Upgrading Avaya Converged Platform 4200 Series using the Management Server Console

Release 4.0
Issue 4
September 2019

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

Heritage Nortel Software

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

Copyright

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

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. 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.

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.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Contents

Chapter 1: Introduction

Purpose

This document provides information and tasks for using the Management Server Console for Avaya Converged 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 Converged Platform 4200 series solution applications and the basic workings of VMware vSphere and Microsoft Windows Server.

Product registration

To prevent service interruption, you must register your Avaya Converged 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.

Management Server Console

The Management Server Console (MSC) is a Microsoft Windows 2016 Standard Edition server virtual machine provided on all Avaya Converged Platform 4200 series Release 4.0. The MSC provides software and utilities to manage and upgrade the Avaya Converged Platform 4200 series Release 4.0 software and components.

Important:

Ensure the Avaya Converged Platform 4200 series Release 4.0 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
- Mozilla Firefox
- Notepad++
- Wireshark
- WinSCP
- PuTTY
- Unisphere thick client
- DNS server enabled
- TFTP server

Avaya Pod Fx upgrades to Avaya Converged Platform 4200 series Release 4.0

Preexisting Avaya Pod Fx platforms can upgrade to Avaya Converged Platform 4200 series Release 4.0 software. For information on supported upgrade paths, see Supported upgrade paths on page 15.

Important:

The Avaya Pod Utility Module has been removed from the Management Server Console software in Release 3.1. Upgrade using the procedures documented in *Upgrading Avaya Converged Platform 4200 series using the Management Server Console* Release 4.0.

Avaya Converged Platform 4200 series Release 4.0 upgrades must be performed by Avaya Professional Services, or by Avaya Converged 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 Converged Platform 4200 series Release 4.0 upgrade, update the following components to the Release 4.0 software baseline:

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

Warning:

Avaya Converged Platform 4200 series Release 4.0 supports VMware release 6.5 and Avaya Aura® release 8.0. 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 Converged Platform 4200 series Release 4.0.

For more information about performing Avaya Converged Platform 4200 series infrastructure upgrades, see Upgrading Avaya Converged Platform 4200 series on page 14

It is recommended that you perform the Avaya Converged Platform 4200 series Release 4.0 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 Converged Platform 4200 series Release 4.0 such as additional storage or servers. To schedule a design review, email acpsales@avaya.com.

Avaya Orchestrator

The Avaya Orchestrator Release 1.4 is a visualization and management application which is used to monitor Avaya Converged Platform 4200 series Release 4.0. Starting with Avaya Converged 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 Converged 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 Converged 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 1.4, 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 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 Converged Platform 4200 series platforms.

Connecting to the Management Server Console

You can access the MSC when the virtual appliance server is deployed and running.

About this task

Use the procedure to remotely connect to the MSC.

Procedure

1. Access the Avaya Converged Platform 4200 series Release 4.0 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*.

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 4.0 builds.

   A request must be sent to acpsales@avaya.com when upgrading to Release 4.0 software. The request must ask for the Avaya Converged Platform 4200 seriesRelease 4.0 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

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.

Chapter 4: Upgrades

Upgrading Avaya Converged 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 Converged Platform 4200 series Release 4.0 infrastructure.
- VMware vCenter and ESXi software
- Deploy new Avaya Orchestrator virtual machine
- Avaya Aura® Virtualized Environment software (Session Manager and Communication Manager)
- Avaya network switches software and firmware
- EMC storage array software and firmware
- 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 4200 series Release 4.0, as Avaya Orchestrator operates independently, there is no dependency on the version of System Manager.

Note:

When deploying OVAs using vSphere 6.5 webclient on Internet Explorer (IE), deployment fails with multiple error messages. Therefore, starting with Avaya Converged Platform 4200 series Release 4.0, deploy OVAs using Mozilla Firefox that is installed on the Management Server Console.

Supported upgrade paths

You can upgrade previous CPOD and Pod Fx releases to Avaya Converged Platform 4200 series Release 4.0 software. Starting with Avaya Converged Platform 4200 series Release 4.0, 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 Converged Platform 4200 series Release 4.0 upgrades must be performed by Avaya Professional Services or by Avaya Converged 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 CPOD and Pod Fx releases to Avaya Converged Platform 4200 series Release 4.0:

Note:

Infrastructure components not specifically listed in this table can be upgraded to its corresponding firmware or software version supported under the Avaya Converged Platform 4200 series 4.0 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 Converged Platform 4200 series Release 4.0	Direct Upgrade
4200 CPOD 1.0 /2.0 / 2.0.1 / Hardware	Not supported. **Software limitation:** • Upgrade from VMware 5.1.X to 6.5 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. • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Hardware limitation:** Lenovo servers are end of life and end of support. ESXi 6.5 is not supported by vendor on Lenovo servers.	Not supported. Last fully supported release: Pod Fx 3.1.
2400 CPOD 2.1	Supported. **VMware:** Vendor supports direct upgrade from release 5.5.x to 6.5. This includes vCenter Server Appliance and ESXi. **Extreme switches:** Vendor does not support direct upgrade from VOSS 4.1 to VOSS 7.1.1. 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. **Management Server Console:** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Considerations:** Validate if existing Avaya applications running in the cluster are supported within VMware release 6.5 prior to upgrading the VMware infrastructure.	Partially supported.

Table continues…

From	To Avaya Converged Platform 4200 series Release 4.0	Direct Upgrade
4200 / 2400 CPOD 2.1.1 Hardware	Supported. **VMware:** Vendor supports direct upgrade from release 5.5.x to 6.5. This includes vCenter Server Appliance and ESXi. **Extreme switches:** Vendor does not support direct upgrade from VOSS 4.2.1 to VOSS 7.1.1. 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. **Management Server Console:** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Considerations:** Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 prior to upgrading the VMware infrastructure. Excludes racks with Lenovo servers.	Partially supported.

Table continues…

From	To Avaya Converged Platform 4200 series Release 4.0	Direct Upgrade
4200 / 2400 Pod Fx 3.0 Hardware	Supported. **VMware:** : Vendor supports direct upgrade from release 5.5.x to 6.5. This includes vCenter Server Appliance and ESXi. **Extreme switches:** Vendor does not support direct upgrade from VOSS 5.0.1 to VOSS 7.1.1. 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. **Management Server Console:** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Considerations:** Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 prior to upgrading the VMware infrastructure. Excludes racks with Lenovo servers.	Partially supported.

Table continues…

From	To Avaya Converged Platform 4200 series Release 4.0	Direct Upgrade
4200 / 2400 Pod Fx 3.0.1 Hardware	Supported. **VMware:** Vendor supports direct upgrade from release 5.5.x to 6.5. This includes vCenter Server Appliance and ESXi. **Extreme switches:** Vendor does not support direct upgrade from VOSS 5.1.1 to VOSS 7.1.1. Upgrade to VOSS 6.1.X first. **Management Server Console:** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Considerations:** Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 prior to upgrading the VMware infrastructure. Excludes racks with Lenovo servers.	Partially supported.

Table continues…

From	To Avaya Converged Platform 4200 series Release 4.0	Direct Upgrade
4200 / 2400 Pod Fx 3.0.2 Hardware	Supported. **VMware:** Vendor supports direct upgrade from release 6.0.x to 6.5. **Extreme switches :** Vendor does not support direct upgrade from VOSS 6.0.1.1 to VOSS 7.1.1. Upgrade to VOSS 6.1.X first. **MSC :** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. • Avaya Converged Platform 4200 series 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC. **Considerations:** Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 prior to upgrading the VMware infrastructure. Excludes racks with Lenovo servers.	Partially supported.
4200 / 2400 Pod Fx 3.1 Hardware	Supported. **MSC:** • Windows 2008 MSC cannot be upgraded to Windows 2016. New OVA deployment is required. **Considerations:** Validate if existing Avaya applications running in the cluster are supported in VMware release 6.5 prior to upgrading the VMware infrastructure. Excludes racks with Lenovo servers.	Supported.

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. Starting in Avaya Aura® System Manager Release 7.1, a valid license is required for normal operation.

4. For Avaya Orchestrator license requirements, see *Configuring and Using Avaya Orchestrator*.

5. A new license for VCSA and ESXi will be required when upgrading from VMware 5.5.x to 6.5.

6. Proceed with the upgrade as outlined in Checklist for upgrading and patching Avaya Converged Platform 4200 series on page 21.

Checklist for upgrading and patching Avaya Converged 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://support.avaya.com/css/P8/documents/101050559) 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 8.0*
- *Checklist for upgrading System Manager vAppliance Release 6.3.x in the Geographic Redundancy setup to Release 8.0*

Note:

Avaya recommends that you install important Windows updates on the Windows Virtual Machines running on an Avaya Converged 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® 8.0. Go to 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 before upgrading.
- Verify that you have separated the VMkernels for iSCSI and vMotion. For more information see *Installing and Maintaining the Avaya Converged Platform 4200 series*.

  Note:

  This is not necessary for Avaya Converged 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 Converged 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 93.
- See Deploying Avaya Diagnostic Server on page 90 for instructions on deploying Avaya Diagnostic Server.
- Ensure 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. **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.

  2. **vCenter**

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

3. **ESXi hosts**

   Confirm 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.

4. **Switches**

   Confirm the ports used to connect the switches to the EMC or Nimble storage arrays in the *Lifecycle Customer Workbook*. Connect to both switches and check the status of these ports. Confirm 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 20.

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	• Avaya Converged Platform 4200 series Release 4.0 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 *Supported Upgrade Paths* 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.
HPE compute server firmware upgrade	Yes	Yes	• 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 Converged 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.

Table continues…

Activity	Software Dependency	Compatibility Dependency	Dependencies
VMware vCenter Server Appliance upgrade	No	Yes	• 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	• This activity must be performed after upgrading VCSA. • Validate 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	• This activity can be performed at the beginning or end of the upgrade when 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 end of the upgrade when best fits the scheduled resources.
PDU firmware upgrade	No	No	This activity can be performed at the beginning or end of the upgrade when 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 Converged Platform 4200 series.

Table 1: High-level upgrade task list

No.	Task	Description	Location	✔
1	Validate existing VMware EVC settings on cluster.	• Validate if EVC is enabled on existing Pod Fx solution. • If EVC feature is currently disabled, enable the feature before upgrading to Avaya Converged Platform 4200 series release 4.0. • For more information on validating and enabling EVC feature, see *PSN005315u* on Avaya support website. **Note:** If EVC feature is disabled, plan in advance and request, on a separate maintenance windows, before conducting the upgrade to Avaya Converged Platform 4200 series 4.0, permission from the customer to conduct the necessary steps to enable EVC on the VMWare cluster.		
2	(Optional) Obtain the network information used to deploy the latest MSC from the *Customer Lifecycle Workbook*.			

Table continues…

No.	Task	Description	Location	✔
3	a. Identify the required software updates. b. Download the required software, patches and OVAs to a PC or USB storage device. **Important:** All updates and firmware files are available for download from the Avaya Support website in the Release 4.0 section. See Download new software on page 30.	• Download the required files to update the MSC and prepare for a Avaya Orchestrator update. **Important:** Deploying the latest MSC OVA is not mandatory but is strongly encouraged to ensure the latest security patches and updates are applied. • Locate and download the VMware vCenter upgrade files. • Locate and download the supported patches and the vCenter Server update. **Important:** Do not download any other patches from the VMware website. • Locate and download the VSP 4000, VSP 7000, and VSP 7200 switch upgrade files. • Locate and download the EMC VNX firmware files. **Note:** To determine if your Avaya Converged Platform 4200 series firmware requires upgrading, see the upgrade section of this checklist. • Locate and download Avaya Aura® patches and other application updates. • Locate and download the Nimble firmware files.		
4	Deploy the new MSC OVA.	Deploying a new MSC OVA takes approximately 15 minutes for an on-site deployment. ACP 4.0 MSC OVA cannot be deployed on VMware 5.X. Upgrade VMware infrastructure to 6.5 first, using existing MSC.		
5	Perform the following upgrades in the order shown:			
	a. Transfer upgrade files from a SCP compatible file server or from a USB device to the `ACP_SW_4.0` directory on the updated MSC.	Manually move the software files to the specific subdirectory in the `ACP_SW_4.0` directory.	See Transferring files on page 31. For more information about the directory structure, see Software and OVA repository on page 29.	

Table continues…

No.	Task	Description	Location	✔
	b. Upgrade compute server firmware. **Important:** This step is mandatory and critical to the successful upgrade of the Avaya Converged Platform 4200 series. Complete this step before proceeding to the next step.	See Upgrading server firmware on page 76 for instructions on updating HP servers. **Important:** Compute servers must be placed in Maintenance Mode before installing updates. This tasks takes up to 45 minutes to complete including the host reboot. **Important:** For existing Avaya Pod Fx series with the Release 3.x hardware and Avaya Converged Platform 4200 series Release 4.0 hardware, use the files `ilo4_261.bin` and `ilo5_137.bin` 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 Converged Platform 4200 series with HPE Gen 8 servers and Avaya Converged Platform 2400 series, the iLO firmware is upgraded when the HP SPP ISO is executed . See Upgrading the HPE iLO firmware on page 79 for information and procedures on installing this separate upgrade.		
	c. Upgrade the VMware vCenter Server Appliance	See Upgrading to VMware vCenter Server Appliance 6.5 Update 2d on page 40. This task takes up to 30 minutes to complete.		
	d. Enable ESXi shell access and SSH			
	e. Upgrade ESXi hosts to VMware ESXi 6.5	See Using VUM to update ESXi hosts on page 50. **Note:** Ensure all running Avaya Aura® applications in the cluster supports VMware vSphere 6.5 before upgrading to ESXi 6.5. Upgrade Avaya Aura® applications to Release 8.0 as required, before proceeding with VMware ESXi upgrade.		
	f. Migrating to Avaya Orchestrator from POS Application	See *Configuring and Using Avaya Orchestrator*.		
	g. Upgrade additional compute server firmware.	For more information, see Installing VMware ESXi 6.5 patches using VUM on page 57 and Configuring vSphere Update Manager on page 50.		

Table continues…

No.	Task	Description	Location	✔
	h. Upgrade the switches.	See Upgrading the switches on page 60 . This task takes up to 30 minutes to complete. Have a console cable available while performing this task.		
	i. Upgrade the firmware for storage devices.	See Upgrading storage devices on page 69. **Important:** It is mandatory to upgrade the firmware of EMC storage devices to the latest firmware version during an upgrade cycle. Upgrading EMC firmware can take from 75 minutes up to several hours to complete. Upgrading Nimble firmware takes up to 60 minutes to complete. For more information, see Installing VMware ESXi 6.5 patches using VUM on page 57.		
	j. Upgrade the firmware for PDUs.	Download and install the appropriate firmware file based on your PDU type. See Upgrading PDU firmware on page 80. 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, verify the G450 Media Gateway is running this software:`g450_sw_40_10_1.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 7.2.2 using the applicable documentation.	Obtain the latest Avaya SBCE documentation for Release 7.2.2.		

Table continues…

No.	Task	Description	Location	✔
	n. Additional applications that are not part of the upgrade process require manual updates.	Obtain software update instructions from each product support site.		
6	(Optional) Configure NTP time source or synchronize to an external time source.	See Configuring NTP on page 83.		
7	Remove previous software versions.	It is a good practice to remove software versions that are no longer used by the components of the Avaya Converged Platform 4200 series Release 4.0. This includes components such as switches, storage arrays, and PDUs. See the product documentation for these components for procedures on removing old software versions.		
8	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 20. Use the procedure at this link to re-host the licenses if necessary.		
9	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 93 for the procedure to delete snapshots.		
10	Current factory builds of Avaya Converged Platform 4200 series are implementing improved best practices that optimize performance. Deployed Avaya Converged 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 Converged Platform 4200 series solution. This is not applicable to Avaya Converged Platform 4200 series solutions with Nimble storage devices.	See Product Support Notice *PSN004864r1* for information and procedures for executing the optimization script.		

Software and OVA repository

The software and OVAs for upgrades, patches, and deployment must be located on the `E:\ACP_4.0_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:\ACP_4.0_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 Converged Platform 4200 series Release 4.0 from the Avaya Support site support.avaya.com. Store the files in the specified subdirectories in the E:/ACP_4.0_SW directory of the MSC.

Filename	Instructions
Management Server Console OVA: Avaya Converged Platform 4.0.0.0.1.ova	Place the file in the following directory: E:\ACP_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:\ACP_4.0_SW/AO_and_Infrastructure/Avaya_Orchestrator
Avaya Aura® System Manager OVA: • 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:\ACP_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:\ACP_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:/ACP_4.0_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 30.
- 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:/ACP_4.0_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:\ACP_4.0_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 Converged Platform 4200 series Release 4.0, 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:\ACP_4.0_SW\` directory folder structure and the files required for each release upgrade.

VMWare	6.5-Updates	ESXi 6.5 P03- build 10884925
		vCenter U2d-Build 10964411
Management_Server	MSC Primary	Avaya Converged Platform 4.0.0.0.1.ova
ADS		AvayaDiagnosticServer-3.0.0.0-vApp-e55-09.ova
IDE	Dashboard	IDE_9.5.0_DASHBOARD.zip
	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_7_0_02-040318.zip (9608/9608G/9611G/9621G/9641G)
		96x1-IPT-H323-R6_7_0_02U-040318.zip(Encrypted)
		96xx-IPT-H323-R3_2_8-091517.zip (9620L/9620C/9630G/9640/9640G/9650/9650C/9670G)
	SIP	96x1-IPT-SIP-R7_1_3_0-081318.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-3.1.8.9809862.tgz.bin.gpg
Nimble	CS1000 Firmware	NimbleOS-5.0.6.0-593144-opt.update.v2
	Nimble Plugin for ESXi 6.5	nimble-ncm-for-esx6.5-5.1.0-650006.zip
PDU Sentry 3	swcdu-v71c.bin	
	smcdu-v71c.bin	
PDU Sentry 4	pro-v80k.bin	
HP SPP	G9	
	G10	
G450	g450_sw_40_10_1.bin	
SBC	HW	sbce-7.2.2.0-11-15522.iso
	VE	sbce-7.2.2.0-11-15522.ova
VSP_Switches	VSP4000	VOSS4K.7.1.1.0.tgz
		VOSSv711_HELP_EDM_gzip.zip

Table continues…

	VSP7200	VOSS7K.7.1.1.0.tgz
		VOSSv711_HELP_EDM_gzip.zip
AAC	vAAC_MediumSimplex_MCP_18.2.7-2018-09-01-1845-1vDisk150Gb_8vCPU_24GBMemory.ova	
	vAAC_Platform_MCP_18.2.7-2018-08-19-2209-1vDisk150Gb_8vCPU_24GBMemory.ova	
	vAAC_MediumPrimary_MCP_18.2.7-2018-09-06-2000-1vDisk150Gb_8vCPU_24GBMemory.ova	
	vAAC_MediumSecondary_MCP_18.2.7-2018-09-06-2000-1vDisk150Gb_8vCPU_24GBMemory.ova	
ACR	acr-152-linux.iso	
	acr-152-windows.iso	
AWFO Select	Awfos_5_2_2.exe	
AES	AES-8.0.1.0.0.5.20181122-e65-00.ova	
AAM	AAM-07.1.0.0.532-e65-0.ova	
AMM	amm-3.5.0.0.263_OVF10.ova	
Equinox MS	EquinoxMediaServer_9_1_0_12_1_OVA.zip	
Equinox MGMT	EquinoxMgmt_9_1_0_8_4_OVA.zip	
Equinox Edge	EquinoxEdge_9_1_0_1_11_OVA.zip	
Equinox Streaming & Recording	EquinoxRecordingGW_9_1_0_17_3.zip	
	assr-system-components-9.1.0.1.002.zip	
	System Components (Windows) aesr-ce-system-9.1.0.3.1.zip	
	manager-9.1.0.227-bin.zip	
	Conference Point - aesr-ce-system-9.1.0.3.1.zip	
	Transcoder - aesr-ce-9.1.0.4.1-Transcoder-9.1.0.6681.zip	
	System Components (Conference Point) 9.0.0.0.22	
	Delivery Node - aesr-dn-9.1.0.1.2.zip	
	Scopia Elite - MCU_8_4_1_12.zip	
	System Components (Delivery Node) aesr-dn-system-9.1.0.1.5.zip	
AMS	MediaServer_8.0.0.169_A6_2018.10.24_OVF10.ova	
CM	CM-Simplex-08.0.0.0.822-e67-1.ova	
	CM-Duplex-08.0.0.0.822-e67-1.ova	
CMS	CMS-R18.1.0.1.ra.d-e65-00.ova	
Breeze	Breeze-3.6.0.0.360009.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	

Table continues…

PS	PresenceServices-Bundle-8.0.1.0.296.zip	
SM	SM-8.0.0.0.800035-e67-01.ova	
SDMClient	Avaya_SDMClient_win64_8.0.1.0.0332099_11.zip	
SMGR	SMGR-PROFILE3-8.0.0.0.931077-e65-18.ova, SMGR-8.0.0.0.931077-e65-18.ova	
US-Utility Services	US-7.1.0.0.0.18-e55-2_OVF10.ova	
SAL	SecureAccessLinkGateway-3.0.0.0-vApp-e55-06.ova	
WebLM	WebLM-8.0.0.0.9-31370-e65-13.ova	
Avaya ANAV	ANAV.4.1.1.200.Full.zip	
Patches	AAC	mcp_core_linux_ple2-18.2.9.iso
		mcp_core_linux_ple2-18.2.9.patches.r-1.ext.iso
		dvd_AAC_MCP_18.2.7.00_2018-08-19-2209_coreApps.iso
	AMM	amm-3.5.1.0.22.bin
	ADS	ADS-ServicePack-3.0.4.0-582.tar.gz
	AES	aesvcs-8.0.1.0.0.5-featurepack.bin
		80_LSUPatch1.bin
	ACR	acr-15.2-1013.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
	Aaura Control Manager - ACCCM	Avaya_ACM_8.0.4.0.1.200_Patch.zip
	AWFO Select	Awfos_5_2_2_Patch_0.zip
	AAMS	MediaServer_System_Update_8.0.0.13_2018.11.07.iso
		MediaServer_Update_8.0.0.173_2018.11.05.iso
	AAM	01.0.532.0-24811.tar
		KERNEL-3.10.0-693.21.1.el7.AV1.tar
		C24012pt+a.rpm
		m71532_002pt+a.rpm
		A22011pt+a.rpm
		PLAT-rhel7.2-0030.tar

Table continues…

	CM	KERNEL-3.10.0-862.3.2.el7.tar
		00.0.822.0-25031.tar
		PLAT-rhel7.4-0020.tar
	CMS	r18ka.p_cmsp1-l.bin
	EliteMultichannel	
	EP	epavl-7.2.0.0.1810.tar.gz
		7.2.1.0.0622.tar.gz.sig
		7.2.1.0.0622.tar.gz
		EPM-7.2.1.0.0605.tar.gz
	POM	POMPDC_311.zip
		POM3111Patch01.zip
		POMDesktopAPI_3_1_1_033.zip
		POMDesktopJavaAPI.zip
	Equinox	EquinoxMediaServer_9_1_0_16_1.zip
		EquinoxMgmt_9_1_0_16_32.zip
		EquinoxEdge_9_1_0_12.zip
	SM	Session_Manager_8.0.1.0.801007.iso
		System_Manager_8.0.1.0_r801008826.bin
	US	util_patch_7.1.3.2.0.01.zip
	WebLM	WebLM_8.0.1.0_r801008761.bin
	POM	POM3111Patch01.zip
ISO_files	CMS	700514308_CMS-R18.1.0.0.pa.e_SFTW_DVD_LINUX.iso
	CallCenterEliteMultichannel	EMC_6_5_0_3.iso
	EP	AAEP-7.2.0.0.1117.iso
		AvayaLinux-RH6.8.64-AV07EP72.30May17.194049.iso
	OCEANA	OCEANA_3.5.0.0-12.iso
		Complete Software Suit for Oceana 3.5 is included in folder structure
	ACCCM	ACM_8.0.4.0_583_20180924_2305.iso
	POM	POM.03.01.01.01.00.003-r35434-x86_64.iso
	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 15.

If your system's hardware is not supported with Avaya Converged Platform 4200 series Release 4.0, contact the Account Manager.

Before you begin

- With Avaya Converged Platform 4200 series Release 4.0, 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 Converged 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 37.
    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 37.

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 37.

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 2d

About this task

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

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 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, 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=N4IghgNiBcILYEsDmAnMAXBB7AdgAjAGdCFD0wd0QBfIA.

  Note:

  The VMware migration assistant file `VMware-Migration-Assitant.exe` is available within the `ACP_40_VMware-VCSA-all-6.5.0-10964411.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 has 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 is required.

Use the following procedure to upgrade to VMware vCenter Server Appliance 6.5 Update 2d from VMware vCenter Server Appliance 5.5 or 6.0.

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 47.
- You will need a new license key when upgrading to Release 6.5 from Release 5.5. You will not need a new license key when upgrading from Release 6.0 to Release 6.5. Contact acpprodmgt@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 44.

Procedure

1. Copy the `VMware-VCSA-all-6.5.0-10964411.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 2d on page 45.
- See Assigning a license key on page 45.

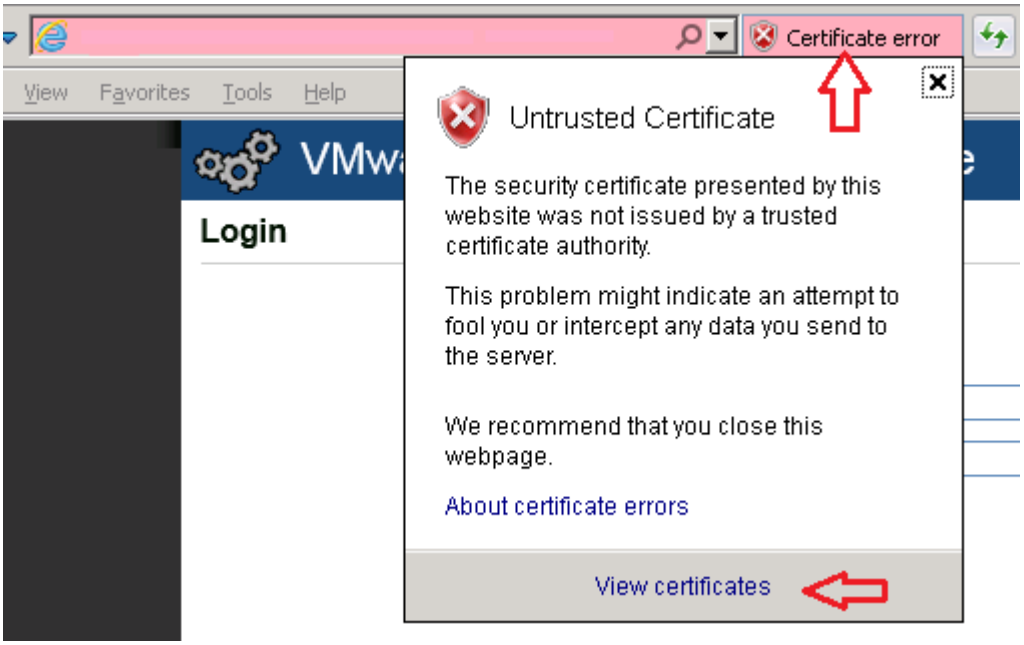
Validating vCenter Server Appliance certificate

About this task

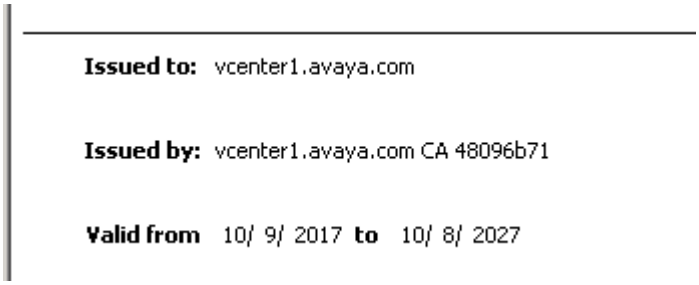
Use this procedure to validate vCenter Server Appliance certificate.

Procedure

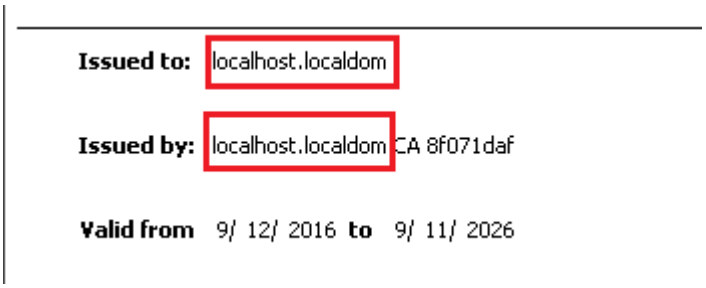
1. Log in to the Management Server Console.
2. Open a new browser tab in Microsoft Internet Explorer.
3. Navigate to `https://<vCenter_IP_Address>:5480`.
4. Click **Certificate error**.
5. Click **View certificates**.



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



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 49 to regenerate the certificate before continuing.



Applying license key to the VMware vCenter Server Appliance 6.5 Update 2d

About this task

Use this procedure to apply the new Release 6.5 license key to the VMware vCenter Server Appliance 6.5 Update 2d.

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.

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 servers.

Important:

For fresh installations this procedure would not be required, its only required when doing upgrades from CPOD 2.1.x and Pod Fx 3.x to Avaya Converged Platform Release 4.0.

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 `QLG-bnx-6.0-8174539.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 QLG-bnx-6.0-8174539.zip`**
   b. **`reboot`**
7. Follow boot up process from the iLO remote console.
8. 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.
9. Proceed with remaining hosts by repeating steps from step 2 to step 7. Always perform the drivers update with one host at a time.
10. For driver validation from the ESXi command-line interface, run **`esxcli software vib list | grep net-bnx2x`**

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 50 to configure VUM with upgrade and update baselines.
- See Upgrading VMware ESXi 5.5 and 6.0 to 6.5 Update 2 on page 55 for upgrading ESXi hosts to the current ESXi release.
- See Installing VMware ESXi 6.5 patches using VUM on page 57 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 4.0 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 57 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-Update2-9298722-HPE-Gen9plus-650.U2.10.3.5.5-Sep2018.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 Converged Platform – ACP 4200 4.0.x and save it on the `E:\` drive.
   - For HPE Gen 8 servers, download the iso file named `ACP_40_VMware-ESXi-6.5.0-Update2-9298722-HPE-preGen9-650.U2.9.6.8.3-Sep2018.iso` from https://support.avaya.com/downloads/ for Avaya Converged Platform – ACP 4200 4.0.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, `ACP 4200 – Upgrades`.
10. In the **Description** field, type the description `Upgrade to 6.5 U2 for the baseline`.
11. Select baseline type as **Host Upgrade**, then click **Next**.
12. Select an ESXi image from the list, then click **Next**.
13. Click **Finish**.

    Note:

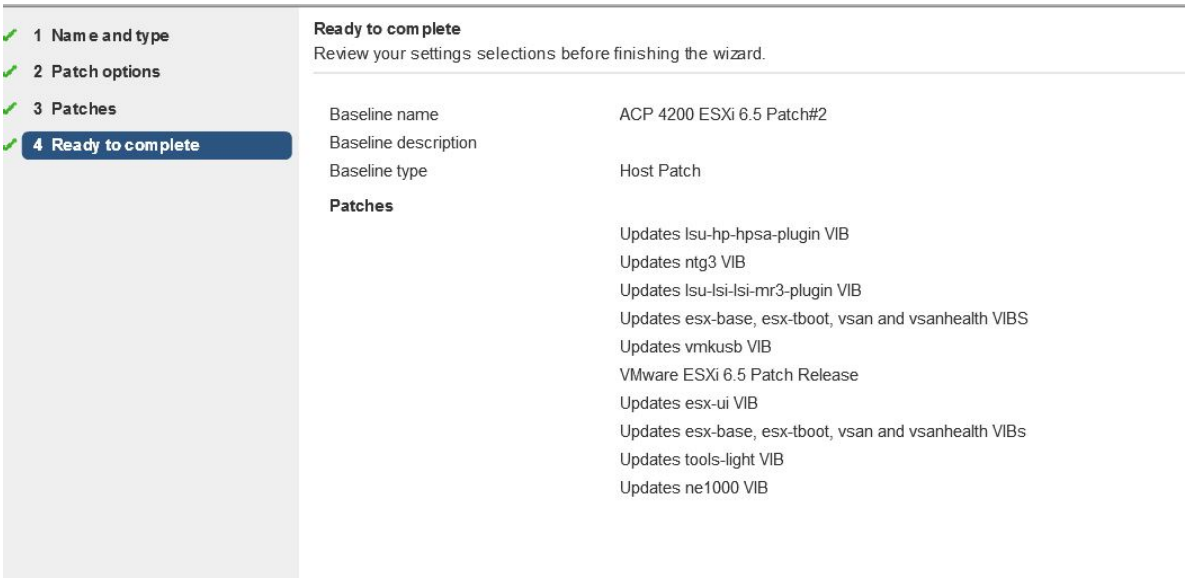
    The ISO is imported and ready for use in upgrades.
14. On the **Patch Repository** tab, click **Import Patches**.
15. Click **Browse**.
16. Locate the patch file `ESXi650-201811002.zip`.
17. Click **Open**.
18. Click **Next**, then click **Finish**.
19. On the **Hosts Baselines** tab, click the green plus sign button on the left to create a new baseline.

20. In the **Name** field, type the name of the new baseline, `Avaya Converged Platform 4200 series 4.0 - Updates`.
21. In the **Description** field, type the description of the new baseline, `VMware ESXi 6.5 Patches`.
22. Select **Hosts Patch**, then click **Next**.
23. 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.
24. Sort the patches by **Release Date**.
25. Select the following patches that are released on 11/28/2018 for ESXi 6.5, then click the down arrow.
    - `Updates lsu-hp-hpsa-plugin VIB`
    - `Updates ntg3 VIB`
    - `Updates lsu-lsi-lsi-mr3-plugin VIB`
    - `Updates esx-base, esx-tboot, vsan and vsanhealth VIBS`
    - `Updates vmkusb VIB`
    - `VMware ESXi 6.5 Patch Release`
    - `Updates esx-ui VIB`
    - `Updates esx-base, esx-tboot, vsan and vsanhealth VIBs`
    - `Updates tools-light VIB`
    - `Updates ne1000 VIB`
26. Click **Next**.

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



28. On the **Patch Repository** tab, click **Import Patches**.
29. Click **Browse**.
30. Locate the patch file `QLG-bnx-6.0-offline_bundle-8174539.zip`.
31. Click **Open**.
32. Click **Next**, then click **Finish**.
33. Click **Import Patches**.
34. Click **Browse**.
35. Locate the file `nimble-ncm-for-esx6.5-5.1.0-650006.zip`.
36. Click **Open**.
37. Click **Next**, then click **Finish**.
38. On the **Hosts Baselines** tab, click the green plus sign button on the left to create a new baseline.
39. In the **Name** field, type the name of the new baseline, `Avaya Converged Platform 4200 series 4.0 - HPE Patches`.
40. In the **Description** field, type the description of the new baseline, `HPE drivers for VMware ESXi 6.5`.
41. Select **Hosts Patch**, then click **Next**.
42. Select **Fixed**, then click **Next**.

Important:

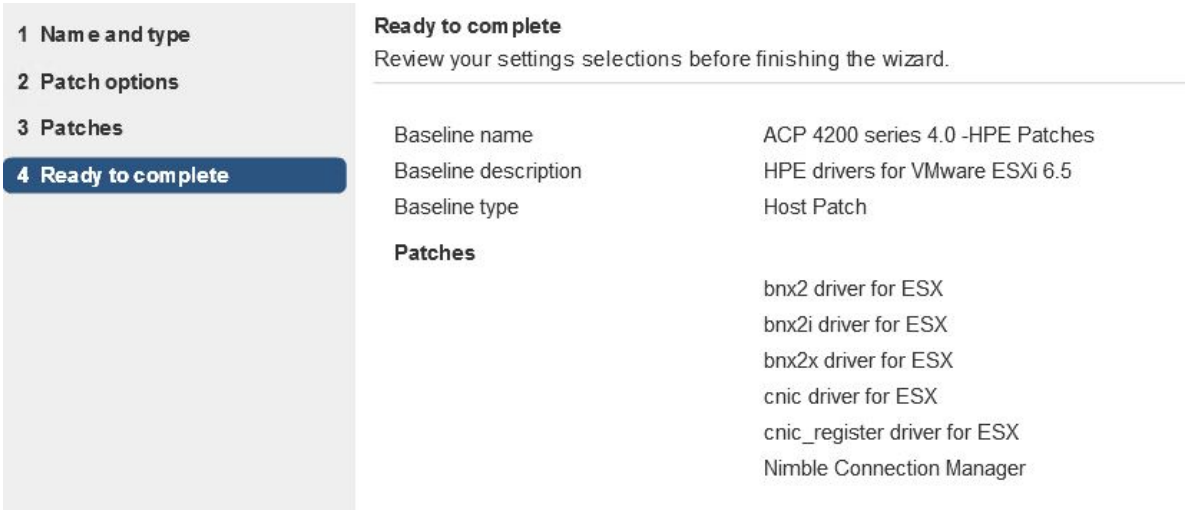
Always add Avaya-approved patches, even if they are not included in the current baseline or listed in the *Release Notes*, prior to any maintenance activity.

43. Type `Qlogic` in the search filter, then press `Enter`.
44. Select the following patches, then click the down arrow.
    - `bnx2 driver for ESX`
    - `bnx2i driver for ESX`
    - `bnx2x driver for ESX`
    - `cnic driver for ESX`
    - `cnic_register driver for ESX`

    Important:

    Do not select `bnx2fc driver`.
45. Type `Nimble` in place of Qlogic in the search filter, then press `Enter`.
46. Select the following patches, then click the down arrow.
    - `Nimble Connection Manager`
47. Click **Next**.
48. Review the list of selected patches.

    The Ready to complete page should display 6 patches.



49. Click **Finish**.
50. On the **Hosts Baselines** tab, click the green plus sign button on the right to create a new baseline group.
51. In the **Baseline group name** field, type the baseline group name `Avaya Converged Platform 4200 series - 4.0 Baseline`.

52. In the **Description** field, type `4.0 Baseline group` and click **Next**.
53. Select the upgrade baseline created in steps 8–13, then click **Next**.
54. Select the updates baseline created in steps 19–27, then click **Next**.
55. Select the HPE patches baseline created in steps 28–49, then click **Next**.
56. Click **Next** to skip extensions.
57. Review the selections, and click **Finish**.
58. Go to **Settings** > **Host/Cluster Settings**, and click **Edit**.
59. Select the **Temporarily disable any removable media** checkbox.
60. 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.
61. Set the retry delay time to 2 minutes.
62. Select the **High Availability Admission control** checkbox.
63. Click **OK**.
64. Go to **Settings** > **Download Schedule**, and click **Edit**.
65. Clear the **Enable schedule task** checkbox.
66. Click **Next**.
67. Review the selection, and click **Finish**.
68. Go to **Settings** > **Notification Check Schedule**, and click **Edit**.
69. Clear the **Enable schedule task** checkbox.
70. Click **Next**.
71. Review the selection, and click **Finish**.

Upgrading VMware ESXi 5.5 and 6.0 to 6.5 Update 2

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.
- vCenter must be running Release 6.5 update 2 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*.

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 **ACP 4200 Baseline Group** baseline.
5. Click **OK**.
6. Click **Scan for Updates**.
7. Select **Patches and Extensions and Upgrades**.
8. Click **OK**.

   The host will be listed as non-compliant when the scan completes. This indicates that the host needs to be upgraded.
9. Click **Remediate**.

   If remediation fails due to conflicting VIBs installed on the ESXi host,
10. Ensure that the **ACP 4200 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 will reboot more than once, especially when upgrading from ESXi 5.5.x to ESXi 6.5.

    After the upgrade is complete, you may be required to manually connect the host to vCenter after the upgrade completes due to licensing considerations.

23. Go to vCenter and assign a valid vSphere 6.5 license to the upgraded host and then connect it to vCenter.

    Perform the following steps if the licensing process fails.

    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.

24. Validate the VMware ESXi release.
25. Remove the host from Maintenance Mode.
26. 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 be running Release 6.5 Update 2 before using this procedure to patch them. They will be incorrectly reported as compliant if they are running any other version. 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 `ACP 4200 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 2) 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. Select **Patch Baselines** and ensure that the `ACP 4200 Baseline Group` baseline is selected.

   Note:

   See Configuring vSphere Update Manager on page 50 to create the Group baseline if it is not available.
9. Click **Next**.
10. **(Optional)** This activity can be scheduled for a future date. It will occur immediately by default.
11. Click **Next**.
12. Review the settings.
13. Click **Next**.
14. 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.
15. 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 Manger (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_2.0.0.42-1OEM.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 Converged Platform 4200 series. Depending on the hardware configuration of your solution, your Avaya Converged 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 Converged 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 Converged 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 Converged Platform 4200 series on page 21.

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 adjancencies` 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 Converged 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 61.
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 61.

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 Converged Platform 4200 series. Depending on the hardware configuration of your solution, your Avaya Converged 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 Release 4.0 baseline, continue with the upgrade procedure. Storage array upgrade is not required otherwise.

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:

    It can take several minutes for the update to complete. 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.

Next steps

Do the following to verify the current software version:

1. Log in to the management interface with the Administrator credentials.
2. Select **Administration** > **Software** from the menu.
3. Verify the software version in use.

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.

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 Converged Platform 4200 series Release 4.0 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. Compare the current array software version with the version in the Avaya Converged Platform 4200 series Release 4.0 baseline, for example, `5.0.5.200-588749-opt.update.v2`, before upgrade.

   If the array version is greater than the version under the Avaya Converged Platform 4200 series Release 4.0 baseline then you do not need to upgrade the array. Do not complete the rest of this procedure.
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 40 minutes per array. You will be logged out of your current session and returned to the login screen when the upgrade completes. Close the browser and open it again to clear the session cache.

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.

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 Converged 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 **Adminstration** > **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 ACP 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 Converged Platform 4200 series on page 21.

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 theAvaya 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 be 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

The Management Server Console serves as the Network Time Protocol (NTP) source for the Avaya Converged Platform 4200 series. Components of the Avaya Converged Platform 4200 series such as the following regularly synchronize to the Management Server Console:

- Storage systems such as the EMC VNXe3200 and VNX5300 and the Nimble CS1000.
- Compute servers such as the HP ProLiant DL360 G9.
- Network switches such as the Extreme Virtual Services Platform 7254XSQ.
- Session border controllers.
- Avaya G450 Media Gateway.

The Management Server Console itself is synchronized with the network NTP source. The network source may be a server maintained within the network or an external source on the Internet. Consult with the system administrator to determine which NTP source should be used.

Avaya Converged Platform 4200 series uses a Microsoft Windows 2016 Standard Management Server Console. This is the Management Server Console that should be synchronized with the network source. NTP server synchronization is typically configured during the deployment of the new MSC. If this step was not carried out or must be performed again, see the procedure Configuring MSC to synchronize with an external NTP time source manually on page 88.

All components and hosts should similarly be pre-configured to synchronize with the MSC. If they are not or this step must be performed again, see the procedure Synchronizing VM and MSC time on page 89.

Important:

The EMC VNXe3200 must be synchronized to the NTP source once the Avaya Converged Platform 4200 series is installed on site.

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 Converged 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 Converged Platform 4200 series* for configuration procedures related to the recommendations in this section. These documents are available on the Avaya Support website.

1. **Infrastructure component synchronization.**
   - Compute servers — Set the Management Server Console (MSC) as the primary NTP server (NTP 1) for ESXi and iLO and TMM interfaces. Use the customer NTP server as the secondary NTP server (NTP 2).
   - Network Switches — Set the MSC as the primary NTP server (NTP 1). Use the customer NTP server as the secondary NTP server (NTP 2).
   - Network Storage (both EMC and HPE Nimble) — Set the MSC as the primary NTP server (NTP 1). Use the customer NTP server as the secondary NTP server (NTP 2).
   - Power Distribution Units — Set the MSC as the primary NTP server (NTP 1). Use the customer NTP server as the secondary NTP server (NTP 2).
   - G450 Media Gateways — Set the MSC as the primary NTP server (NTP 1). Use the customer NTP server as the secondary NTP server (NTP 2).
2. **Management Server Console synchronization.**

   The MSC should synchronize with the NTP source listed in the *Lifecycle Customer Workbook*. Confirm the source usage, and edit if necessary, with the following steps:

   a. Connect to the MSC using RDP.
   b. Open the Windows File Explorer.
   c. Navigate to `C:\Tools`.
   d. Right-click the `NTPConfig` file.
   e. Click **Edit**.
   f. Validate the IP entry next to `set var=IP_Address` element. Compare it with the information in the *Lifecycle Customer Workbook* or confirm the value with the customer.

g. Replace the existing IP address with a new one if necessary.

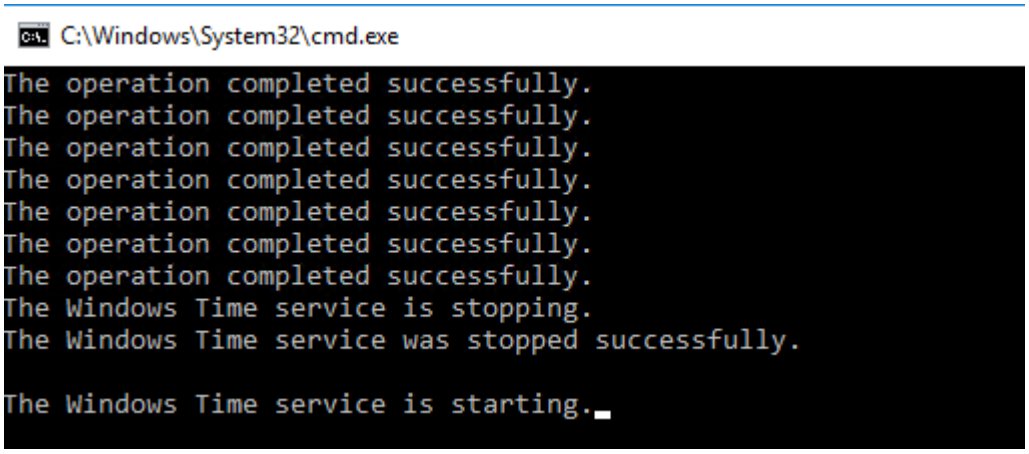
h. Save the `NTPConfig` file.

i. Close the `NTPConfig` file.

j. Right-click the `NTPConfig` file.

k. Click **Run as administrator**.

l. The file will execute on the command line and close after the settings are updated. The following is an example of the file output.



3. **VMware Tools time synchronization is disabled on the MSC.**

a. Connect to vCenter from the MSC using the vSphere web client.

b. From the **Host and Cluster** view, select and right-click the Management Server Console VM.

c. Click **Edit Settings**.

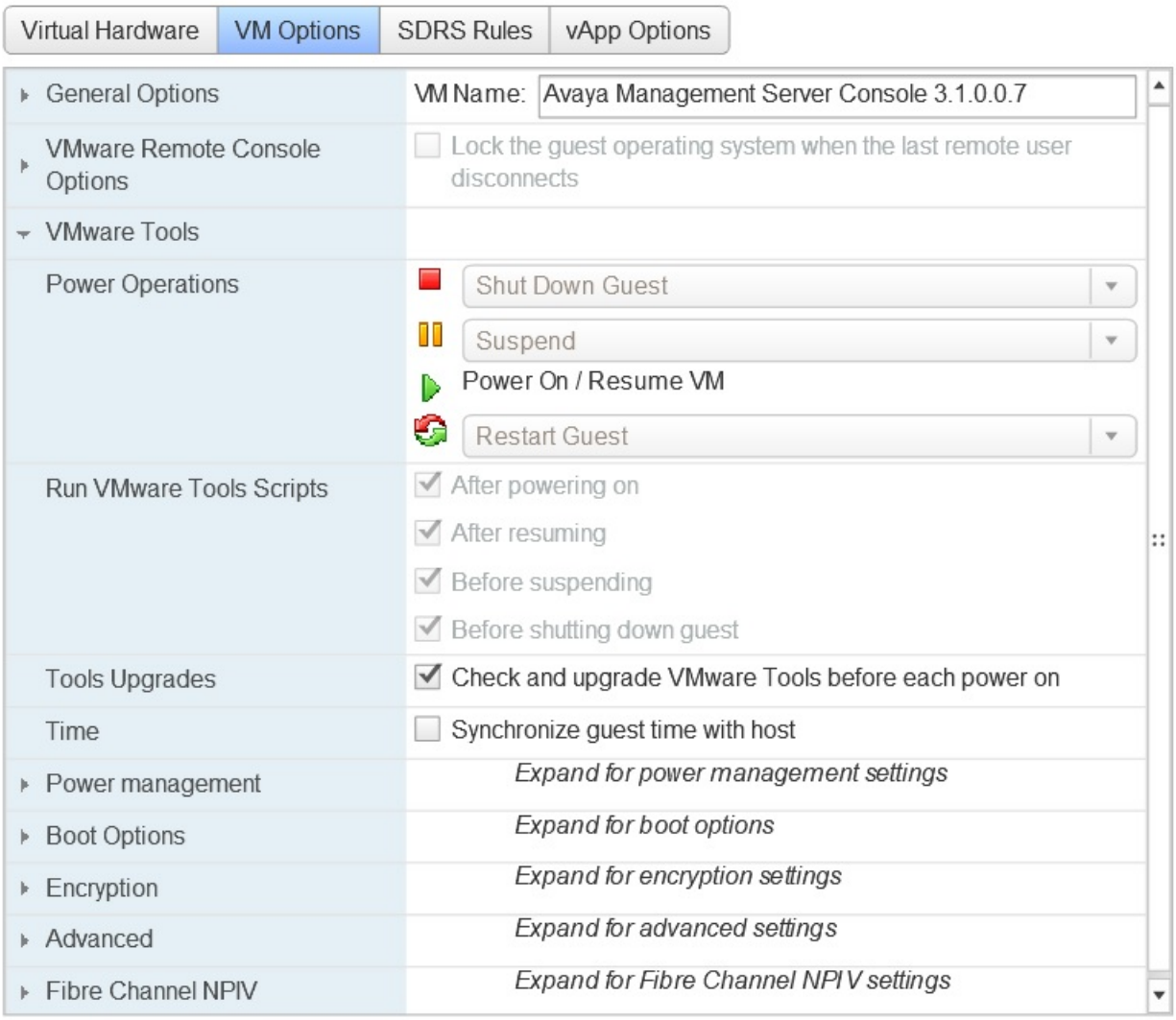
d. Select the **VM Options** tab.

e. Select **VMware Tools**.

f. Make sure **Synchronize guest time with host** is not selected.

g. Clear the checkbox if it is selected.

h. Click **OK** to save the changes.



4. **Avaya Aura® application synchronization.**

   Note:

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

   Set the MSC as the primary NTP server (NTP 1) for each Avaya Aura® application on the cluster. Use the customer NTP server as the secondary NTP server (NTP 2).

   VMware Tools time synchronization should be disabled.

   a. Connect to vCenter from the MSC using the vSphere thick client.
   b. Select **Host and Cluster** view.

c. Right-click the Avaya Aura® application VM.
d. Click **Settings**.
e. Select the **Options** tab.
f. Select **VMware Tools**.
g. Confirm **Synchronize guest time with host** in the **Advanced** section is not selected.
h. Clear the checkbox if it is selected.
i. Click **OK**.
j. Repeat these steps for all Avaya Aura® applications in the cluster.

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
  ```

Configuring the MSC as a NTP time source

Use the following procedure to configure the Management Server Console (MSC) as an NTP time source.

Procedure

1. Go to `C:\Tools`.
2. Open **NTPConfig.bat** with a text editor.

3. Change the value of the variable *var* to a DNS IP Address for the external Time Source to be synced.
4. Save the changes.
5. Execute **NTPConfig.bat** to configure the MSC as an NTP server.

Configuring MSC to synchronize with an external NTP time source manually

Use the following procedure to configure the MSC to synchronize with an external NTP time source if you did not do so when deploying the MSC. This procedure is optional and applicable to ESXI 6.5.

Note:

If NTP check box is selected and time server is provided. The following steps are performed automatically during deployment.

Procedure

1. Click the time display on the lower-right corner of the MSC desktop.
2. Click **Change date and time**.
3. Select the **Internet Time** tab.
4. Click **Change settings**.
5. Click **Synchronize with an Internet time server**.
6. Enter the IP address or FQDN of the NTP server in the **Server** field.

   Note:

   The FQDN must be DNS resolvable.
7. Click **Update Now**.
8. Click **OK**.
9. Click **OK** to save the changes.

   Note:

   Check connectivity and firewall settings if the synchronization fails.

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.

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

Synchronizing VM and MSC time

In some instances the VM and MSC time may not be synchronized properly.

About this task

Use the following procedure to force time synchronization.

Procedure

1. Using the vSphere web client login to vCenter.
2. From the hosts and the cluster view, locate and select the VM where the time is not properly synchronized.
3. Right-click on the VM.
4. Click **Edit Settings**.
5. In the **VM** options tab, click **VMware Tools**.
6. Uncheck **Synchronize Guest Time with Host**.
7. Click **Ok**.

   If **Synchronize Guest Time with Host** option is already unchecked, validate that the application has been configured to synchronize time with the MSC as first option and customer's NTP as second option.

Configuring NTP synchronization for the Nimble CS1000

About this task

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

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

Table continues…

Title	Description	Audience
Installing and Maintaining the Avaya Converged Platform 4200 series	Describes how to install Avaya Converged Platform 4200 series.	IT Management, sales and deployment engineers, solution architects, and support personnel.
Upgrading Avaya Converged Platform 4200 series using the Management Server Console	Provides an overview of Management Server Console for Avaya Converged 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.
Configuring and Administering Avaya Orchestrator	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.

Related links

Finding documents on the Avaya Support website on page 95
Avaya Documentation Portal navigation on page 95

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 94

Avaya Documentation Portal navigation

Customer documentation for some programs is now available on the Avaya Documentation Portal at https://documentation.avaya.com.

Important:

For documents that are not available on the Avaya Documentation Portal, click **Support** on the top menu to open https://support.avaya.com.

Using the Avaya Documentation Portal, you can:

- Search for content in one of the following ways:
  - Type a keyword in the **Search** field.
  - Type a keyword in **Search**, and click **Filters** to search for content by product, release, and document type.
  - Select a product or solution and then select the appropriate document from the list.
- Find a document from the **Publications** menu.
- 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 **My Content** > **My Docs** menu, and do any of the following:
  - Create, rename, and delete a collection.
  - Add content 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 content that others have shared with you.
- Add yourself as a watcher by using the **Watch** icon (👁).

  Navigate to the **My Content** > **Watch list** menu, and do the following:
  - Set how frequently you want to be notified, starting from every day to every 60 days.
  - 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 portal.
- 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 in to the portal. The available functionality depends on the role with which you are logged in.

Related links

Documentation on page 94

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 98

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 97

Index