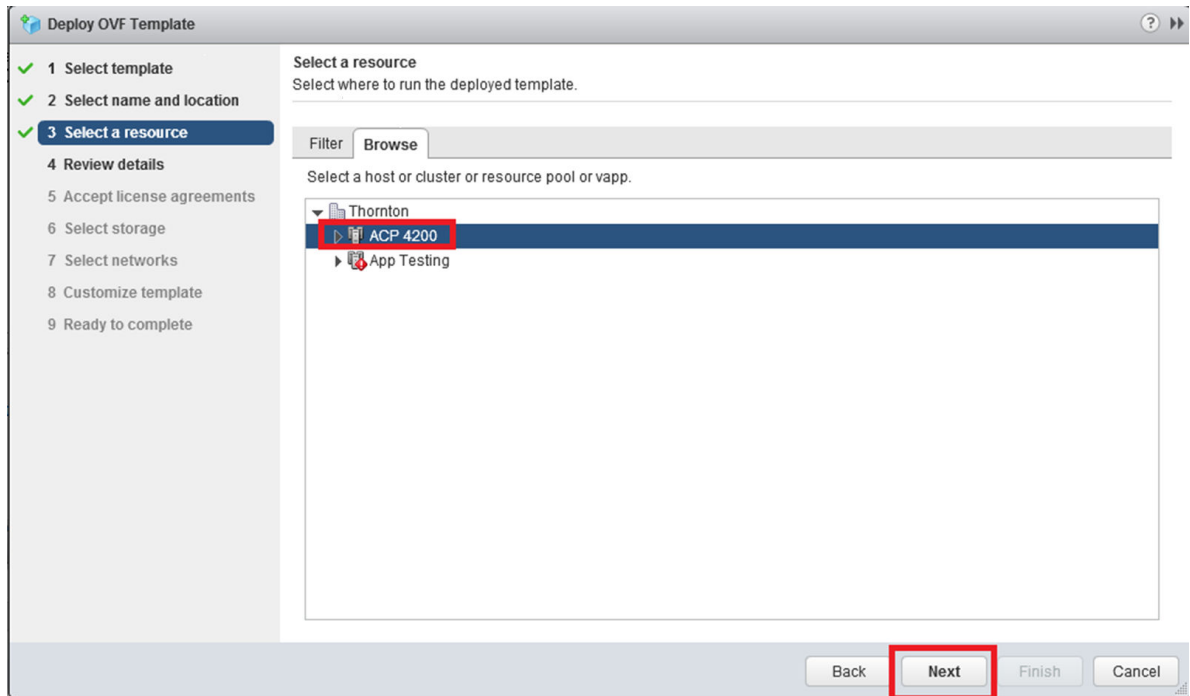
6. Click **Browse** to locate the OVA file downloaded to the E drive earlier, select the file and click **Next**.



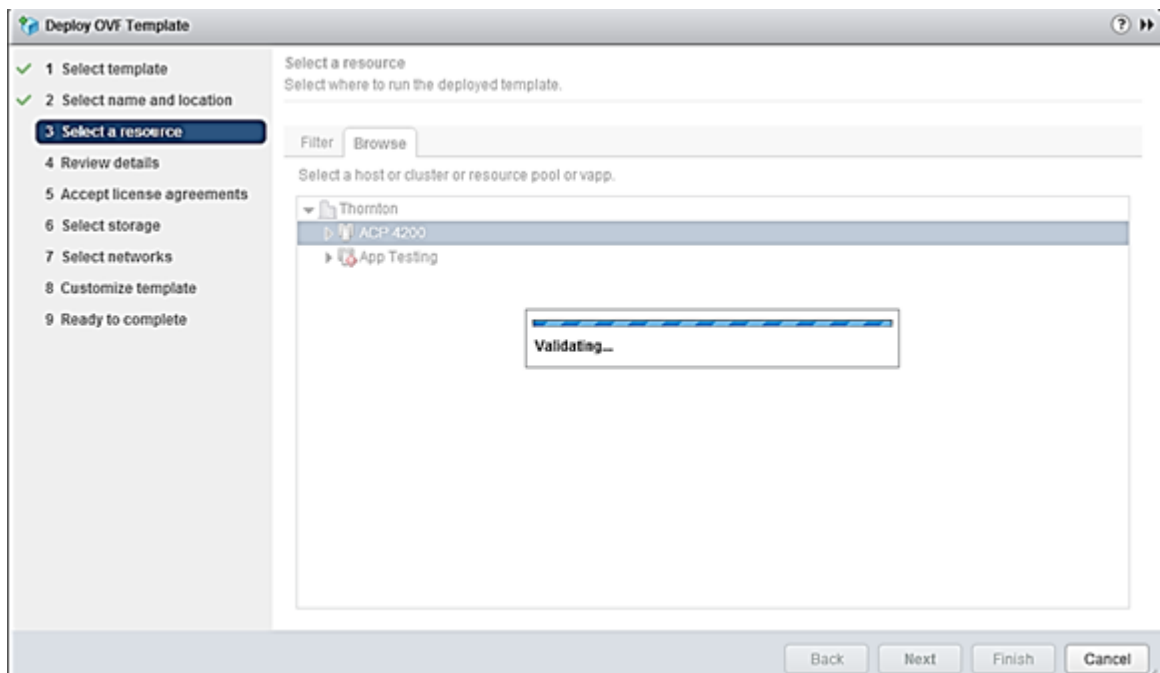
7. Do not change the default names. Click **Next**.



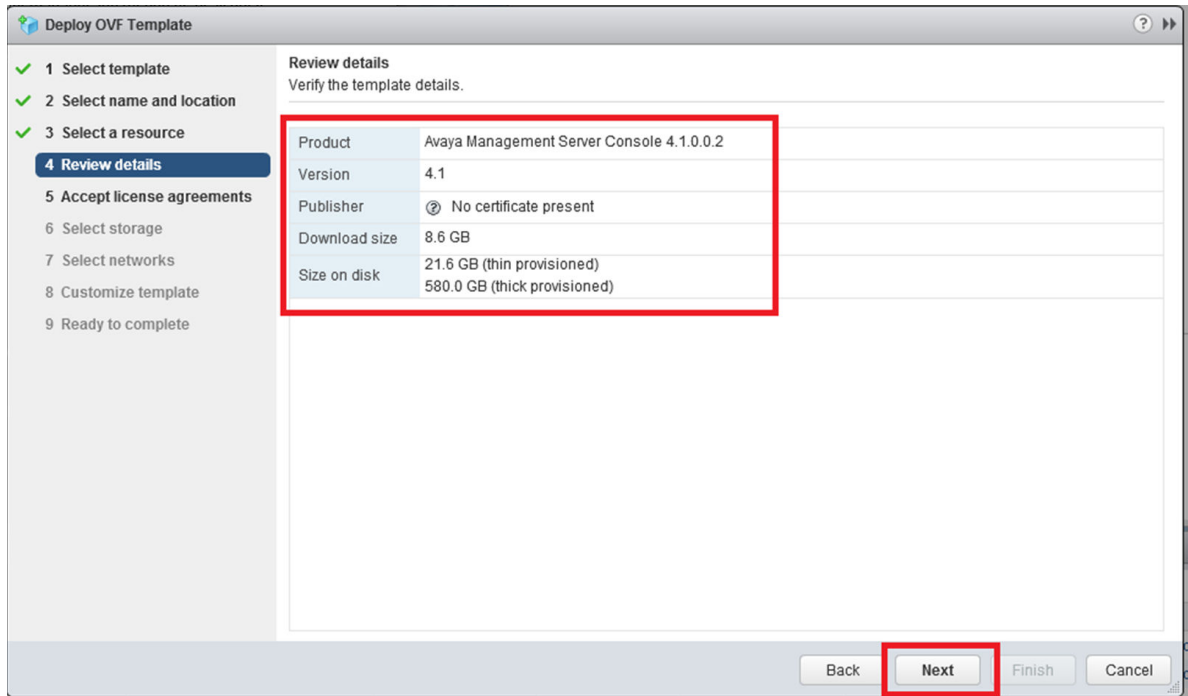
8. Select the existing cluster to allow VMware to select the appropriate host based on the load balancing algorithms. When the task is complete, click **Next**.



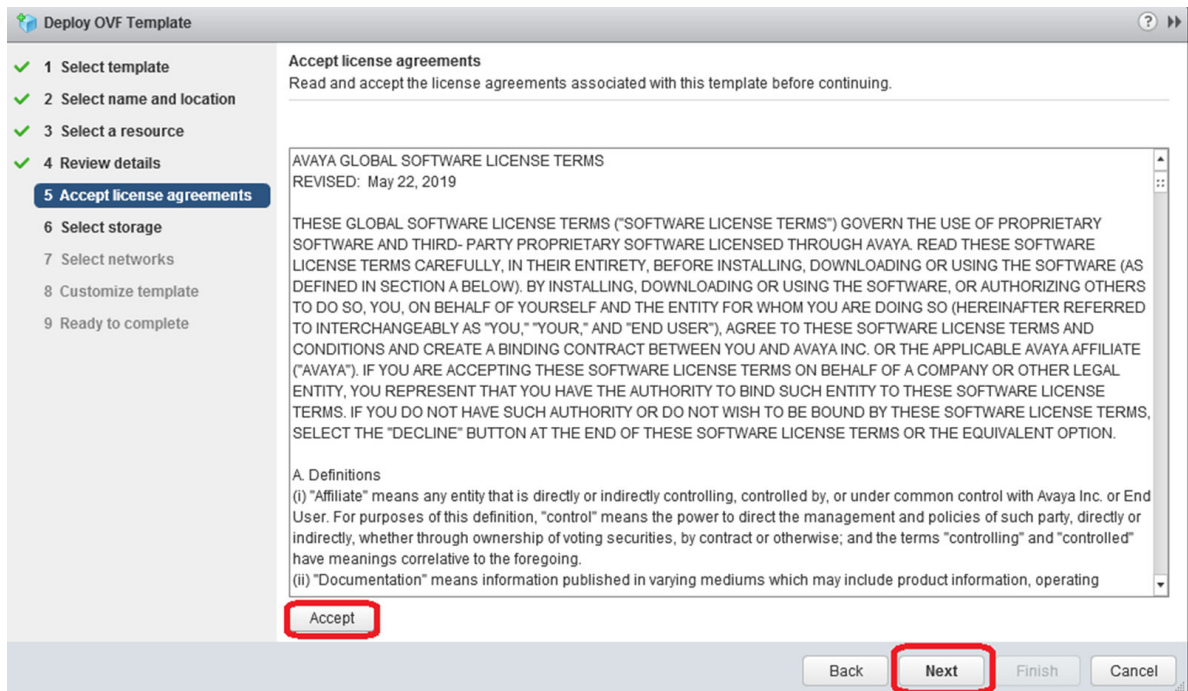
9. VMware spends a few seconds to calculate the capacity available in a specific host selection as well as the location to deploy the OVA if the Cluster level option was previously selected. Do not cancel or press any additional buttons. This process can continue for 20 seconds in large and more populated vCenters.



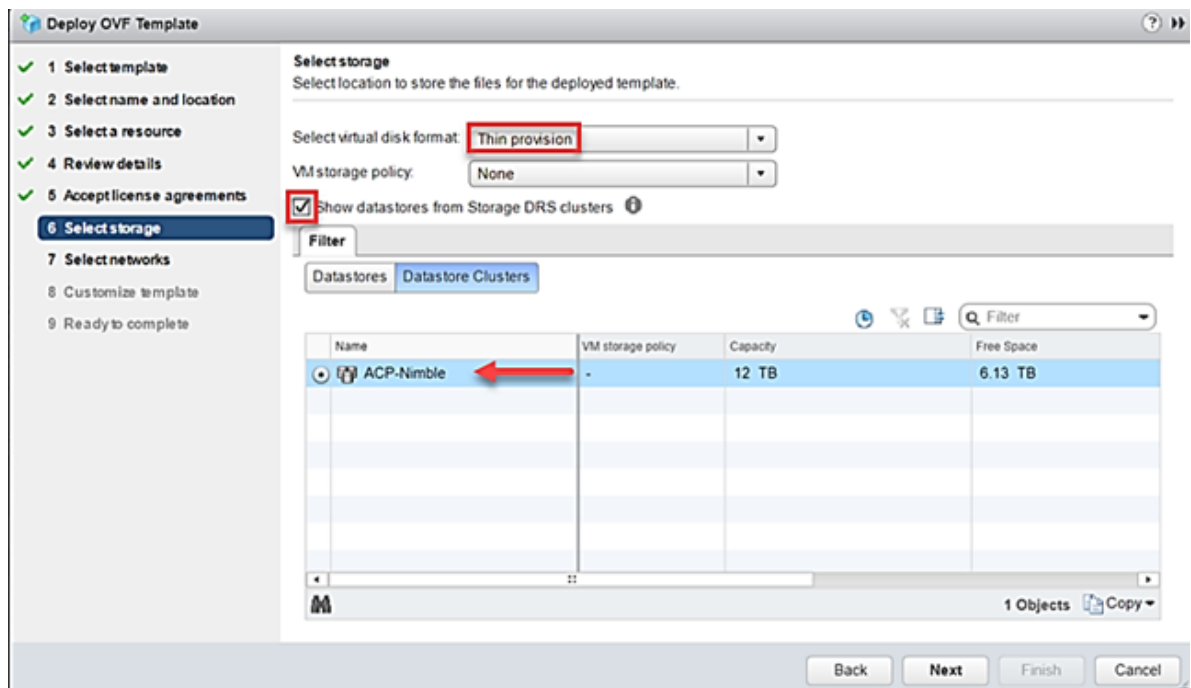
10. Review the details before proceeding. Click **Next**.



11. Check the Avaya End User License Agreement (EULA). Click **Accept** and then **Next**.



12. Select **Thin provision** for virtual disk format. Select **Datastore Clusters** if the cluster has a Data store cluster configured; otherwise select the **Application** (shared) Datastore. Click **Next**.



- **DNS:** Configure the customer’s DNS separated by comma. Obtain the values from LCW.
- **Domain name:** Obtain the value from LCW.

*** Note:**

The domain name set up using OVF deployment does not get applied to the Windows VM during the first bootup. See [Manual steps for changing the domain name in the MSC](#) on page 22 to rectify this issue.

- **Time Zone:** Select the time zone from the drop down list. You can either use the correct value obtained from the updated LCW or adjust the time to match ASP 4200 Rack physical location.
- **NTP:** Enter the customer’s NTP server. Obtain the value from the updated LCW.

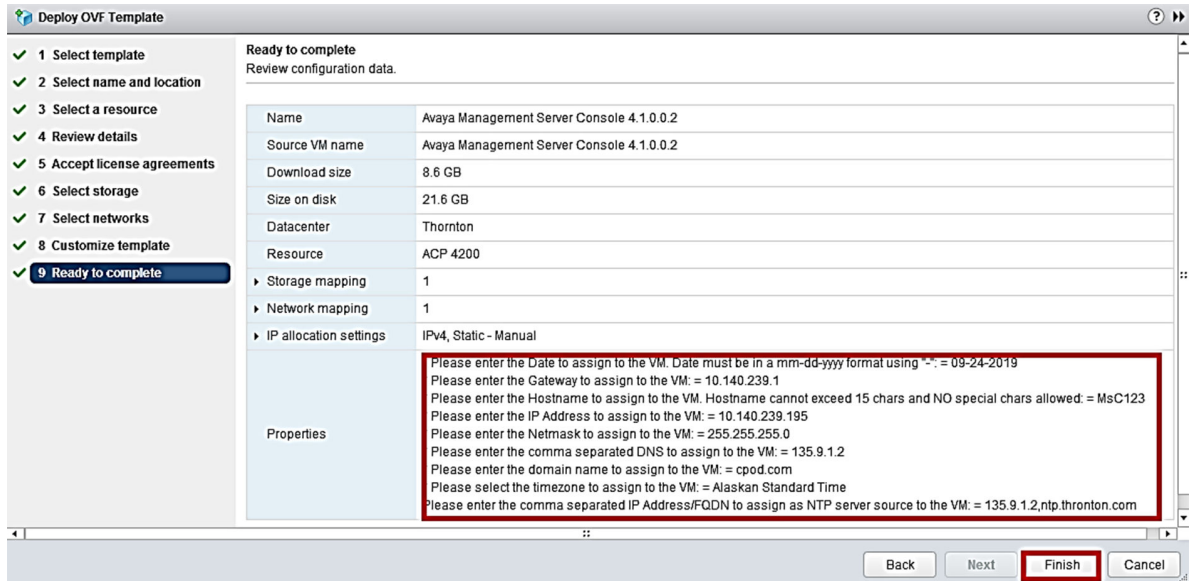
Review the selections to make updates if required. Click **Next**.

The screenshot shows the 'Deploy OVF Template' wizard in the Management Server Console. The 'Customize template' step is active, showing 9 settings for VM configuration. The settings are:

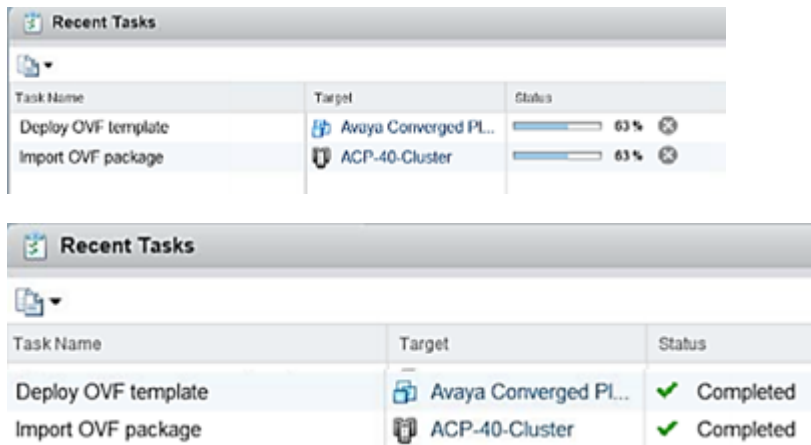
- * Please enter the Date to assign to the VM. Date must be in a mm-dd-yyyy format using "-":
- * Please enter the Gateway to assign to the VM.
- * Please enter the Hostname to assign to the VM. Hostname cannot exceed 15 chars and NO special chars allowed.
- * Please enter the IP Address to assign to the VM:
- * Please enter the Netmask to assign to the VM: 255.255.255.0
- * Please enter the comma separated DNS to assign to the VM:
- * Please enter the domain name to assign to the VM:
- * Please select the timezone to assign to the VM: Afghanistan...
- Please enter the comma separated IP Address/FQDN to assign as NTP server source to the VM:

The 'Next' button is highlighted with a red box.

- Review the administration details. If there are any incorrect entries, click **Back**. Once the entries are confirmed, click **Finish**.



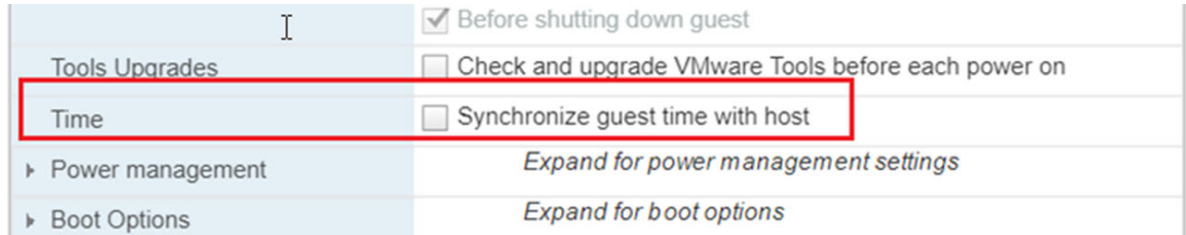
- The OVA import can take several minutes to complete. If the OVA is imported across a WAN connection, the process can take 30 minutes or more, depending on network bandwidth and reliability.



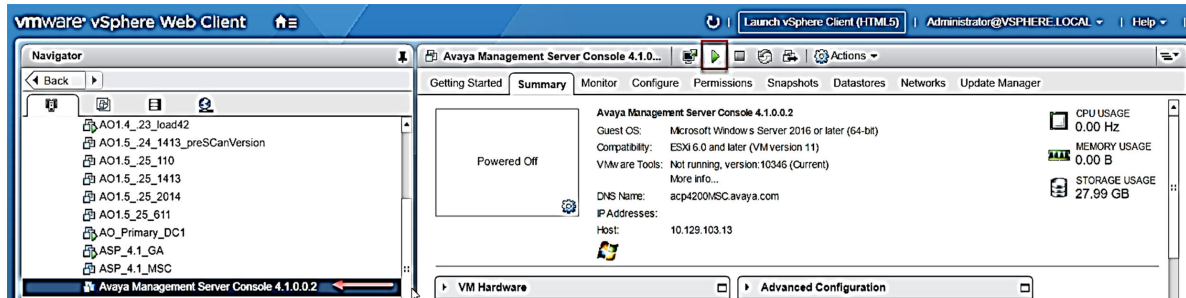
- Once the VM is deployed, go to the vCenter **Hosts and Clusters** view. Select the new MSC VM, right click and select **Edit Settings**.

*** Note:**

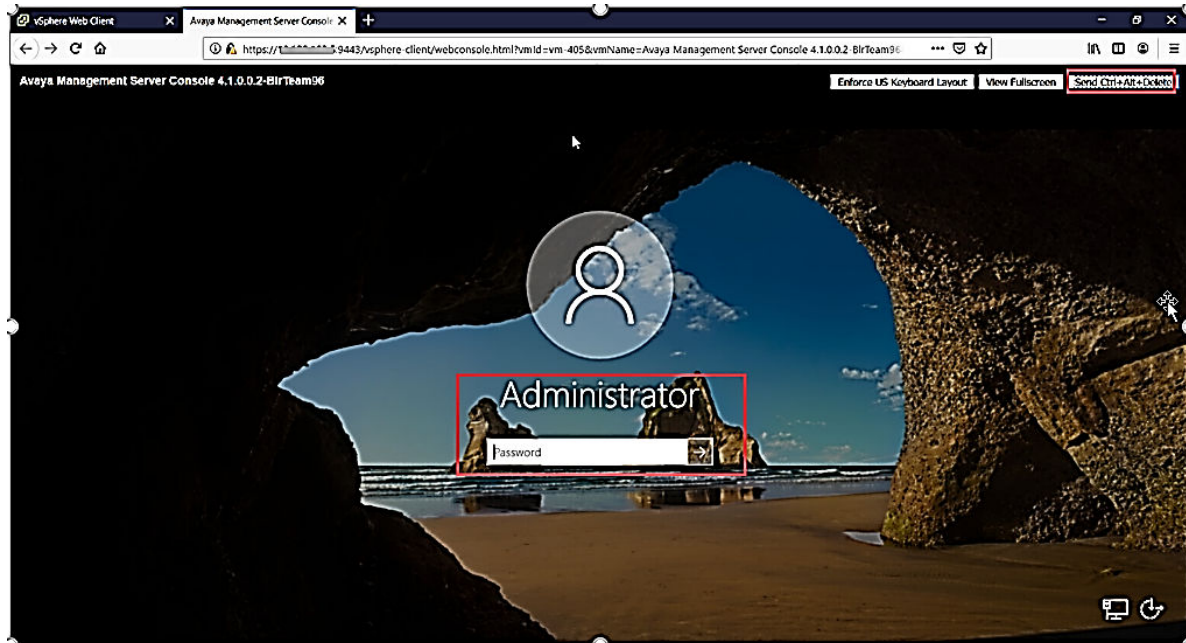
Ensure that the Time field is unchecked.



18. You can now power up the VM. Select the newly deployed MSC VM within the selected cluster and click the green power-on arrow from the tool bar.



19. Once the VM has powered up, select the monitor icon on the tool bar and open the VM console.
20. Log in using the default Administrator credentials.



Connecting to the Management Server Console

You can access MSC through the network. This is a mandatory task after the first boot script is completed and the MSC VM gets rebooted.

*** Note:**

Ensure that the newly deployed MSC VM is up and running before proceeding.

About this task

Use the procedure to remotely connect to the MSC.

Procedure

1. Access the Avaya Solutions Platform 4200 series Release 4.1 management network.
2. Use a remote desktop connection application such as the Microsoft Windows Remote Desktop Connection application to connect to the MSC IP address or host name.
3. Enter the appropriate credentials to connect to the remote instance.

You can also connect to the network through SAL.

*** Note:**

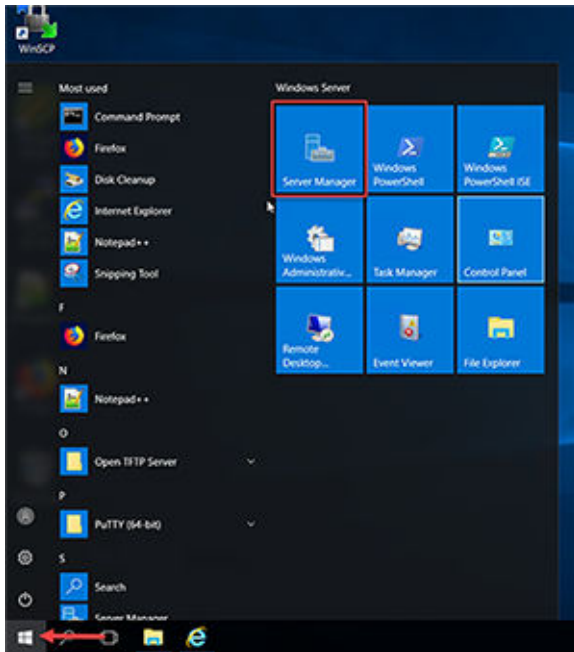
Obtain the credentials from the *Customer Lifecycle Workbook*.

Manual steps for changing the domain name in the MSC

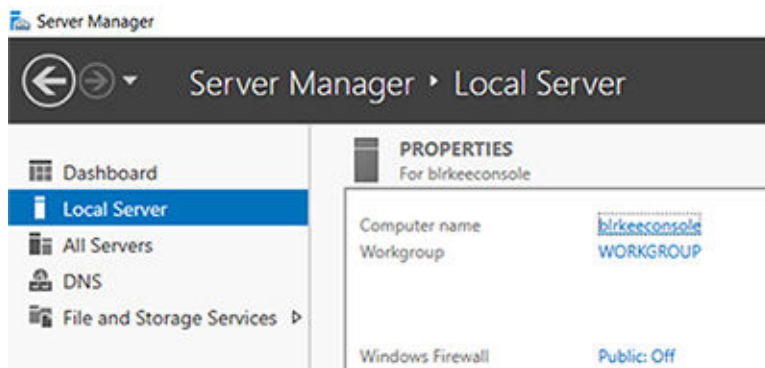
Perform the following procedures to change the domain name in MSC manually.

Validating DNS Suffix and NetBIOS Computer Name Procedure

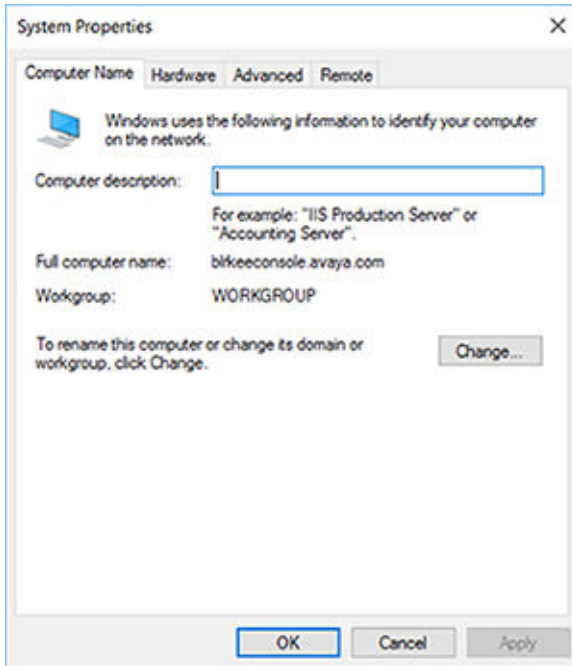
1. Click the windows icon and launch **Server Manager**.



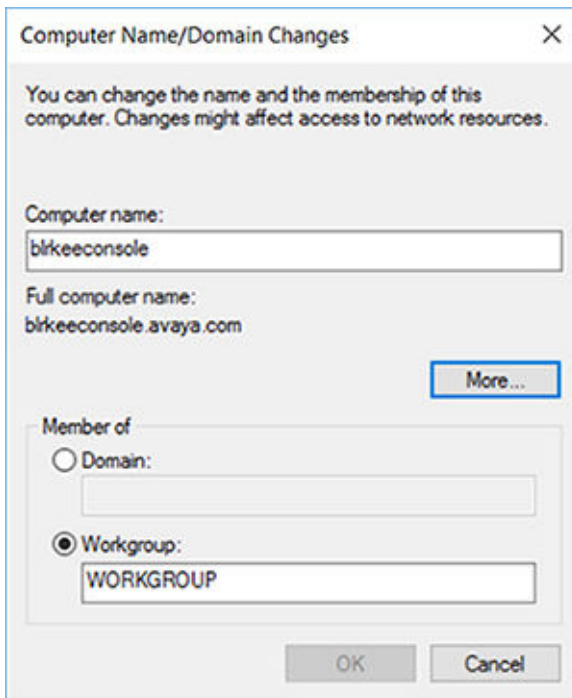
2. Select Local Server and click the computer name.



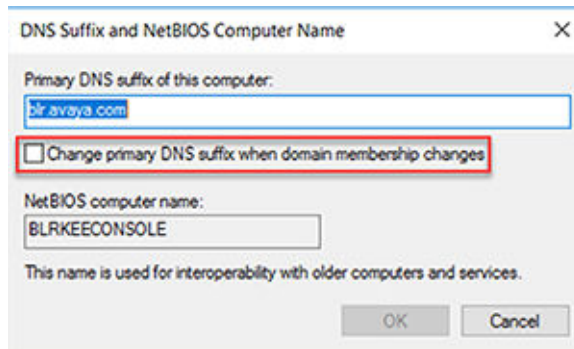
3. In the **System Properties** window that pops-up, select **Change...** button under the **Computer Name** tab.



4. In **Computer Name/Domain Changes** window, click **More....**



- Ensure that the checkbox for **DNS Suffix and NetBIOS Computer Name selection** is unchecked.



Changing the domain name manually

Procedure

- Open a Command Prompt window.
- Replace <DOMAIN NAME> with **actual suffix/domain name** and then execute the following registry changes:

*** Note:**

Avaya recommends to copy the registry entries to a Notepad first to make the domain name changes and then copy the updated entries into the command prompt windows.

```
REG add "HKLM\SOFTWARE\Policies\Microsoft\System\DNSClient" /v "NV PrimaryDnsSuffix" /t REG_SZ /d "<DOMAIN NAME>" /f
```

```
REG add "HKLM\SOFTWARE\Policies\Microsoft\System\DNSClient" /v "PrimaryDnsSuffix" /t REG_SZ /d "<DOMAIN NAME>" /f
```

```
REG add "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" /v "NV Domain " /t REG_SZ /d "<DOMAIN NAME>" /f
```

```
REG add "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" /v "Domain " /t REG_SZ /d "<DOMAIN NAME>" /f
```

The following image shows an example of modifying the windows domain name to "avaya.com":

```
Select Administrator: Command Prompt
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>REG add "HKLM\SOFTWARE\Policies\Microsoft\System\DNSClient" /v "NV PrimaryDnsSuffix" /t REG_SZ /d "avaya.com" /f
The operation completed successfully.

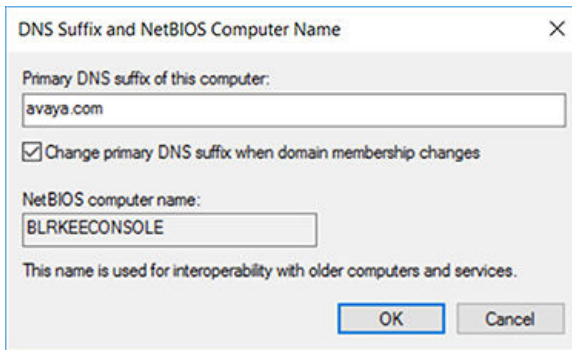
C:\Users\Administrator>REG add "HKLM\SOFTWARE\Policies\Microsoft\System\DNSClient" /v "PrimaryDnsSuffix" /t REG_SZ /d "avaya.com" /f
The operation completed successfully.

C:\Users\Administrator>REG add "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" /v "NV Domain " /t REG_SZ /d "avaya.com" /f
The operation completed successfully.

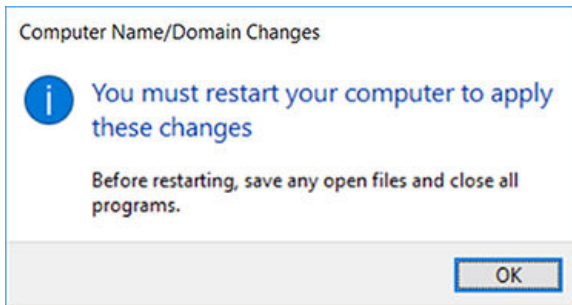
C:\Users\Administrator>REG add "HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters" /v "Domain " /t REG_SZ /d "avaya.com" /f
The operation completed successfully.

C:\Users\Administrator>
```

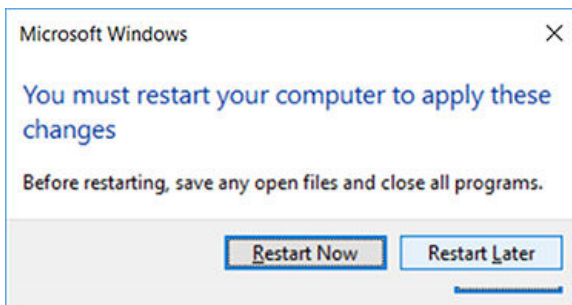
3. Click the Windows icon and launch **Server Manager**.
4. Select Local Server and click the computer name.
5. In the **System Properties** window that pops-up, select **Change...** button under the **Computer Name** tab.
6. Click **More...** .
7. Select the check box for **Change primary DNS suffix when domain membership changes**.



8. Click **OK**.
9. In the **Computer Name/Domain Changes** window, click **OK**.



10. Close **System Properties**.
11. In **Microsoft Windows**, click **Restart Now** for the domain changes to take place.



Deleting Residual FQDN after changing DNS Suffix

About this task

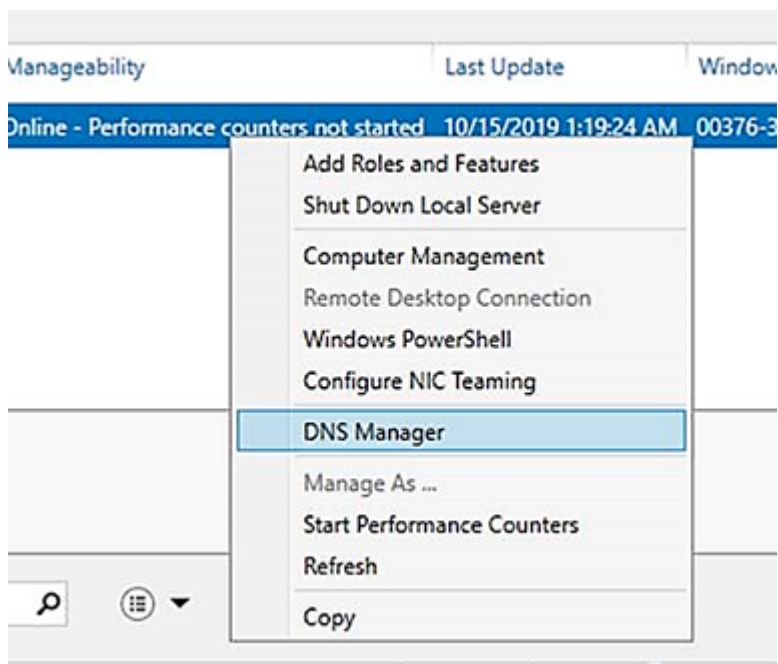
Use the following procedure to delete reference to default DNS suffix created when deploying the Management Server Console for the ASP 4200 4.1 baseline.

Before you begin

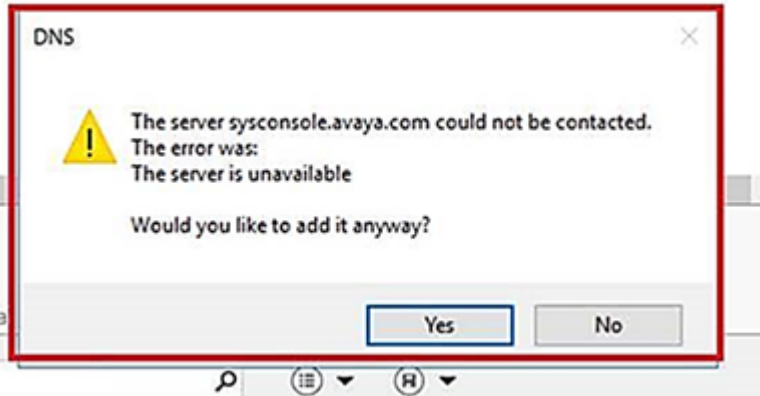
Perform [Manual steps for changing the domain name in the MSC](#) on page 22 prior to deleting residual FQDN.

Procedure

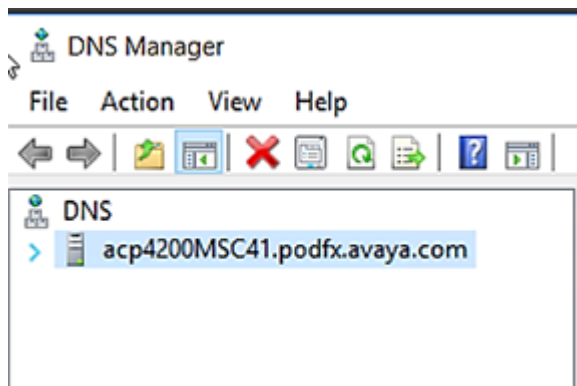
1. Use a Remote Desktop Connection (RDP) to access the existing Management Server Console and login using the Administrator credentials.
2. Click the windows icon and launch Server Manager.
3. Select **DNS**.
4. Right click and open **DNS Manager**.



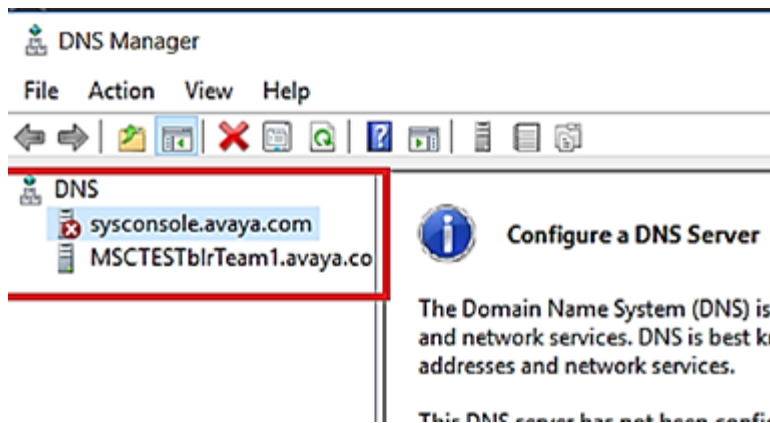
5. A pop-up window appears with an error message to notify that DNS server **sysconsole.avaya.com** configured is unavailable. Select **No**.



6. The pop-up window closes and DNS Manager opens up showing a single entry with updated FQDN.



7. Close DNS Manager window and disconnect from MSC.
8. If **Yes** is selected in the pop-up window by error, then residual FQDN gets added and you will have to manually delete it. When DNS Manager window appears, proceed as described in the steps below:
 - a. Select **sysconsole.avaya.com**
 - b. Delete residual FQDN. You can either click the red button, or right-click the residual FQDN **sysconsole.avaya.com** and select **Delete**.



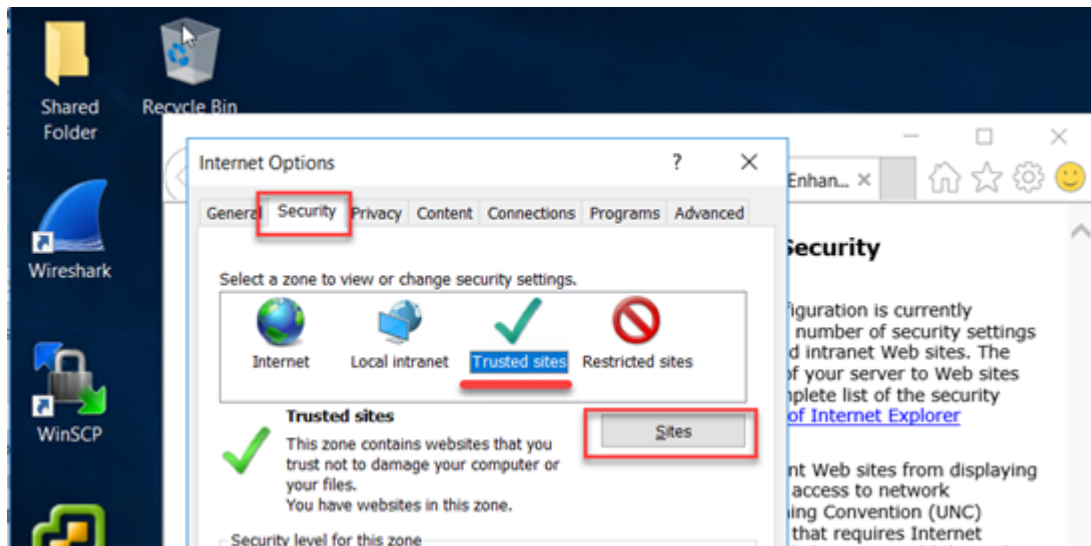
Configuring Trusted Site on Internet Explorer

Procedure

1. Connect to the newly deployed Management Server Console using Remote Desktop (RDP). Login using Administrator credentials.
2. Launch Internet Explorer and Navigate to **Settings** > **Internet Options**.



3. In the **Internet Options** pop-up window, select **Security** > **Trusted Sites** > **Sites**.



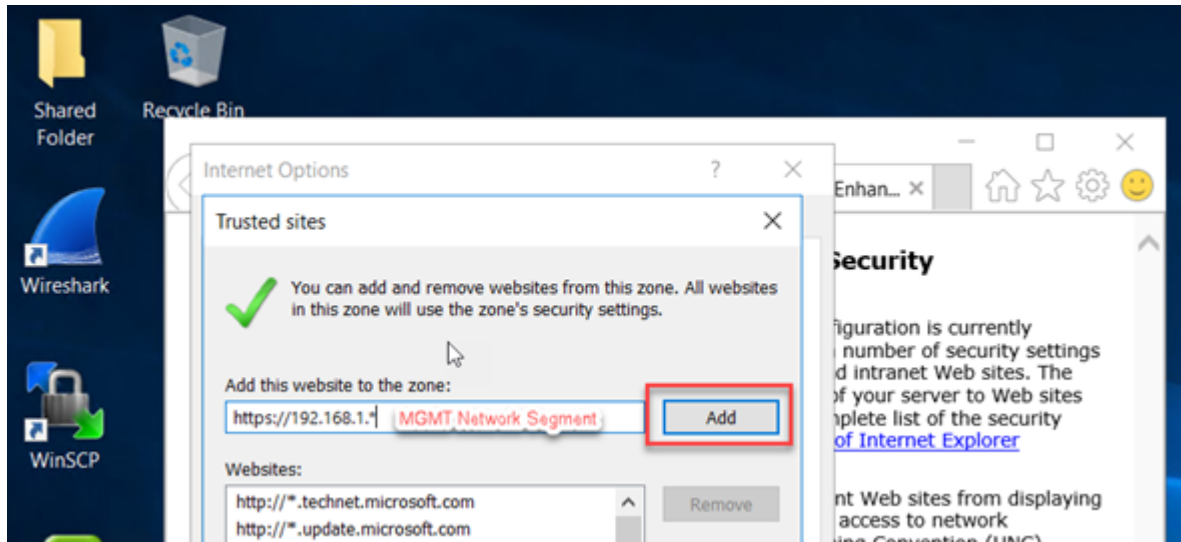
4. Add the following websites to the trusted sites:

*** Note:**

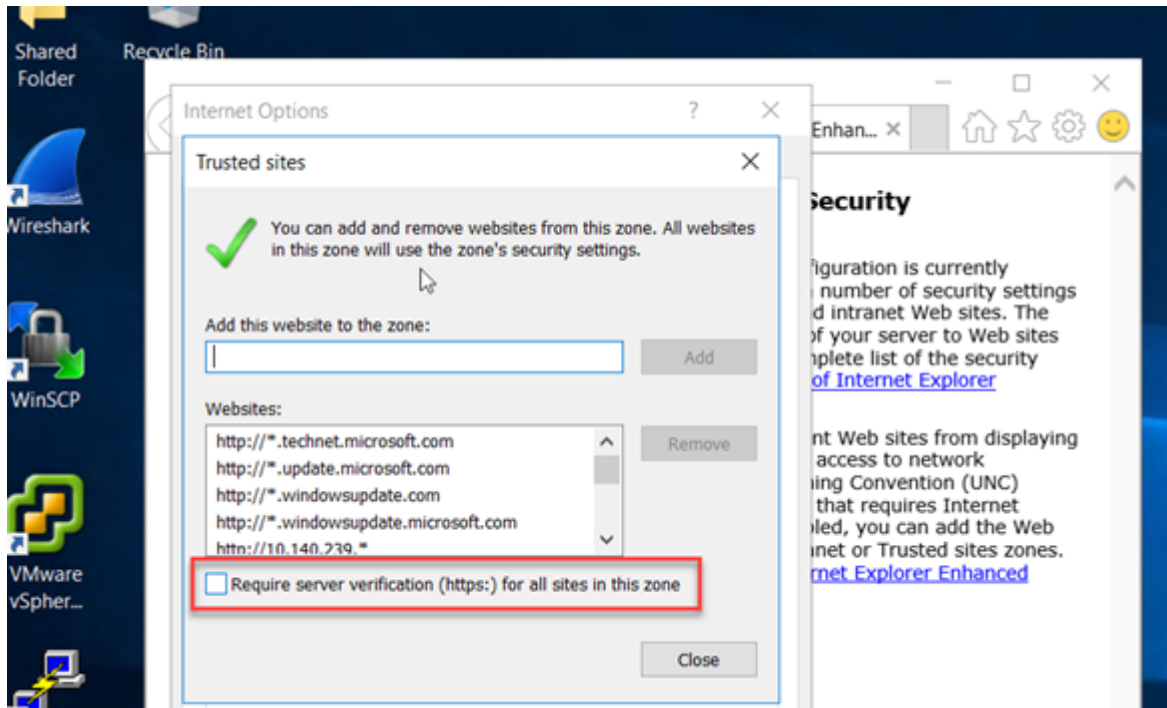
Use a wildcard URL to prevent the addition of multiple entries to each component within the rack. Based on the first 3 octets of each Network Identity, the URLs are differentiated from each other and the applicable networks are added to the trusted zone. The last octet is represented with a wildcard value.

This is applicable if you are using IE to connect to the VCSA Web Client and iLO GUI.

- **Management** network segment: Example *https://192.168.1.**
- **Application 1** network segment: Example *https://192.168.2.**



5. Uncheck **Require server verification (https:)** for all sites in this zone to prevent from adding only https addresses.



6. Add the **Application 1** network segment using *http*, Example *http://192.168.2.**

*** Note:**

This is required when connecting to the server's remote console using the iLO integrated remote console feature and IE.

7. Close windows and exit the browser when the procedure is complete.

Configuring and licensing the Management Server Console

Avaya professionals must complete the initial customer configuration, security, and licensing for the MSC.

About this task

Perform the following high level tasks for the MSC initial customer configuration and licensing requirements.

Procedure

1. **(Optional)** Configure the browser proxies.
2. Configure the browser security.

3. Install and activate the Windows Server license by selecting **Start > Control Panel > System and Security > System > Windows Activation > Change product key** in Windows.

 **Note:**

The license sticker is on the top right chassis lid of Compute Server 1 for new Release 4.1 builds.

A request must be sent to aspsales@avaya.com when upgrading to Release 4.1 software. The request must ask for the Avaya Solutions Platform 4200 series Release 4.1 MSC Upgrade Media Kit, Material Code 700513602. This kit contains the media and licenses necessary for upgrading the MSC to Windows Server 2016.

4. Install and activate any customer-supplied anti-virus software.
5. Download and install Microsoft Windows updates.

Windows Firewall (Optional)

The Windows Firewall of the Windows Management Server Console is disabled by default. Windows Firewall can be enabled or disabled as required by the individual security requirements of the networking environment. If you are using Internet Explorer, cookies are not enabled by default. You will get prompts to allow or block cookies.

Configuring Windows 2016 MSC As NTP Client (Optional)

About this task

When you are using *w32time* as NTP client, the performance is dependent on the *w32time* software version. You can achieve better accuracy with *w32time* if you are using the version that is shipped with **Windows Server 2016**.

If a Windows machine gets the time from an NTP server on the network, it becomes a client of that server and starts to send NTP `client` request packets. The server sends NTP `server` response packets in return.

w32time service can be configured automatically. *w32time* queries the time from a domain controller in an Active Directory domain if the machine is a member of an AD domain, or from one of Microsoft's public NTP servers if the machine is a standalone machine or an AD domain controller. Microsoft's public NTP servers can be accessed by *time.microsoft.com*.

The *w32tm* command can be run in a console (cmd) window with administrator permissions to configure and monitor the *w32time* service.

MSC uses the *w32time* service for configuring MSC as NTP client. By default, MSC deployment takes NTP server source and configures NTP client on MSC. The following procedure allows you to verify or manually configure NTP client.

Procedure

1. Perform the following procedure to verify the status of NTP client. The procedure confirms if the NTP client is not active or not configured.

The following command checks if the NTP server FQDN/IPAddress is available as part of the configuration details:

```
C:\Users\Administrator>w32tm /query /configuration
```

```
[Configuration]
```

```
EventLogFlags: 2 (Local)
```

```
AnnounceFlags: 5 (Local)
```

```
TimeJumpAuditOffset: 28800 (Local)
```

```
MinPollInterval: 6 (Local)
```

```
MaxPollInterval: 10 (Local)
```

```
MaxNegPhaseCorrection: 54000 (Local)
```

```
MaxPosPhaseCorrection: 54000 (Local)
```

```
MaxAllowedPhaseOffset: 1 (Local)
```

```
FrequencyCorrectRate: 4 (Local)
```

```
PollAdjustFactor: 5 (Local)
```

```
LargePhaseOffset: 50000000 (Local)
```

```
SpikeWatchPeriod: 900 (Local)
```

```
LocalClockDispersion: 10 (Local)
```

```
HoldPeriod: 5 (Local)
```

```
PhaseCorrectRate: 1 (Local)
```

```
UpdateInterval: 100 (Local)
```

```
[TimeProviders]
```

```
NtpClient (Local)
```

```
DllName: C:\Windows\SYSTEM32\w32time.DLL (Local)
```

```
Enabled: 1 (Local)
```

```
InputProvider: 1 (Local)
```

```
AllowNonstandardModeCombinations: 1 (Local)
```

```
ResolvePeerBackoffMinutes: 15 (Local)
```

ResolvePeerBackoffMaxTimes: 7 (Local)

CompatibilityFlags: 2147483648 (Local)

EventLogFlags: 1 (Local)

LargeSampleSkew: 3 (Local)

SpecialPollInterval: 86400 (Local)

Type: NTP (Local)

NtpServer: time.windows.com (Local)

VMICTimeProvider (Local)

DllName: C:\Windows\System32\vmictimeprovider.dll (Local)

Enabled: 1 (Local)

InputProvider: 1 (Local)

NtpServer (Local)

DllName: C:\Windows\SYSTEM32\w32time.DLL (Local)

Enabled: 0 (Local)

InputProvider: 0 (Local)

2. If NTP server details are missing, execute the following commands in a command-prompt to reconfigure the NTP server time source. Replace the **NTP server FQDN/IPAddress**.

 **Note:**

When configuring NTP, you can set up multiple external time sources. Enter FQDNs/IP Addressees separated with a comma.

- w32tm.exe /config /manualpeerlist:<NTP SERVER FQDN/IPADDRESS> /syncfromflags:manual /reliable:YES /update
- net stop w32time && net start w32time
- w32tm /resync /force

3. Execute the following command to verify if the provided NTP server is reachable from MSC.

```
C:\Users\Administrator>w32tm /query /peers
```

```
#Peers: 1
```

```
Peer: time.windows.com
```

```
State: Active
```

```
Time Remaining: 31.8019537s
```

```
Mode: 3 (Client)
```

Stratum: 0 (unspecified)

PeerPoll Interval: 0 (unspecified)

HostPoll Interval: 6 (64s)

- Execute the following command to know if NTP is configured. Source is displayed as Local CMOS CLOCK if NTP is not configured.

```
C:\Users\Administrator>w32tm /query /status
```

Leap Indicator: 0(no warning)

Stratum: 1 (primary reference - syncd by radio clock)

Precision: -6 (15.625ms per tick)

Root Delay: 0.0000000s

Root Dispersion: 10.0000000s

ReferenceId: 0x4C4F434C (source name: "LOCL")

Last Successful Sync Time: 9/9/2019 3:10:27 AM

Source: Local CMOS Clock

Poll Interval: 6 (64s)

- Execute the following command to check if the time syncs between the source and the NTP source provided.

```
C:\Users\Administrator>w32tm /query /status
```

Leap Indicator: 0(no warning)

Stratum: 4 (secondary reference - syncd by (S)NTP)

Precision: -6 (15.625ms per tick)

Root Delay: 0.0303835s

Root Dispersion: 7.7686979s

ReferenceId: 0x87090102 (source IP: 135.9.1.2)

Last Successful Sync Time: 9/19/2019 6:15:07 PM

Source: 135.9.1.2

Poll Interval: 10 (1024s)

Result

Confirming the source validates that the NTP client configuration on MSC has been successful.

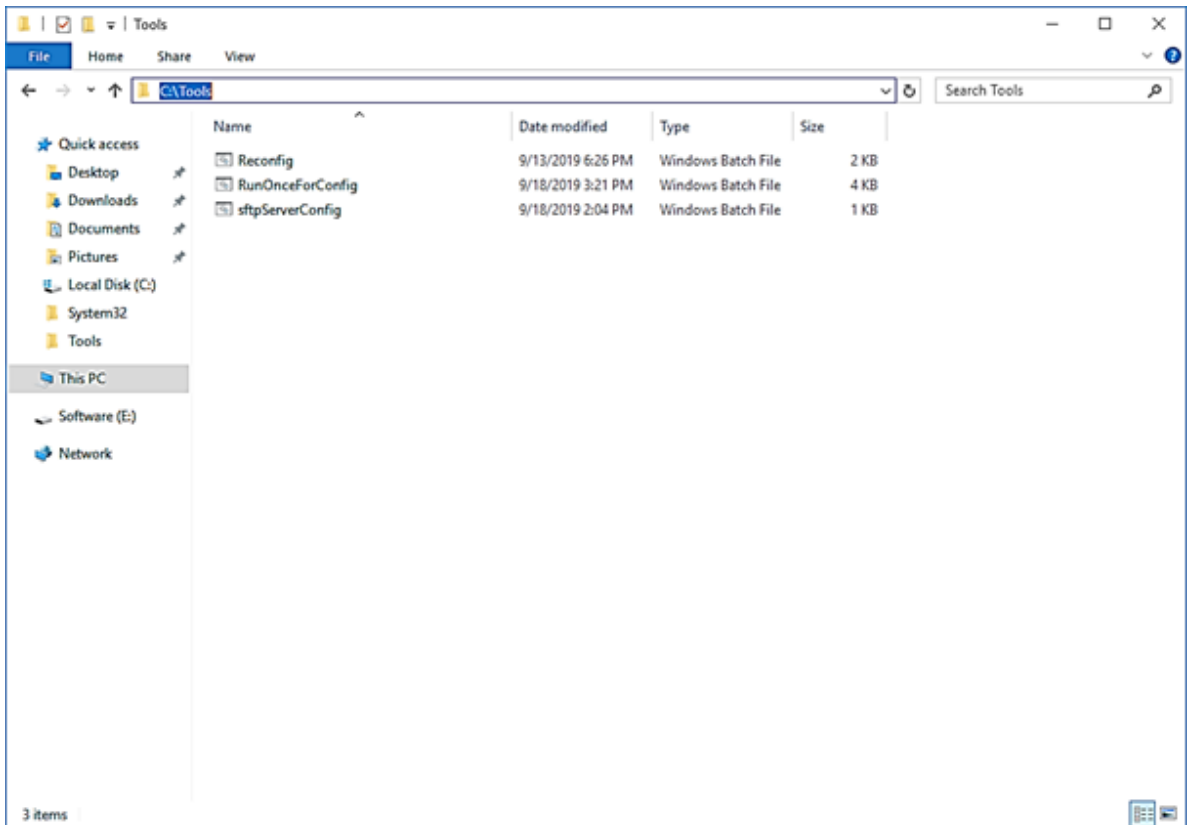
Using Windows 2016 MSC as SFTP Server (Optional)

About this task

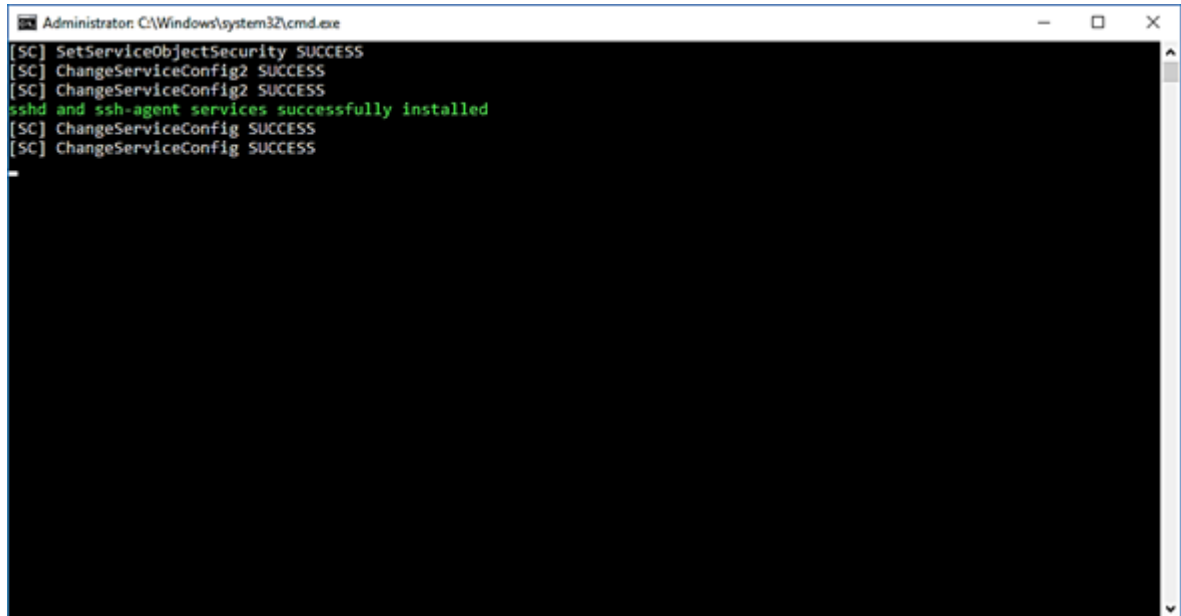
MSC can be used as sftp server on demand. Perform the following procedure to configure MSC as SFTP server.

Procedure

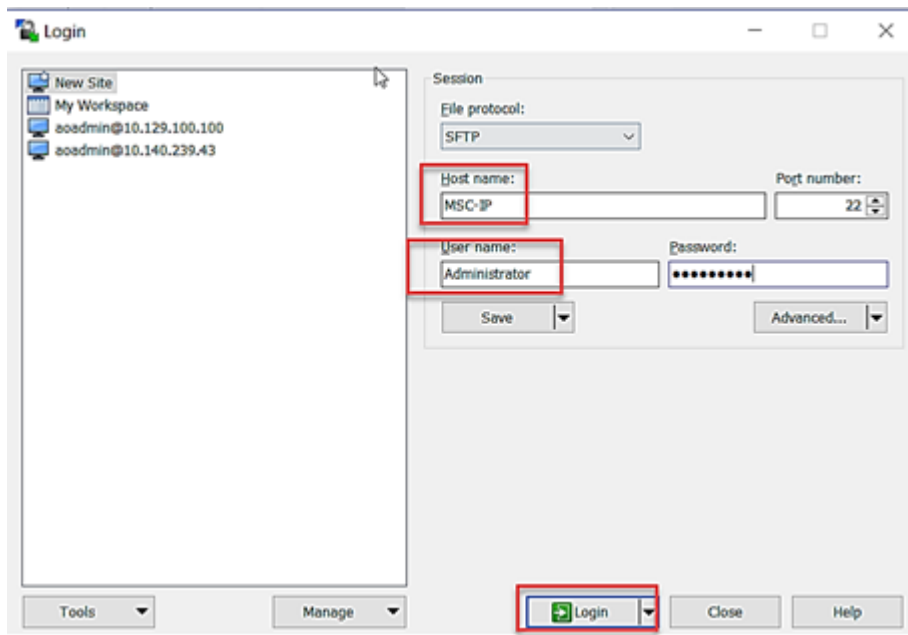
1. Connect to the Management Server Console using Remote Desktop (RDP) and log in using the Administrator credentials.
2. In the File Explorer, navigate to C:\Tools Folder.



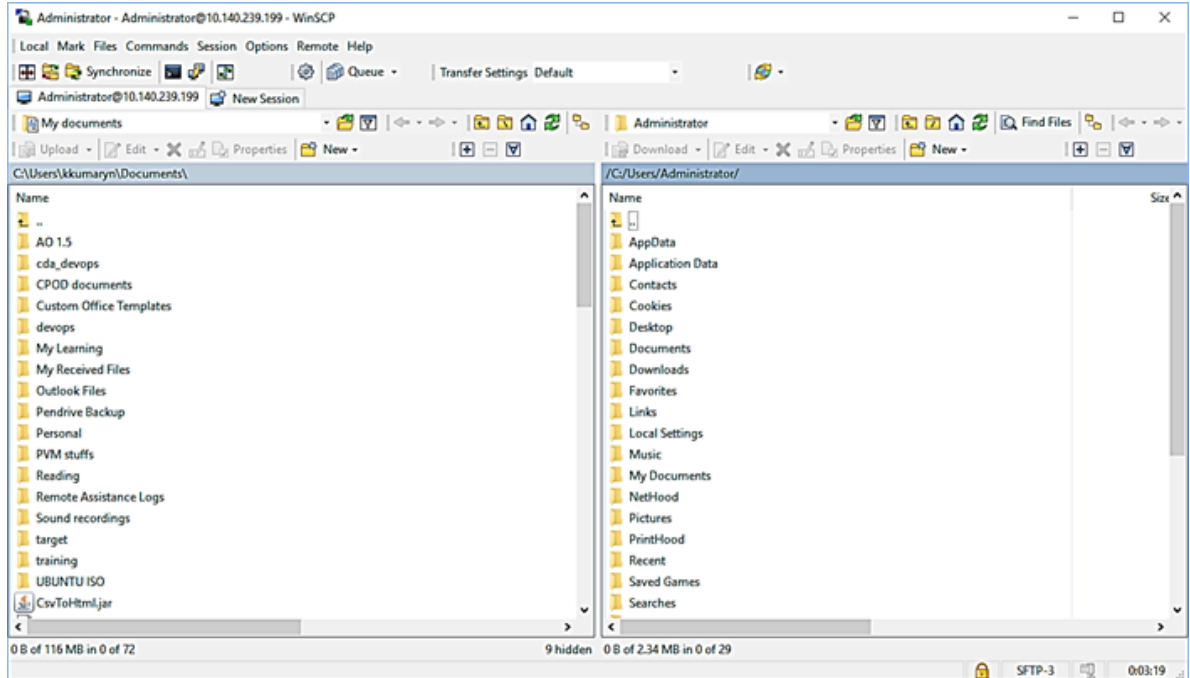
- Execute *sftpServerConfig.bat* file either from the command prompt or by double clicking the file.



- From a client pc, log into SFTP server using WinSCP client with the current MSC credentials.



MSC software and configuration



You can now use MSC as the SFTP server.

Chapter 4: Upgrades

Upgrading Avaya Solutions Platform 4200 series

This chapter provides the tasks involved in upgrading and patching software.

Upgrades must be performed by Avaya Professional Services, or an Avaya certified Solution Integrator (SI). The SI must plan and prepare to perform the upgrades, such as downloading and transferring all the upgrade files required, before starting any component upgrades.

- Avaya Management Server Console (MSC)
- Avaya Aura[®] System Manager and remaining Avaya Aura[®] Applications

*** Note:**

You can upgrade Avaya Aura[®] Applications before upgrading or after upgrading the Avaya Solutions Platform 4200 series Release 4.1 infrastructure.

- VMware vCenter and ESXi software
- Upgrade existing Avaya Orchestrator virtual machine

*** Note:**

Customers with existing POS Applications (Pod Fx 3.1 and older) must deploy a new Avaya Orchestrator instance.

- Avaya Aura[®] Virtualized Environment software (Session Manager and Communication Manager)
- Extreme Networks switches and firmware
- EMC storage array software and firmware
- HPE Nimble storage array software and firmware
- HP compute servers BIOS and firmware
- ServerTech power distribution unit (PDU) firmware

*** Note:**

Optional or additional component application upgrades for specific solution configurations are not included in the upgrade procedures. The SI must refer to the individual product upgrade instructions, and upgrade the components and applications to the versions officially supported in this release.

*** Note:**

Starting with the Avaya Converged Platform Release 4.0 and later, Avaya Orchestrator operates independently. There are no software version dependencies with System Manager.

*** Note:**

When deploying OVAs using vSphere 6.5 webclient on Internet Explorer (IE), deployment fails with multiple error messages. Therefore, deploy OVAs using Mozilla Firefox that is installed on the Management Server Console.

Supported upgrade paths

You can upgrade previous Avaya Collaboration Pod, Avaya Pod Fx releases, and Avaya Converged Platform Release 4.0 to Avaya Solutions Platform 4200 series Release 4.1. Starting with Avaya Converged Platform Release 4.0 and later, existing supported POS applications (VPFM, PVM) will be replaced by the new network management system tool, Avaya Orchestrator. There is no migration path for POS application data. This means any data backed up prior to disabling POS applications cannot be restored or imported to Avaya Orchestrator.

Avaya Solutions Platform 4200 series Release 4.1 upgrades must be performed by Avaya Professional Services or by Avaya Solutions Platform 4200 series Certified Business Partner. They must plan and prepare to perform the upgrades, such as downloading and transferring all the upgrade files required before starting any component upgrades.

The following table provides information related to the supported upgrades of all previous Avaya Collaboration Pod, Avaya Pod Fx, and Avaya Solutions Platform 4200 series Release 4.0 to Avaya Solutions Platform 4200 series Release 4.1:

*** Note:**

Infrastructure components not specifically listed in this table can be upgraded to its corresponding firmware or software version supported under the Avaya Solutions Platform 4200 series 4.1 baseline. Review the Interoperability Matrix document for the complete software list on <https://downloads.avaya.com/css/P8/documents/101055017>.

*** Note:**

This table is not a replacement nor should be used as an upgrade procedure or as an upgrade work flow.

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
<p>4200 CPOD 1.0 /2.0 / 2.0.1 / Hardware</p>	<p>Not supported.</p> <p>Software limitation:</p> <ul style="list-style-type: none"> • Upgrade from VMware 5.1.X to 6.5 u3 is not supported by vendor. This includes vCenter Server Appliance and ESXi. • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • <u>Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X.</u> Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Hardware limitation: Lenovo servers are end of life and end of support. ESXi 6.5 is not supported by vendor on Lenovo servers.</p> <p>Extreme Switches:</p> <p>VSP 4850: Vendor does not support direct upgrades from VOSS 3.1 to VOSS 7.1.4. Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x. (VOSS 8.0.6 is not supported)</p>	<p>Not supported.</p> <p>Last fully supported release: Pod Fx 3.1.</p>

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
2400 CPOD 2.1	<p>Supported.</p> <p>VMware: Vendor supports direct upgrade from release 5.5.x to 6.5 u3. This includes vCenter Server Appliance and ESXi.</p> <p>Extreme switches:</p> <p>VSP 4850: Vendor does not support direct upgrade from VOSS 4.1 to VOSS 7.1.4. Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x. (VOSS 8.0.6 is not supported)</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported within VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p>	Partially supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
4200 / 2400 CPOD 2.1.1 Hardware	<p>Supported.</p> <p>VMware: Vendor supports direct upgrade from release 5.5.x to 6.5 u3. This includes vCenter Server Appliance and ESXi.</p> <p>Extreme switches: .</p> <p>VSP 4850: Vendor does not support direct upgrade from VOSS 4.2.1 to VOSS 8.0.6. Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x. (VOSS 8.0.6 is not supported)</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Partially supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
4200 / 2400 Pod Fx 3.0 Hardware	<p>Supported.</p> <p>VMware: : Vendor supports direct upgrade from release 5.5.x to 6.5 u3. This includes vCenter Server Appliance and ESXi.</p> <p>Extreme switches:</p> <p>VSP 7200: Vendor does not support direct upgrade from VOSS 5.0.1 to VOSS 8.0.6. Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x.</p> <p>VSP 4850: Vendor does not support direct upgrades from VOSS 5.0.1 to VOSS 7.1.4, Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Partially supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
4200 / 2400 Pod Fx 3.0.1 Hardware	<p>Supported.</p> <p>VMware: Vendor supports direct upgrade from release 5.5.x to 6.5 u3. This includes vCenter Server Appliance and ESXi.</p> <p>Extreme switches:</p> <p>VSP 7200: Vendor does not support direct upgrade from VOSS 5.1.1 to VOSS 8.0.6. Upgrade to VOSS 6.1.X first.</p> <p>VSP 4850: Vendor does not support direct upgrades from VOSS 5.1.1 to VOSS 7.1.4. Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Partially supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
4200 / 2400 Pod Fx 3.0.2 Hardware	<p>Supported.</p> <p>VMware: Vendor supports direct upgrade from release 6.0.x to 6.5 u3.</p> <p>Extreme switches :</p> <p>VSP 7200: Vendor does not support direct upgrade from VOSS 6.0.1.1 to VOSS 8.0.6. Upgrade to VOSS 6.1.X first.</p> <p>VSP 4850: Vendor does not support direct upgrades from VOSS 6.0.1.1 to VOSS 7.1.4, Upgrade to VOSS 6.1.X first. Validated upgrade paths to VOSS 6.1 are: VOSS 5.1.1.x, VOSS 5.1.2.x, or VOSS 6.0.1.x</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Solutions Platform 4200 series 4.1 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 u3 first, using existing MSC. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Partially supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
4200 / 2400 Pod Fx 3.1 Hardware	<p>Supported.</p> <p>VMware: : vendor supports direct upgrade from release 6.0.x to 6.5 u3</p> <p>Extreme switches :</p> <p>VSP 7200: Vendor supports direct upgrades from VOSS 6.1.x to VOSS 8.0.6.</p> <p>VSP 4850: Vendor supports direct upgrades from VOSS 6.1.x to VOSS 7.1.4. (VOSS 8.x is not supported).</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • It is highly recommended to deploy the Avaya Solutions Platform 4200 series 4.1 MSC OVA to include latest bug and vulnerabilities fixes. • License key from existing 3.1 MSC can be re-used when deploying the ASP 4.1 MSC OVA after decommissioning previous 3.1 MSC version. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Supported.

Table continues...

From	To Avaya Solutions Platform 4200 series Release 4.1	Direct Upgrade
ACP 4200 4.0 / Pod Fx 2400 4.0 Hardware	<p>Supported</p> <p>VMware: : vendor supports direct update from release 6.5 to 6.5 u3.</p> <p>Extreme switches :</p> <p>VSP 7200: Vendor supports direct upgrades from VOSS 7.x to VOSS 8.0.6.</p> <p>VSP 4850: Vendor supports direct upgrades from VOSS 7.1.x to VOSS 7.1.4. (VOSS 8.x is not supported)</p> <p>Management Server Console:</p> <ul style="list-style-type: none"> • It is highly recommended to deploy the Avaya Solutions Platform 4200 series 4.1 MSC OVA to include latest bug and vulnerabilities fixes. • License key from existing ACP 4.0 MSC can be re-used when deploying the ASP 4.1 MSC OVA after decommissioning previous 4.0 MSC version. <p>Considerations: Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 u3 prior to upgrading the VMware infrastructure.</p> <p>Excludes racks with Lenovo servers.</p>	Supported

HPE Nimble supported upgrade paths

HPE and Avaya recommends using the current software version. Starting with ASP 4200 Release 4.1, the current Nimble OS version is **5.1.2.100**. If the existing Nimble OS version running on the array is not current, an upgrade is required.

*** Note:**

The new ASP 4200 Release 4.1 builds from the factory can come with a higher version. You do not require a downgrade.

Vendor does not support direct upgrades to version **5.1.2.100** from all previous OS versions, therefore perform an upgrade to **5.1.2.100** in the following order:

From versions 5.x

If the current Nimble OS version running on the array is **5.0.4.0** or later, then upgrade to **5.1.2.100** directly.

If the current Nimble OS version running on the array is **5.0.3.100** or older, then upgrade to **5.0.7.300** first. Once the array has been successfully upgraded to **5.0.7.300**, proceed with upgrading to **5.1.2.100**.

From versions 4.x

If the current Nimble OS version running on the array is **4.5.4.0**, then upgrade to **5.1.2.100** directly.

If the current Nimble OS version running on the array is **4.5.3.0** or older, then upgrade to **5.0.7.300** first. Once the array has been successfully upgraded to **5.0.7.300**, proceed with upgrading to **5.1.2.100**.

Refer the following tables to see the complete list of the Nimble OS versions supported by the vendor and the verified upgrade paths to version **5.1.2.100**:

Nimble OS 5.1.2.100 Verified Upgrade paths

Table 1: From Versions 5.x

From Version	To Version
5.1.2.0	5.1.2.100
5.1.1.0	5.1.2.100
5.0.7.300	5.1.2.100
5.0.7.200	5.1.2.100
5.0.7.100	5.1.2.100
5.0.7.0	5.1.2.100
5.0.6.0	5.1.2.100
5.0.5.200	5.1.2.100
5.0.5.0	5.1.2.100
5.0.4.0	5.1.2.100
5.0.3.100	5.0.7.300
5.0.3.0	5.0.7.300
5.0.2.0	5.0.7.300
5.0.1.100	5.0.7.300
5.0.1.0	5.0.7.300

Table 2: From Versions 4.x

From Version	To Version
4.5.4.0	5.1.2.100
4.5.3.0	5.0.7.300
4.5.2.0	5.0.7.300
4.5.1.0	5.0.7.300
4.5.0.0	5.0.7.300

Determining licensing requirements

About this task

It is important to determine the licensing considerations of an upgrade before beginning the upgrade process. Use this procedure to determine whether licensing changes or updates will be required after the upgrade process.

Procedure

1. Determine the type of licensing manager used by the solution.

Solutions will either make use of a standalone Avaya WebLM implementation or one that is embedded with Avaya Aura® System Manager.

2. If the solution uses an Avaya WebLM implementation deployed with Avaya Aura® System Manager, note the Host ID of the current Avaya Aura® System Manager instance.

 **Note:**

All application licenses are hosted with the Avaya Aura® System Manager instance of Avaya WebLM. Application licenses must be moved to the new Avaya Aura® System Manager and be re-hosted after the upgrade is complete.

3. For Avaya Aura® System Manager Release 7.1 and later releases, a valid license is required for normal operation.
4. For VMware Licenses Release 5.5 to 6.X, email the current set of keys to aspprodmgt@avaya.com. You will receive the upgraded keys in an email.
For Release 6.0 and 6.5 - You can use the same license key. No upgrade is required.
5. For Avaya Orchestrator license Release 1.5, see *Configuring and Administering Avaya Orchestrator*.
6. For MSC license Pre-3.1 to release 3.1, Microsoft 2016 license is required. Order using the material code 700513602. It will be shipped to the site.
For Release 3.1 to 4.1, no license upgrade is required. Both releases use 2016 version.
From Avaya Support portal, pick up the required MSC Software for Release 4.1. Existing license key can be used to authorize the new MSC Instance.
7. Proceed with the upgrade as outlined in [Checklist for upgrading and patching Avaya Solutions Platform 4200 series](#) on page 50.

Checklist for upgrading and patching Avaya Solutions Platform 4200 series

Review the following prerequisites before starting any upgrade or patching activity:

! Important:

If you have a Geographic Redundancy setup, use the information and procedures documented in the noted checklists in *Upgrading Avaya Aura® System Manager* (<https://downloads.avaya.com/css/P8/documents/101057990>) regardless of whether you are using SDM or not to upgrade Avaya Aura® System Manager.

- *Checklist for upgrading System Manager Release 7.0.x in the Geographic Redundancy setup to Release 8.1*
- *Checklist for upgrading System Manager vAppliance Release 6.3.x in the Geographic Redundancy setup to Release 8.1*

*** Note:**

Avaya recommends that you install important Windows updates on the Windows Virtual Machines running on an Avaya Solutions Platform 4200 series as a best practice. See and follow your corporation security policies regarding Windows updates.

- Verify existing EVC settings on the existing Pod Fx solution. For more information on validating or configuring EVC within the cluster, see *PSN005315u* on Avaya support website.
- Verify that all applications are compatible with Avaya Aura® 8.1. See the Product Compatibility Matrix at support.avaya.com/compatibilityMatrix/Index.aspx.
- Verify that all applications are compatible with VMware 6.5. Upgrade incompatible applications to a VMware 6.5 compatible version.
- Verify that you have separated the VMkernels for iSCSI and vMotion. For more information see *Installing and Maintaining the Avaya Solutions Platform 4200 series*.

*** Note:**

This is not necessary for Avaya Solutions Platform 4200 series currently using the Release 2.1 or later software baseline.

- Verify that you have completed separate NIC teaming settings for each host. For more information, see *Installing and Maintaining the Avaya Solutions Platform 4200 series*.
- Perform a backup before beginning the upgrade process.
- Avaya recommends making DNS reachable as a best practice.
- Avaya recommends deleting all previously applied System Manager service packs and patches from the `/tmp/`, `/var/`, `/swlibrary`, and `/home/admin` directories as a best practice.
- Delete all snapshots for Avaya Aura® System Manager virtual machines.
See [Deleting VMware snapshots](#) on page 121.
- See [Deploying Avaya Diagnostic Server](#) on page 118 for instructions on deploying Avaya Diagnostic Server.
- Ensure that storage array redundancy is configured correctly before conducting a switch upgrade. Use the following checklist for guidance in this task.

*** Note:**

Contact Avaya Support if you require support in completing these validation steps.

1. Racks with HPE Nimble

Validate in the iSCSI settings that both Controller A and Controller B have iSCSI ports configured and the state of these ports is UP.

2. Racks with EMC VNX5300 and VNXe3200 storage arrays

Validate in the iSCSI settings that both SPA and SPB have iSCSI ports configured and the state of these ports is UP.

3. vCenter

For each ESXi host connected to the cluster, ensure that all the paths connected to each LUN are active and that these paths are going to both SPA or SPB for EMC storage arrays or Controller A or Controller B for Nimble arrays.

4. ESXi hosts

Confirm that ESXi hosts connected to the Cluster can communicate with each iSCSI target configured. Open an SSH connection to one of the ESXi hosts connected to the Cluster and use PING to test the connection to each iSCSI target. The iSCSI targets are the IP addresses configured on each iSCSI port for SPA and SPB in EMC storage arrays or Controller A and Controller B in Nimble arrays.

5. Switches

Confirm the ports used to connect the switches to the EMC or Nimble storage arrays in the *Customer Lifecycle Workbook*. Connect to both switches and check the status of these ports. Confirm that the status is UP and the expected MAC addresses are discovered on these ports.

! Important:

You must read, review, and take the necessary licensing actions required as described in [Determining licensing requirements](#) on page 50.

The following table lists the various dependencies that exist when engaged in upgrade activities.

Activity	Software Dependency	Compatibility Dependency	Dependencies
Deploy new MSC	No	Yes	<ul style="list-style-type: none"> Avaya Solutions Platform 4200 series Release 4.1 Management Server Console OVA can be deployed in VMware 6.0.x or later. For the customers with 5.x, proceed as recommended in the <i>Supported Upgrade Paths</i> table. Plug-ins for running vCenter Web Client 6.5 are installed on latest MSC. VMware vSphere thick client 6 is installed on latest MSC.

Table continues...

Activity	Software Dependency	Compatibility Dependency	Dependencies
HPE compute server firmware upgrade	Yes	Yes	<ul style="list-style-type: none"> Do not upgrade the VMware infrastructure to Release 6.5 prior to running the HP SPP ISO (firmware upgrade file) on each server. Upgrade the iLO firmware manually prior to running the HP SPP ISO for new hardware design Avaya Solutions Platform 4200 series.
Avaya Aura [®] applications upgrade	No	Yes	Verify that all applications are compatible with VMware 6.5 before upgrading the VMware infrastructure.
Avaya Orchestrator	Yes	Yes	This activity must be performed after upgrading the VMware infrastructure.
VMware vCenter Server Appliance upgrade	No	Yes	<ul style="list-style-type: none"> This activity must to be performed prior to upgrading the ESXi host servers. Run vCenter wizard installation from the latest MSC.
ESXi hosts server upgrade	No	Yes	<ul style="list-style-type: none"> This activity must be performed after upgrading VCSA. Validate that all running VMs are compatible with VMware Release 6.5 prior to upgrading the ESXi hosts. All hosts should be updated during the same maintenance window. Do not leave the ESXi host servers running on different VMware releases.
Switch upgrade	No	No	<ul style="list-style-type: none"> This activity can be performed at the beginning or at the end of the upgrade as best fits the scheduled resources. Do not leave the switches running on different releases.
Storage firmware upgrade	No	No	This activity can be performed at the beginning or at the end of the upgrade as best fits the scheduled resources.
PDU firmware upgrade	No	No	This activity can be performed at the beginning or at the end of the upgrade as best fits the scheduled resources.
G450 firmware upgrade	Yes	Yes	Upgrade the Media Gateway if Communication Manager has been upgraded.

The following checklist provides a high-level task list to upgrade Avaya Solutions Platform 4200 series.

Table 3: High-level upgrade task list

No.	Task	Description	Location	✓
1	Validate existing VMware EVC settings on cluster.	<ul style="list-style-type: none"> • Validate if EVC is enabled on existing Pod Fx solution. • If EVC feature is currently disabled, enable the feature before upgrading to Avaya Solutions Platform 4200 series release 4.1. • For more information on validating and enabling EVC feature, see <i>PSN005315u</i> on Avaya support website. <p>* Note:</p> <p>If EVC feature is disabled, plan in advance, and on a separate maintenance window, before conducting the upgrade to Avaya Solutions Platform 4200 series 4.1, request permission from the customer to conduct the necessary steps to enable EVC on the VMWare cluster.</p>		
2	(Optional) Obtain the network information used to deploy the latest MSC from the <i>Customer Lifecycle Workbook</i> .	—		

Table continues...

No.	Task	Description	Location	✓
3	<p>a. Identify the required software updates.</p> <p>b. Download the required software, patches, and OVAs to a PC or USB storage device.</p> <p>! Important:</p> <p>All updates and firmware files are available for download from the Avaya Support website in the Release 4.1 section.</p> <p>See Download new software on page 60.</p>	<ul style="list-style-type: none"> Download the required files to update the MSC and prepare for Avaya Orchestrator update. <p>! Important:</p> <p>Deploying the latest MSC OVA is not mandatory but is strongly encouraged to ensure that the latest security patches and updates are applied.</p> <ul style="list-style-type: none"> Locate and download the VMware vCenter upgrade files. Locate and download the supported patches and the vCenter Server update. <p>! Important:</p> <p>Do not download software and patches from the VMware website. Always get these from the Avaya support web site.</p> <ul style="list-style-type: none"> Locate and download the VSP 4000, VSP 7000, and VSP 7200 switch upgrade files. Locate and download the EMC VNX firmware files. <p>* Note:</p> <p>To determine if the storage array requires upgrading, see the upgrade section of this checklist.</p> <ul style="list-style-type: none"> Locate and download the Nimble firmware files. <p>* Note:</p> <p>This would only be required for offline upgrades. For more information, see Upgrading Nimble OS on online arrays on page 100.</p> <ul style="list-style-type: none"> Locate and download Avaya Aura® patches and other application updates. 		
4	<p>Deploy the new MSC OVA.</p>	<p>Deploying a new MSC OVA takes approximately 15 minutes for an on-site deployment.</p> <p>ASP 4.1 MSC OVA cannot be deployed on VMware 5.x. Upgrade VMware infrastructure to 6.5 first, using existing MSC.</p>		

Table continues...

No.	Task	Description	Location	✓
5	Reconfigure NTP settings	Starting with ASP 4200 R4.1, the MSC does not serve as the NTP server. See Configuring Network Time Protocol on page 114 to make necessary changes prior to continuing with the upgrade.		
6	<p>Perform the following upgrades in the order shown:</p> <p>a. Transfer upgrade files from a SCP compatible file server or from a USB device to the <code>ASP_SW_4.1</code> directory on the updated MSC.</p> <p>b. Upgrade compute server firmware.</p> <p>! Important: This step is mandatory and critical to the successful upgrade of the Avaya Solutions Platform 4200 series. Complete this step before proceeding to the next step.</p> <p>c. Upgrade the VMware vCenter Server Appliance to 6.5 U3b</p> <p>d. Enable ESXi shell access and SSH</p>	<p>Manually move the software files to the specific subdirectory in the <code>ASP_SW_4.1</code> directory.</p> <p>See Upgrading server firmware on page 108 for instructions on updating HP servers.</p> <p>! Important: Compute servers must be placed in Maintenance Mode before installing updates. This task takes up to 45 minutes to complete including the host reboot.</p> <p>! Important: For existing Avaya Pod Fx series with the Release 3.x hardware and Avaya Solutions Platform 4200 series Release 4.0 hardware, use the files <code>ilo4_270.bin</code> and <code>ilo5_146.bin</code> to upgrade the iLO firmware, which are available at http://support.avaya.com/. This step must be conducted prior to running the HP SPP ISO. For Avaya Solutions Platform 4200 series with HPE Gen 8 servers and Avaya Solutions Platform 2400 series, the iLO firmware is upgraded when the HP SPP ISO is executed . See Upgrading the HPE iLO firmware on page 110 for information and procedures on installing this separate upgrade.</p> <p>See Upgrading to VMware vCenter Server Appliance 6.5 Update 3b on page 70. This task takes up to 30 minutes to complete.</p> <p>—</p>	<p>See Transferring files on page 60. For more information about the directory structure, see Software and OVA repository on page 59.</p>	

Table continues...

No.	Task	Description	Location	✓
	e. Upgrade ESXi hosts to VMware ESXi 6.5 U3a	<p>See Using VUM to update ESXi hosts on page 80.</p> <p>* Note:</p> <p>Ensure all running Avaya Aura® applications in the cluster support VMware vSphere 6.5 before upgrading to ESXi 6.5 U3a. Upgrade Avaya Aura® applications to Release 8.1 as required, before proceeding with VMware ESXi upgrade.</p> <p>! Important:</p> <p>It is mandatory to apply PSN005451r2 after upgrading ESXi hosts to VMware ESXi 6.5 U3a.</p> <p>* Note:</p> <p>To avoid placing ESXi hosts into maintenance mode, and to avoid the VMs being vmotioned multiple times, conduct this task after VUM completes the upgrading and patching of each host. This task must be conducted prior to exiting the maintenance mode.</p>		
	f. Migrating to Avaya Orchestrator from POS Application	See Migrating to Avaya Orchestrator from POS applications on page 66.		
	g. Upgrade additional compute server firmware.	For more information, see Installing VMware ESXi 6.5 patches using VUM on page 89 and Configuring vSphere Update Manager on page 81.		
	h. Upgrade the switches.	<p>See Upgrading the switches on page 91 .</p> <p>This task takes up to 30 minutes to complete. Have a console cable available while performing this task.</p>		
	i. Upgrade the firmware for storage devices.	<p>See Upgrading storage devices on page 100.</p> <p>! Important:</p> <p>It is mandatory to upgrade the firmware of EMC storage devices to the latest firmware version during an upgrade cycle.</p> <p>Upgrading EMC firmware can take from 75 minutes up to several hours to complete. For more information, see Upgrading the EMC VNXe3200 operating system on page 103.</p> <p>Upgrading Nimble firmware takes up to 15 minutes to complete. For more information, see Upgrading Nimble OS on online arrays on page 100.</p>		

Table continues...

No.	Task	Description	Location	✓
	j. Upgrade the firmware for PDUs.	Download and install the appropriate firmware file based on your PDU type. See Upgrading PDU firmware on page 111. This task takes up to 10 minutes to complete.		
	k. Manually apply additional application patches and Avaya Aura® updates to baseline.	Manual updates are required for additional applications. You must obtain software update instructions from each product support site.		
	l. If the Avaya Aura® Communication Manager has been upgraded to release 8.1, verify the G450 Media Gateway is running this software:g450_sw_41_9_0.bin. Upgrade to this software version if applicable. If the Avaya Aura® Communication Manager has not been upgraded, skip this step.	Obtain the latest G450 Media Gateway documentation for information about verifying or upgrading software.		
	m. Upgrade Avaya SBCE on dedicated servers: ! Important: Confirm the upgrade path from the version of Avaya SBCE to Release 8.0 FP1 using the applicable documentation.	Obtain the latest Avaya SBCE documentation for Release 8.0 FP1.		
	n. Additional applications that are not part of the upgrade process require manual updates.	Obtain software update instructions from each product support site.		
7	(Optional) Configure NTP time source to an external time source.	See Configuring NTP on page 114.		
8	Remove previous software versions.	It is a good practice to remove software versions that are no longer relevant by the components of the Avaya Solutions Platform 4200 series Release 4.1. This includes components such as switches, storage arrays, and PDUs. See the product documentation for these components for procedures on removing old software versions.		
9	Re-host application licenses if necessary.	The need to re-host application licenses would have been determined before the upgrade took place using the procedure Determining licensing requirements on page 50. Use the procedure at this link to re-host the licenses if necessary.		

Table continues...

No.	Task	Description	Location	✓
10	Delete temporary snapshots.	Snapshots created during the upgrade should be deleted within 72 hours of the verified, successful completion of the upgrade process. See Deleting VMware snapshots on page 121 for the procedure to delete snapshots.		
11	Current factory builds of Avaya Solutions Platform 4200 series are implementing improved best practices that optimize performance. Deployed Avaya Solutions Platform 4200 series solutions with EMC storage devices can implement these optimizations using a script available for download from PLDS. This script is executed against the vCenter instance running on the Avaya Solutions Platform 4200 series solution.	See Product Support Notice <i>PSN004864r1</i> for information and procedures for executing the optimization script. For new Avaya Pod Fx 3.1 & ACP 4.0 customers with the HPE Nimble storage array, improved best practices might not have been implemented at the factory. See <i>Configuring advanced settings on the new iSCSI targets</i> of the <i>Installing and Maintaining the Avaya Solutions Platform 4200 series</i> document to validate and update settings as needed.		

Software and OVA repository

The software and OVAs for upgrades, patches, and deployment must be located on the E:\ASP_4.1_SW directory on the Management Server Console.

The following table provides a description of the high-level folder structure.

Root folder	Next level folders	Purpose
E:\ASP_4.1_SW	AO_and_Infrastructure	All files, such as OVAs and patches, for Avaya Orchestrator, VMware, and the Management Server Console.
	Firmware	All firmware files, such as Phones, EMC, Gateways, Compute Servers, Session Border Controllers, and VSP Series Switches.
	Avaya_AURA	All files, OVAs, patches for Avaya Aura Products, and patches and upgrades.

Download new software

Download new software for the Avaya Solutions Platform 4200 series Release 4.1 from the Avaya Support site support.avaya.com. Store the files in the specified subdirectories in the E: / ASP_4.1_SW directory of the MSC.

Filename	Instructions
Management Server Console OVA: Avaya Management Server Console 4.1.0.0.2.ova	Place the file in the following directory: E:\ASP_4.0_SW/ AO_and_Infrastructure/MSC
Avaya Orchestrator OVA: AvayaOrchestrator_1.4.0.0.19012135_vmx .ova	Place the file in the following directory: E:\ASP_4.0_SW/AO_and_Infrastructure/ Avaya_Orchestrator
Avaya Aura® System Manager OVA: <ul style="list-style-type: none"> • SMGR-8.0.0.0.931077-e65-18.ova • SMGR-PROFILE3-8.0.0.0.931077-e65-18.ova 	Place the files in the following directory: E:\ASP_4.0_SW/Avaya_AURA/SMGR
Avaya Aura® System Manager Upgrades System_Manager_8.0.1.0_r801008826.bin	Place the files in the following directory: E:\ASP_4.0_SW/Avaya_AURA/Patches/SMGR

*** Note:**

Use the checksum values published with these files to ensure that the files are complete and are not corrupted after transferring them to the Management Server Console.

Transferring files

About this task

Use the following procedure to transfer software update files from your PC or USB storage device to the E: / ASP_4.1_SW/ directory on the Management Server Console (MSC).

Before you begin

- You have already downloaded the required files to your PC or USB storage device. For more information about the software files to download, see [Downloading new software](#) on page 60.
- You have network access to the management network VLAN or you have physical access to the ESXi host compute server that runs the MSC.
- You must use a file server that supports file transfers using a SCP compatible protocol for network file transfer to the MSC.

Procedure

1. Log in to the existing Windows Management Server Console (MSC).

2. Start a session with the browser.
3. Connect to the IP address of the file transfer server.
4. Transfer the files to the MSC.
5. Build the `E:\ASP_4.1_SW\` directory structure on the MSC and move the files into the specific folders.
6. Enable any firewall software if applicable.

File transfer options

You must transfer the files to the `E:\ASP_4.1_SW\` directory on the existing Windows-based MSC after you have downloaded the required software updates to your PC or USB storage device.

The following provides you with some file transfer options:

- Network file transfer: If you downloaded your software updates to a PC, you can locally connect the PC to the management network for the fastest and most reliable file transfer.

*** Note:**

You can also transfer the software updates over the WAN or an internet connection but speed and reliability are reduced.

- Direct file transfer: If you downloaded your software updates to a USB device and you have physical access to Avaya Solutions Platform 4200 series Release 4.1, you can directly connect your USB storage device to the ESXi host compute server that runs the MSC. For instructions about mounting a USB device on a VM, go to the VMware website at www.vmware.com.

*** Note:**

All software and OVAs can be downloaded to the respective folders on the existing Windows-based MSC .

The following table shows the `E:\ASP_4.1_SW\` directory folder structure and the files required for each release upgrade.

VMWare	6.5-U3A Updates	ESXi 6.5u3a - build 14320405
		TLS configurator
		vCenter - build 14389939
Management_Server	MSC	TBD
ADS	SALGW-SLAMON	AvayaDiagnosticServer-3.0.0.0-vApp-e55-09.ova
IDE	Dashboard	IDE_9.5.0_DASHBOARD.zip

Table continues...

	Guest Manager	IDE_9.5.0_GUEST_AND_IOT_MANAGER_OVA_ESX_6_1_AND_6_5
	Ignition Server	IDE_9.5.0_IGNITION_SRVR_OVA_ESX_6_1_AND_6_5.zip
96xxPhones	H323	96x1-IPT-H323-R6_8_2_02-061319.zip
		96x1-IPT-H323-R6_8_2_02U-061319.zip (Encrypted)
		96xx-IPT-H323-R3_2_8-091517.zip (9620L/9620C/9630G/9640/9640G/9650/9650C/9670G)
	SIP	96x1-IPT-SIP-R7_1_6_1-072419.zip (9601/9608/9608G/9611G/9621G/9641G)
		96xx-IPT-SIP-R2_6_17-172303.zip (9620L/9620C/9630G/9640/9640G/9650/9650C)
EMC	VNXe3200	VNXe-Series-2-Drive-Firmware-V3-Dec-01-16.tgz.bin.gpg
		VNXe-3.1.10.9946299.tgz.bin.gpg
Nimble	CS1000 Firmware	5.1.2.100-649697-opt
	Nimble Plugin for ESXi 6.5	nimble-ncm-for-esx6.5-6.0.0-650005.zip
Server Technologies	Sentry 3 PDU	swcdu-v71d.bin
		smcdu-v71d.bin
	Sentry 4 PDU	pro-v80p.bin
HP SPP	Gen9-Gen10	bp-avaya-dl360g9-g10-ASP4200-4-1-2-New-only.iso
	Gen8-Podfx2400-Gen9	bp-avaya-dl360g9-g8-ASP4200-4-1-2-PodFx2400-Legacy-only.iso
	Gen10	ilo5_146.bin
	Gen9-Gen8	ilo4_270.bin
G450	FW	g450_sw_41_9_0.bin
SBC	HW	sbce-8.0.1.0-10-17555.iso
	VE	sbce-8.0.1.0-10-17555.ova
VSP_Switches	VSP4000	VOSS4K.7.1.4.0.tgz
		VSP4000v711_HELP_EDM_gzip.zip
	VSP7200	VOSS7K.8.0.6.0.tgz
		VOSSv805_HELP_EDM_gzip
AAC	vAAC_MediumSimplex_MCP_18.2.8-2019-01-23-2100-1vDisk150Gb_8vCPU_24GBMemory	
	vAAC_Platform_MCP_18.2.8-2018-12-14-2000-1vDisk150Gb_8vCPU_24GBMemory	

Table continues...

	vAAC_MediumPrimary_MCP_18.2.8-2018-12-14-2000-1vDisk150Gb_8vCPU_24GBMemory
	vAAC_MediumSecondary_MCP_18.2.8-2018-12-14-2000-1vDisk150Gb_8vCPU_24GBMemory
ACR	acr-152-linux.iso
	acr-152-windows.iso
AWFO Select	Awfos_5_2_2.exe
AES	AES-8.1.0.0.0.9.20190509-e65-00.ova
AAM	AAM-07.1.0.0.532-e65-0.ova
AMM	amm-3.5.0.0.263_OVF10.ova
Equinox MS	Equinox/MediaServer/OVA/EquinoxMediaServer_9_1_8_1_OVA.zip
Equinox MGMT	Equinox/Management/OVA/EquinoxMgmt_9_1_8_118_OVA.zip
Equinox Edge	Equinox/H323Edge/OVA/EquinoxEdge_9_1_0_16_OVA.zip
Equinox Streaming & Recording	EquinoxRecordingGW_9_1_8_1_OVA.zip
	EquinoxRecordingGW_9_1_8_1.zip
	EquinoxMgmt_9_1_0_8_4_OVA.zip
	assr-system-components-9.1.8.0.001.zip
	manager-9.1.0.255-bin.zip
	Conference Point System - aesr-ce-system-9.1.0.3.1.zip
	Transcoder - aesr-ce-9.1.8.0.10-Transcoder-9.1.8.7087.zip
	Delivery Node - AESR-DN-9.1.5.0.zip
	Scopia Elite -MCU_8_4_1_22.zip
	System Components (Delivery Node) aesr-dn-system-9.1.0.3.1.zip
AMS	MediaServer_8.0.0.169_A6_2018.10.24_OVF10.ova
CM	CM-Simplex-08.1.0.0.890-e67-0.ova
	CM-Duplex-08.1.0.0.890-e67-0.ova
CMS	CMS-R19.0.0.0.ea.d-e76-00.ova
Breeze	Breeze-3.6.0.2.360203.ova
EP	ExperiencePortal-MPP-7.2.0.0.1117-e55-1.ova
	ExperiencePortal-PrimaryEPM-7.2.0.0.1117-e55-1.ova
	ExperiencePortal-AuxiliaryEPM-7.2.0.0.1117-e55-1.ova
PS	PresenceServices-Bundle-8.1.0.0.398.zip
Session Manager	SM-8.1.0.0.810007-e67-01.ova
SDMClient	Avaya_SDMClient_win64_8.0.1.2.0033393_8.zip
SMGR	SMGR-8.1.0.0.733078-e65-47.ova
US-Utility Services	US-7.1.0.0.0.18-e55-2_OVF10.ova

Table continues...

Upgrades

SAL	SecureAccessLinkGateway-3.0.0.0-vApp-e55-06.ova	
WebLM	WebLM-8.1.0.0.7-32857-e65-8.ova	
Avaya ANAV	ANAV.4.1.1.200.Full.zip	
Patches	AAC	mcp_core_linux_ple2-18.2.14.patches.r-1.ext.iso
		mcp_core_linux_ple2-18.2.14.iso
		dvd_AAC_MCP_18.2.14.00_2019-06-04-1501_coreApps.iso
	AMM	ucapp-system-3.4.0.1.10.tgz
	ADS	ADS-ServicePack-3.0.5.0-601.tar.gz
		PolicyManager_SSHProxy-ServicePack-3.1.1.0.4.tar
	AES	aesvcs-8.0.1.0.1-superpatch.bin
	ACR	acr-15.2-1030.zip
		WFO-15.2-SRV-15.2.0.71-15.2.0.71.zip
		15.1.13.zip
		KB150241.zip
		KB150246.zip
		KB150228.zip
		Database-Permissions-Configuration-Tool-11.2.4.0111.zip
	WFO_15.2_SP0_HFR3.iso	
	Aura Control Manager - ACCCM	ACC_7.1.0.1_FeaturePack00ServicePack01_GA_Patches-17.zip
	AWFO Select	Awfos_5_2_2_1_Patch_3.zip
	AMS	MediaServer_Update_8.0.1.121_2019.04.29.iso
		MediaServer_System_Update_8.0.0.16_2019.04.05.iso
	Breeze	
	AAM	01.0.532.0-24811.tar
		KERNEL-3.10.0-957.1.3.el7.AV2.tar
		C24012pt+a.rpm
		m71532_002pt+a.rpm
		A22011pt+a.rpm
		MSG-01.0.532.0-002_0100.tar
	CM	KERNEL-3.10.0-957.21.3.el7.CM80.tar
01.0.890.0-25617.tar		

Table continues...

		PLAT-rhel7.4-0040.tar
	CMS	r19ea.d_cmspl-1.bin
	EliteMultichannel	
	EP	epavl-7.2.0.0.1907.tar.gz
		7.2.3.0.0441.tar.gz
		EPM_7.2.3.0.0441.tar.gz
	POM	POM3121Patch01.zip
		PomPDCInstallerSite_3.01.02.028.zip
		POM.03.01.02.00.00.031-DesktopJavaAPI.zip
		POM.03.01.02.01.00.007-POMDesktopJavaAPI.zip
	Equinox Media Server	EquinoxMediaServer_9_1_8_1.zip
	Equinox Management	EquinoxMgmt_9_1_8_118.zip
	Equinox Edge	EquinoxEdge_9_1_0_16.zip
	SM	Session_Manager_8.0-SSP-002.bin
	SMGR	System_Manager_R8.1_Patch_r810009814.bin
		System_Manager_R8.1GA_HotFix1_r810009880.bin
		System_Manager_SSP_R8.1.0.0_Patch1_810009957.bin
	US	util_patch_7.1.3.4.0.05.zip
	WebLM	WebLM_8.0.1.2_r80130087.bin
ISO_files	CMS	700514515_CMS-R19.0.0.0.ea.d_SFTW_DVD_LINUX.iso
	SM	Session_Manager_8.0.1.2.801204.iso
	CallCenterEliteMultichannel	EMC_6_6_0.iso
	EP	AAEP-7.2.0.0.1117.iso
		AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso
	OCEANA	OCEANA_3.6.1.0-2.iso
		Complete Software Suit for Oceana 3.6.1.0 is included in folder structure (Avaya Oceana 3.6.1.0 Solution Release Notes)
ACCCM	ACM_8.1.0.1_59_20190717_0827.iso	
POM	POM.03.01.02.01.00.007-r181c015-x86_64.iso	

Table continues...

	IDE	IDE_9.5.0_RHEL_6.7_SOURCE_CODE_DVD1.zip
		IDE_9.5.0_RHEL_6.7_SOURCE_CODE_DVD2.zip

Migrating to Avaya Orchestrator from POS applications

About this task

Use this procedure to migrate to Avaya Orchestrator from POS applications. For information on supported upgrade paths, see [Supported upgrade paths](#) on page 40.

If your system's hardware is not supported with Avaya Solutions Platform 4200 series Release 4.1, contact the Account Manager.

Before you begin

- Starting with Avaya Solutions Platform 4200 series Release 4.0 and later releases, Avaya Orchestrator replaces the existing Avaya Pod Orchestration suite.
- Avaya Orchestrator does not require System Manager to operate. Avaya Orchestrator runs independently.
- To avoid excessive administration changes, Avaya recommends to re-use the VPFM IP address when deploying the Avaya Orchestrator VM.
- Optional: Export any relevant reports from VPFM that customer would like to archive. For more information on VPFM reports, see the [Managing Fault and Performance on Avaya Visualization Performance and Fault Manager](#).
- For customers using a single System Manager to manage the POS applications and Avaya Aura applications, remove the POS applications links from System Manager. For more information, see the *Removing POS links* section in the *Installing and Maintaining the Avaya Solutions Platform 4200 series* guide.

Procedure

1. If you are using a standalone System Manager to manage POS applications, do the following:
 - a. Connect to vCenter using the vSphere web client.
 - b. Locate and power down the following VMs:
 - PVM
 - VPFM
 - IPFM/COMVPS (If available)
 - c. Deploy and configure Avaya Orchestrator. For deploying and configuring Avaya Orchestrator, see *Configuring and Administering Avaya Orchestrator*.
 - d. After Avaya Orchestrator is successfully deployed and configured, delete the System Manager for POS applications, PVM and VPFM VMs from the disk. For more information, see [Disassociating VPFM from Applications and infrastructure components](#) on page 67.

- e. If the Avaya Orchestrator VM was deployed with a new IP address instead of re-using the VPFM IP Address, remove VPFM entries from each component. For more information, see [Disassociating VPFM from Applications and infrastructure components](#) on page 67.
2. If you are using single System Manager to manage POS applications and Avaya Aura applications, do the following:
 - a. Connect to vCenter using the vSphere web client.
 - b. Locate and power down the following VMs:
 - PVM
 - VPFM
 - IPFM/COMVPS (If available)
 - System Manager for POS applications

 **Warning:**

Ensure that you have removed integration links from System Manager before shutting down the POS applications VM.

- c. Deploy and configure Avaya Orchestrator. For deploying and configuring Avaya Orchestrator, see *Configuring and Administering Avaya Orchestrator*.
- d. If the Avaya Orchestrator VM was deployed with a new IP address instead of re-using the VPFM IP Address, remove VPFM entries from each component. For more information, see [Disassociating VPFM from Applications and infrastructure components](#) on page 67.

Disassociating VPFM from Applications and infrastructure components

Use these procedures to avoid applications and infrastructure components to continue sending traps to VPFM after successfully deploying and configuring Avaya Orchestrator.

Use these procedures only if the Avaya Orchestrator VM has been deployed with a different IP other than the IP Address previously used by VPFM.

Disassociating VPFM from VSP 7200 and VSP 4058 switches

Procedure

1. Log in to the SSH console of VSP switch using administrator credentials.
2. Run the following commands:

```
Enable
Configure terminal
no snmp-server host <VPFM_IP> v2c readview
show syslog host 1
```

3. If syslog id 1 has an IP Address set to VPFM, run the following commands:

```
no syslog host 1
exit
save config
```

If the syslog id is not 1, run the **exit** command and **save config** command.

4. Repeat the same procedure with the second switch.

Disassociating VPFM from HPE iLO interface

Procedure

1. Log in to the HPE iLO interface of the first compute server using administrator credentials.
2. On the Home page, click **Administration > Management > SNMP Settings**.
3. Remove the VPFM IP next to the **SNMP Alert Destination (s)** field.
4. Click **Apply** to save settings.
5. Repeat the above steps for other compute servers.

Disassociating VPFM from PDU

Procedure

1. Log in to the PDU UI interface using administrator credentials.
2. On the Home page, click **Configuration > SNMP/Thresholds**.
3. Validate entries in Trap Destination 1 and 2.
4. Remove the VPFM IP address from Trap destination 1 or 2.
5. Click **Apply**.

Disassociating VPFM from VMware ESXi

Procedure

1. Log in to the SSH Console of a VMware ESXi host using root credentials.
2. Run following command:

```
esxcli system snmp set -t <Avaya_Orchestrator_IP>@162/avaya123,<SAL_GW_IP>@162/avaya123
```

3. Repeat the procedure for other servers.

Disassociating VPFM from VNXe3200

Procedure

1. Log in to the EMC Unisphere using administrator credentials.
2. Click **Settings > More Configuration > Alert Settings**.
3. Under **SNMP Alerts**, select the VPFM IP Address.

4. Click **Remove**.
5. Click **Apply**.

Disassociating VPFM from System Manager and Session Manager

Procedure

1. Log in to the System Manager web console.
2. On the Home page of the System Manager web console, click **Services > Inventory > Manage Serviceability Agent > Serviceability Agents**.
3. Select the **SMGR** instance.
4. Click **Manage Profiles**.
5. Click **SNMP Target Profiles**.
6. Expand the **Removable Profiles** view.
7. Select the **VPFM** profile and click **Remove**. The profile will be moved to the Assignable Profiles.
8. Click **SNMPv3 User Profiles**.
9. Expand the **Removable Profiles** view.
10. Select the user assigned to the **VPFM** profile and click **Remove**. The user will be moved to the Assignable Profiles.
11. Click **Commit**.
12. Repeat the above steps for each Session Manager instance one at the time.
13. Click **SNMP Target Profiles**.
14. Select the configured **VPFM SNMP** profile.
15. Click **Edit**.
16. Select the **Attach/Detach User Profile** tab.
17. Expand the **Removable Profiles** view.
18. Select the **VPFM** profile and click **Remove**. The profile will be moved to the Assignable Profiles.
19. Click **Commit**.
20. Select the configured **VPFM SNMP** profile.
21. Click **Delete**.

Disassociating VPFM from Communication Manager

Procedure

1. Log in to the Communication Manager web interface.
2. Click **Administration > Sever (Maintenance)**.

3. Under SNMP click on **Access**.
4. Select the **VPFM access** profile and click **Delete**.
5. On the Confirmation page, click **Delete**.
6. Click **FP Traps**.
7. Select the **VPFM trap** profile and click **Delete**.
8. On the Confirmation page, click **Delete**.
9. Repeat procedure for another Communication Manager.

Disassociating VPFM from Session Border Controller

Procedure

1. Log in to the EMS web interface using ucsec credentials.
2. Click **Device Specific Settings > SNMP**.
3. Select **Appliance** name.
4. Select the **SNMP v3** tab.
5. Select **Delete** option corresponding to the VPFM snmp v3 account.
6. The system displays a configuration pop-up window to confirm your selection.
7. Select **Yes** to delete the SNMP user.
8. The system deletes the selected SNMP v3 user and updates the SNMP v3 tab.
9. Click the **Management Servers** tab.
10. Select the **Delete** option corresponding to VPFM.

 **Note:**

For any other remaining Avaya Aura Applications not listed in this procedure reference to each applications administration guide.

11. Repeat these steps for each device.

Upgrading to VMware vCenter Server Appliance 6.5 Update 3b

About this task

Upgrading the VCSA and Platform services controller from 5.5.x or 6.0.x to the VCSA 6.5 U3b.

The underlying OS in the VCSA in vSphere 6.5 is changing from SLES to VMware's proprietary OS. For more information, see <https://vmware.github.io/photon/>"Photon OS - <https://vmware.github.io/photon/assets/files/photon-os-datasheet.pdf>.

The VCSA leverages Postgresql in 6.5 for the embedded database that is used by Virtual Center and VMware Update Manager.

- Starting with vCenter Server Appliance release 6.5 vSphere Update Manager (VUM) comes embedded with the vCenter appliance. Thus, installing VUM on the MSC VM is no longer required as in previous releases.
- **VUM Data migration (Optional):** For existing customers who already are running the external VUM on the MSC VM (Pod Fx 3.0.2/3.1) and would like to retain existing database when upgrading to VCSA release 6.5 U3b, need to run the VMware Migration Assistance on the MSC VM where VUM is running before initiating the upgrade of the vCenter server appliance as documented in <https://docs.vmware.com/en/VMware-vSphere/6.5/com.vmware.vsphere.upgrade.doc/GUID-6A39008B-A78C-4632-BC55-0517205198C5.html?hWord=N4lghgNiBclLYEsDmAnMAXBB7AdgAjAGdCFD0wd0QBfIA>.

*** Note:**

The VMware migration assistant file `VMware-Migration-Assitant.exe` is available within the `VMware-VCSA-all-6.5.0-14389939.iso` ISO file. When mounting the ISO on the MSC as part of the VCSA upgrade procedure, navigate to the migration-assistant folder to locate and transfer the file locally to the MSC, where vSphere Update Manager is currently running. This must to be performed before starting the vCenter upgrade.

- VUM data migration is not mandatory. It is safe to upgrade from previous VCSA releases to VCSA 6.5 without running the migration assistance. Follow the upgrade procedure as documented in this section.

*** Note:**

Regardless whether the VUM database is migrated during the VCSA upgrade procedure, a new baseline to upgrade and patch ESXi host to 6.5 U3a is required.

Use the following procedure to upgrade to VMware vCenter Server Appliance 6.5 Update 3b from VMware vCenter Server Appliance 5.5.x or 6.0.x.

Before you begin

- Deploy the Management Server Console.
- Ensure that the DNS servers are accessible throughout the network.
- Ensure that DNS records are updated with the existing vCenter FQDN. If the existing vCenter FQDN is not updated in the DNS records, the upgrading operation will fail. This includes creating a forward lookup and reverse PTR record for the vCenter FQDN.
- Reset the `administrator@vsphere.local` password. See [Resetting the vCenter Server Appliance Administrator password](#) on page 77.
- If you are upgrading from vCenter Server Release 5.5 to Release 6.5 U3b, ensure that the embedded SSO account (`administrator@vsphere.local`) is configured before you proceed to the upgrade.

For more information, see **Checking if the embedded SSO account is configured** in *Installing and Maintaining the Avaya Solutions Platform 4200 series*.

- if you are upgrading from Release 5.5.x to Release 6.5.x, you need a new license key. You do not need a new license key if you are upgrading from Release 6.0.x to Release 6.5.x.

Contact aspprodmgmt@avaya.com before attempting this upgrade if you do not have the license key and request a new key.

- Determine if the vCenter Server Appliance certificate is valid. See [Validating vCenter Server Appliance certificate](#) on page 74.

Procedure

1. Copy the `VMware-VCSA-all-6.5.0-14389939.iso` file to the Management Server Console.
2. Copy the ISO file to the **Application1** datastore.
3. Mount the ISO file to the MSC CD/DVD drive.
4. Browse the mounted CD/DVD drive.
5. Go to `vcsa-ui-installer/win32` and double-click the installer.
6. On the home page, click **Upgrade**.
7. To start Upgrade Stage 1, click **Next**.
8. Click **I accept the terms of the license agreement** and click **Next**.
9. In the **IP Address or FQDN** field, enter the IP address or FQDN of source vCenter Server Appliance that you want to upgrade.
10. Click **Connect to Source**.
11. Enter the information about the vCenter Server Appliance for Single Sign-On.
12. Enter the ESXi host information that manages the vCenter Server Appliance in the appropriate fields.
13. Click **Next**.
14. If you receive any certificates warning, click **Yes**.
15. In the Deployment Type, click **Embedded Platform Services Controller** and click **Next**.
16. If you receive any certificates warning, click **Yes**.
17. On the Set up target appliance VM page, provide the appropriate information, and click **Next**.
18. In the **Deployment Size** field, click **Small**.

Important:

If the database size is too big, the upgrading may encounter an issue.

You can refer to the following message in the log file:

```
WARNING upgrade_commands The following disks are too small to  
fit the source_disk requirement  
ERROR upgrade_commands Current deployment size is too small for  
the existing inventory
```

For more information or assistance on reclaiming disk space, see <https://kb.vmware.com/s/article/2056448>.

19. In the **Storage Size** field, select **Default**, and click **Next**.
20. From the list of available datastores, select the **Application 1** datastore, and click **Next**.
21. To configure temporary network settings for deployment, do the following:
 - a. In the **Network** field, select the Management Network.
This value must be same as the current vCenter deployment to ensure network connectivity.
 - b. In the **IP Version** field, click **IPv4**.
 - c. In the **IP Assignment** field, click **Static**.
 - d. In the **Temporary IP Address** field, select the temporarily available IP address available on the Management segment.
 - e. In the **Subnet Mask** field, select the management network subnet which is same as the current vCenter.
 - f. In the **Default Gateway** field, select the management network gateway which is same as the current vCenter.
 - g. In the **DNS Server** field, select an applicable DNS Server.
22. Click **Next**.
23. On the Ready to complete stage 1 page, review the upgrade settings, and click **Finish** to complete stage 1.
After the upgrade stage 1 is complete, you will receive a notification.
24. Click **Continue** to start the stage 2 of the Upgrade process.
25. Click **Next** to continue to Stage 2.
26. Specify the site name for VMware Single Sign-on of the Appliance, and click **Next**.
27. On the Select Migration data page, select the data that you want to copy from the old vCenter Server.
The data includes:
 - Configuration
 - Configuration, events, and tasks
 - Configuration, events, tasks and performance metrics
28. Click **Next**.
29. Click **Join the VMware Customer Experience Improvement Program** and **Next**.
30. Review and verify the upgrade settings.
31. Select the check box at the bottom of the page to acknowledge that the necessary back up has been made.
32. Click **Finish**.
The system displays the following message:

The source vCenter will be shut down once the network configuration is enabled on destination vCenter Server.

33. Click **OK**.

Next steps

- See [Applying license key to the VMware vCenter Server Appliance 6.5 Update 3b](#) on page 75.
- See [Assigning a license key](#) on page 75.

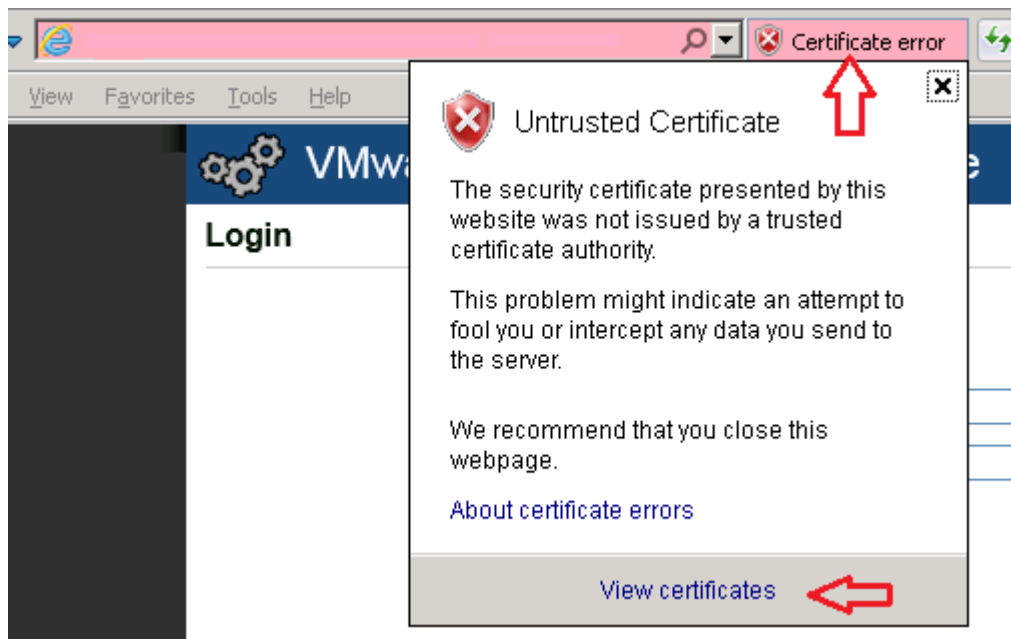
Validating vCenter Server Appliance certificate

About this task

Use this procedure to validate vCenter Server Appliance certificate.

Procedure

1. Log in to the Management Server Console.
2. Open a new browser tab in Microsoft Internet Explorer.
3. Navigate to `https://<vCenter_IP_Address>:5480`.
4. Click **Certificate error**.
5. Click **View certificates**.



6. Confirm both the **Issue to** and **Issue by** fields match the vCenter FQDN and the date range has not expired.

Issued to: vcenter1.avaya.com

Issued by: vcenter1.avaya.com CA 48096b71

Valid from 10/ 9/ 2017 **to** 10/ 8/ 2027

If either field does not match the vCenter FQDN, or the date range has expired, you must regenerate the certificate. See [Regenerating vCenter Server Appliance 5.x certificates](#) on page 79 to regenerate the certificate before continuing.

Issued to: localhost.localdom

Issued by: localhost.localdom CA 8f071daf

Valid from 9/ 12/ 2016 **to** 9/ 11/ 2026

Applying license key to the VMware vCenter Server Appliance 6.5 Update 3b

About this task

Use this procedure to apply the new Release 6.5 license key to the VMware vCenter Server Appliance 6.5 Update 3b.

* Note:

Applying a new license key is required when upgrading from Release 5.5 to Release 6.5. A new license key is not required when upgrading from Release 6.0 to Release 6.5

Procedure

1. Log in to the vSphere Client with administrator credentials.
2. On the Home page, click **Administration > Licensing > Manage vSphere Licenses**.
3. In the **Enter new vSphere license keys** field, enter the license key (one new key per line).
4. Click **Add License Key**.
5. Click **Next** to assign licenses to the vCenter Server or the ESXi hosts.

Ensure that you have assigned licenses to all ESXi hosts.

Assigning a license key

About this task

Use this procedure to assign a key if licenses were not applied while adding a new license.

Procedure

1. Log in to the vSphere Client as an administrator.
2. On the Home page, click **Administration > Licensing**
3. Click **Evaluation Mode**.
4. Expand the list to find the element that requires the key.
5. Right-click the element and click **Change License Key**.
6. Assign the appropriate key from the list.
7. Click **OK**.
8. Verify that the key is assigned properly.

Updating the vCenter Server Appliance

About this task

Use this procedure to update a deployed and operational instance of vCenter Server Appliance after it has been upgraded. This procedure requires restarting the vCenter Server Appliance. Perform this procedure during a scheduled maintenance window.

Note:

Follow this procedure only when required to update VCSA.

Procedure

1. Copy the update ISO file to the MSC.
2. Copy the ISO file to the `Application1` datastore.
3. Mount the ISO file to the vCenter VM CD/DVD drive.
4. Open a new web browser window.
5. Log in to vCenter with the URL `https://<vcenter-ip>:5480` using the root credentials.
Substitute `<vcenter-ip>` with the IP address of the vCenter instance.
6. Click **Update** in the pane to the left of the screen.
7. Click **Check Updates**.
8. Click **Check CDROM**.
9. Click **Install Updates**.
10. Click **Install CDROM updates**.
11. Click **I accept the terms of the license agreement** after reading and accepting the EULA.
12. Click **Install**.

*** Note:**

Use Google Chrome or Mozilla Firefox for updating the vCenter Server Appliance. Using Internet explorer will result in an error.

13. Click **OK** when the update completes.
14. Click **Reboot** to apply the update.

Resetting the vCenter Server Appliance Administrator password

About this task

Use this procedure to reset the vCenter Server Appliance Administrator (administrator@vsphere.local) password.

Refer to the following VMware Knowledge Base article for a procedure to reset the `root` password: [HTTPS://KB.VMWARE.COM/S/ARTICLE/2147144](https://kb.vmware.com/s/article/2147144).

Before you begin

- Obtain the vCenter Server Appliance `root` user credentials.

Procedure

1. Using the SSH Console, log in to vCenter Server Appliance with the `root` user credentials.
2. Do one of the following depending on the version of vCenter:
 - a. For vCenter 5.x, run the following commands to run the service tool:

```
/usr/lib/vmware-vmdir/bin/ vdcadmintool
vdcadmintool
```

- b. For vCenter 6.0, run the following commands:

```
shell.set --enabled true
shell
vdcadmintool
```

- c. For vCenter 6.5, run the following commands:

```
shell.set --enabled true
shell
vdcadmintool
```

The command line displays the following for vCenter 5.5 and vCenter 6.0:

```
=====
0. Exit
1. Test LDAP connectivity
2. Force start replication cycle
3. Reset account password
4. Set log level and mask
5. Set vmdir state
=====
```

The command line displays the following for vCenter 6.5:

```
=====
0. Exit
1. Test LDAP connectivity
2. Force start replication cycle
3. Reset account password
```

```
4. Set log level and mask
5. Set vmdir state
6. Get vmdir state
7. Get vmdir log level and mask
=====
```

3. Press 3 to enter the account reset workflow.
4. For vCenter 5.5 and vCenter 6.0, when prompted for the Account DN, type `cn=Administrator,cn=users,dc=vSphere,dc=local`.
5. For vCenter 6.5, when prompted for the Account UPN, type, `Administrator@vsphere.local`.

A new password is generated.

 **Note:**

Ensure that the new password is compliant with the list of unsupported passwords and vSphere 6.5 password requirements.

The following special characters are not supported in SSO passwords:

- Non-ASCII characters
- Ampersand (&)
- Semicolon (;)
- Double quotation mark (")
- Single quotation mark (')
- Circumflex (^)
- Backslash (\)
- Percentage (%)
- Angle brackets (< , >)

Repeat the above procedure if the generated password is not compliant.

6. Log in to the vSphere web client using the `administrator@vsphere.local` user name and the password generated in the previous step.
7. On the home page, click **Administration > Single Sign-On > Users and Groups**.
8. Select the **Administrator** user.
9. Right-click on the user and click **Edit User**.
10. Create a new password.
11. Confirm the changes.
12. Click **OK**.
13. Sign out of the web client.
14. Verify the password was changed by logging back into the web client with the new credentials.

Regenerating vCenter Server Appliance 5.x certificates

About this task

Use this procedure to regenerate vCenter Server Appliance 5.x certificates.

* Note:

This procedure is required when you upgrade the vCenter Server Appliance from Release 5.x to 6.x and the installed SSL certificate installed does not contain the vCenter FQDN.

This procedure is not applicable when you upgrade from the vCenter Server Appliance Release 6.0 to the Release 6.5.

Procedure

1. Log in to the Management Server Console.
2. Open a new browser tab.
3. Navigate to **https://<vCenter_IP_Address>:5480**.
4. Click **Administration**.
5. Select **Yes** for **Certificate Regeneration Enabled**.
6. Click **Submit**.
7. Restart the vCenter Server Appliance.

Upgrading the HPE Qlogic driver

About this task

Use the following procedure to upgrade the Qlogic driver of HPE DL360 Generation 9 and 10 servers.

! Important:

This procedure is not required for fresh installations. Its only required when doing upgrades from CPOD 2.1.x , Pod Fx 3.x, ACP 4.0 to Avaya Solutions Platform Release 4.1.

* Note:

VUM is the preferred method and is used to automate the Qlogic driver upgrade across all hosts connected to the cluster.

Procedure

1. Log in to vCenter using the Administrator credentials.
2. From the **Hosts and Clusters** view, select the first host within the cluster and place it in maintenance mode.
3. Using **winscp**, connect to the ESXi host in maintenance mode using the root credentials and transfer the **QLogic-Network-iSCSI-FCoE-v1.0.95-offline_bundle-14045158.zip** file to **/var/log/vmware**.

4. With Putty, SSH to the ESXi hosts in maintenance mode using the root credentials.
5. Move to the location where the offline bundle was transferred to: `cd /var/log/vmware`
6. Execute the following commands to apply updates:
 - a. `esxcli software vib update -d QLogic-Network-iSCSI-FCoE-v1.0.95-offline_bundle-14045158.zip`
 - b. `reboot`
7. Follow boot up process from the iLO remote console.
8. Review and apply [PSN005451r2](#) if applicable.
9. From the **Hosts and Clusters** view, select the host from step 2 and exit it out of maintenance mode once it gets connected to the cluster.
10. Proceed with remaining hosts by repeating steps from step 2 to step 7. Always perform the drivers update with one host at a time.
11. For driver validation from the ESXi command-line interface, run `esxcli network nic get -n vmnicx` where x is either 4 or 5.

*** Note:**

Starting with ACP 4200 4.0 and later releases, the qllogic driver changes from `net-bnx2x` to the native `qfle3`.

The following image shows an example of driver module, FW and driver version running on Qlogic board. Always validate the specifications against the current ASP 4200 Baseline:

```
[root@cpd6-esxi6:~] esxcli network nic get -n vmnic4
  Advertised Auto Negotiation: false
  Advertised Link Modes: 10000BaseTwinax/Full
  Auto Negotiation: false
  Cable Type: DA
  Current Message Level: 0
  Driver Info:
    Bus Info: 0000:04:00:0
    Driver: qfle3
    Firmware Version: FW: 7.13.109.0 BC: 7.15.56
    Version: 1.0.77.2
```

Using VUM to update ESXi hosts

This section contains information on how to update ESXi hosts using the VMware Update Manager (VUM). You must install VUM before it can be used. You do not need to reinstall VUM after it has been installed.

- See [Configuring vSphere Update Manager](#) on page 81 to configure VUM with upgrade and update baselines.

- See [Upgrading VMware ESXi 5.5 and 6.0 to 6.5 Update 3a](#) on page 86 for upgrading ESXi hosts to the current ESXi release.
- See [Installing VMware ESXi 6.5 patches using VUM](#) on page 89 for installing ESXi patches.

*** Note:**

The procedures in this section provide the information necessary to upgrade hosts and install patches. Additional steps may be required to support specific solutions. Consult the VMware documentation for additional information.

*** Note:**

The procedures in this section contain file names specific to the initial Release 4.1 baseline. These procedures can be adapted to cover the deployment and installation of upgrades or patches by substituting the file names used in the procedures.

Configuring vSphere Update Manager

About this task

Use the following procedure to upgrade and patch ESXi hosts using vSphere Update Manager (VUM). Refer to the section [Installing VMware ESXi 6.5 patches using VUM](#) on page 89 to apply only patches.

Procedure

1. Log in to vCenter using the administrator credentials.
2. On the Home page, under the **Hosts and Clusters**, select the host.
3. On the **Update Manager** tab, click **Admin View**.
4. On the **ESXi Images** tab, click **Import ESXi Image**.
5. Click **Browse**.
6. Transfer the `VMware-ESXi-6.5.0-Update3-14320405-HPE-Gen9plus-650.U3.10.4.5.41-Aug2019.iso` file located on the E:\ drive.

*** Note:**

- If the ISO file is not available, download it from <https://support.avaya.com/downloads/> for Avaya Solutions Platform – ASP 4200 4.1.x and save it on the E:\ drive.
 - For HPE Gen 8 servers, download the iso file named `VMware-ESXi-6.5.0-Update3-13932383-HPE-preGen9-650.U3.9.6.8.8-Jun2019.iso` from <https://support.avaya.com/downloads/> for Avaya Solutions Platform – ASP 4200 4.1.x.
7. Click **Close**.
 8. Click **Hosts Baselines** to create a baseline using the ISO.
 9. In the **Name** field, type the name of the new baseline `Avaya Solutions Platform 4200 Series 4.1 - VMware Upgrades & Updates`.

 **Note:**

If you have racks with mix server environment, Avaya strongly recommends creating different baselines with each corresponding ISOs. This prevents upgrading or updating servers with the wrong ISO files. For instance, HPE Gen9 and Gen10 servers require one baseline whereas HPE Gen8 servers require another one.

10. In the **Description** field, type the description `Upgrades and Updates to VMware vSphere 6.5 U3 for ASP 4200 4.1 baseline`.
11. Select baseline type as **Host Upgrade**, then click **Next**.
12. Select an ESXi image imported during **step 6**, then click **Next**.
13. Click **Finish**.

 **Note:**

The ISO is imported and ready for use in upgrades.

14. On the **Patch Repository** tab, click **Import Patches**.
15. Click **Browse** to locate the patch file `ESXi650-201908001.zip` in the `E: Drive`.

 **Note:**

This is required only for racks with **HPE DL360p Gen8** servers. At the time of publishing this document, neither HPE nor VMware has published the custom ISO with **ESXi 6.5U3a** for the Gen8 servers.

16. Click **Open**.
17. Click **Next**, then click **Finish**.
18. On the **Hosts Baselines** tab, click the green plus sign button on the left to create a new baseline.
19. In the **Name** field, type the name of the new baseline `Avaya Solutions Platform 4200 series 4.1 - VMware Patches`.
20. In the **Description** field, type the description of the new baseline `VMware ESXi 6.5 U3 Patches for ASP 4200 4.1 baseline`.
21. Select **Hosts Patch**, then click **Next**.
22. Select **Fixed**, then click **Next**.

 **Important:**

Always add Avaya-approved patches, even if they are not included in the current baseline or listed in the *Release Notes*, prior to any maintenance activity.

23. Sort the patches by **Release Date**.
24. Select the following patches that are released on 08/19/2019 for ESXi 6.5:
 - VMware ESXi 6.5 Patch Release

- Updates esx-base, esx-tboot, vsan and vsanhealth VIBs

25. Click **Next**.

26. Review the list of selected patches, then Click **Finish**.



27. On the **Patch Repository** tab, click **Import Patches**.

28. Click **Browse**.

29. Locate the patch file `QLogic-Network-iSCSI-FCoE-v1.0.95-offline_bundle-14045158.zip` file.

30. Click **Open**.

31. Click **Next**, then click **Finish**.

32. Click **Import Patches**.

33. Click **Browse**.

34. Locate the file `nimble-ncm-for-esx6.5-6.0.0-650005.zip`.

35. Click **Open**.

36. Click **Next**, then click **Finish**.

37. Click **Import Patches**.

38. Click **Browse**.

*** Note:**

You must import all relevant files to the Patch repository if ESXi hosts with different server types are connected to the cluster.

39. **For HPE Gen 10 Servers:**

a. Locate and select the file `ams-esxi6.5-bundle-11.4.0-6.zip`.

b. Click **Open**.

c. Click **Next**.

d. Click **Finish**.

e. Repeat steps to import file `VMW-ESX-6.5.0-smartpqi-1.0.3.2309-offline_bundle_13601768.zip`.

For HPE Gen 9/8 servers:

- a. Locate and select the file `ams-esxi6.5-bundle-11.4.0-6.zip`.
 - b. Click **Open**.
 - c. Click **Next**.
 - d. Click **Finish**.
 - e. Repeat steps to import file `VMW-ESX-6.5.0-nhpsa-2.0.42-offline_bundle-13902712.zip`.
40. On the **Hosts Baselines** tab, click the green plus sign button on the left to create a new baseline.
 41. In the **Name** field, type the name of the new baseline `Avaya Solutions Platform 4200 series 4.1 - HPE Patches`.
 42. In the **Description** field, type the description of the new baseline, `HPE drivers for VMware ESXi 6.5`.
 43. Select **Hosts Extension**, then click **Next**.
 44. Select **Fixed**, then click **Next**.

! Important:

Always add Avaya-approved patches, even if they are not included in the current baseline or listed in the *Release Notes*, prior to any maintenance activity.

45. Type `qfle3` in the search filter, then press `Enter`.
46. Select the following patch:
 - `qfle3: Network driver for Qlogic E3 Controller Release date 6/25/2019`

! Important:

Do not select `qfle3f/i`.

47. Type `Nimble` in place of `qfle3` in the search filter, then press `Enter`.
48. Select the following patch:
 - `Nimble Connection Manager Product Release date 4/3/2019`

49. Type `ams` in place of `Nimble` in the search filter, then press `Enter`.

50. Select the following patch:
 - `ESXi 6.5.0 Agentless Management Service Bundle 11.4.0-6`

*** Note:**

Same file is applicable for all 3 supported HPE Model types Gen 8,9 & 10.

51. For HPE Gen 10 servers

- a. Type `smartpqi` in place of `ams` in the search filter, then press **Enter**.

- b. Select the patch `Smartpqi: SmartPqi Native driver`.

For HPE Gen8/9 servers

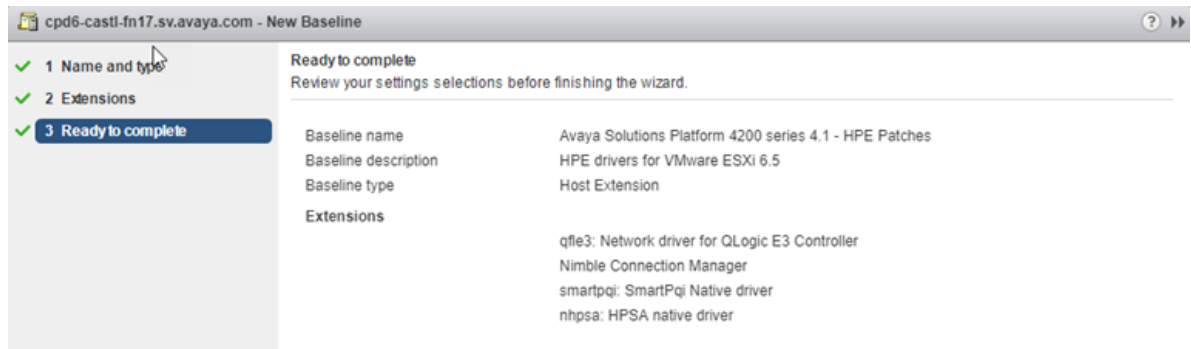
- a. Type `nhpsa` in place of `smartpqi` in the search filter, then press **Enter**.
- b. Select the patch `Nhpsa: HPSA native driver`.

*** Note:**

There must be 4 selected objects if the cluster contains different types of HPE server models or 3 objects if there is only a single type of server model.

52. Click **Next**.
53. Review the list of selected patches.

The following image shows an example of the selected patches when cluster combines different HPE server model type.



54. Click **Finish**.
55. On the **Hosts Baselines** tab, click the green plus sign button on the right to create a new baseline group.
56. In the **Baseline group name** field, type the baseline group name `Avaya Solutions Platform 4200 series - 4.1 Baseline`.
57. In the **Description** field, type `4.1 Baseline group` and click **Next**.
58. Select the **upgrade** baseline created in steps 8–13, then click **Next**.
59. Select the **patches** baseline created in steps 18–26, then click **Next**.
60. Select the **Extensions** baseline created in steps 27–54, then click **Next**.

61. Review the selections, and click **Finish**.



62. Go to **Settings > Host/Cluster Settings**, and click **Edit**.
63. Select the **Temporarily disable any removable media** checkbox.
64. Select the **Migrate powered off and suspend virtual machines to other hosts** checkbox.

*** Note:**

Some virtual machines in the cluster may have attached media devices that prevent them from entering Maintenance Mode. Despite the ability of VUM to temporarily disable these media devices, it has been reported that some Aura applications, such as Communication Manager, trigger an interchange due to a kernel panic while disconnecting the DVD drive. Avaya recommends using vMotion to manually migrate these VMs to other hosts within the cluster prior to a host remediation if this feature is to be used.

65. Set the retry delay time to 2 minutes.
66. Select the **High Availability Admission control** checkbox.
67. Click **OK**.
68. Go to **Settings > Download Schedule**, and click **Edit**.
69. Clear the **Enable schedule task** checkbox.
70. Click **Next**.
71. Review the selection, and click **Finish**.
72. Go to **Settings > Notification Check Schedule**, and click **Edit**.
73. Clear the **Enable schedule task** checkbox.
74. Click **Next**.
75. Review the selection, and click **Finish**.

Upgrading VMware ESXi 5.5 and 6.0 to 6.5 Update 3a

About this task

Use the following procedure to upgrade to the supported ESXi version.

Before you begin

- Ensure that you have valid VMware vSphere 6.5 licenses installed on vCenter before proceeding. The upgraded ESXi hosts will not be able to connect to vCenter if valid licenses are not installed. See [Determining licensing requirements](#) on page 50 to determine if the new licenses are required.
- vCenter must be running Release 6.5 update 3b or higher. The upgraded ESXi hosts will not be able to connect to vCenter if a lesser version is running.
- Using this procedure to upgrade does not support a rollback to previous versions. Perform this procedure on one host at a time.
- Perform this procedure only in a dedicated and customer-approved environment, and in a maintenance window attended by an Avaya certified engineer or business partner. This procedure is potentially service affecting if all precautions and considerations are not taken into account.

* Note:

Avaya Aura Applications could get impacted while vMotioning the application VMs between hosts during ESXi host upgrade. Therefore, always conduct the upgrade activity during an approved maintenance window or during low traffic hours.

Applications that do not support the VMware vMotion feature should be powered-off while the host goes into maintenance mode for host upgrade.

! Important:

Ensure that there are no conflicting VIBs installed on the ESXi. Conflicting VIBs that are installed on the ESXi host cause remediation failure during upgrade. To remove conflicting VIBs from the ESXi host, see [Removing conflicting VIBs from the ESXi host](#) on page 90.

Procedure

1. Log in to vCenter using the vSphere web client and Administrator credentials.
2. Go to **Home > Hosts and Clusters**, and select a host.
3. On the **Update Manager** tab, click **Attach Baseline**.
4. Select **Avaya Solutions Platform 4200 Series- 4.1 Baseline Group**.
5. Click **OK**.
6. Click **Scan for Updates**.
7. Select **Patches, Extensions and Upgrades**.
8. Click **OK**.

* Note:

When the scanning completes, the host is listed as non-compliant. This indicates that the host needs to be upgraded.

9. Click **Remediate**.

* Note:

If remediation fails due to conflicting VIBs installed on the ESXi host, see [Removing conflicting VIBs from the ESXi host](#) on page 90.

10. Ensure that the **Avaya Solutions Platform 4200 Series- 4.1 Baseline Group** baseline is selected.
11. Ensure that the target host is selected.
12. Click **Next**.
13. Accept the EULA.
14. Click **Next**.
15. Click **Next**.
16. **(Optional)** The upgrade can be scheduled for a future time. By default, it will occur immediately.
17. Click **Next**.
18. Review and confirm all settings.
19. Click **Next**.
20. Click **Next**.
21. Review and confirm all settings.
22. Click **Finish**.

 **Note:**

The host is placed in Maintenance Mode and the upgrade starts. You can connect to the server console using the iLO to monitor the upgrade progress.

During the upgrade, the server reboots more than once, especially when upgrading from ESXi 5.5.x to ESXi 6.5.

Due to the licensing considerations, you can manually connect the host to vCenter after the upgrade is complete.

23. Go to vCenter and assign a valid vSphere 6.5 license to the upgraded host and then connect it to vCenter.
24. If the licensing process fails, perform the following steps:
 - a. Log in to the ESXi host using root credentials.
 - b. On the Menu, click **Manage > Licensing > Assign License**.
 - c. Enter the license key information.
 - d. Return to vCenter.
 - e. Connect the host to vCenter.
25. Validate the VMware ESXi release.
26. Remove the host from Maintenance Mode.

27. Repeat this process for the next host in the cluster.

Installing VMware ESXi 6.5 patches using VUM

About this task

Use the following procedure to install ESXi patches using VUM.

Before you begin

All ESXi hosts must run Release 6.5 Update 3 before performing ESXi patch procedures. A different version can incorrectly report as compliant. Hosts marked as compliant will not have patches applied.

Procedure

1. Log in to vCenter using the vSphere web client and Administrator credentials.
2. Go to **Home > Hosts and Clusters**, and select a host.
3. On the **Update Manager** tab, click **Attach Baseline**.
4. Select the baseline `Avaya Solutions Platform 4200 Series - 4.1 Baseline group`.
5. Click **Scan for Updates**.
6. Select both the options and click **OK**.

A green check mark should appear beside the Upgrades baseline and a red X mark sign appear beside the Updates baseline. This indicates the host is compliant with the Upgrade baseline (upgraded to Release 6.5 Update 3), but not compliant with the Updates baseline. Non-compliance with the Updates baseline indicates you can proceed with applying the patches.

7. Click **Remediate**.
8. Under **Individual Baselines by Type**, select **Patch Baselines**.
9. Under **Baselines**, select the `Avaya Solutions Platform 4200 series 4.1 - VMware Patches` baseline.

Note:

See [Configuring vSphere Update Manager](#) on page 81 to create the Group baseline if it is not available.

10. Click **Next**.
11. Click **Next**.
12. Validate Target selection.
13. Validate that the patch selection aligns with the ASP 4200 4.1 baseline.
14. Click **Next**.

*** Note:**

This activity can be scheduled for a future date. It will occur immediately by default.

15. Click **Next**.
16. Review the remediation settings, and click **Finish**.

The patch installation process starts.

The host will show as compliant with both baselines once the installation process completes and the host connects to vCenter.

17. Repeat this procedure for the next host in the cluster.

Removing conflicting VIBs from the ESXi host

About this task

When upgrading from ESXi 5.5/6.0 to ESXi 6.5 using vSphere Update Manager (VUM), remediation fails due to conflicting VIBs installed on the ESXi host. Removal of conflicting VIBs is required before proceeding with the upgrade.

Before you begin

Identify the vendor that provided the conflicting VIB for ESXi before removing the conflicting VIB installed on the host. You can identify the vendor and the conflicting VIB from the status details of the interrupted upgrade.

For example, if the status detail shows `Mellanox_bootbank_net-mst_2.0.0.0-1OEM.550.0.0.600000` as the conflicting VIB, you can identify that the vendor is Mellanox, and the conflicting VIB is net-mst.

*** Note:**

Applications and services can be impacted for a short period when VMs are being vMotioned, therefore, only perform such activity during an approved maintenance window. Avaya Aura Applications that do not support the VMware vMotion feature should be powered off and should remain on the host when the host goes into maintenance mode.

Procedure

1. From vCenter, move the ESXi host with conflicting VIBs into maintenance mode.
2. Use PuTTY to set up an SSH connection to log in to the host with root credentials.
3. List the vendor specific VIBs installed on the ESXi host to identify the conflicting VIB, using the command `esxcli software vib list | grep <vendor name>`.

Here, replace `<vendor name>` with the actual name of the vendor of the conflicting VIB.

For example:

- If the status detail shows `Mellanox_bootbank_net-mst_2.0.0.0-1OEM.550.0.0.600000` as the conflicting VIB, then the command is:

```
[root@cpd3-esxi2:~] esxcli software vib list | grep Mellanox
net-mlx4-core    1.9.9.4-1OEM.550.0.0.1331820  Mellanox  VMwareCertified
2018-09-27
net-mlx4-en      1.9.9.4-1OEM.550.0.0.1331820  Mellanox  VMwareCertified
```

```
2018-09-27
net-mst      2.0.0.0-1OEM.550.0.0.600000 Mellanox PartnerSupported
2018-09-27
```

- If the status detail shows

HUAWEI_bootbank_hio_2.0.0.421OEM.550.0.0.1331820 as the conflicting VIB, then the command is:

```
[root@] esxcli software vib list | grep HUAWEI
hio      2.0.0.421OEM.550.0.0.1331820 HUAWEI VMwareCertified
2016-05-27
```

4. After identifying the conflicting VIB, remove it from the host using the command `esxcli software vib remove -n <VIB name>`.

Here, replace <VIB name> with the actual name of the conflicting VIB. For example:

- If the status detail shows Mellanox_bootbank_net-mst_2.0.0.0-1OEM.550.0.0.600000 as the conflicting VIB, then the command is:

```
esxcli software vib remove -n net-mst
Removal Result
  Message: The update completed successfully, but the system needs to be
rebooted for the changes to be effective.
  Reboot Required: true
  VIBs Installed:
  VIBs Removed: Mellanox_bootbank_net-mst_4.0.0.20 1OEM.550.0.0.1331820
VIBs Skipped:
~ # reboot
```

- If the status detail shows

HUAWEI_bootbank_hio_2.0.0.421OEM.550.0.0.1331820 as the conflicting VIB, then the command is:

```
[root@] esxcli software vib remove -n hio
Removal Result
Message: The update completed successfully, but the system needs to be
rebooted for the changes to be effective.
Reboot Required: true
VIBs Installed:
VIBs Removed: HUAWEI_bootbank_hio_2.0.0.42-1OEM.550.0.0.1331820
VIBs Skipped:
[root@] reboot
```

Upgrading the switches

This section provides procedures for upgrading the switches present in your Avaya Solutions Platform 4200 series. Depending on the hardware configuration of your solution, your Avaya Solutions Platform 4200 series may have Extreme Virtual Services Platform 4000 Series, Extreme Virtual Services Platform 7000 Series, or Extreme Virtual Services Platform 7200 Series switches.

Switches are placed in the Avaya Solutions Platform 4200 series in redundant pairs. Upgrading a switch will not cause an impact to overall system functionality.

Important:

Each switch must be upgraded one at a time. Ensure the upgraded switch is fully operational before attempting an upgrade on the next switch.

Perform the following tasks before upgrading the switch software:

- Back up data externally.
- Back up all configuration and logs externally.
- Verify switch logs to ensure there are no issues with the switch that would impede the upgrade.
- Verify the switch has enough free storage space to store the new software. Delete old logs and software to free space if needed.
- Verify system logs for any major alarms before upgrading the switches. Fix any identified problems before attempting the upgrade.
- Upgrade all switch software to the versions in the current release baseline, including switch plug-ins.

Consult the switch documentation suite for information on conducting these activities.

 **Warning:**

Consult the switch documentation for information on switch upgrade paths. In some instances, a direct upgrade from the currently deployed release to the release supported in the current Avaya Solutions Platform 4200 series baseline may not be supported. It may be necessary to upgrade to an intermediary release first.

 **Important:**

Refer to the information on ensuring storage array redundancy is configured correctly before conducting a switch upgrade. This information is found in [Checklist for upgrading and patching Avaya Solutions Platform 4200 series](#) on page 50.

Verifying system redundancy

Use the following procedure to verify that all links are operational and switches are fully redundant before attempting an upgrade.

About this task

 **Note:**

The customer routers and switches and can be different for each customer.

Procedure

1. Verify that the links, which are plugged into the switches, are operational.
 - a. Log in to the MSC, start PuTTY and open an SSH session on each of the VSP 4000 switches.
 - b. Log in to each VSP 4000 switch, and run the `show isis adjancencies` command to verify that the VSP 7000 or VSP 7200 switches are listed, as shown in the following example.

```

base1-vsp4k2:1#en
base1-vsp4k2:1#con t
Enter configuration commands, one per line. End with CNTL/Z.
base1-vsp4k2:1(config)#show isis adj
base1-vsp4k2:1(config)#show isis adjacencies
=====
ISIS Adjacencies
=====
INTERFACE L STATE      UPTIME PRI HOLDTIME SYSID          HOST-NAME
-----
Port1/49 1 UP      5d 23:46:24 127    23 0000.0beb.0001  base1-vsp7k1
Port1/50 1 UP      5d 23:46:20 127    20 0000.0beb.0002  base1-vsp7k2
-----
2 out of 2 interfaces have formed an adjacency
=====

```

2. At the command prompt, type `exit`.
3. Log in to the MSC, start PuTTY and open an SSH session on each of the VSP 7000 or VSP 7200 switches.
4. Log in to each VSP 7000 or VSP 7200 switch, and run the `show isis adjacencies` command to verify that the VSP 4000 switches and the neighbor VSP 7000 or VSP 7200 switch are displayed . If there are Extension Pods, more entries are displayed.

```

base1-vsp7K1#enable
base1-vsp7K1#config terminal
Enter configuration commands, one per line. End with CNTL/Z.
base1-vsp7K1(config)#show isis adjacencies
=====
ISIS Adjacencies
=====
INTERFACE L STATE    UPTIME PRI HOLDTIME SYSID      HOST-NAME
=====
Port: 21 1 UP      1d 23:56:23 127 22 b4a9.5a05.4465 base1-vsp4k1
Port: 22 1 UP      5d 23:49:42 127 22 b4a9.5a04.f865 base1-vsp4k2
Trunk: 64 1 UP     5d 23:59:00 127 25 0000.0beb.0002 base1-vsp7k2
=====
3 interfaces have formed an adjacency
=====

```

5. At the command prompt, type `exit`.

Upgrading the VSP 4000 switches

Use the following procedure to upgrade the VSP 4000 switches.

Before you begin

Ensure the preceding procedures have been completed prior to upgrading the VSP 4000 switches.

Procedure

1. Log in to the Windows MSC.
2. Connect to the switch using WinSCP. See the customer completed *IP template* to obtain the IP address and login credentials.
3. Copy the downloaded TGZ upgrade file to the root level of the VSP 4000 switch.
4. On the MSC, open an SSH session on the same VSP 4000.
5. Log in to the VSP 4000, and enter the following commands:
 - a. `enable`
 - b. `configure terminal`

- c. `software add <upgrade_TGZ_file>`
 - d. `software activate <upgrade_file_GA>`
 - e. `reset`
6. Wait for the switch to reboot. After the VSP 4000 restarts, start PuTTY and open an SSH session to the VSP 4000.
 7. Use the command **show software** to verify that the software version has been updated to the new release.

The following is an example of the command output. Confirm the new software release is listed as the (Primary Release) as shown below.

```

base1-vsp4K2:1(config)#show software
=====
software releases in /intflash/releases/
=====
4.0.0.0.GA
4.2.1.0.GA (Backup Release)
6.0.1.1.GA (Primary Release)
-----
Auto Commit           : enabled
Commit Timeout       : 10 minutes

```

8. If upgrading a VSP 4000 on a Avaya Solutions Platform 4200 series only, perform the following commands:
 - a. `enable`
 - b. `config terminal`
 - c. `no password access-level ro`
 - d. `no password access-level l1`
 - e. `no password access-level l2`
 - f. `no password access-level l3`
 - g. `save config`
9. Perform a sanity check on the VSP 4000. See [Verifying system redundancy](#) on page 92.
10. Use the `software remove` command to remove previous software versions.

*** Note:**

The following is an example of using the `show software` and `software remove` commands to remove software from the flash memory.

```

base1-vsp4k1:1(config)#show software
=====
software releases in /intflash/release/
=====
3.1.0.3.GA
VSP4000.4.1.0.0.GA (Backup Release)
VOSS4K.6.0.1.1.GA (Primary Release)

base1-vsp4k1:1(config)#software remove 3.1.0.3.GA

```

```
Executing software remove for version 3.1.0.3.GA.
Release 3.1.0.3.GA removed successfully.
```

11. *** Note:**

Wait for 10 minutes after the first VSP 4000 switch has been upgraded before continuing with the second VSP 4000 switch.

On the second VSP 4000, repeat steps 2 through 10.

*** Note:**

Follow the procedure in the next step if the SNMP configuration is lost during the upgrade.

12. **(Optional)** Start PuTTY and open an SSH connection to the VSP 4000.

- a. Enter the command `snmp-server community avaya123 index avaya secname readview`.
- b. Enter the command `no snmp-server community public`.
- c. Enter the command `snmp-server community avaya321 index avayawrite secname initialview`.
- d. Enter the command `no snmp-server community private`.
- e. Enter the command `snmp-server host <AO_IP> v2c readview`.

Upgrading the VSP 7000 switches

Use the following procedure to upgrade the VSP 7000 switches.

Before you begin

Ensure the preceding procedures have been completed prior to upgrading the VSP 7000 switches.

Procedure

1. Start the TFTP server service on the MSC.
2. Copy the IMG and BIN upgrade files to the root level of the TFTP folder.
3. Start PuTTY and open an SSH session on the VSP 7000.
4. Log in to the VSP 7000.
5. Use the command `show mac-address-table port 1-2` to validate the storage links.

You should only see a single MAC address for each switch.

! Important:

If anything else displays, you must troubleshoot the issue before proceeding.

6. Enter the following commands:

⚠ Caution:

The **download** command causes the switch to reboot by default. Append the **no-reset** parameter to the end of the download command to stop the switch from rebooting after the software download completes.

- a. **enable**
- b. **config terminal**
- c. **download address <MSC_IP_address> image <upgrade_IMG_file> no-reset**
- d. **exit**

7. Enter the following commands:

⚠ Caution:

The **download** command causes the switch to reboot after the software download completes.

- a. **enable**
- b. **config terminal**
- c. **download address <MSC_IP_address> image <upgrade_BIN_file> no-reset**
- d. **exit**

8. Start PuTTY and open an SSH session to the VSP 7000 after it reboots.

9. Use the command **show system** to verify the software version.

The following output is an example of what is displayed.

```
base1-vsp7K1(config)#show system
System Information:
Operation Mode: Switch
MAC Address: 70-30-18-23-C0-00
Reset Count: 106
Last Reset Type: Software Download
Autotopology: Enabled
Base Unit Selection: Base unit using rear-panel switch
sysDescr: Virtual Services Platform 7024XLS HW:03 FW:10.3.1.5 SW:v10.4.3.053
sysObjectID: 1.3.6.1.4.1.45.3.79.1
sysUpTime: 0 days, 00:03:41
sysNtpTime: NTP not synchronized.
sysRtcTime: Wednesday 2014/12/10 18:31:57
sysServices: 6 sysContact:
sysName: base1-vsp7K1
sysLocation:
Stack sysAssetId:
```

10. Perform a sanity check on the VSP 7000. See [Verifying system redundancy](#) on page 92.

11. * **Note:**

Wait for 10 minutes after the first VSP 7000 switch has been upgraded before continuing with the second VSP 7000 switch.

Repeat steps 2 through 10 on the second VSP 7000.

* **Note:**

Follow the procedure in the next step if the SNMP configuration is lost during the upgrade.

12. **(Optional)** Start PuTTY and open an SSH connection to the VSP 7000.

- a. Enter the command `no password security`.
- b. Enter the command `snmp-server community avaya123 ro`.
- c. Enter the command `snmp-server community avaya123 rw`.
- d. Enter the command `snmp-server enable`.
- e. Enter the command `snmp-server name "base1-vsp7k1"` (use "base1-vsp7k2" for switch 2).
- f. Enter the command `snmp-server host <AO_IP> avaya123`.

Upgrading the VSP 7200 switches

Use the following procedure to upgrade the VSP 7200 switches.

Before you begin

Ensure the preceding procedures have been completed prior to upgrading the VSP 7200 switches.

Procedure

1. Log in to the Windows MSC.
2. Connect to the switch using WinSCP. See the customer completed *IP template* to obtain the IP address and login credentials.
3. Copy the downloaded TGZ upgrade file to the root level of the TFTP folder.
4. Start PuTTY and open an SSH session on the VSP 7200.
5. Log in to the VSP 7200.
6. Enter the following commands:
 - a. `enable`
 - b. `configure terminal`
 - c. `boot config flag ftpd`
7. Download the files to the switch using SCP.

8. Enter the following commands:

- a. `exit`
- b. `software add <upgrade_TGZ_file>`
- c. `software activate <upgrade_file_GA>`
- d. `reset`

The switch will reboot and run the new software image after it starts.

9. Login to the switch when it restarts.
10. Use the command `enable` to enter Privileged EXEC configuration mode.
11. Use the command `show software` to confirm the software is upgraded.
12. Use the command `software commit` to commit the software upgrade.
13. Use the command `software remove` to remove previous software versions.

* **Note:**

The following is an example of using the `show software` and `software remove` commands to remove software from the flash memory.

```

base1-vsp7k1:1(config)#show software
=====
software releases in /intflash/release/
=====
3.1.0.3.GA
VSP7200.4.1.0.0.GA (Backup Release)
VOSS7K.6.0.1.1.GA (Primary Release)

base1-vsp7k1:1(config)#software remove 3.1.0.3.GA
Executing software remove for version 3.1.0.3.GA.
Release 3.1.0.3.GA removed successfully.

```

14. * **Note:**

Wait for 10 minutes after the first VSP 7200 switch has been upgraded before continuing with the second VSP 7200.

Repeat the above steps for the second VSP 7200.

* **Note:**

Follow the procedure in the next step if the SNMP configuration is lost during the upgrade.

15. (Optional) Start PuTTY and open an SSH connection to the VSP 7200.

- a. Enter the command `snmp-server community avaya123 index avaya secname readview`.
- b. Enter the command `no snmp-server community public`.
- c. Enter the command `snmp-server community avaya321 index avayawrite secname initialview`.

- d. Enter the command `no snmp-server community private`.
- e. Enter the command `snmp-server host <AO_IP> v2c readview`.

Example

Upgrading storage devices

This section provides procedures for upgrading the storage devices present in your Avaya Solutions Platform 4200 series. Depending on the hardware configuration of your solution, your Avaya Solutions Platform 4200 series may have the following devices:

- Nimble CS1000
- EMC VNXe3200
- EMC VNX5300

Upgrading Nimble OS on online arrays

About this task

Use this procedure to upgrade the version of Nimble OS running on a storage array with access to HPE InfoSight.

 **Note:**

Contact Avaya Support before upgrading Nimble OS with a version that is not part of the release baseline.

Before you begin

Do the following if you need to determine the Nimble OS version.

1. Open a new browser window or tab on the MSC.
2. Enter the management IP address of the storage array.
3. Log in to the management interface with the Administrator credentials.
4. Select **Help > About Array Group** from the menu.
5. The version number is listed just below the Nimble Storage logo.
6. Click **OK**.
7. Verify the current array software version. If the current software version is lower than the version available on the Avaya Support portal with the ASP 4200 Release 4.1 baseline, continue with the upgrade procedure. Storage array upgrade is not required otherwise.

For more information on Nimble Storage array upgrade, see [HPE Nimble supported upgrade paths](#) on page 48.

Procedure

1. Open a new browser window or tab on the MSC.
2. Enter the management IP address of the storage array.

3. Log in to the management interface with the Administrator credentials.
4. Select **Administration** > **Software** from the menu.
5. Click **Download**.
6. Select a software version from the list.
7. Click **Download**.
8. Wait for the software upgrade to be directly downloaded from HPE Nimble Storage Support.
9. Click **Update**.

Checks are performed on the storage array before the upgrade begins. Contact Nimble Support using the following link if these checks fail: <https://www.hpe.com/us/en/services/nimble-storage.html#support>.

10. Scroll to the bottom on the screen and select **Accept Terms and Conditions**.
11. Click **Agree**.

 **Note:**

The upgrade process takes approximately 20 minutes per array. When the upgrade completes, you must clear your browser cache and reload this page to ensure that the interface uses the newly updated version.

A controller failover and a browser reload occur automatically during the upgrade. The array itself remains online and available throughout the update. If you have multiple arrays in a storage group, all group arrays are updated, one at a time, to the same version of Nimble OS.

If you disconnect from the array during the update, refresh the browser window to regain access to the Nimble array. You cannot connect to the array until the update is done.

High availability and sensitive applications could be impacted during the controller failover. Avaya recommends to conduct such upgrade activity during a controlled maintenance window or during low volume calls for contact centers.

12. Verify the current software version by performing the following tasks:
 - a. Log in to the management interface with the Administrator credentials.
 - b. Select **Administration** > **Software** from the menu.
 - c. Verify the software version in use.
 - d. Repeat the upgrade procedure if applicable.

For more information, see [HPE Nimble supported upgrade paths](#) on page 48.

Upgrading Nimble OS on offline arrays

About this task

Use this procedure to upgrade Nimble OS on arrays not connected to the Internet.

Before you begin

Ensure you have the following items before you begin:

- A computer that has access to the array using SSH (port 22) and Internet access for a remote Zoom session and for transferring ASUPs through FTP.
- A SSH tool such as PuTTY installed on the computer.
- A FTP tool such as FileZilla or WinSCP installed on the computer.
- A phone to call the appropriate [Nimble Support Hotlines](#).
- The array serial number.
- At least 72 hours of lead time before the planned update so ASUPs can be analyzed.
- If the current software version of Nimble OS is lower than the version available on the Avaya Support portal with the ASP 4200 Release 4.1 baseline, upgrade to the recommended version. For more information, see [HPE Nimble supported upgrade paths](#) on page 48.

Procedure

1. Call the appropriate Nimble Support number for ASUPs collection.
2. Wait for ASUPs analysis to be completed.
3. Download the update image applicable to Avaya Solutions Platform 4200 series Release 4.1 from the Avaya Support website.

 **Note:**

This image can only be used on arrays certified to perform the update.

Only the update image provided by Avaya Support can be used to upgrade arrays. Do not download the software provided on the HPE FTP site.

4. Open a new browser window or tab on the MSC.
5. Enter the management IP address of the storage array.
6. Log in to the management interface with the Administrator credentials.
7. Select **Administration** > **Software** from the menu.
8. Click **Upload**.
9. Verify the current array software version. If the current software version is lower than the version available on the Avaya Support portal with the ASP 4200 Release 4.1 baseline, continue with the upgrade procedure. Storage array upgrade is not required otherwise.
10. Select the upgrade image downloaded from Avaya Support.
11. Click OK.

The file is uploaded to the array.

 **Note:**

You may be shown a timeout error. This error is displayed because the array cannot communicate with the Nimble Support portal. Continue with the upgrade operation.

Communication with the Nimble Support portal is not necessary for the offline upgrade to complete.

12. Click **Update**.
13. Scroll to the bottom of the EULA window.
14. Click the checkbox.
15. Click **Agree**.
16. Click **OK**.

 **Note:**

The upgrade process takes approximately 20 minutes per array. When the upgrade completes, you must clear your browser cache and reload this page to ensure that the interface uses the newly updated version.

A controller failover and a browser reload occur automatically during the upgrade. The array itself remains online and available throughout the update. If you have multiple arrays in a storage group, all group arrays are updated, one at a time, to the same version of Nimble OS.

If you disconnect from the array during the update, refresh the browser window to regain access to the Nimble array. You cannot connect to the array until the update is done.

High availability and sensitive applications could be impacted during the controller failover. Avaya recommends to conduct such upgrade activity during a controlled maintenance window or during low volume calls for contact centers.

17. Log in to the management interface with the Administrator credentials.
18. Select **Administration** > **Software** from the menu.
19. Confirm the new software was successfully installed.
20. Repeat the upgrade procedure if applicable. For more information, see [HPE Nimble supported upgrade paths](#) on page 48.

Upgrading the EMC VNXe3200 operating system

About this task

Use the following procedure to upgrade the EMC VNXe3200 operating system.

A video demonstration of this process is available at: <https://www.youtube.com/watch?v=5g50DponXrk>.

 **Important:**

The disk firmware is upgraded as part of the overall operating system upgrade. It is not necessary to update the disk firmware separately following an operating system upgrade. Disk firmware is always included in the OS image for VNXe 3200s.

Before you begin

- Valid EMC support credentials.
- Check for any faults in the system logs. Clear these faults before beginning the upgrade procedure.

Procedure

1. Access the device by opening the IP address of the device in a browser tab or from the PVM storage component view.
2. Enter the username and password in the provided fields.
3. Click **Login**.
4. On the dashboard, navigate to **Settings > Update Software**.
5. Perform the following tasks to upgrade the operating environment:

Important:

Steps A to E assume the Avaya Solutions Platform 4200 series has Internet access. If it does not, the software must be downloaded on a workstation that has Internet access. The software must then be transferred to the MSC. After transferring the software to the MSC, you should proceed to step F to complete the upgrade process.

- a. Select the **Software** tab.
- b. Click **Obtain Candidate Version Online**.
- c. Provide your EMC support credentials to initiate the download.
- d. Select a location on the MSC to download the software package.
- e. Wait for the software download to complete.
- f. Click **Perform Health Check**.
- g. Ensure no issues are detected before continuing with the upgrade. Correct all issues before continuing.
- h. Click **Upload Candidate Version**.
 - i. Browse to where the software package was stored on the MSC and select it.
 - j. Click **Install Candidate Version** after the upload completes.
- k. The upgrade wizard will install the upgrade. This process takes approximately an hour.
- l. The wizard will notify you when the upgrade completes successfully.

Next steps

Perform the following checks to ensure the upgrade was successful:

- Log into the management IP address for Unisphere and confirm the settings and software version
- Check overall system health in Unisphere by selecting **VNXe > System > System Health** from the menu. All components should show green icons.

- Check the device logs to ensure no errors occurred during the upgrade process.
- Confirm there are no faults in the storage device.
- Verify the vCenter application and heartbeat datastores are available.
- Verify all VMs are still available and powered on.
- Perform a VoIP phone text between two stations.
- Place a call from a mobile phone to the company main number. It should be operational and answered either by an agent or messaging services.

Upgrading the EMC VNXe3200

About this task

Use the following procedure to upgrade the EMC VNXe3200 storage firmware.

A video demonstration of this process is available at: <https://www.youtube.com/watch?v=5g50DponXrk>.

Before you begin

- Valid EMC support credentials.

Procedure

1. Access the device by opening the IP address of the device in a browser tab or from the PVM storage component view.
2. Enter the username and password in the provided fields.
3. Click **Login**.
4. On the dashboard, navigate to **Settings > Update Software**.
5. The current software version is displayed on the **Software** tab and the current firmware is displayed on the **Disk Firmware** tab.
6. Update the disk firmware by clicking **Obtain Disk Firmware Online** at the bottom of the **Disk Firmware** tab and following the provided wizard.
7. Perform the following tasks to upgrade the operating environment:
 - a. Select the **Software** tab.
 - b. Click **Obtain Candidate Version Online**.
 - c. Provide your EMC support credentials to initiate the download.
 - d. Select a location on the MSC to download the software package.
 - e. Wait for the software download to complete.
 - f. Click **Perform Health Check**.
 - g. Ensure no issues are detected before continuing with the upgrade. Correct all issues before continuing.
 - h. Click **Upload Candidate Version**.

- i. Browse to where the software package was stored on the MSC and select it.
- j. Click **Install Candidate Version** after the upload completes.
- k. The upgrade wizard will install the upgrade. This process takes approximately an hour.
- l. The wizard will notify you when the upgrade completes successfully.

Upgrading the EMC VNX5300 operating system

About this task

Use the following procedure to upgrade the EMC VNX5300 storage firmware.

Before you begin

- Valid EMC support credentials.

Procedure

1. Open Unisphere Service Manager on the Windows MSC.
2. Log in with the required username and password credentials.
3. Click **Login**.
4. Log in as sysadmin, and accept any certificates.
5. Navigate to **Software > System Software**.
6. Click **Prepare for installation (Step-1)**, and click **Next**.
 - a. Click **Browse**, and navigate to the directory where the upgrade file is stored.
 - b. Double-click the upgrade file (**.PBU** file) to unpack and transfer the files.
 - c. Click **Next** when the transfer completes. It takes several minutes to complete.

Note:

If you are presented with a screen with the option **Override HA status for all servers**, check the box before proceeding. Verify the High Availability status of all servers after completing the upgrade.

- d. Click **Next**.
 - e. Click **Next** to collect diagnostic information. It takes several minutes to complete.
 - f. After the process completes, click **Next**. After the health check runs, review any warnings.
 - g. Click **Next**.
 - h. Click **Finish**.
7. Click **Install Software (Step-2)**, and click **Next**.
 - a. Select **Express Install**.
 - b. Click **Next**.

- c. On the verification screen, click **Next**. It can take several hours for the process to complete. Do not interrupt the installation process.
 - d. After the installation completes, click **Next**.
 - e. Clear the **Notify your service provider** check box.
 - f. Click **Finish**.
8. Close Unisphere Service Manager.
 9. Use Microsoft Internet Explorer in Compatibility View to launch Unisphere and navigate to SPA or SPB.
 10. In the pop-up window, allow any Java applets to run.

 **Note:**

If the pop-up window does not appear, ensure all pop-up blockers are disabled.

11. At the certificate warning prompt, click **Accept Always**.
12. Log in as sysadmin.

 **Note:**

If you are automatically logged out at any time during the upgrade process, you can log back in.

13. In the upper-left area, click the VNX system that is listed.
14. Confirm the **Block Software Version** has been updated.
15. Select **vCenter > Hosts > Configuration > Storage > Datastore** from the menu.
16. Click **Rescan All** to update the storage.

Next steps

Perform the following checks to ensure the upgrade was successful:

- Log into SPA and confirm the settings and software version
- Log into SPB and confirm the settings and software version.
- Select **APMxxx > System > Hardware > Storage Hardware** from the Unisphere menu. Confirm there are no faults.
- Check the device logs to ensure no errors occurred during the upgrade process.
- Confirm there are no faults in the storage device.
- Verify the vCenter application and heartbeat datastores are available.
- Verify all VMs are still available and powered on.
- Perform a VoIP phone text between two stations.
- Place a call from a mobile phone to the company main number. It should be operational and answered either by an agent or messaging services.

Upgrading server firmware

About this task

The following procedure describes how to update Avaya-approved firmware on an HPE DL360 servers. Booting from the update tool indicates the current firmware versions on the server for comparison to the latest version. The tool will automatically select updated versions and apply them during the update process.

This task may take up to 45 minutes for all the server firmware to update.

Before you begin

Download the applicable iLO firmware file and HP firmware upgrade ISO image from the Avaya Support website. Transfer the files to the Management Server Console.

Warning:

ESXi hosts must be placed into Maintenance Mode before proceeding to avoid any service impact. The server will reboot several times during the firmware upgrade process.

Procedure

1. Log in to the Management Server Console.
2. Open a web browser.
3. Connect to the server iLO web interface.
4. Log in to the iLO web interface.
5. Select **Administration > Firmware > Firmware Update** from the menu.

Note:

This is required only for HPE Gen 9 and Gen 10 servers on 4200 Pod Fx 3.X hardware and 4200 ASP Hardware racks.

For HPE Gen 8 servers and Gen 9 servers in 2400 Pods go directly to step 11.

6. Click **Chose File/Browse**.
7. Select the iLO firmware transferred to the MSC.
8. Click **Upload**.
The firmware is uploaded and installed. The iLO connect will be reset.
9. Return to the MSC.
10. Log in to the iLO web interface.
11. Launch the remote console.
12. Select **Virtual Drive > Image File CD-ROM/DVD**.
13. Browse to the location where the ISO file was stored on the MSC.
14. Select the ISO file.

15. Click **Open**.

*** Note:**

If you select Virtual Drive after mounting the ISO file, you should see a check mark next to **Image File CD-ROM/DVD**.

16. Select the server in vCenter.

17. Right-click the server.

18. Select **Reboot**.

19. Press **F11** on the remote console during the POST process to access the **Boot Menu**.

20. Select **iLO Virtual USB 2 : HPE iLO Virtual USB CD/DVD ROM**.

21. Press **Enter**.

The system displays the following message:

```
The Automatic Firmware Update Version 2018.06.0
```

*** Note:**

No intervention is necessary while the update tool runs. The update tool performs the following tasks:

- Analyzes the system and checks the current firmware and driver version.
- Creates an inventory of the components to be upgraded.
- Performs the upgrade to the components in the package inventory list.
- Shuts down server after completion.

*** Note:**

The remote console and iLO interface will reset during the iLO firmware upgrade. You will lose connectivity to the remote console. Wait several minutes before attempting to reconnect.

*** Note:**

You will see no display on the remote console when the upgrade completes. This is an expected behavior. The tool shuts down the server after the upgrade completes.

22. Log in to the iLO web interface.

23. Select **Power Management > Server Power > Momentary Press** from the menu to power on the server.

24. Follow the boot process on the remote console.

25. When the servers starts booting up the ESXi hypervisor, return to the iLO web interface, and click **Virtual Media > Boot Order** from the menu.

26. Select **Embedded RAID 1 : Smart Array P440ar Controller -279.37GiB, RAID 1 Logical Drive** from server boot order list.

27. Start clicking on **Up** until it is in the second position below **Embedded SATA Port 10 CD/DVD ROM : hp DVD D DU8D6SH**.
28. Click **Apply**.

 **Important:**

Do not attempt Steps 27 to 30 during the boot up or POST process as it will create an error.

Next steps

 **Important:**

You must complete the following tasks that are applicable to your server type after the server firmware upgrade. Failure to do so may result in failed upgrades or improper functioning of your compute servers.

Checking the server firmware version

About this task

Use this procedure for checking the firmware version on the HPE compute servers.

Procedure

1. Log in to the Windows MSC.
2. Open a web browser.
3. Connect to the iLO web interface.
4. Select **Information > System Information** from the menu.
5. View the different tabs to see the version information.

Upgrading the HPE iLO firmware

About this task

Use the following procedure to upgrade the iLO firmware on HPE servers.

Procedure

1. From the Avaya Support site, download the corresponding iLO firmware bin file for the server type.
2. Connect to the Management Server Console.
3. Save the `.bin` file to a location on the Management Server Console.
4. Log in to the server's iLO interface using the existing administrator credentials.
5. Go to **Administration > Firmware > Firmware Update**.
6. Click **Choose File/Browse** and select the bin file that you previously downloaded in the step 1 of this procedure.
7. Click **Upload** at the bottom right of the screen.

The firmware is uploaded and then installed.

8. The iLO connection will be reset.
9. Log in back to the iLO interface.

Example

The following is an example of the output provided by the upgrade file.

```
iLO Flasher v1.5-1 for VMware ESXi
(C) Copyright 2002-2017 Hewlett Packard Enterprise Development LP
Firmware image: ./ilo4_255.bin
Current iLO 4 firmware version 2.50; Serial number ILOMXQ54206RT

Component XML file: ./CP032489.xml
./CP032489.xml reports firmware version 2.55
This operation will update the firmware on the
iLO 4 in this server with version 2.55.
Continue (y/N)?y
Current firmware is 2.50 (Sep 23 2016 00:00:00)
Firmware image is 0x1001b1c(16784156) bytes
Committing to flash part...
***** DO NOT INTERRUPT! *****
Flashing is underway... 100 percent programmed. -
Succeeded.
***** iLO 4 reboot in progress (may take up to 60 seconds.)
***** Please ignore console messages, if any.
iLO 4 reboot completed.
```

Upgrading PDU firmware

About this task

Use the following procedure to upgrade PDU firmware.

Before you begin

Determine the model of PDU you are upgrading. Download the appropriate PDU firmware from the Avaya Support portal.

Note:

Some Sentry PDU models do not support HTTP upgrades. Use the FTP method indicated in the procedure if the HTTP option is not available. Upgrading using the HTTP method is the preferred upgrade option to upgrade Sentry PDUs.

Procedure

1. Perform the following tasks to upgrade Sentry3 PDUs using the HTTP method:
 - a. Log in to the PDU management interface.

Note:

Refer to the *Lifecycle Workbook* for the PDU management IP address.

- b. Select **Tools > Firmware** from the menu.
- c. Click **Browse** and select the new firmware file from the appropriate location.

- d. Click **Upload**.

The PDU restarts after the update is complete. Log in after the PDU restarts to confirm the firmware update.

2. Perform the following tasks to upgrade Sentry4 PDUs using the HTTP method:

- a. Log in to the PDU management interface.

 **Note:**

Refer to the *Lifecycle Workbook* for the PDU management IP address.

- b. Select **Configuration > System > Files** from the menu.
- c. Click **Browse** and select the new firmware file from the appropriate location.
- d. Click **Upload**.

The PDU restarts after the update is complete. Log in after the PDU restarts to confirm the firmware update.

3. Perform the following tasks to update PDUs that could not be updated using the HTTP method:

 **Note:**

The MSC does not include the FTP server. The FTP server must be installed on the MSC to proceed with this procedure.

- a. Transfer the firmware file to a folder on the MSC where the location is accessible by the FTP server.
- b. Create a new user in the FTP server that will be used to transfer the firmware file.
- c. Assign this new user access to the folder where the firmware file has been transferred to on the MSC.
- d. Start the FTP server.
- e. Open a new browser window on the MSC.
- f. Log in to the PDU management interface.

 **Note:**

Refer to the *Lifecycle Workbook* for the PDU management IP address.

- g. Click the **FTP** tab.
- h. Check the FTP server.
- i. Enter the name of the folder on the MSC used in step A in the **FTP Server Registered user root directory** field.
- j. Click **OK**.
- k. Restart the PDU.
- l. Log in to the PDU management interface.

- m. Select one of the following menu items depending on the type of PDU being upgraded:
 - Sentry3 — Select **Configuration** > **FTP**.
 - Sentry4 — Select **Configuration** > **Network** > **FTP**.
- n. Enter the host name or IP address of the FTP server.
- o. Enter the user name and password of the user created in step B.
- p. Enter a directory of /.
- q. Enter the firmware file name.
- r. Click **Test** to test the connection to the FTP server.
Correct any errors before continuing.
- s. Click **Apply**.
- t. Select **Tools** > **Restart** from the menu.
- u. Select **Restart and download firmware via FTP**.
- v. Click **Apply**.
- w. Wait 2 to 3 minutes for the update to complete.

Next steps

Return to [Checklist for upgrading and patching Avaya Solutions Platform 4200 series](#) on page 50.

Upgrading ESXi Hosts manually using Command Line



About this task

Use this procedure to upgrade or update Avaya Pod Fx ESXi host manually using the command line.

Before you begin

Download the Avaya Pod Fx ESXi host upgrade or update .zip file from the [Avaya support website](#).

Procedure

1. Log in to the **vCenter Server Appliance** that administers the Avaya Pod Fx ESXi host.
2. Go to **Home** > **Datastores and Datastore Clusters** > **Datastores and Datastore Clusters** tab.
3. Right-click the **Application Datastore** that is accessible by the host then select **Browse Datastore**
4. Click the  to create a new folder called **Patches** then select the  icon to upload the Avaya Pod Fx ESXi host .zip file to the datastore.

5. Place the Avaya Pod Fx ESXi host into maintenance mode.
6. SSH into the Avaya Pod Fx ESXi host using PuTTY.
7. Run the following commands to validate that the .zip file is in the Application Datastore:

```
cd /vmfs/volumes/"Application_Datastore_Name"/Patches ls
```

Validate that the .zip file is shown.

8. Run the following command to do a pre-check or dry run of the upgrade or updates before install:

```
esxcli software vib update -d /vmfs/volumes/"Application_Datastore_Name"/Patches/"the .zip file" --dry-run
```

Example output:

```
Installation Result
Message: Dryrun only, host not changed. The following installers will be applied:
[BootBankInstaller]
VIBs Installed: (This section will list several VMware_bootbank files)
```

9. Run the following command to install the upgrade or updates:

```
esxcli software vib update -d /vmfs/volumes/"Application_Datastore_Name"/Patches/"the .zip file"
```

Example output:

```
Installation Result
Message: The update completed successfully, but the system needs to be rebooted
for the changes to be effective.
Reboot Required: true
VIBs Installed: (This section will list several VMware_bootbank files)
```

10. Log in to vCenter, **right-click the ESXi host**, and **Reboot** to reboot the host.
11. Take the Pod Fx ESXi host out of maintenance mode.
12. After reboot, log in to vCenter and verify the VMware ESXi version of the host.
13. Run the same procedure on the remaining Pod Fx ESXi hosts in the cluster.

Configuring Network Time Protocol

Starting with Avaya Solutions Platform 4200 series Release 4.1, the Management Server Console does not serve as a Network Time Protocol (NTP). You must reconfigure all existing applications and the following hardware components to use customer's NTP server instead of MSC:

- Storage systems such as the EMC VNXe3200, the VNX5300, and the Nimble CS1000.
- Compute servers such as the HP ProLiant DL360 G8/9/10.
- Network switches such as the Extreme VSP 7000, VSP 4000, and VSP 7200 series.
- Session border controllers.
- Avaya G450 Media Gateway.

Network Time Protocol best practices

Avaya recommends the use of the Network Time Protocol (NTP) as a time source instead of VMware Tools periodic time synchronization between the VMs and the ESXi hypervisor. Avaya recommends the following configuration best practices when using NTP:

*** Note:**

See *Configuring Network Time Protocol in Upgrading Avaya Solutions Platform 4200 series using the Management Server Console* and *Updating DNS and NTP settings for ESXi hosts and Avaya Aura® core applications in Installing and Maintaining the Avaya Solutions Platform 4200 series* for configuration procedures related to the recommendations in this section. These documents are available on the Avaya Support website.

Infrastructure component synchronization

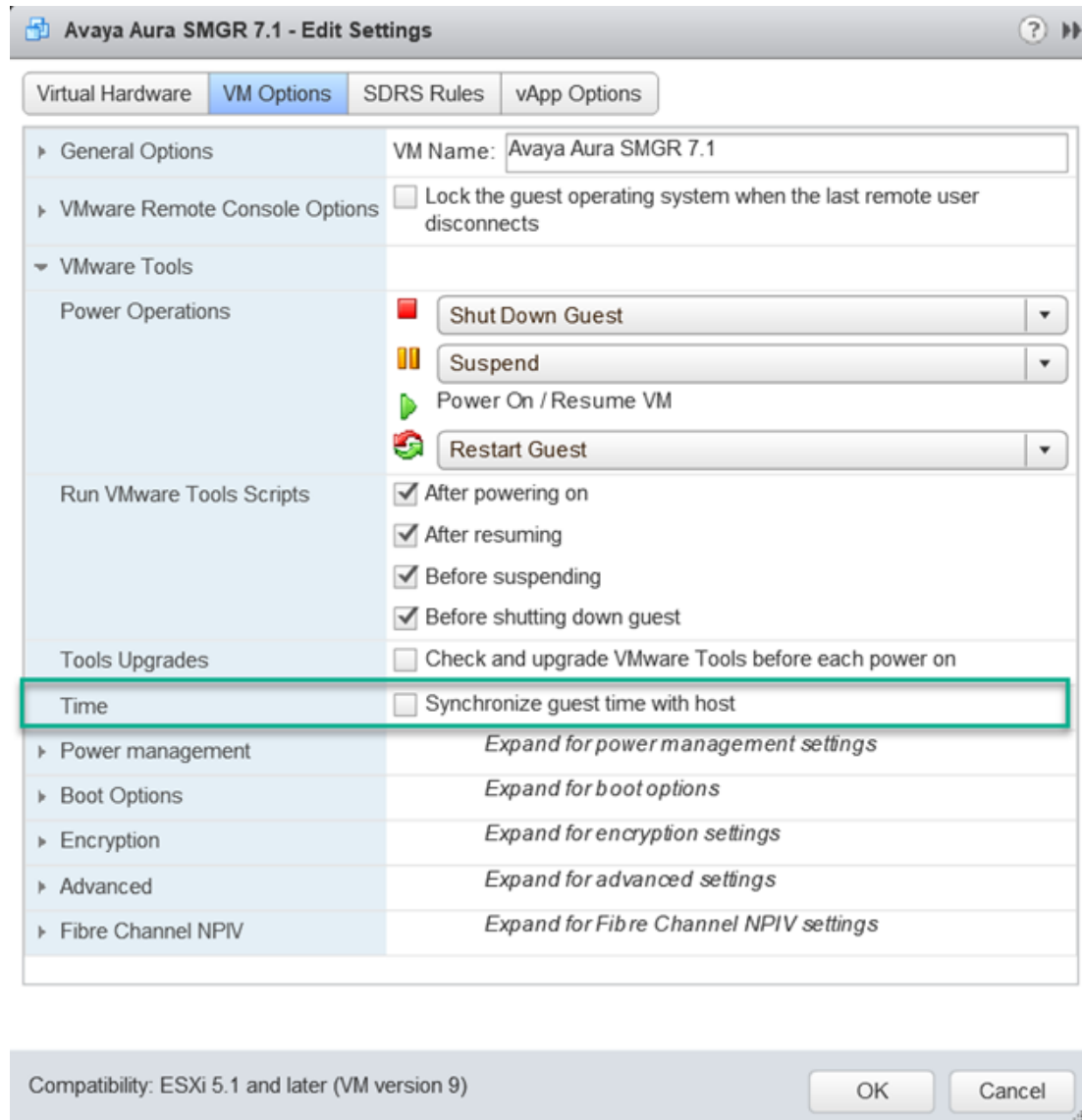
- Compute servers: For the ESXi and iLO interfaces, set Customer's NTP servers as primary NTP (NTP 1) server and secondary NTP (NTP 2) server, available in customer LCW.
- Network Switches: For primary NTP (NTP 1) server and secondary NTP (NTP 2) server, set the customer NTP server. Information available in customer LCW.
- Network Storage (both EMC and HPE Nimble): For primary NTP (NTP 1) server and secondary NTP (NTP 2) server, set the customer NTP server. Information available in customer LCW.
- Power Distribution Units: For primary NTP (NTP 1) server and secondary NTP (NTP 2) server, set the customer NTP server. Information available in customer LCW.
- G450 Media Gateways: For primary NTP (NTP 1) server and secondary NTP (NTP 2) server, set the customer NTP server. Information available in customer LCW.

Avaya Aura® application synchronization

*** Note:**

The instructions provided here are for all supported Avaya Aura® referenced in the Avaya Solutions Platform 4200 series documentation. See individual application deployment or administration documentation for instructions on updating the NTP settings for unsupported Avaya Aura® applications.

- For primary NTP (NTP 1) server and secondary NTP (NTP 2) server, set the customer NTP server. Information available in customer LCW.
 1. VMware Tools time synchronization should be disabled.
 - a. Connect to vCenter using the vSphere web client.
 - b. Select **Host and Cluster** view.
 - c. Right-click the Avaya Aura® application VM.
 - d. Click **Edit Settings**.
 - e. Select the **VM Options** tab.
 - f. Expand for **VMware Tools** settings.
 - g. Confirm **Synchronize guest time with host** is not checked.



- h. Clear the checkbox if it is selected.
 - i. Click **OK**.
 - j. Repeat these steps for all Avaya Aura® applications in the cluster.
2. Use the following commands to validate the status of VMware Tools time synchronization:
 - Linux-based applications:
 - a. Connect to the VM using PuTTY and SSH.
 - b. Log in using the administrative credentials.
 - c. Use the command `/usr/bin/vmware-toolbox-cmd timesync status` to validate time synchronization status.

*** Note:**

The following is an example of the command output:

```
[root@pod1]# /usr/bin/vmware-toolbox-cmd timesync status
Disabled
```

- Windows-based applications:
 - a. Open the Command Prompt.
 - b. Navigate to C:\Program Files\VMware\VMware Tools.
 - c. Use the command **VMwareToolboxCmd timesync status** to validate time synchronization status.

*** Note:**

The following is an example of the command output:

```
C:\Program Files\VMware\VMware Tools>VMwareToolboxCmd timesync status
Disabled
```

Applying the NTP server Hot Fix on ESXi server

Use the following procedure to configure ESXi to synchronize time with the Windows server Active Directory Domain Controller.

*** Note:**

Conduct the following procedure only if the customer NTP servers are windows base.

Procedure

1. Log in to the **vSphere Web Client** with administrator credentials.
2. Click on **Hosts and Clusters**.
3. Select the **ESXi host** from the list.
4. Click **Manage > Settings**.
5. Expand System and select **Time Configurations**.
6. Click **Edit**.
7. Enter the Windows server Domain Controller(s) information.

*** Note:**

For more information, see <https://kb.vmware.com/s/article/1035833>.

Configuring NTP synchronization for the Nimble CS1000

About this task

Use the following procedure to configure NTP synchronization for a Nimble CS1000.

Before you begin

Ensure that the Nimble array can connect to the NTP server. This procedure cannot be completed if the NTP server cannot be contacted.

Procedure

1. Open a new browser window or tab on the MSC.
2. Enter the management IP address of the storage array.
3. Log in to the management interface with the Administrator credentials.
4. Select **Administration > Date / Timezone** from the menu.
5. Select **Use NTP Server**.
6. Enter the IP address or FQDN of the Customer NTP server.
7. Select the applicable timezone from the **Time Zone** drop down list.
8. Click **Save**.

Configuring NTP synchronization for VNXe3200

About this task

Use this procedure to configure NTP synchronization for an EMC VNXe3200.

Before you begin

Ensure the VNXe3200 can connect to the NTP server. This procedure cannot be completed if the NTP server cannot be contacted.

Procedure

1. Log in to Unisphere using the appropriate credentials.
2. Select **Settings > Management Settings > Network > System Time Configuration** from the menu.
3. Click **Change Time Settings**.
4. Select the **Enable NTP synchronization** check box.
5. Enter the IP address of the NTP server.
6. Click **Add**.
7. Click **Apply**.

Deploying Avaya Diagnostic Server

About this task

Use the following procedure to deploy a new instance of Avaya Diagnostic Server(ADS).

Procedure

1. Log in to VCSA with administrator credentials.
2. Select **File > Deploy OVF Template** from the menu.
3. Click **Browse**.

4. Navigate to where the ADS OVA is stored.
5. Click **OK**.
6. Click **Network Mapping**.
7. Select **Out of Band Management** from the **Source Networks** column.
8. Click **Properties**.
9. Configure the properties of the virtual machine as specified in the following table.

Property	Value
Timezone setting	The applicable timezone.
Hostname	The fully qualified domain name of the virtual machine.
Default gateway	The default gateway for the virtual machine This is not necessary if DHCP is enabled.
DNS	The comma-separated list of DNS servers. This is not necessary if DHCP is enabled.
Network 1 IP Address	The IP address of the virtual machine. This is not necessary if DHCP is enabled.
Network 1 Netmask	The subnet mask of the virtual machine. This is not necessary if DHCP is enabled.
OOBM Selection	The out of bands management port setting. Disable the out of bands management port by selecting No.

10. Click **Next**.
11. Review the settings.
12. Click **Finish**.
13. The ADS OVA is deployed.
14. Connect to the ADS VM using SSH.
15. Log in using the `root` default credentials of `admin / admin01`.
16. You will be prompted to change the default password. Change the default password to `Avaya123$`.
17. The SSH session closes.
18. Start a new SSH session with the ADS VM.
19. Log in using the new `root` default credentials.
20. Enter the command `su - root`.
21. Enter the command `cd /installer`.
22. Enter the command `tar xvzf <name_of_installer.tar.gz> -C /tmp/`.
23. Enter the command `cd tmp/<name_of_installer_without_tar.gz>`
24. Enter the command `vi ADS_Response.properties`.

25. Set the following properties to the values shown.
 - ADS_AGREELICENSE=y
 - ADS_COMPONENT_TO_INSTALL=3
 - ADS_SLAMON_INSTALL=y
 - ADS_SAL_INSTALL=y
 - AGREE_ADS_COMPONENTS_CORESIDENT=y
 - WEBLMLOCAL=n
 - WEBLMIP=<SMGR_IP_address>
 - IPTABLES=y
 - SYSLOG=y
 - IPTABLESelect=true
 - SYSLOGSelect=true
 - SMTP_HOST=<SMTP_Host>
 - SMTP_PORT=<SMTP_Port>
 - SMTP_ADMIN_EMAIL=<SMTP_Admin_Email>
 - GATEWAY_SOLUTION_ELEMENTID=<SEID_from_LCW>
 - SPIRIT_ALARMID=<AlarmID_from_LCW>
26. Save changes to the properties file and close.
27. Enter the command `./install.sh -unattended`.
28. Wait for the installation to complete before proceeding.
29. Enter the command `cd /installer`.
30. Enter the command `tar xvzf <name_of_service_pack_installer.tar.gz> -c /tmp/`.
31. Enter the command `cd tmp/`
`<name_of_service_pack_installer_without_tar.gz>`
32. Enter the command `vi ADS_Response.properties`.
33. Set the property ADS_AGREELICENSE=y.
34. Save changes to the properties file and close.
35. Enter the command `./install.sh -unattended`.
36. Use the command `swversion | grep -i version` to confirm the installed version.
The version information should be as follows:
 - Avaya Diagnostic Server-3.0.0.0-vApp-e55-09

- Avaya Diagnostic Server Version: 3.0.1.0
 - SLAMon Server Version: 3.0.1.0-4176
 - SAL Gateway Version: 3.0.1.0-10
37. Log out of ADS.
 38. Log in to ADS with SSH using the `root` credentials.
 39. Use the command `/opt/avaya/slamon/bin/installdemocert` to install the demo certificate on the server.
 40. Enter `yes` to confirm certificate installation.
 41. Enter the command `systemctl restart slamonsrvr`.
 42. Enter the command `systemctl restart slamonweb`.

Deleting VMware snapshots

About this task

Use this procedure to delete VMware snapshots.

Procedure

1. Log in to vCenter using the vSphere Web Client.
2. From the host and the cluster view, locate the virtual machine in the client listing.
3. Right-click the virtual machine.
4. Select **Snapshot > Manage Snapshots** from the menu.
5. Confirm that snapshots exist for the virtual machine.
6. Click **All Actions > Delete All snapshots** to remove all snapshots.

Chapter 5: Resources

Resources

Documentation

The following documents are available on Avaya support site at <http://support.avaya.com/>:

Title	Description	Audience
Avaya Solutions Platform 4200 series		
<i>Avaya Solutions Platform 4200 series Solution Description</i>	Describes the key features of Avaya Solutions Platform	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Avaya Solutions Platform 4200 series Baseline</i>	Describes Avaya Solutions Platform 4200 series software and hardware baseline components.	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Avaya Solutions Platform 4200 series Read Me First</i>	Identifies Avaya Solutions Platform 4200 series media kit and refers to the documentation reference for all Avaya Solutions Platform 4200 series components.	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Documentation Reference for Avaya Solutions Platform 4200 series</i>	Identifies Avaya Solutions Platform 4200 series customer documentation as well as the Avaya and non Avaya products included in the Avaya Solutions Platform 4200 series solution, and lists the associated customer documentation.	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Installing and Maintaining the Avaya Solutions Platform 4200 series</i>	Describes how to install Avaya Solutions Platform 4200 series.	IT Management, sales and deployment engineers, solution architects, and support personnel.

Table continues...

Title	Description	Audience
<i>Upgrading Avaya Solutions Platform 4200 series using the Management Server Console</i>	Provides an overview of Management Server Console for Avaya Solutions Platform 4200 series. This document also provides instructions to access and use applications in the Management Console.	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Configuring and Administering Avaya Orchestrator</i>	Provides an overview of Avaya Orchestrator and instructions to access and use Avaya Orchestrator.	IT Management, sales and deployment engineers, solution architects, and support personnel.
<i>Avaya Solutions Platform 4200 series Troubleshooting</i>	Contains advice, solutions, and procedures for dealing with common issues encountered while using Avaya Solutions Platform 4200 series.	End users, Avaya certified technicians, Avaya partners, Avaya Sales Engineers (SE), Avaya System Integrators (SI).
<i>Avaya Solutions Platform 4200 series Interoperability Matrix</i>	Contains information on the hardware and software components supported in each release.	IT Management, sales and deployment engineers, solution architects, and support personnel.

Related links

[Finding documents on the Avaya Support website](#) on page 123

[Avaya Documentation Center navigation](#) on page 124

Finding documents on the Avaya Support website

Procedure

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

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

7. Click **Enter**.

Related links

[Documentation](#) on page 122

Avaya Documentation Center navigation

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

Important:

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

Using the Avaya Documentation Center, you can:

- Search for content using one of the following:
 - Type a keyword in **Search**, and click **Filters** to search for content by product, release.
 - From **Products & Solutions**, select a solution and product, and select the appropriate document from the list.
- Sort documents on the search results page by last updated dated and relevance.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection by using **My Docs** (☆).

Navigate to the **Manage Content > My Docs** menu, and do any of the following:

- Create, rename, and delete a collection.
 - Add topics from various documents to a collection.
 - Save a PDF of selected content in a collection and download it to your computer.
 - Share content in a collection with others through email.
 - Receive collection that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

Navigate to the **Manage Content > Watchlist** menu, and do the following:

- Enable **Include in email notification** to receive email alerts.
- Unwatch selected content, all content in a document, or all content on the Watch list page.

As a watcher, you are notified when content is updated or deleted from a document, or the document is removed from the website.

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

*** Note:**

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

Related links

[Documentation](#) on page 122

Training

Product training is available on the Avaya Learning website. For more information or to register, see <http://avaya-learning.com>.

Avaya Mentor videos

Avaya Mentor videos are available on an Avaya-run Internet channel dedicated to technical content.

Playlist categories include:

- Unified Communications (tested on Internet Explorer and Firefox).
- Contact Centers.
- Networking.
- Small and Midsize Business.
- Uploaded videos. A composite of all available Avaya Mentor videos.

Before you begin

You must have a valid Internet browser installed and working on your device.

About this task

The Avaya Mentor videos include the following content categories:

- How to install Avaya products.
- How to configure Avaya products.
- How to troubleshoot Avaya products.

Procedure

To go to Avaya Mentor videos, click the following link:

<http://www.youtube.com/avayamentor>

and perform one of the following actions:

- Enter a key word or words in the **Search channel** dialog box to search for a specific product or topic.

- Click the name of a playlist to scroll through the available videos.

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.

Related links

[Using the Avaya InSite Knowledge Base](#) on page 126

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to <http://www.avaya.com/support>.
2. Log on to the Avaya website with a valid Avaya user ID and password.
The system displays the Avaya Support page.
3. Click **Support by Product > Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

[Support](#) on page 126

Index

A

applying the NTP server Hot Fix on ESXi server [117](#)
Avaya support website [126](#)

C

checklist
 upgrade and patch [50](#)
collection
 delete [124](#)
 edit name [124](#)
 generating PDF [124](#)
 sharing content [124](#)
content
 publishing PDF output [124](#)
 searching [124](#)
 sharing [124](#)
 sort by last updated [124](#)
 watching for updates [124](#)

D

disassociating
 System Manager and Session Manager [69](#)
disassociating Communication Manager [69](#)
disassociating HPE iLO interface [68](#)
disassociating PDU [68](#)
disassociating Session Border Controller [70](#)
disassociating VMware ESXi [68](#)
disassociating VNXe3200 [68](#)
Disassociating VPFM from Applications and infrastructure
components [67](#)
disassociating VSP 7200 and VSP 4058 switches [67](#)
documentation [122](#)
documentation center [124](#)
 finding content [124](#)
 navigation [124](#)
documentation portal [124](#)
 finding content [124](#)
 navigation [124](#)

E

ESXi host
 Removing conflicting VIBs [90](#)

F

finding content on documentation center [124](#)

I

InSite Knowledge Base [126](#)

M

Management Server Console [12](#)
Manual Update [113](#)
Manual Upgrade [113](#)
Manual upgrade/update ESXi Hosts [113](#)
My Docs [124](#)

S

searching for content [124](#)
sharing content [124](#)
sort documents by last updated [124](#)
support [126](#)

U

Update ESXi Host [113](#)
Update ESXi Host using Command Line [113](#)
Upgrade ESXi Host [113](#)
Upgrade ESXi Host using Command Line [113](#)
upgrading
 Avaya Solutions Platform 4200 Series [39](#)
 HPE driver [79](#)
 Qlogic driver [79](#)

V

validating
 vCenter Server Appliance certificate [74](#)

W

watch list [124](#)