Configuring and Administering Avaya Orchestrator

Release 1.4
Issue 3
May 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. Note, unless otherwise stated, that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

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

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

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER’S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR

EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

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

Chapter 1: Introduction to Avaya Orchestrator

Overview

This document provides administration guidelines for configuring and supporting Avaya Orchestrator 1.4, for Avaya Converged Platform (ACP) 4200, after initial site installation and deployment.

Avaya Orchestrator (AO) is a new maintenance support tool that replaces the previous set of alarm and support tools known as Pod Orchestration Suite (POS). Pod Orchestration Suite is end-of-sale with Pod Fx 3.1. The process of upgrading from POS to Avaya Orchestrator will be supported by Avaya Professional Services, Business Partners, solution integrators, or other professional technical staff representatives. Prior to a migration and upgrade, existing POS systems must be backed up and removed. For more information about backing up all POS data and removing the applications and their supporting infrastructure, see the *Installing and Maintaining the Avaya Converged Platform 4200* guide at https://support.avaya.com.

In AO Release 1.4, you can administer and monitor up to 300 nodes. A node is defined as a device or object with an IP address assigned. For example, an Avaya G450 media gateway requires one administered node/IP address to administer in AO, and an HPE host server requires two nodes to be administered in AO: 1 ESXi IP address + 1 HPE iLO IP address. Information about node assignments for each device is covered later in this document.

Avaya Orchestrator (AO) 1.4 is a visualization and management application used to monitor your Avaya ACP 4200 4.0 release.

The following are the features of Avaya Orchestrator:

- ✓ Works in conjunction with the SAL Gateway to monitor and escalate product alarms and notifications across all ACP 4200 infrastructure hardware.
- ✓ Supports ESXi alarming updates from all ACP 4200 4.0 server hosts.
- ✓ Provides a single dashboard view for monitoring state of health of all ACP 4200 racks, components, and services.
- ✓ Presents robust data access in a simple and uncluttered manner.
- ✓ Allows SMS and email notifications for product hardware alarm escalations.
- ✓ Provides consistent proactive, as well as reactive, monitoring of all administered hardware components.

For Avaya Orchestrator Release 1.4, software applications continue to support alarms through the SAL gateway. Software alarm support will be available in a later release.

Each new release of AO will target improvements and innovations to meet the requirements and needs of Avaya's user communities.

Avaya Orchestrator configuration and considerations

The following sections describe the Avaya Orchestrator configuration and provides some technical guidelines and considerations for maintaining optimal application performance and behaviors.

Software

Avaya Orchestrator is a Red Hat Linux 7.5 virtual appliance intended for use by customers and Avaya support services teams.

Avaya Orchestrator Release 1.4 has a standardized virtual footprint.

Storage (disk)	**120 GB**
CPU	**16 vCPUs**
RAM	**24 GB**
Network	**1 VNIC**

It is meant to support a one-size-fits-all approach, allowing several simultaneous user requests and monitoring activities, without inhibiting product responsiveness to proactive maintenance investigations and alerting.

If the monitored ACP site consists of a single rack with very limited components, the footprint can be easily adjusted to a smaller size and still provide enough capacity for a multi-user environment. Customers can contact an Avaya technical representative for more information about such options.

Virtual network

In VMware infrastructures, for applications, such as AO, that depend on communication with their server host's iLO port, ensure that you keep the network VLAN of the VM on a different network VLAN than that of the iLO port. The Avaya services deployment teams adheres to this rule during the initial application installation. AO is deployed on the Management VLAN and the iLO IP is deployed on the Application VLAN. It is important for the user community to continue abiding by this rule so that AO continues to perform optimally.

Recommended practices

Historical reports

The Avaya Orchestrator reporting engine is a multi-faceted tool that reviews vast amounts of information prior to consolidating the requested information into an historical report. Therefore,

Avaya recommends that users consider this fact when requesting data and not consistently click on the report request buttons if more detailed reports are not displayed immediately. Consistent clicks/requests cause the report generation process to restart and can slow the report requests of other users.

Configuration administration

The ACP Configuration Wizard consumes most AO threads and cycles as each rack is taken through the *Finish* sequence. During this timeframe, an extensive discovery process is underway and blocks all other AO application requests until the process is finished. All alarm monitoring and processing continues in the background and is not impacted, but no UI responses are provided until the *Finish* (discovery) process is concluded. Therefore, Avaya recommends that you perform all Wizard Configuration activities during maintenance windows or low use timeframes.

Connecting to Avaya Orchestrator

About this task
You can access Avaya Orchestrator when the virtual appliance server is deployed and running. Avaya recommends that you use Chrome or Firefox when connecting to Avaya Orchestrator.

Procedure
1. On a web browser, go to: http://*<AO IP Address>/orchestrator*
2. Type the appropriate credentials to log in.

Note:
All deployed IP address and credentials are documented in the *Customer Lifecycle Workbook*. The following are the default credentials for Avaya Orchestrator UI access.
Login: ***orchestratoradmin***
Password: ***Avaya123$***

Licensing

Avaya professionals must complete the initial customer configuration and licensing for the application. All required licensing is applied during product installation. For more information about licensing, contact your Avaya sales representative.

Configuring DNS/FQDN information

Without the administration of FQDN host information, by default, all reports display only the source IP address for each trap that is received or proactively collected. Therefore, to produce an easily distinguishable reference name for each trap/alarm, you must configure an FQDN or host name and DNS authentication for each element that is monitored.

Important:

If you want device names to appear, instead of IP address information, in all AO reporting output, you must create all DNS or /etc/hosts file entries before administering devices in the ACP Configuration Wizard.

If devices have already been administered into the Configuration Wizard, the subsequent administration of FQFN information in a DNS server or /etc/hosts file in AO will not provide the required device naming presentation. To display the FQDN information instead of the IP addresses, remove the devices from the Wizard and re-administer them, so that next time AO populates all related device tags, that is, an FQDN instead of an IP address.

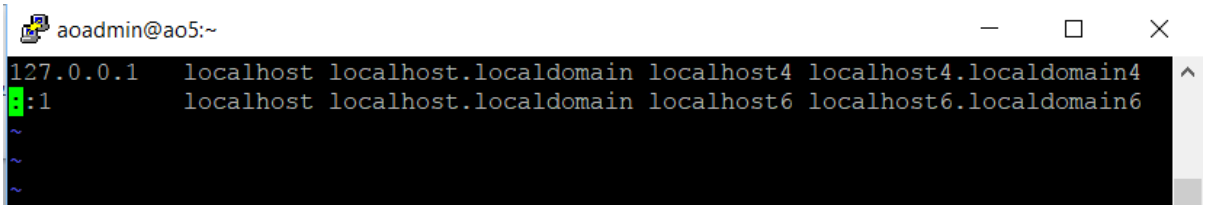
Procedure

Option 1: Administer the FQDN information in a DNS server.
Based on the FQDN information provided in the Life Cycle Workbook (LCW)[1], administer the IP address and FQDN information for each ACP 4200 device node into a DNS server that supports the production environment. This information will be aligned with Avaya Orchestrator trap reporting output.

Option 2: Build an FQDN or host table inside Avaya Orchestrator.

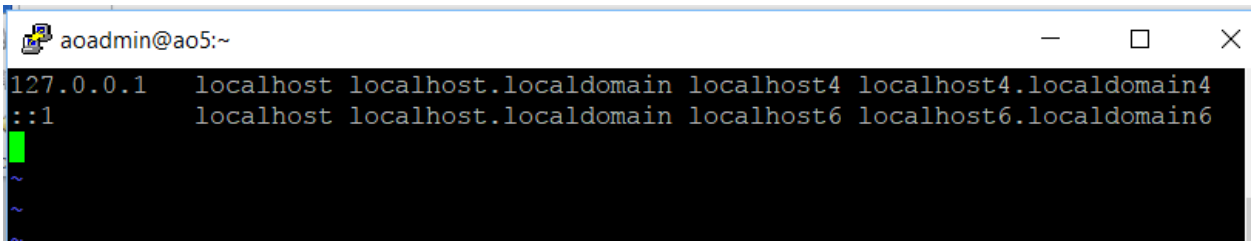
If a DNS server is not available for the environment, you can administer a table within the Avaya Orchestrator application to provide the same FQDN naming outcome. You can get the FQDN naming information for each node from the Life Cycle Workbook. Do the following:

1. SSH into Avaya Orchestrator by using the *aoadmin* login credentials from the Customer IP Template Workbook.
2. At the Linux prompt, type: *sudo vi /etc/hosts*
   The *hosts* file is opened for editing.
3. Use the arrow keys on your keyboard to move the cursor down to the bottom row of entries. Press the *Esc* key and then *o.*



The cursor repositions on a new line for you to insert the entries.

[1] The FQDN information in the LCW was used when deploying ACP 4200 devices.



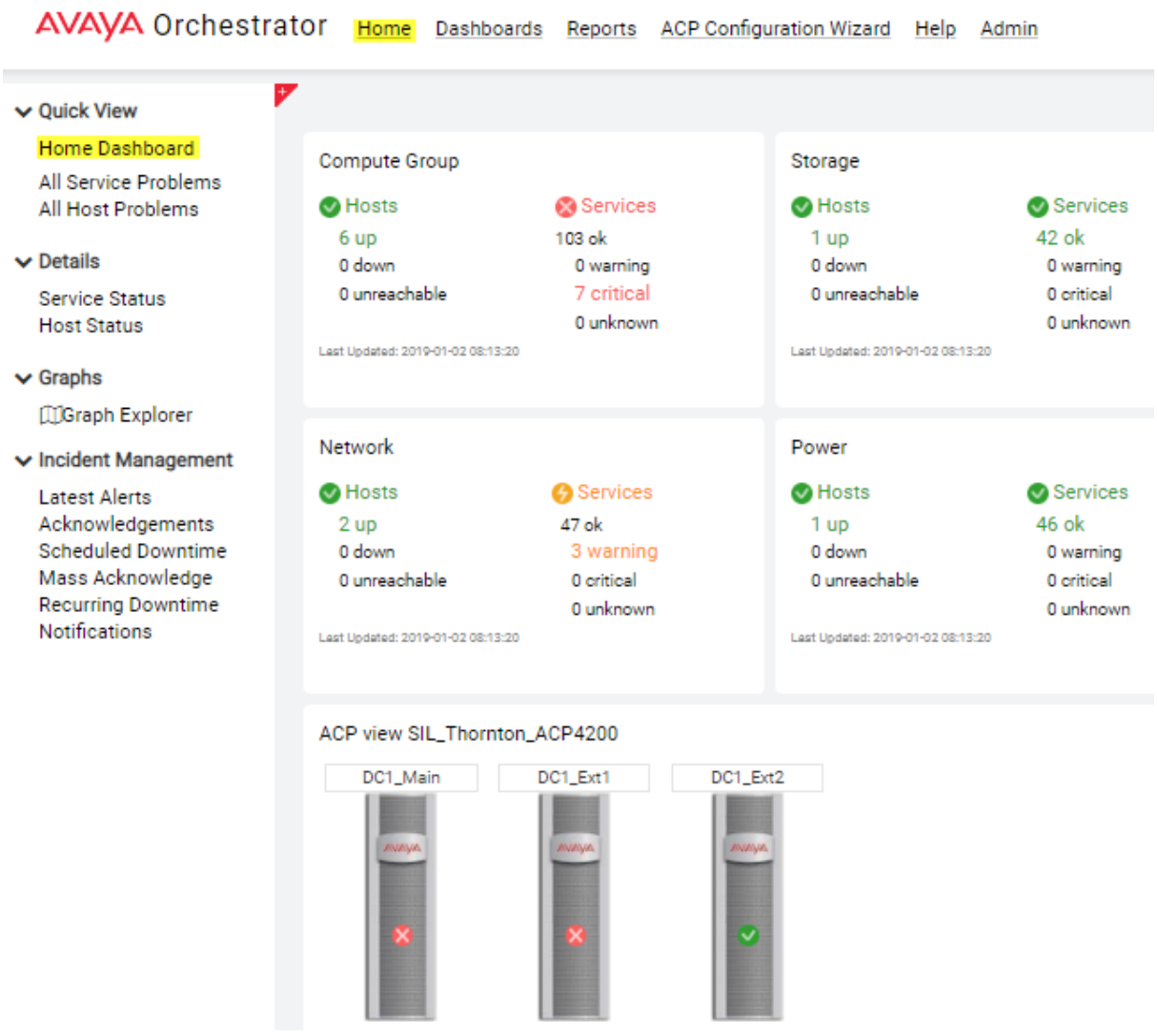
4. Use the following Linux vi procedure to update the *hosts* table:
   1. Type the IP address for the first device, and then press the *Tab* key.
   2. Type the host name and press the *Tab* key.
      Note: This host name is presented with each trap from the device.
   3. Type the associated FQDN/host entry. For example: net1dc1.avaya.com
   4. Press Return and type the information of the next host.
   5. After you type the final IP address, press Esc to stop the vi editing process.
   6. To write and save the file information, type :wq!
   7. To close the window, type *exit.*

Chapter 2: Dashboard overview

This chapter provides information about how to use and interpret the various dashboard options in Avaya Orchestrator.

Avaya Converged Platform (ACP) Dashboard

The ACP dashboard is available on **Home** > **Quick View** > **Home Dashboard**.



The main dashboard displays summary information about the devices and related services installed in a solution. There are two perspectives represented on the primary dashboard. The

first provides a one-stop glance at the state-of-health per device group, and the second presents the relationship of those states within each rack.

Dashlets

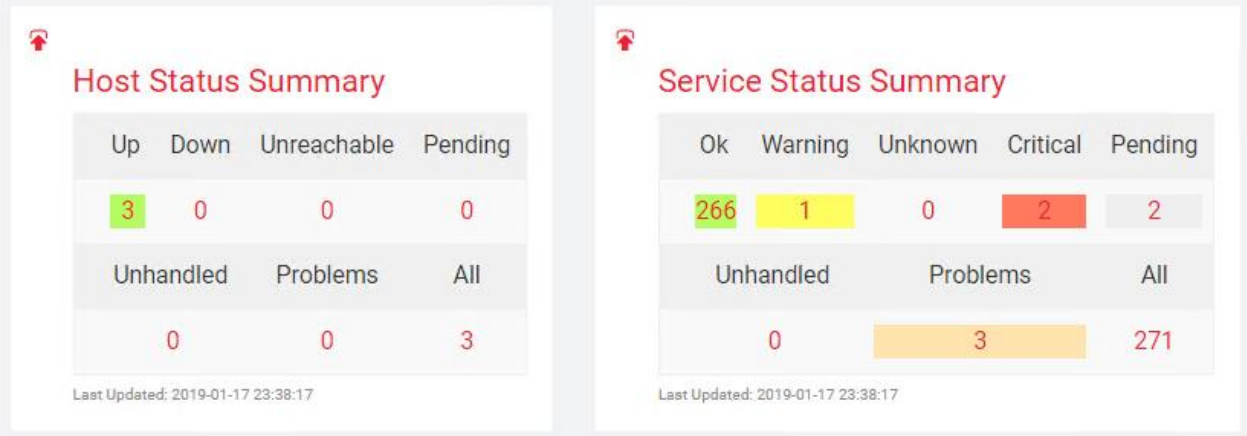
Each dashlet summarizes information for the corresponding group of devices:

Compute group: Compute servers
Storage: Storage devices
Network: Network switches
Power: PDUs

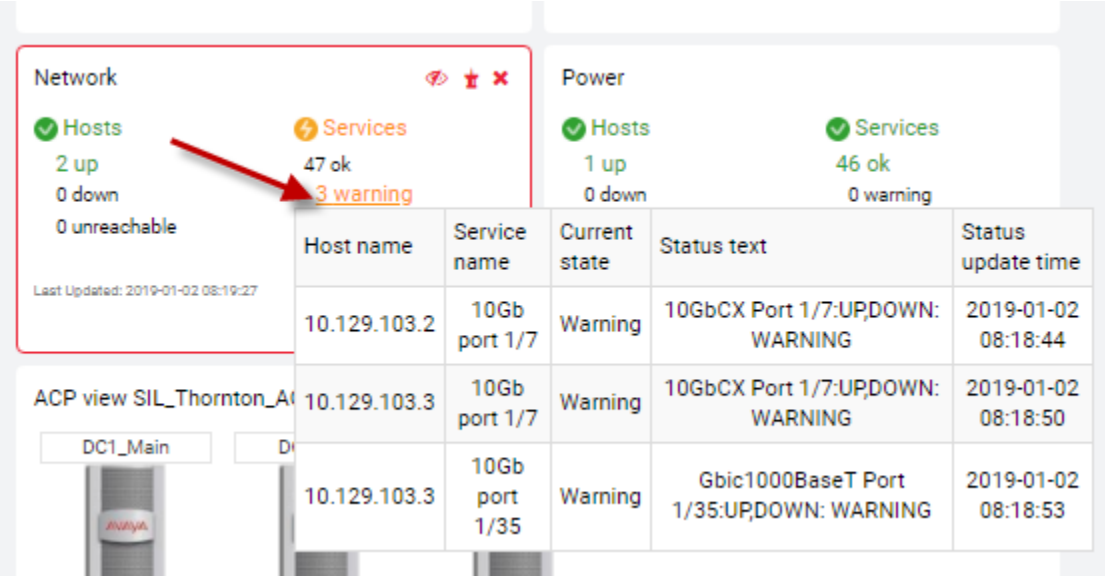
The related information displayed for each group depends on the specific view being monitored. For example, on the main dashboard below, the dashlets provide group information for the entire ACP solution. However, in the drill-down rack views, the dashlet groups and their representative information show status for a specific rack only.

Within each dashlet group is a run-down of the various active states for each host and related service state: Up, Down, Unreachable, Ok, Warning, Critical, Unknown, and Acknowledged. You can hover the mouse over each of the dashlet's green, amber, or red state-of-health links to view a summary of the most recent and high runner related events.

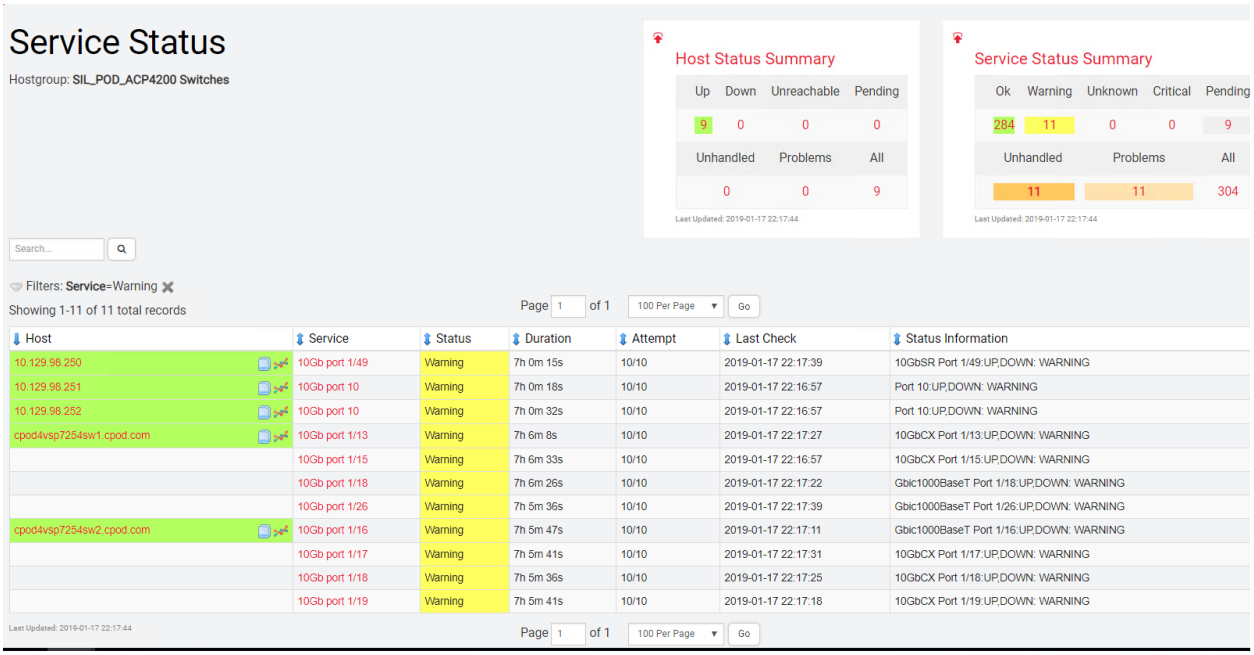
The **Host Status Summary** and **Service Status Summary** dashlets are consistently presented across the top of many report views. They provide a collective bird's eye view of overall solution state-of-health and are automatically updated every 60 seconds. These dashlets are visible from the service and host problem reports as well as the service and host status reports.



The following is an example of a dashlet summary:



The preceding dashlet view shows the three Warnings in the Network device node grouping. If there are more issues than can be easily displayed and read in the pop-up window, you can click on the numerical values, in this case the **3 warning** link, for a drill-down view of all the **Service Status** report incidents, as can be seen in the following screenshot. This report provides a variety of options for prioritizing the list by allowing you to click any of the blue arrows within the list header: Host, Service, Status, Duration, Attempt, Last Check or Status Information prioritization.



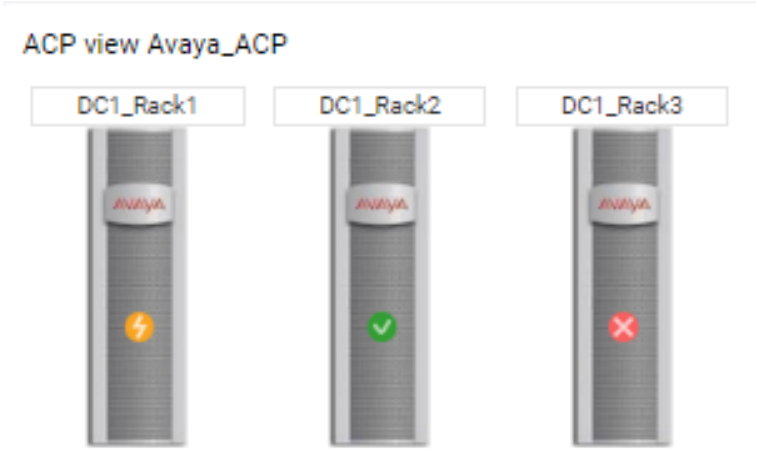
You can view a similar **Service Status** report through a menu option on the far-left side of the AO Home menu page under **All Service Problems**. However, the default view reported within

each selection is different and is based on the intent of each menu selection. In the **All Service Problems** view, all issues for all device services are presented – no OK status states are represented. In the previous example, by clicking on the link for **3 warnings** within the Network group box, only the specific warning alarms/traps for the network group are presented. By contrast, all *status* reports will provide all host and service related information – all known issues plus all known OK states.

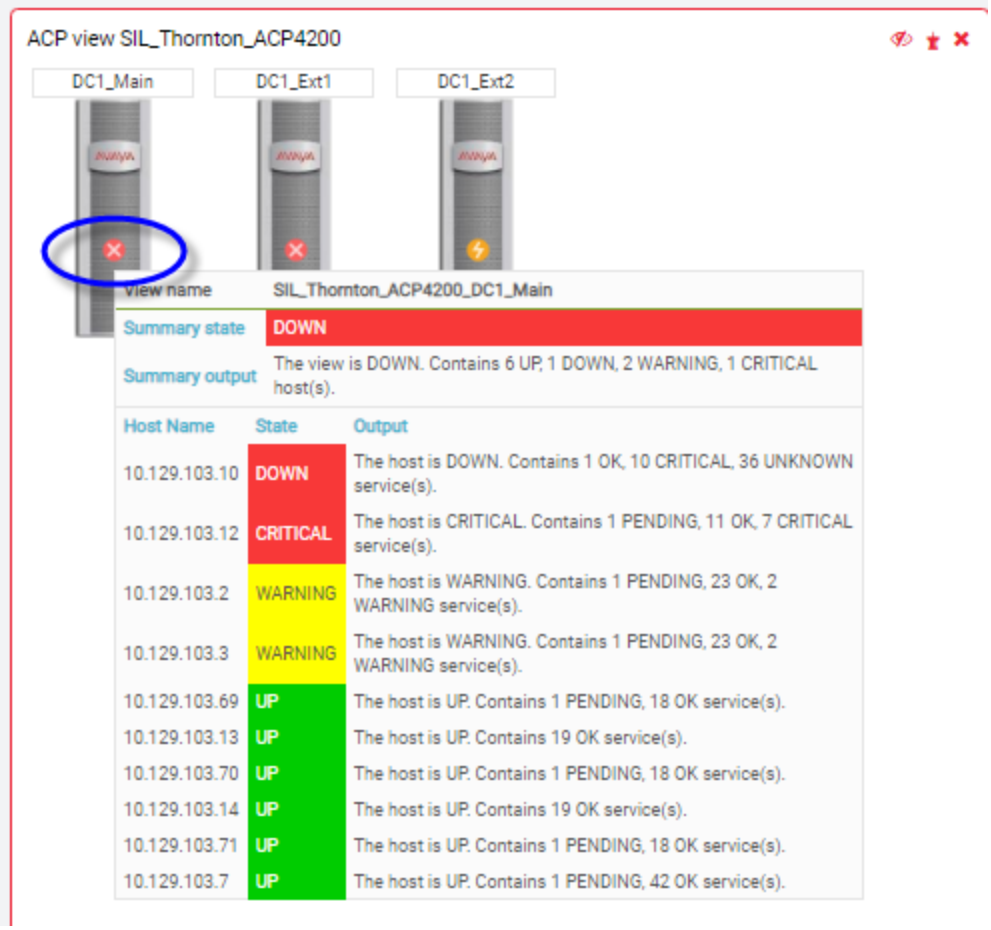
State-of-health information is also shown in the rack view. At the bottom of the Home Dashboard view are rack icons that provide state-of-health indications for the hardware devices deployed within each rack.

For example, if the Network dashlet reports a critical alarm in the Storage block, the rack containing the alarming storage array reports the critical alarm also. Thus, targeting the location of the alarmed device. You can click on the rack that contains the device to get a more detailed view of the device.

The rack status icon reflects the highest level of trap. For example, if the alarms for devices inside DC1_Rack3 are represented by four warnings and one critical trap received, the rack icon shows a red icon that represents the highest-level critical alarm. In the following example, DC1_Rack1 has at least one warning on a deployed device, DC1_Rack2 has no warnings and no critical alarms, and DC1_Rack3 has at least one critical alarm.

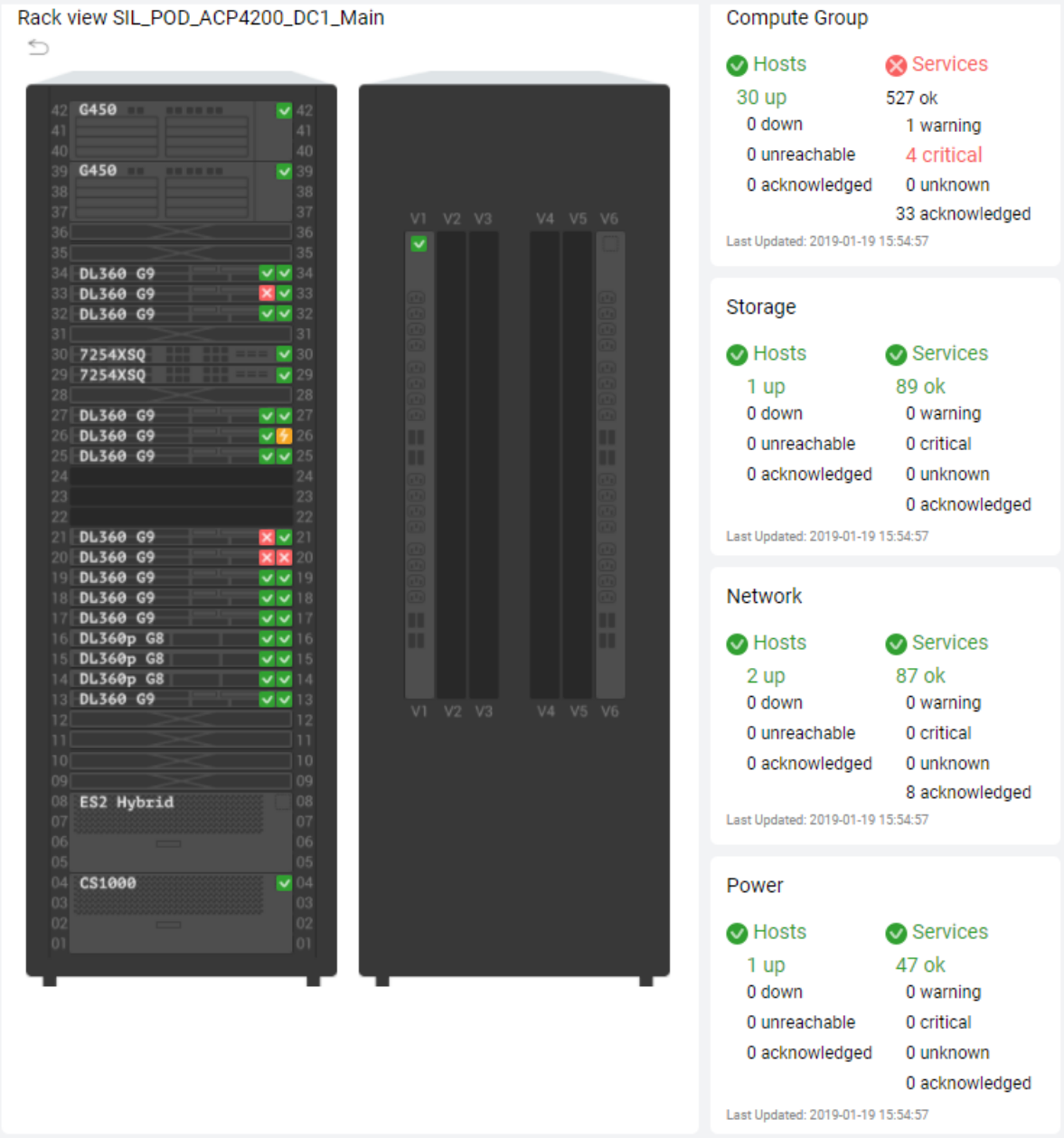


You can hover over a rack status icon to view the state summary. The hover list reports the most critical issues at the top of the list, if issues are present. Similar to the dashlet links, you can drill down into each specific area for a complete view.



Rack dashboard

The Rack dashboard contains detailed information about the rack elements. This is the likely primary area you can use to begin any investigative work when reviewing issues with devices. The dashboards available within the rack view offer more than just a visual reference. You can use the administrative controls within the drill-down option to edit service settings, send notifications, and even control the representation of alarms to the user communities.



The same familiar group of dashlets are present to provide a high-level state-of-health status. Each dashlet summarizes information of the corresponding group of devices within the rack bring viewed: Compute group, Storage, Network, and Power.

Within each grouping, are the two process areas that are monitored: Hosts and Services.

Hosts Status

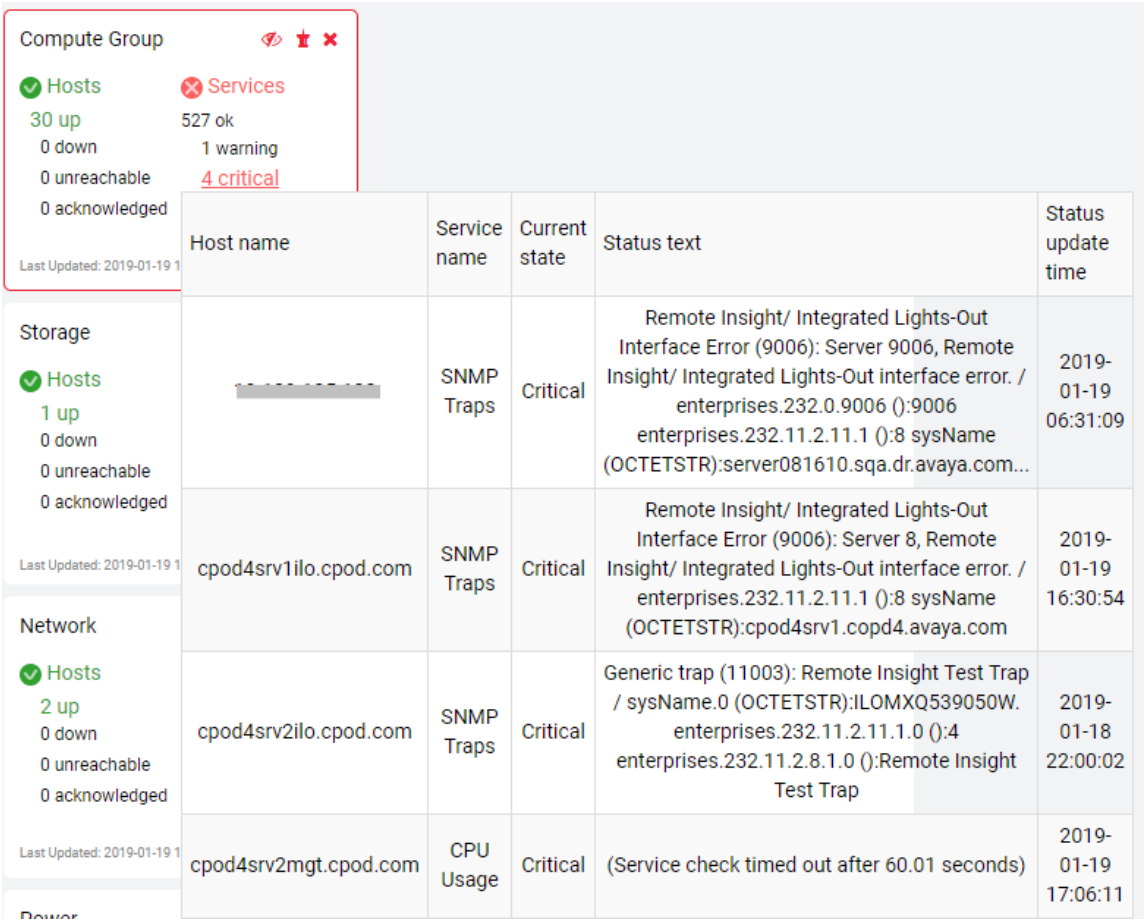
The Host status represents the accessibility of the IP address of each node/device.

Service Status

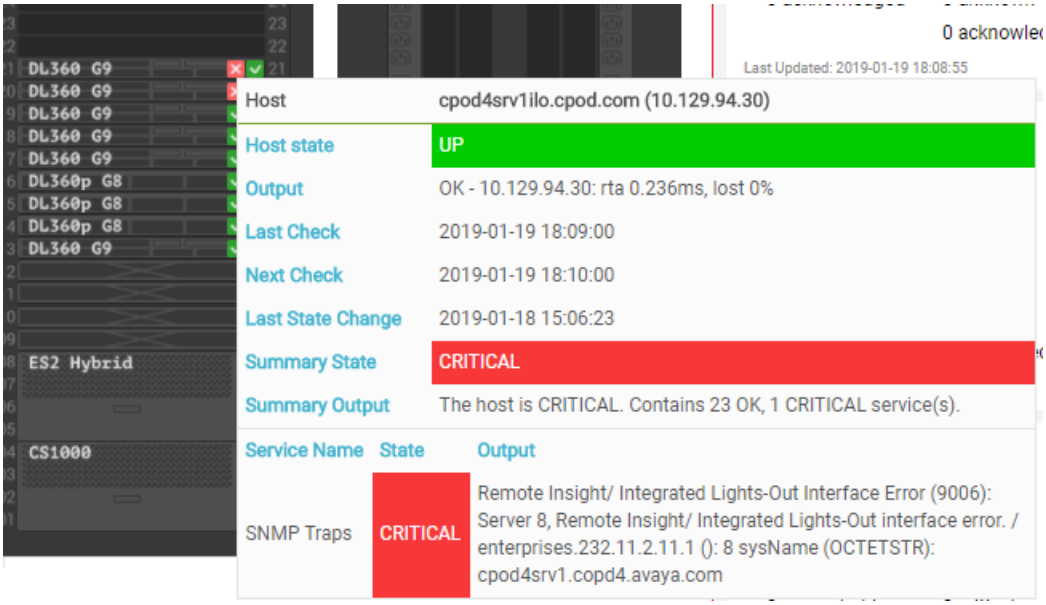
The Service Status represents the individual function on each device that provides state-of-health information through SNMP trap information or through a REST or CLI API information exchange with AO.

Each status area has an *acknowledged* state; this represents an intentional and manual intervention on the part of users. This is a key status area to review, because it can explain what appears to be a conflict in the other status states represented. For more information about the status area, see Service Status Detail.

You can hover over each dashlet or drill down into the colored dashlet links to view a reporting window. The interactive reports provide the state-of-health for the selected element group in the rack being viewed.



The colored status icons on each device in the rack image provide a similar high-level view when hovering your mouse over a green, amber, or red status lamp. The following is an example when you hover over a critical indicator on a Compute Group element (server).

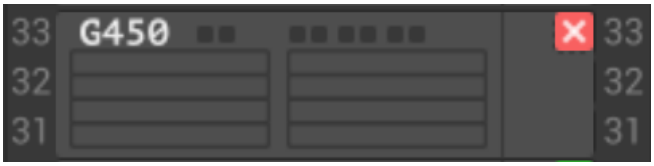


You can also click directly on a device to drill down into a more detailed view of a specific component. For more information, see Device dashboard.

The Rack dashboard also contains a visual representation of the elements in the rack. The following table contains information about the icons that represent various element states.

Element state	Icon
Operational and running without warnings	
Operational but some warnings present	
Not operational or critical issues present	
Unreachable	
Unchecked	

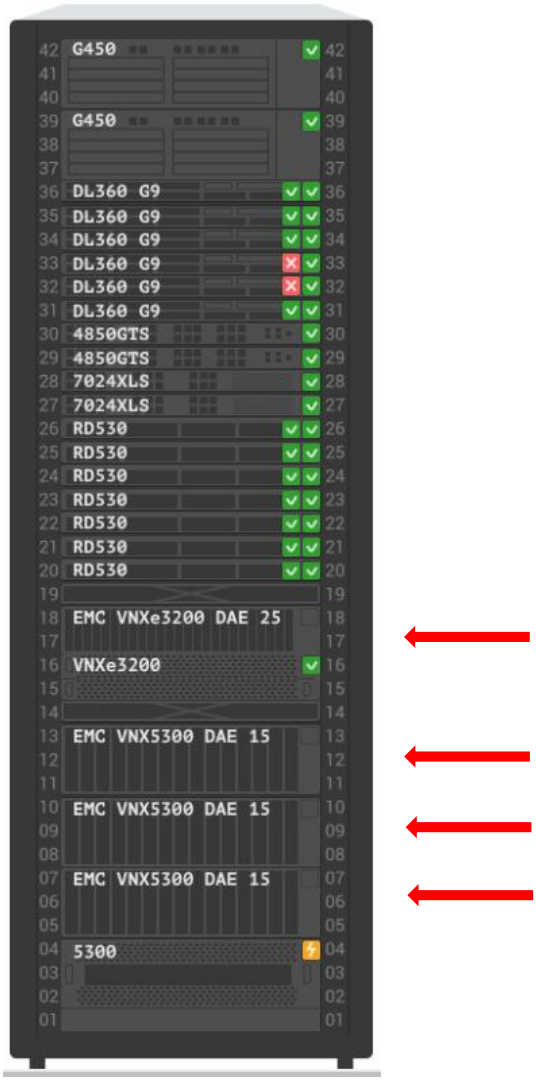
The following is an example of a representation of a G450 that is not operational or has critical issues.



Some rack slots contain fillers, storage extensions, and other elements that do not have detailed information to display. When you click these elements, the Device Dashboard is not displayed.

In the following example, the storage extensions for the EMC 3200 and 5300 Storage Arrays represent these type of elements. They do not have their own IP addresses, and therefore, cannot report their state-of-health status to AO. Instead, their status is reported by the EMC

Controller, seen at the bottom of the rack. However, it is important to have representation for the expansion units in their proper rack position. The expansion components are added during the administration process, which is covered later in this guide. The same type of configuration is true for the CS1000 Nimble Array and its expansion units.



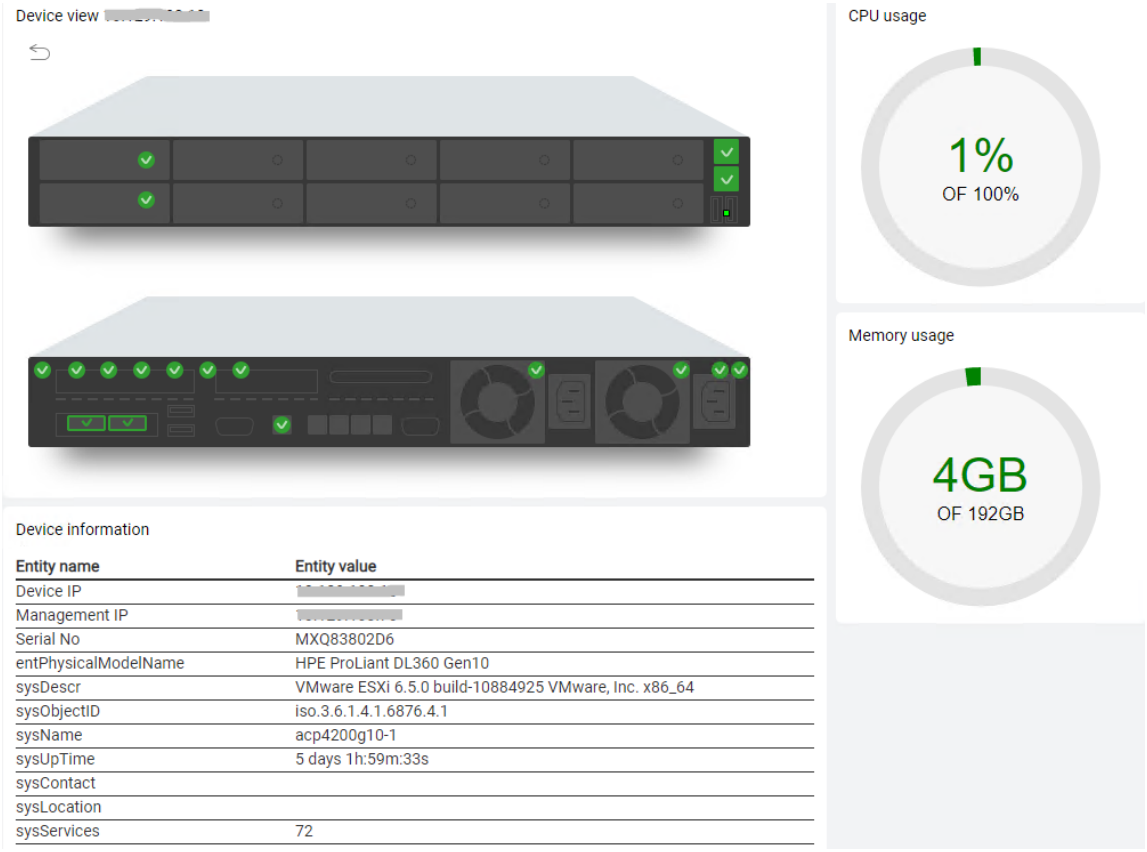
Device dashboard

You can click any element in the Rack dashboard to view the Device dashboard[2].

The following is an example of the Device dashboard for a compute server:

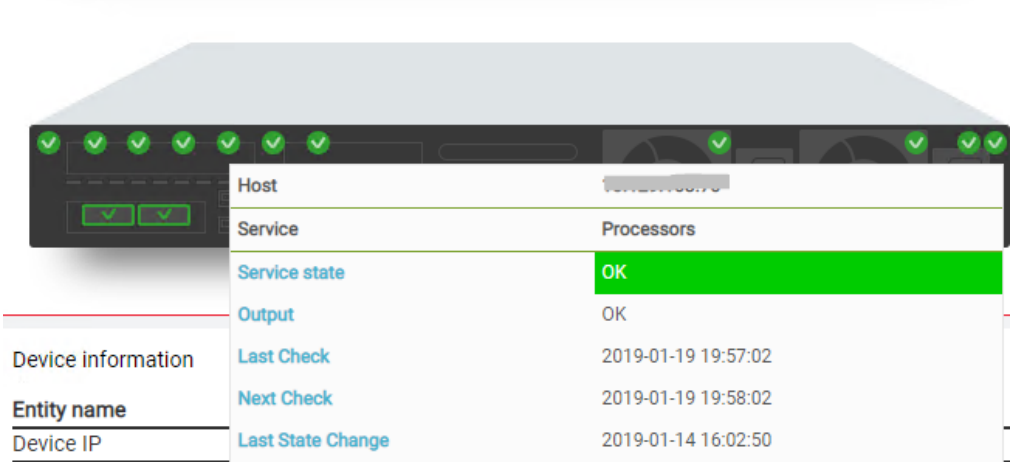
[2] This applies to device elements that are not fillers for slots or media devices, or expansion units for storage arrays.

HPE Gen10 Compute Server



The compute server has two IP addresses assigned: ESXi and iLO interfaces. The Device IP represents the ESXi element and the Management IP represents the iLO element. Other helpful product information is also captured in this dashboard, such as, product serial number, product model number, vendor product description, and host name. Additionally, there is a bird's eye view of the CPU and Memory usage consumption along with the total available memory footprint displayed alongside the device view.

You can hover over each individual status icon to view high-level service description, state-of-health report, IP address of the "host" providing the service status, and the time stamp of the last health check-in.



Services Status Detail

Each hardware device has a unique set of service icons represented in the GUI image. Some are located, where possible, atop or near the elements they are monitoring. Others, such as the ones seen on the upper left of the compute server, represent key hardware functions that are proactively monitored by AO. For example, memory, processors, temperature, and fans.

Other status details, such as the icons on the lower left of the compute server, monitor the Ethernet connections or the power supplies. There are always icons present for SNMP trap receipt reporting. The status changes for the SNMP icon relate to several areas of elemental changes on the device. For more information about this icon, see “Chapter 7: Maintenance and troubleshooting.”

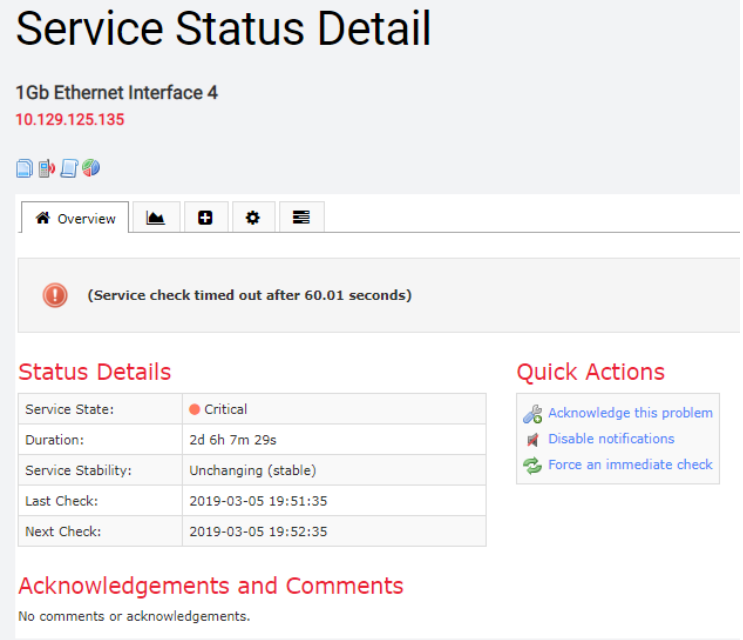
Clicking on the service icon as shown in the preceding example, that is, the “Processors” related green-check icon, opens an additional level of detail about the specific service state.

Overview tab

The following screen shot shows the view of a healthy processor. The highlighted icons provide additional drill-down:

From left to right, the icons represent one-click redirection to the following reports:

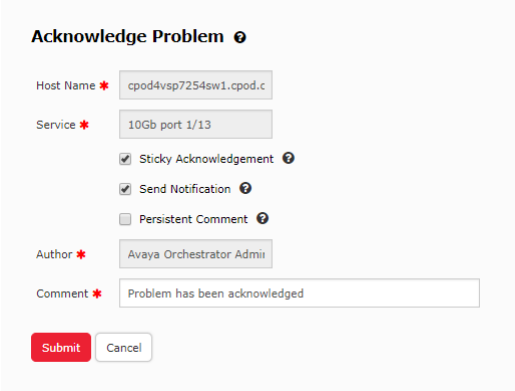
- Current Status for Host Service (Service Status report)
- View Service Notifications
- View Service History
- View Service Availability



Quick Actions

- **Acknowledge this problem**

  When a user is handling a specific issue and wants to stop the associated Email/SMS notification process for the issue, the acknowledgement process is capable of stopping notifications until the problem is resolved.



  The following are the options for an acknowledgement message:

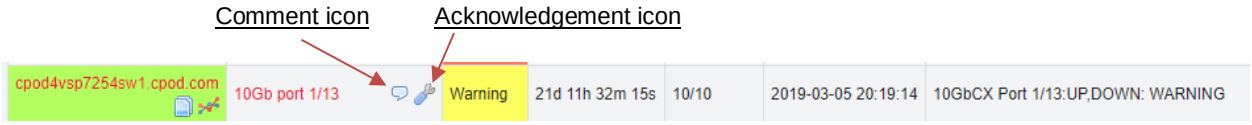
  - **Sticky Acknowledgement**:
    - Selecting the **Sticky Acknowledgement** check box causes the acknowledgement to consistently stop any further notification Email/SMS messages until the problem is resolved. At that time, the acknowledgement is removed and is no longer required.

    - Clearing the **Sticky Acknowledgement** check box causes notifications to continue to be sent until the associated problem is resolved.

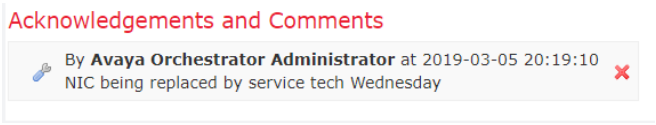
- **Send Notification**:
  - Selecting the **Send Notification** check box creates an Email/SMS notification stating the specific problem is acknowledged.

- **Persistent Comment**:
  - Select the **Persistent Comment** check box to retain the comment after the problem is resolved or the acknowledgement is removed.

Acknowledging a problem provides the ability to associate a comment to the problem and creates a wrench icon next to the service or host problem that is acknowledged.



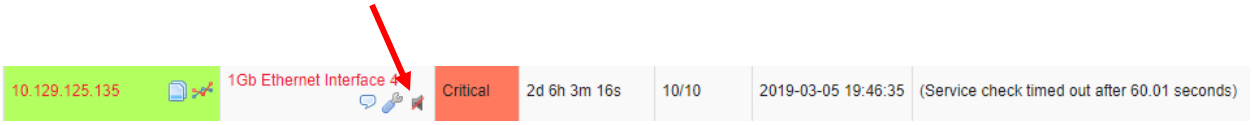
After you add a comment, the comment appears at the bottom of the Host or Service Detail Overview tab.



- **Disable notifications**

If the processor in this example is serviced and taken down, you can click on the **Disable notifications** option to prevent Email and SMS notifications from being sent while the processor is unavailable. After you click the **Disable notifications** option, the option changes to **Enable notifications**, so that when the processor is brought back into service, you can click the **Enable notifications** option to re-establish alerting notifications.

When you click the **Disable notifications** option, the associated icon appears next to the service or host that has the notifications disabled by using this method. The following is an example from the All Service Problems report.

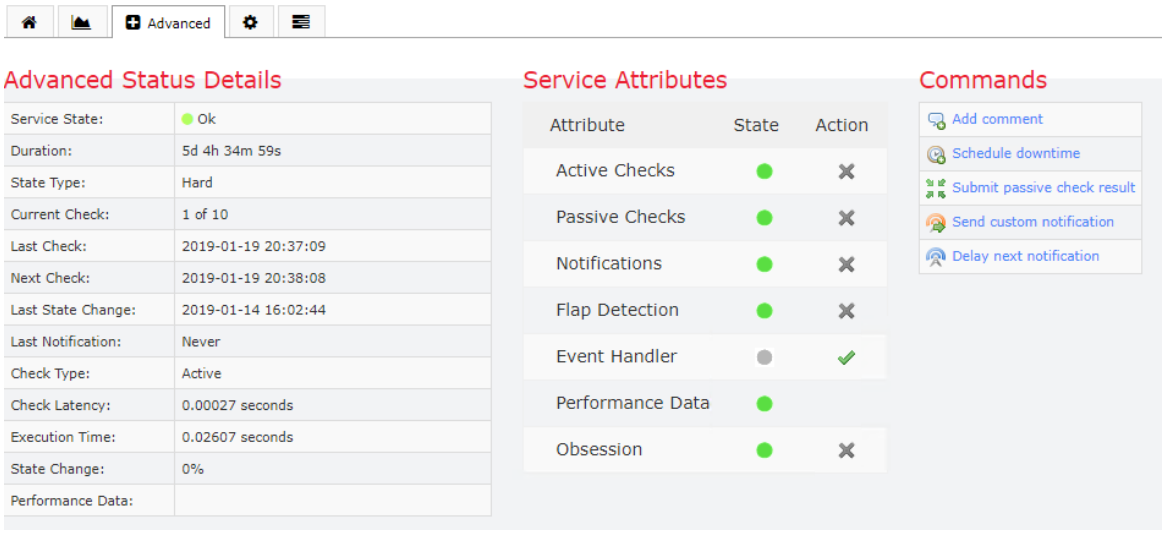


- **Force an Immediate Check**

This option prompts AO to start a proactive monitoring check on the service. If a service is impaired and then repaired, clicking this option can restore an OK state of the service.

Advanced tab

The following is an example of the **Advanced** tab that is provided in the service drill-down option.



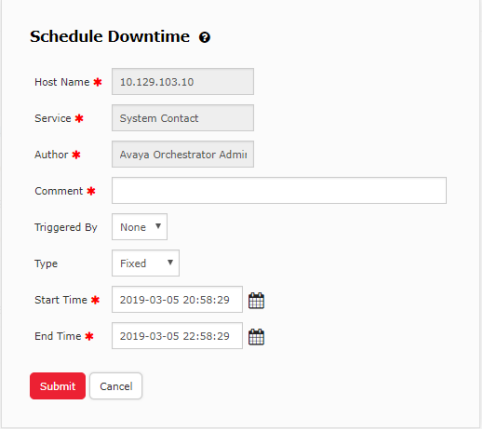
Service Attributes

These elements control the data collection process. There should be no need to change any of the settings in this area. These are more for Avaya services personnel to use during debug timeframes.

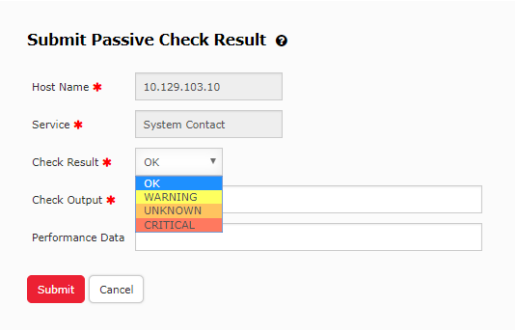
Commands options

The ***Commands*** area has options to configure the required downtime for the service.

- **Add comment**: Use this option to add a comment for the problem, without acknowledging the problem.
- **Schedule downtime**: There is a separate menu item for this activity, but it is also accessible here in the **Advanced** tab. You can add comments as well as administer specific window of downtime that stops all notifications during that period.



- **Submit passive check result**: Use this option to change the reference alarm level and the associated alarm out message for problems. The option that you select in the **Check Result** field is the new reflected level of alarm, and the option that you select in the **Check Output** field is the associated alarm verbiage represented in reports.



- **Send customer notification**: Use this option to send an updated comment to an Email or SMS notification. Select the “Forced” option to send the notifications immediately, regardless of the users’ administered Time-of-Day selection for notification receipt.

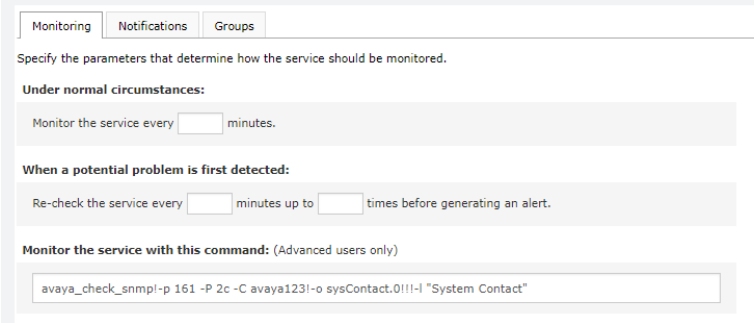
- **Delay next notification**: Use this option to delay notifications for up to 999 minutes instead of acknowledging an issue and stopping notifications all together.

Configure tab

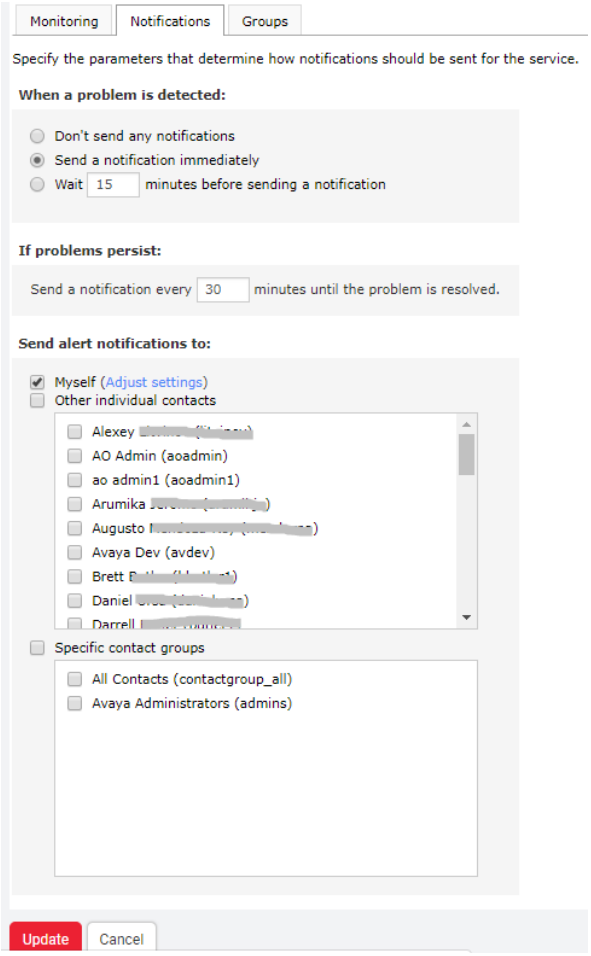
On the **Configure** tab, you can delete the service from the device, or edit some of the service settings.

The following are examples of settings available under **Re-configure this service**.

- **Monitoring**: Administer the time/rate the service is monitored by AO.



- **Notifications**: Stop notifications, delay notifications, or set specific time frames for consistent notifications when alarms for the service are received. Select the users and/or groups to receive notifications related to the service.



Chapter 3: Hardware configuration

This chapter contains information about how to administer each hardware device with the appropriate SNMP, REST API, and CLI API settings.

Overview

Prior to administering new devices in the ACP Configuration Wizard, each hardware device must be administered for SNMP. When the SNMP administration is finished, the device detection activity in Avaya Orchestrator succeeds during the subsequent rack administration of the deployment process. This section explains how to configure each hardware element with the appropriate level of SNMP.

SNMP protocol assignments

For more information about SNMP assignment for all hardware components supported in an ACP 4200 4.0 solution, see Protocol requirements for hardware components. It also provides additional port assignment information that is required to configure Avaya Orchestrator to communicate with each hardware element.

Configuring SNMP on VSP 7254 network devices

Procedure

1. SSH into VSP 7254 device.

2. At the command prompt, run the following commands in succession:
   enable
   configure terminal

3. Run the following commands to configure VSO:
   snmp-server community avaya123 index avaya
   snmp-server host <AO_IP_Address> v2c readview

4. If SAL Gateway is also being deployed in the solution, run the following command to configure SAL Gateway:
   snmp-server host <IP of SAL GW> v2c avaya123

5. Run the following commands to save the changes and exit the configuration:
   exit
   save config

6. At the command prompt, run the following command to verify SNMP administration.
   show running-config

   Press the space bar to scroll through the configuration to find the SNMP settings and values.

Configuring SNMP on G450 Media Gateways

Procedure

1. SSH into the G450 media gateway by using root credentials.

2. At the command prompt, run the following commands in succession:
   set port trap enable
   snmp-server enable notifications
   snmp-server host <AO_IP_Address> traps v2c avaya123

3. If SAL Gateway is also being deployed, run the following command:
   snmp-server host <AO_IP_Address>,<SAL_GW_IP> traps v2c avaya123

4. Run the following commands to write and save changes and add the configuration to the boot parameters:
   copy running-config startup-config
   reset
5. At the command prompt, type the following command to verify SNMP administration:
   show snmp

Configuring SNMP on HPE servers

Note: Servers require two elements to be administered: ESXi and iLO.

Configuring SNMP v2c on ESXi

Procedure

1. Using SSH, access the ESXi host IP address.

2. Run the following command to enable SNMP on the ESXi host:
   esxcli system snmp set --enable true

3. Run the following command to set the community string to be exchanged between the ESXi host and the trap receivers:
   esxcli system snmp set --communities <community string>

4. Run the following command to configure the trap receiver target for the ESXi SNMP output:
   ***esxcli system snmp set -t <target IP* Address>@162/CommunityString, SAL_GW_IP@162/CommunityString**

   Port 162 is the standard and default SNMP port for receiving, but any port number can be assigned.
   Up to three trap destinations can be administered and must be separated by commas with no subsequent space.

5. Run the following command to enable the traps to be send to the target receivers:
   esxcli system snmp set -e yes

6. Run the following command to review and confirm the SNMP settings:
   esxcli system snmp get

```
[root@cpod4srv9mgt:~] esxcli system snmp get
   Authentication:
   Communities: avaya123
   Enable: true
   Engineid: 00000063000000a100000000
   Hwsrc: indications
   Largestorage: true
   Loglevel: info
   Notraps:
   Port: 161
   Privacy:
   Remoteusers:
   Syscontact:
   Syslocation:
   Targets: [redacted]@162 avaya123, [redacted]@162 avaya123
   Users:
   V3targets:
[root@cpod4srv9mgt:~]
```

7. Run the following command to send a test trap and confirm that the administered destination receives notifications:
   esxcli system snmp test

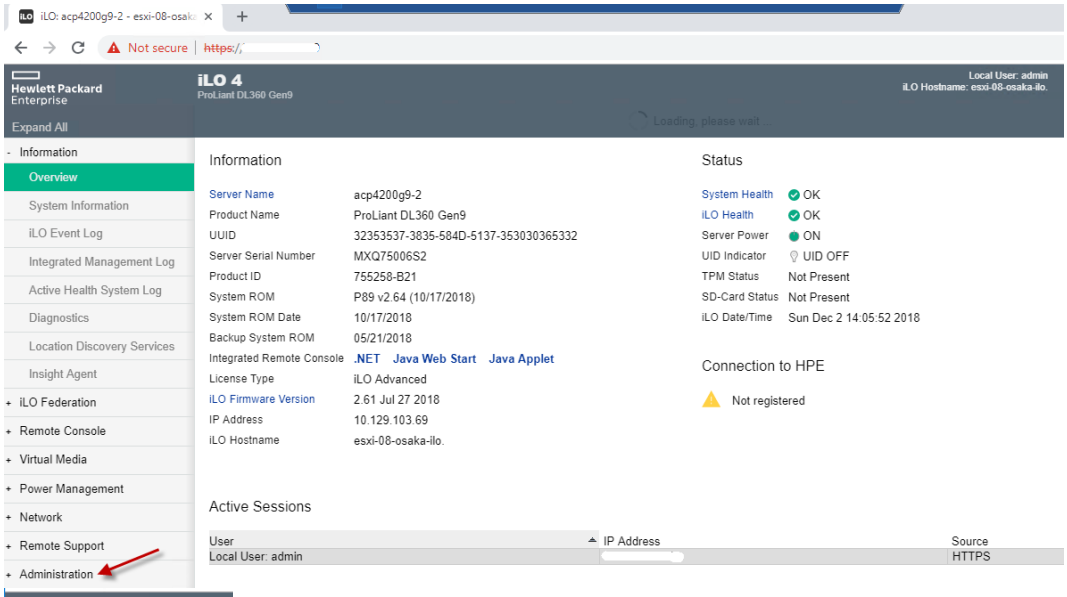
Configuring SNMP v2 on iLO

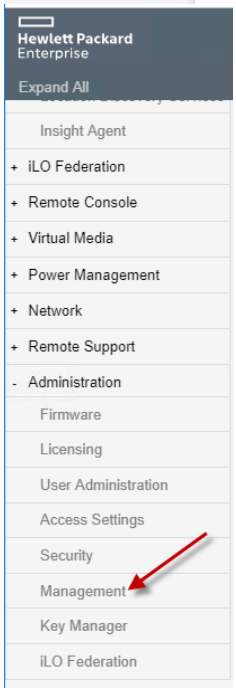
Configuring SNMP v2 for HPE Gen 9 servers and iLO 4

Procedure

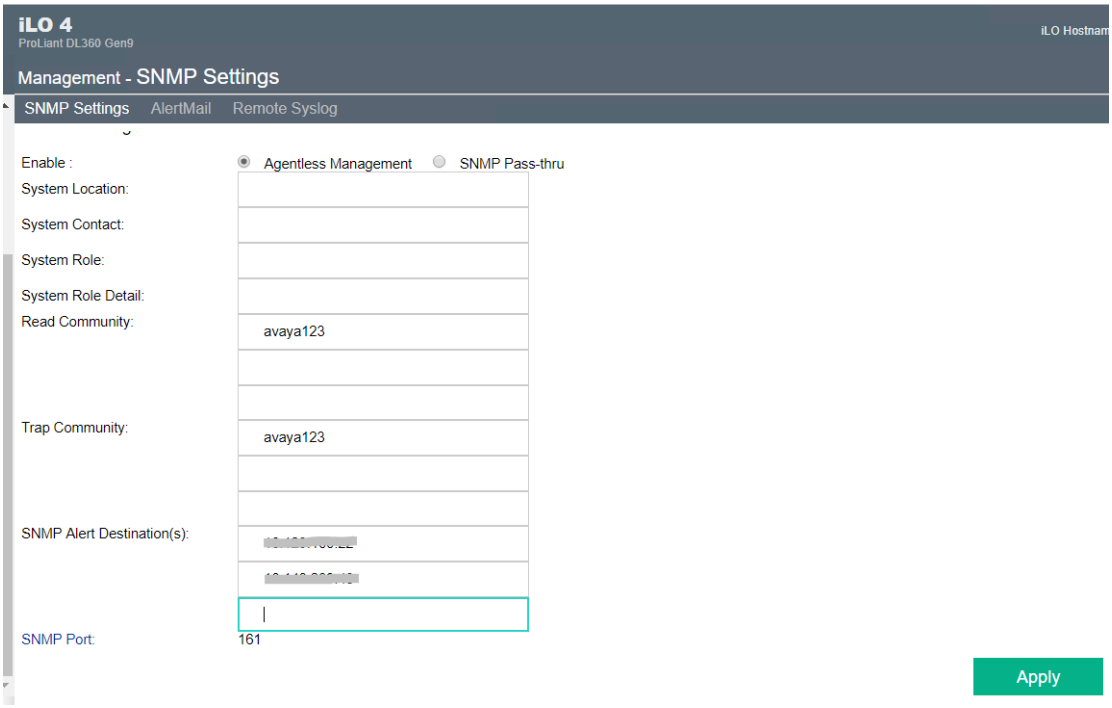
1. On the web UI, type the IP address of the iLO.

2. In the left navigation pane, click **Administration** > **Management**.





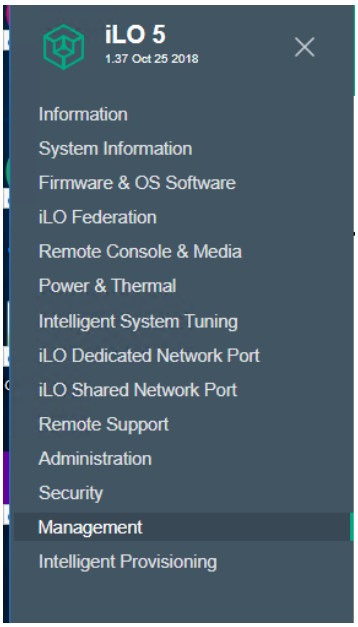
3. In the SNMP Settings area, do the following.
   - Click **Agentless Management.**
   - In the **Read Community** and **Trap community** fields, type the community string *avaya123.*
   - In the **SNMP Alert Destination(s)** field, type the IP addresses of Avaya Orchestrator and SAL Gateway.
   - Click **Apply**.



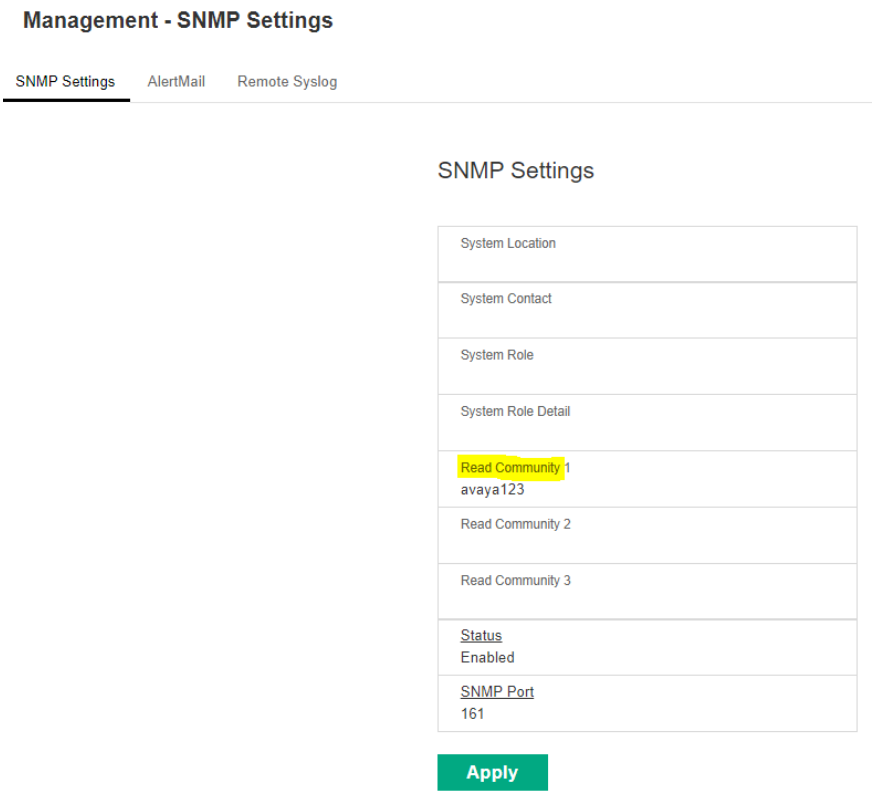
Configuring SNMP v2 for HPE Gen 10 servers and iLO 5

Procedure

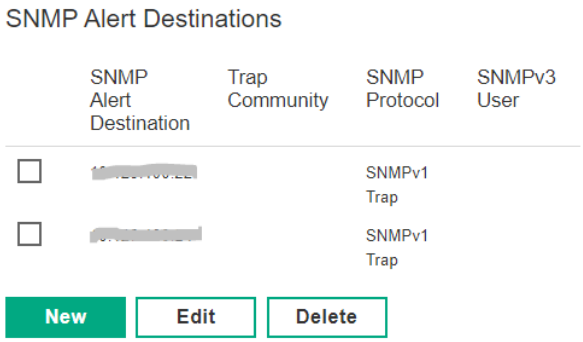
1. On the web UI, type the IP address of the iLO from the LCW.
2. In the left navigation pane, click **Management**.



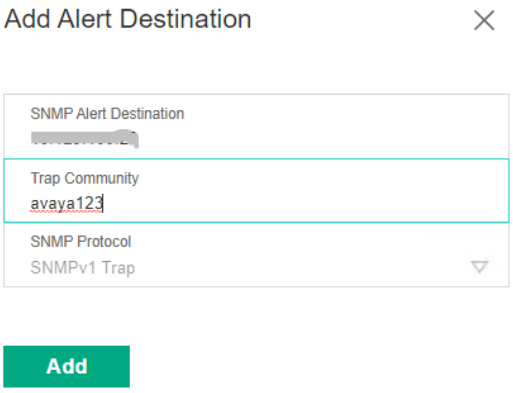
3. On the top portion of the administrative screen, in **Read Community**, type *avaya123,* and then click **Apply**.



4. At the bottom portion of the administrative screen, in the **SNMP Alert Destinations** area, click **New** to add a new SNMP trap receiver.



5. In the **SNMP Alert Destination** field, type the IP address of AO.
6. In the **Trap Community** field, type *avaya123*.
7. Click **Add**.
8. Repeat the new entry process and include the SAL Gateway IP address as a trap receiver.

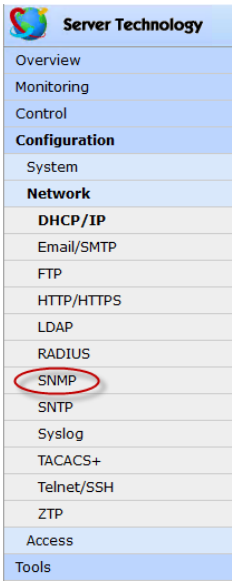


Configuring SNMP v2c on Sentry 4 PDUs

Procedure

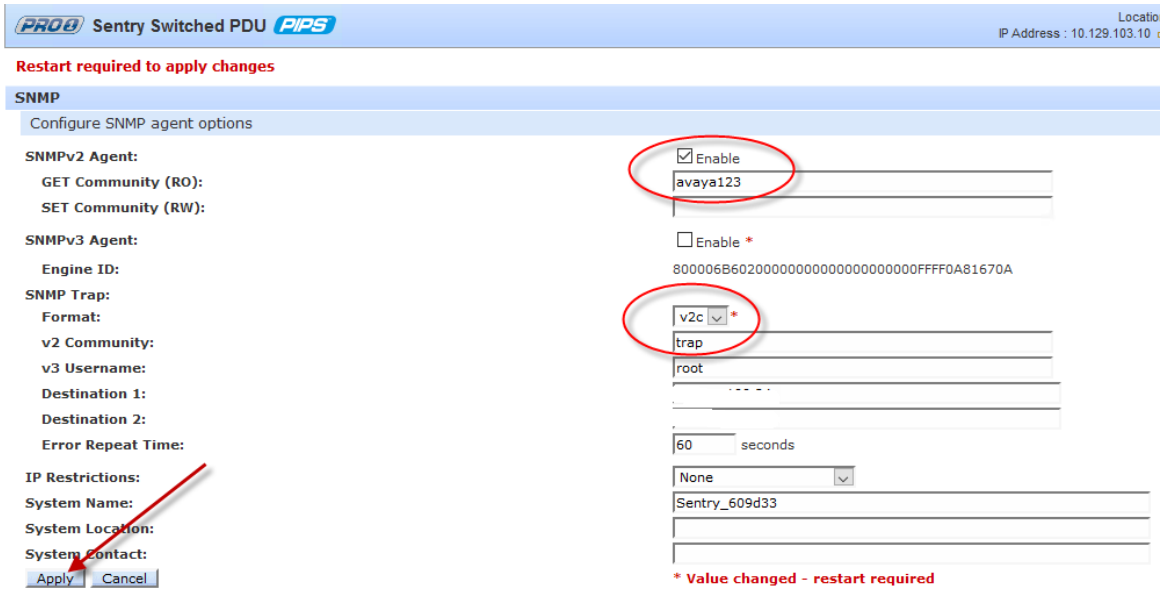
1. Start Chrome and access the PDU IP address by using the credentials provided in the IP template.
2. In the left navigation pane, click **Configuration** > **Network**.

3. Click **SNMP**.

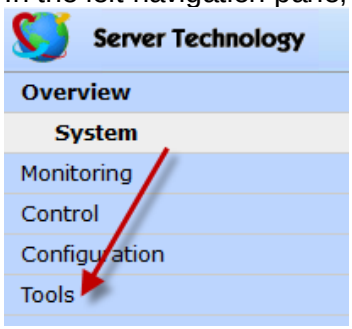


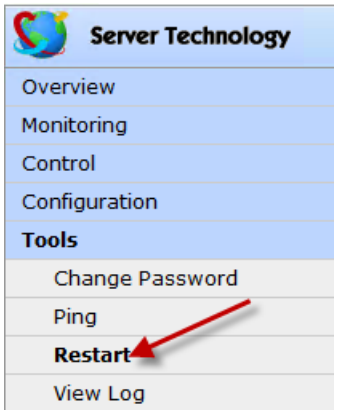
4. Select the **Enable** check box corresponding to the **SNMPv2c Agent** field.
5. In **Get Community (RO)** field, type the community string: avaya123
6. In **SNMP Trap**, in the **Format** field, click **v2c**.

7. Leave remaining default values and click **Apply**.

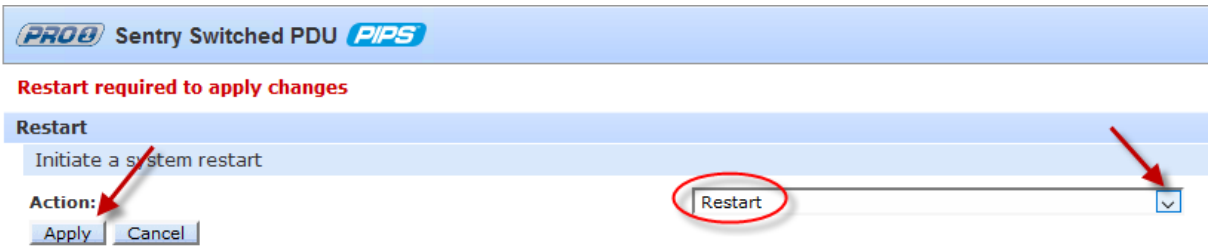


8. In the left navigation pane, click **Tools** > **Restart**.





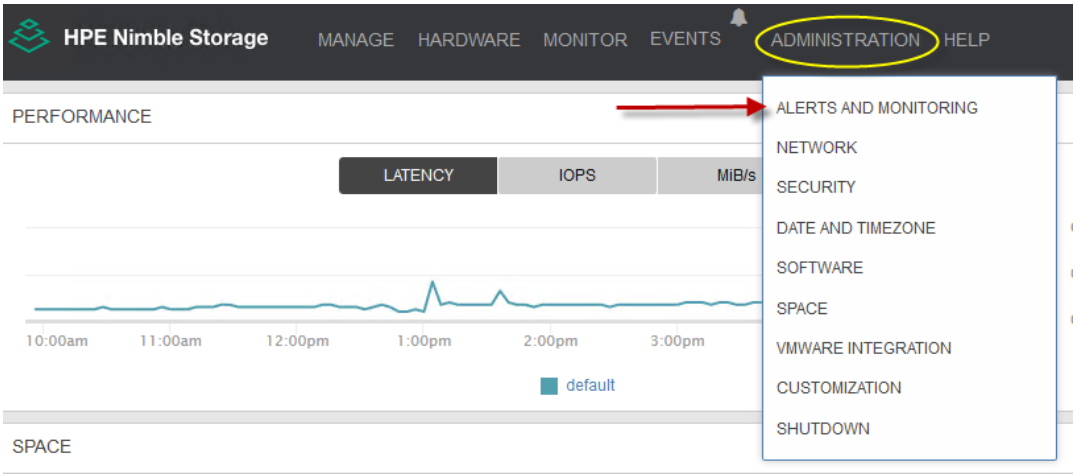
9. In the **Action** field, click **Restart**, and then click **Apply**.



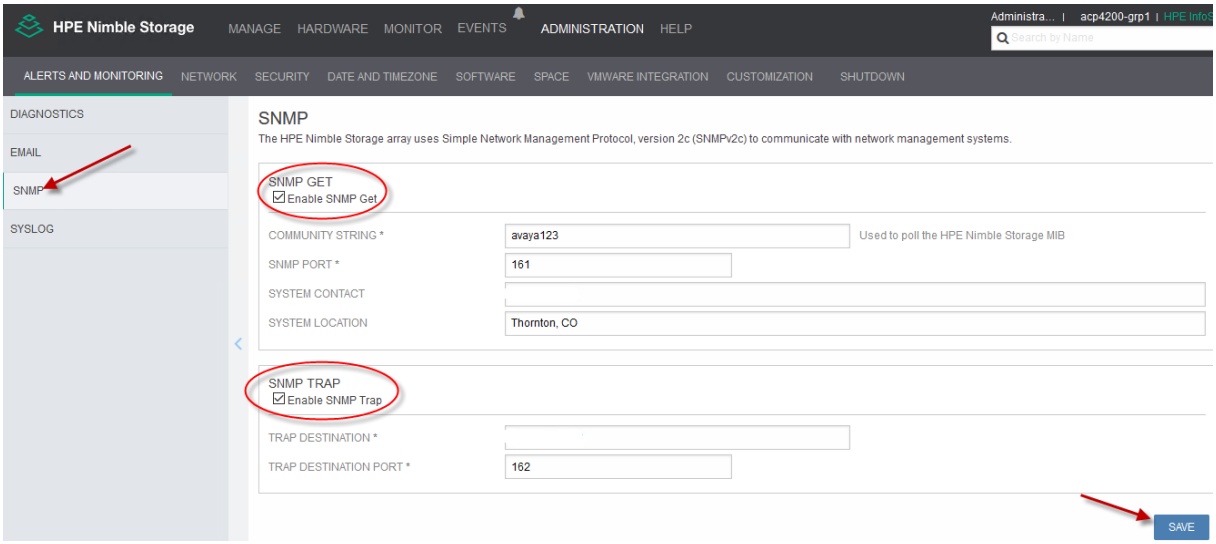
Configuring SNMP v2c on a Nimble Core

Procedure

1. Using the credentials in the IP template, access the Nimble Core IP address through a web UI and https.
2. Click **Administration** > **Alerts and Monitoring**.



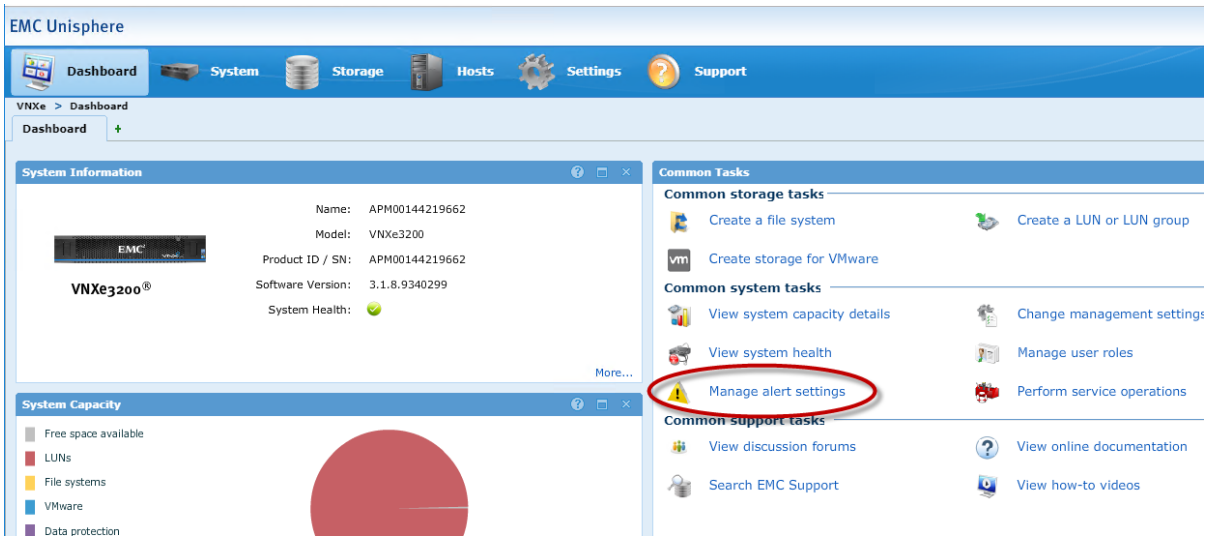
3. On the **Alerts and Monitoring** menu, click **SNMP**.
4. On the SNMP page, do the following:
5. Select the **Enable SNMP Get** and **Enable SNMP Trap** check boxes.
6. In the **Community String** field, type *avaya123*.
7. In the **Trap Destination** field, type the IP address of the SAL Gateway that is provided in the IP template, and then click **Save**.



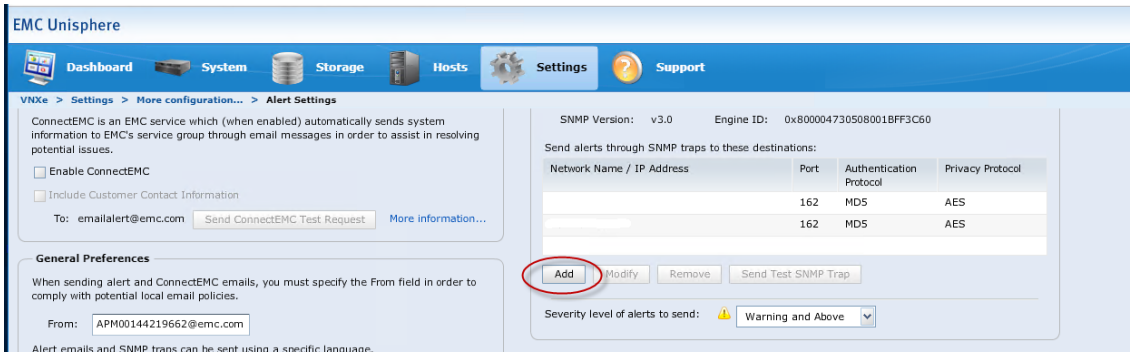
Configuring SNMP on an EMC VNX 3200e

Procedure

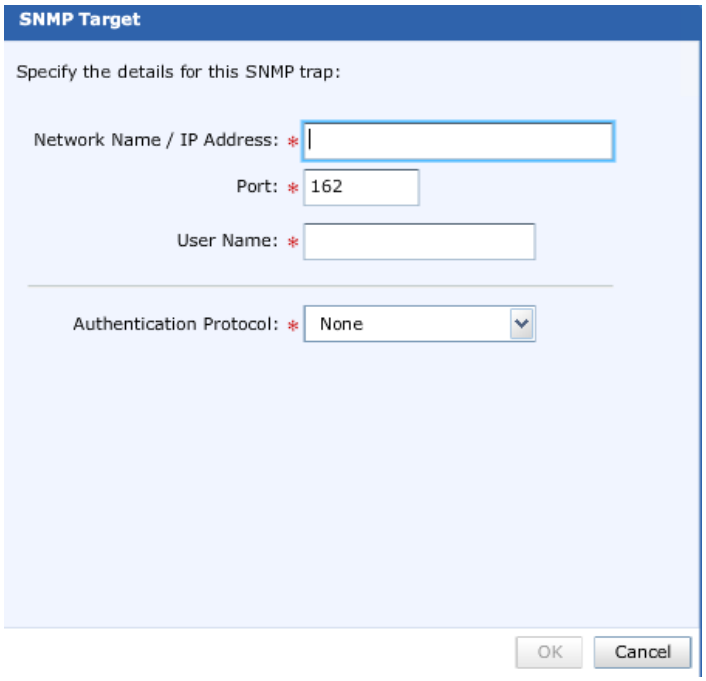
1. Open a web browser and access the 3200 device by using the IP and administrator login credentials provided in the IP template.
2. Click **Dashboard**.
3. In the **Common system tasks** area, click **Manage alert settings**.



4. Click **Add** to administer Avaya Orchestrator as an SNMP trap destination.

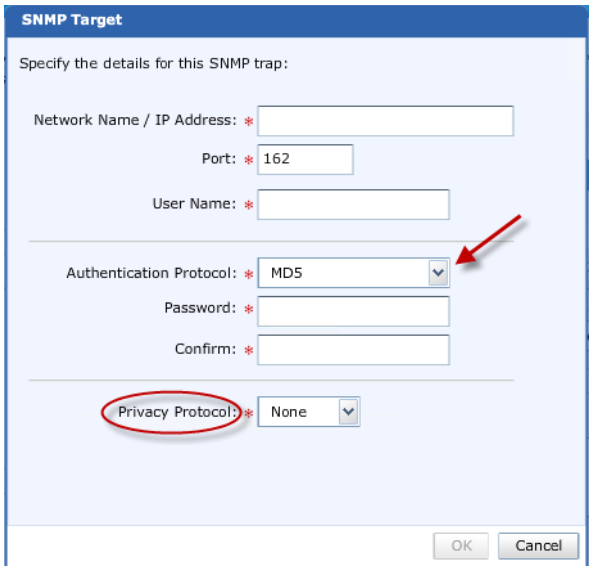


The **SNMP Target** dialog box appears.



5. In the **Network Name / IP Address** field, type the IP address of Avaya Orchestrator.
6. In the **Port** field, retain the default port number 162.
7. In the **User Name** field, type *avaya*.
8. In the **Authentication Protocol** field, click **MD5**.
9. In the **Password** field, type *avaya123*.
10. In the **Confirm** field, retype the password.
11. In the **Privacy Protocol** field, click **AES**.

    The **Privacy Protocol** field appears after you select the authentication protocol in the **Authentication Protocol** field.



12. In the **Privacy password** field, type *avaya123*.
13. In the **Confirm** field, retype the privacy password.

14. Click **OK**.

Chapter 4: Solution configuration

Overview

This chapter provides information about using the Configuration Wizard to administer ACP 4200 racks for alarm monitoring. After the ACP 4200 racks are administered, all devices are supported in Avaya Orchestrator for incoming traps and proactive state-of-health monitoring.

Configuring racks

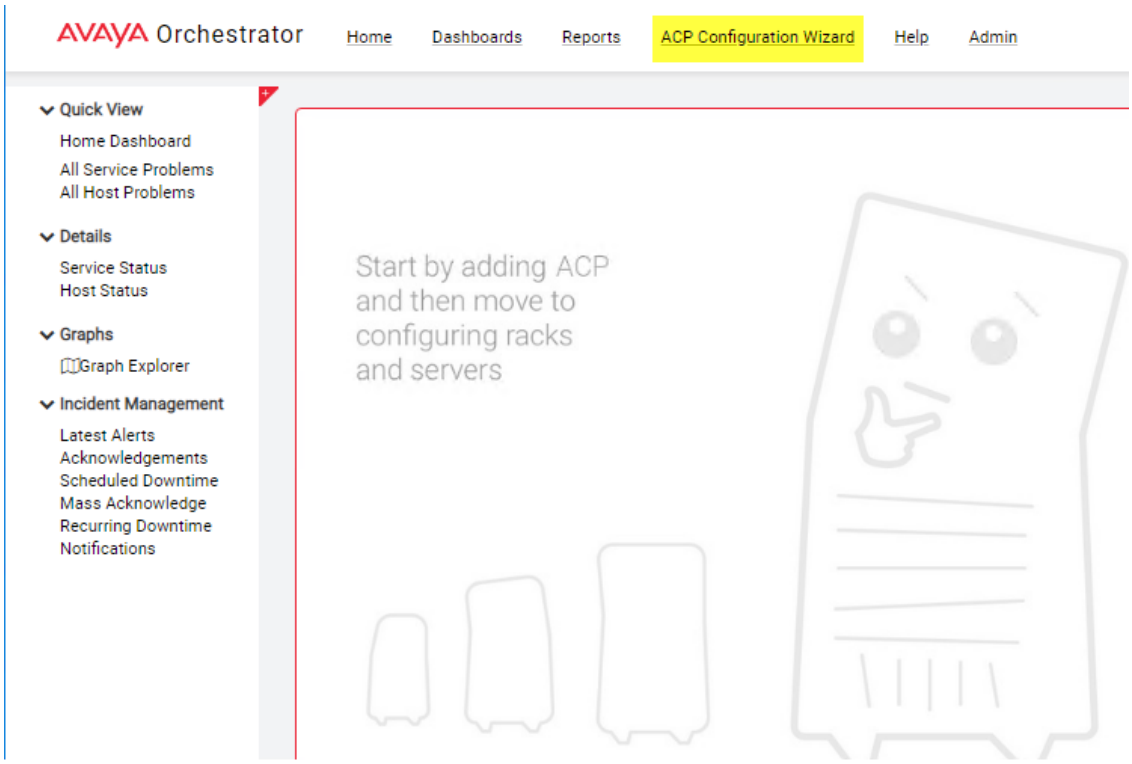
Important:
The ACP rack creation and configuration procedures are completed after you click **Finish**. If you leave the page either by pressing a back space or a web UI time-out occurs, all new un-submitted administration changes are lost. You must re-enter and re-submit the administration information.

Initial configuration

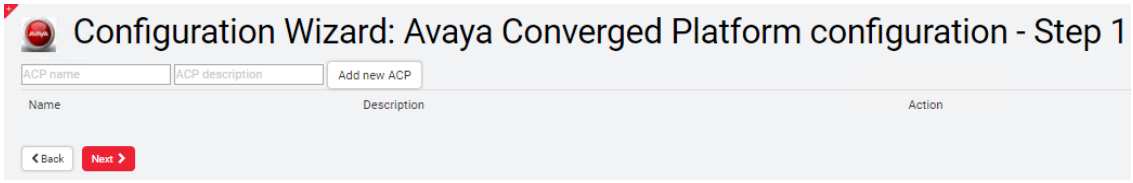
Before you begin
You must have administrative user rights or have the **Can configure hosts and services** permission to access the ACP Configuration Wizard.
For more information, see Managing permissions.

Procedure

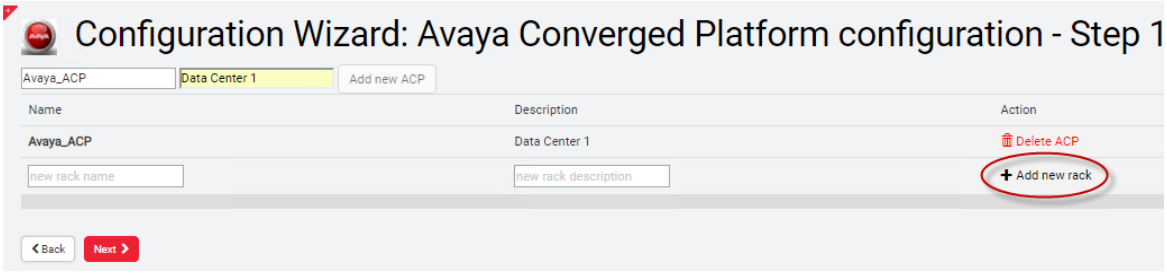
1. Log in to Avaya Orchestrator.
2. On the menu bar, click **ACP Configuration Wizard** to start the wizard.



Step 1 of the Configuration Wizard appears.

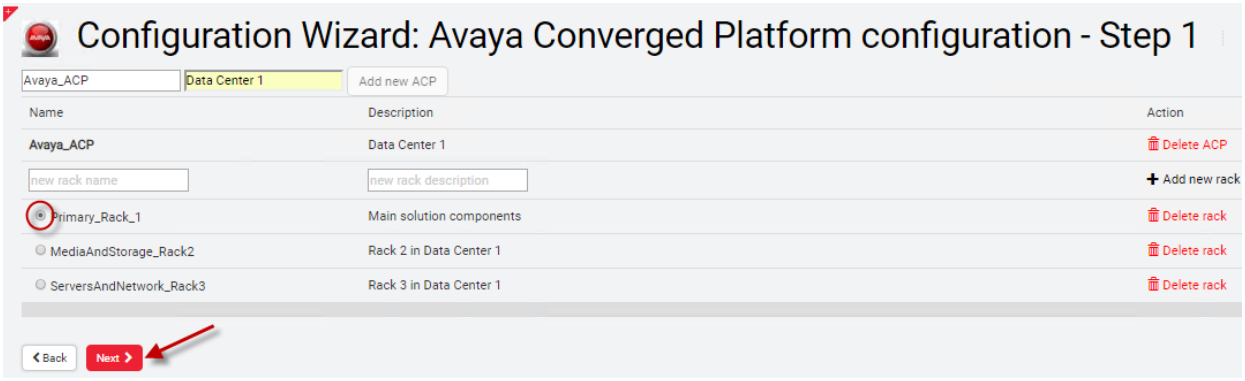


3. Do the following to add a new ACP:
   a. In the **ACP name** field, type the name intended for the new ACP solution as mentioned in the IP template.
      Note:
      Only digits, a-z, A-Z letters, underscore (_), hyphen (-), and dot (.) symbols are allowed for the ACP name. Limit for symbols in the ACP name is 25. Spaces between characters are not permitted.
   b. In the **ACP description** field, type a description for the new ACP solution.
      ACP description is optional.
   c. Click **Add new ACP** to add the new ACP solution.

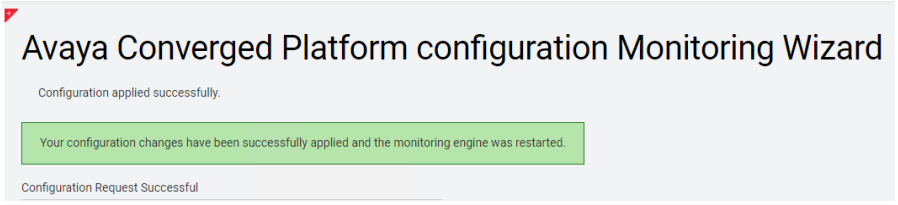


4. Do the following to add a new rack:
   a. In the **New rack name** field, type a name for the first rack.
      Note:
      Only digits, a-z, A-Z letters, underscore (_), hyphen (-), and dot (.) symbols are allowed for rack name. Limit for symbols in rack name is 25.
   b. In the **New rack description** field, type a description for the new rack.
      The rack description is optional.
   c. Click **Add new rack** to add the new rack.

5. Repeat Step 4 to add all racks in the solution.

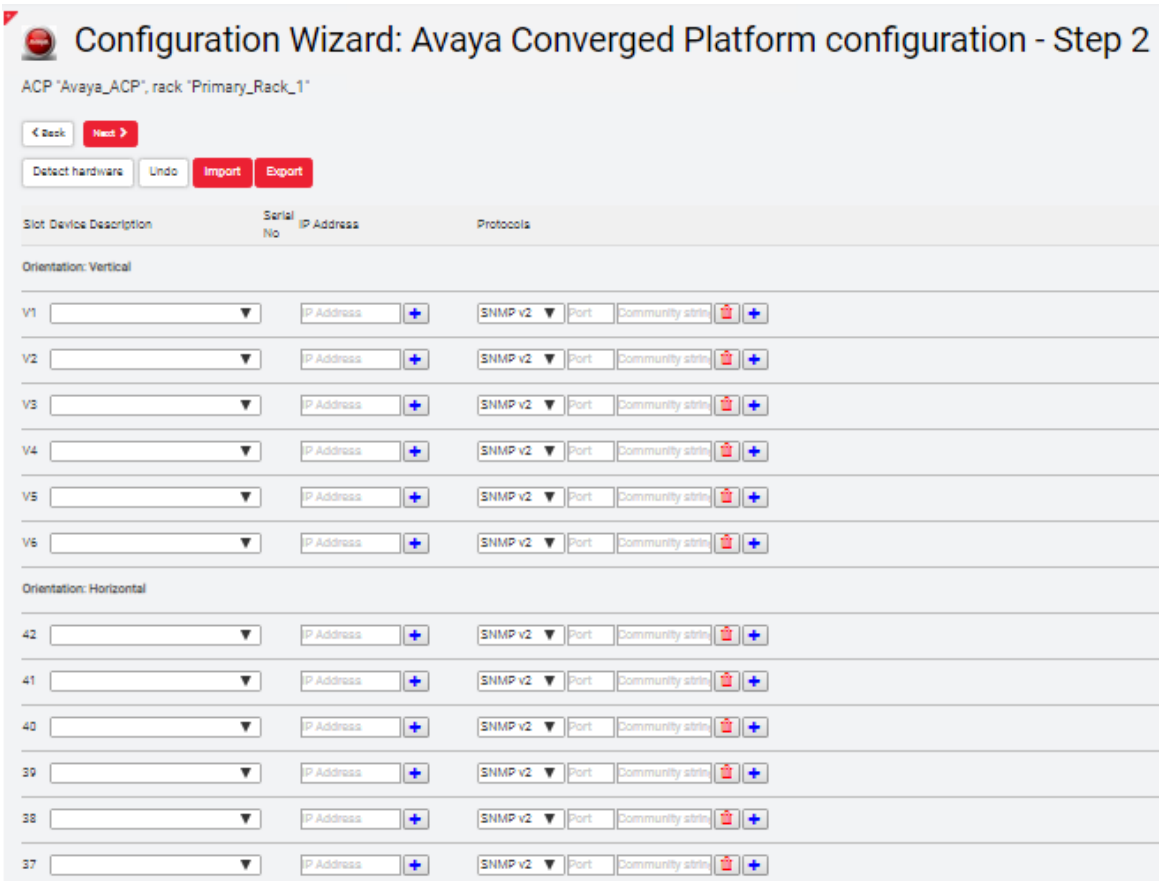


Note:
At this point, administers can continue to build the AO solution by clicking **Next** to proceed to the next section, or can opt to save the solution and rack information by clicking **Next**, and then **Finish** on the subsequent page. The current administered information is saved when you click **Finish**.



6. To administer rack elements, select the radio button corresponding to the rack that you want to deploy as shown in the screen shot in Step 5, and then click **Next**.

Step 2 of configuration wizard appears.



Total 48 slots are displayed.

The first six slots (V1-V6) represent vertical equipment placement on the rear side of the rack, that is, PDU devices. The following charts indicate the placement of the devices based on the rack size being deployed.

48" Rack View of Vertical PDU Assignments					
V1	V2	V3	V4	V5	V6
Primary 3	Secondary 1	Primary 1	Primary 2	Secondary 2	Secondary 3

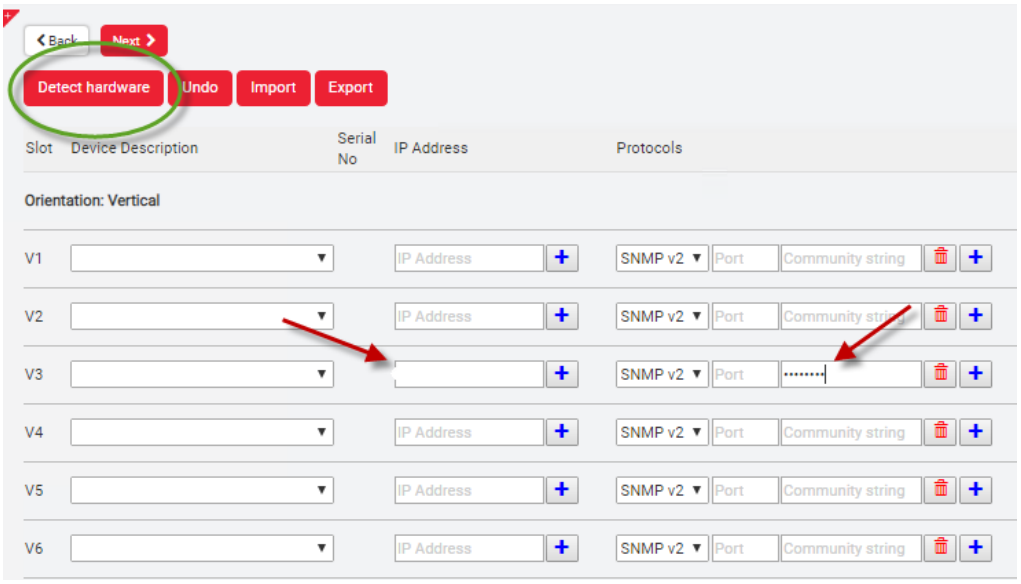
42" Rack View of Vertical PDU Assignments					
V1	V2	V3	V4	V5	V6
Secondary 1	Primary 1	Unused	Unused	Primary 2	Secondary 2

Slots 1-42 represent the horizontal MTUs that can be viewed from the front side of the rack and can support the following devices: servers, network switches and routers, storage arrays, media servers, and some horizontal PDUs.

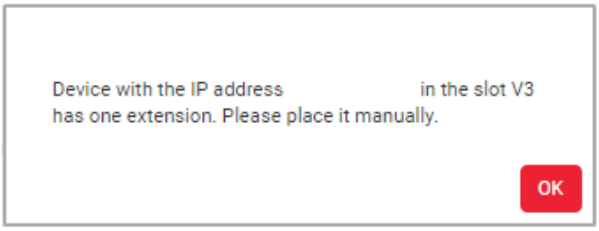
There is no limit to the number of devices that you can add at any one time. However, the greater the quantity of devices and elements being simultaneously entered, the longer the Finish process takes to complete.

Note:
There are filler components that you can select for each slot. You can hover over the **Slot Device Description** field to view these filler components. One example of such a filler is the *Horizontal filler* that is used to represent empty slots, whether empty for air flow considerations or for representing the availability of a slot for future hardware deployments.

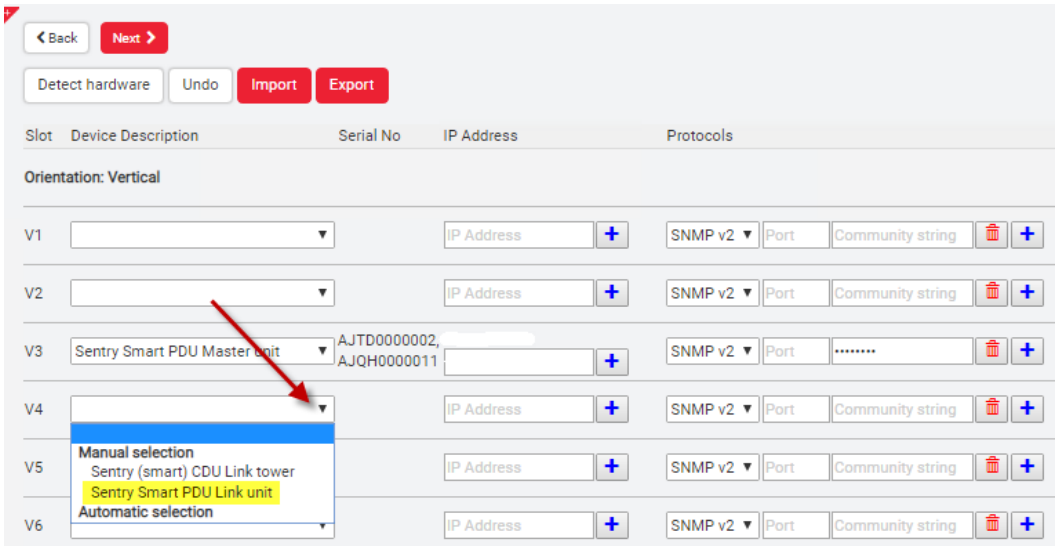
7. Do the following to add a PDU:
   a. In the **IP address** field corresponding to slot V3, type the IP address of the first master PDU.
   b. In the corresponding SNMP **Community string** field, type *avaya123*.
   c. Add any additional PDUs in slots V2 and V1.
   d. Click **Detect hardware**.



The expansion units associated with each master PDU do not have an IP address to administer. The AO tool reminds administrators to place a filler field where the partner expansion unit is to be located after the administrators click **Detect hardware**.



e. Based on the PDU administration in slots V1-V3, click **Sentry Smart PDU Link unit** as filler information in the lists corresponding to slots V4-V6.

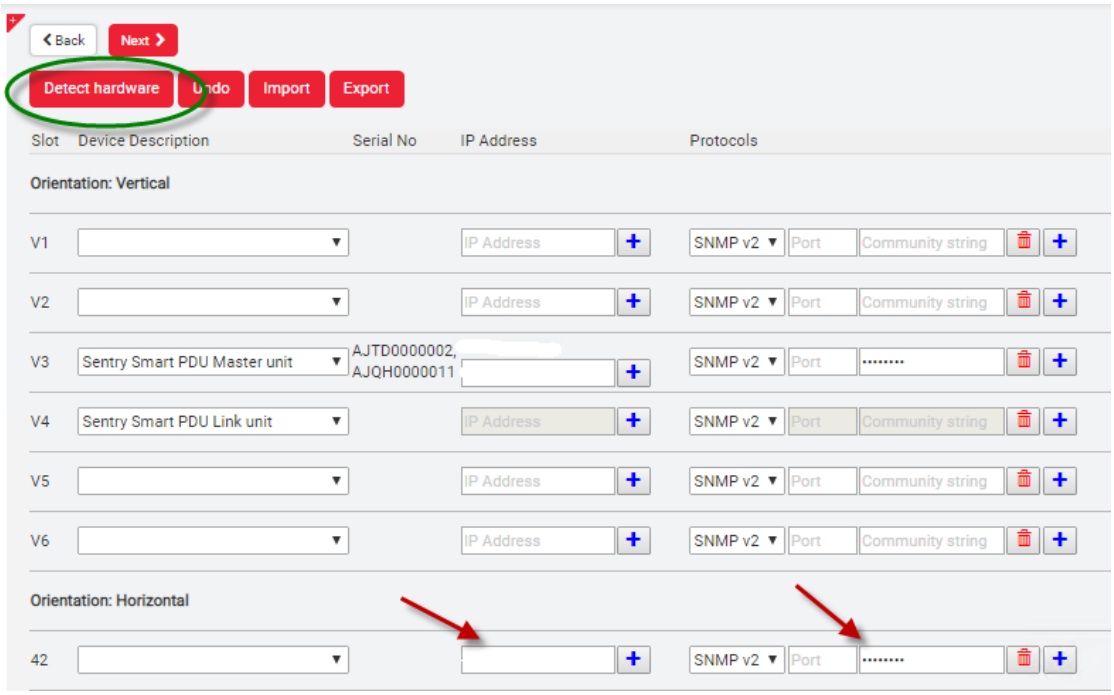


Note:

At this point, administrators can do one of the following:

- Continue to the next device to be administered.
- Click **Detect hardware**, click **Next**, and then click **Finish** to save the current administered values.

8. Do the following to administer VSP devices:
   a. At the slot location for the first VSP device, type the IP address that is provided in the IP template.
   b. In the **Community string** field corresponding to SNMP v2c, type *avaya123*.

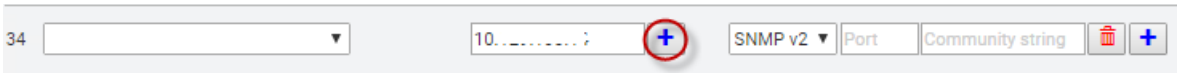


Note:

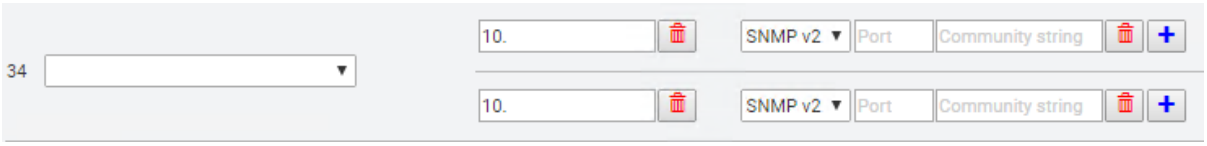
At this point, administrators can do one of the following:

- Continue to the next device to be administered.
- Click **Detect hardware**, click **Next**, and then click **Finish** to save the current administered values.

9. Do the following to administer servers:
   a. Locate the slot for the first server and type the IP address for the ESXi element.

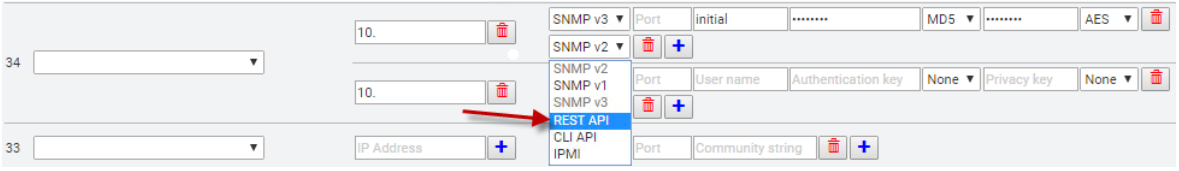


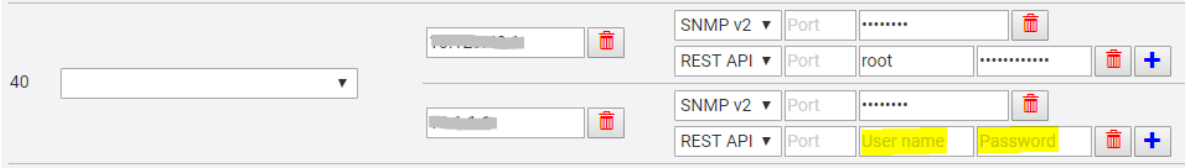
   b. After you enter the ESXi IP address, click the + icon to add a second IP address field for the iLO IP address.



   c. After you enter the ESXi and iLO IP addresses, administer the SNMP protocols for each element. The ESXi and iLO elements each require two APIs: SNMP v2 and REST. Configure the SNMP v2 settings for both.

   d. After SNMP administration is finished, click the + icon located at the right of each SNMP row to add a REST API entry for each element. In the drop-down list for the second entry, click **REST API**.



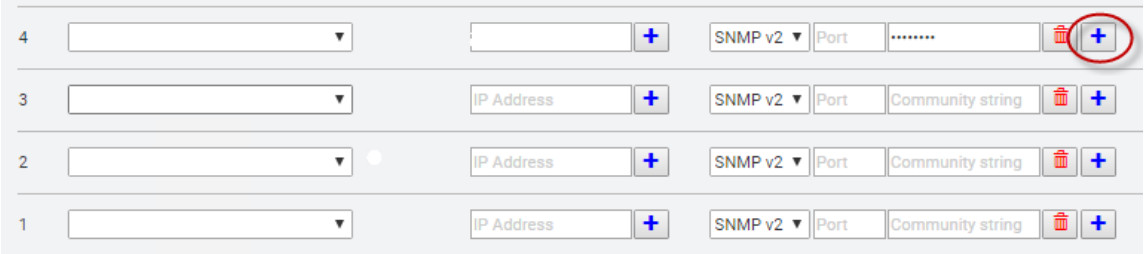


e. Type the *user name* and *password* for each REST API entry. These entries will be the login credentials for the ESXi and iLO elements for each server.

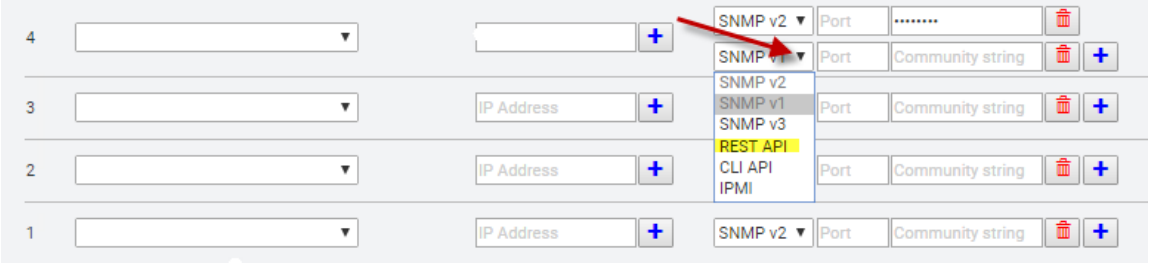
Note:

Use the delete icon to remove unwanted protocols and IP credential entries.

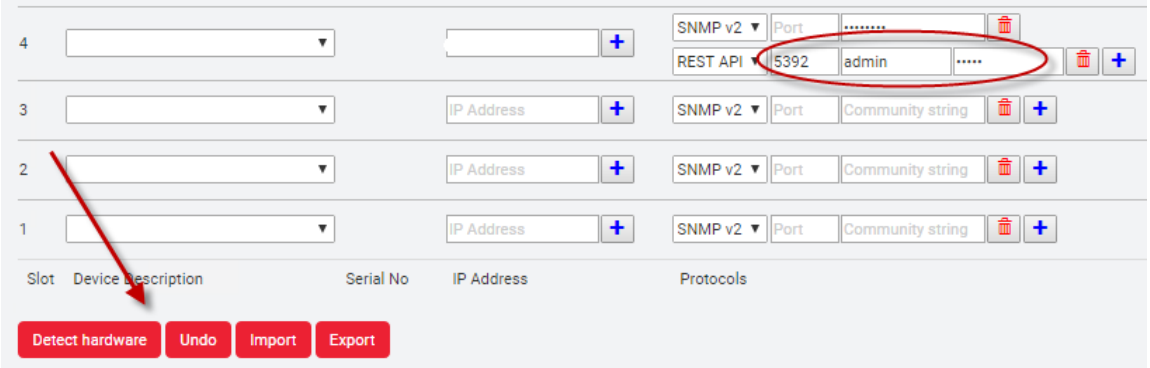
10. Do the following to administer Nimble Storage Array:
    a. Locate the upper-most slot location for the Nimble core. This is where the IP address is administered so that AO can populate the subsequent three slots below the IP entry as the 4-U physical device.
    b. The Nimble device requires two API interfaces: SNMP and REST.
        i. Administer the SNMP v2c interface first. In the **Community string** field, type *avaya123*.
        ii. Click the + icon corresponding to the SNMP v2c entry to create a second entry interface.



        iii. In the new API drop-down list, click **REST API**.

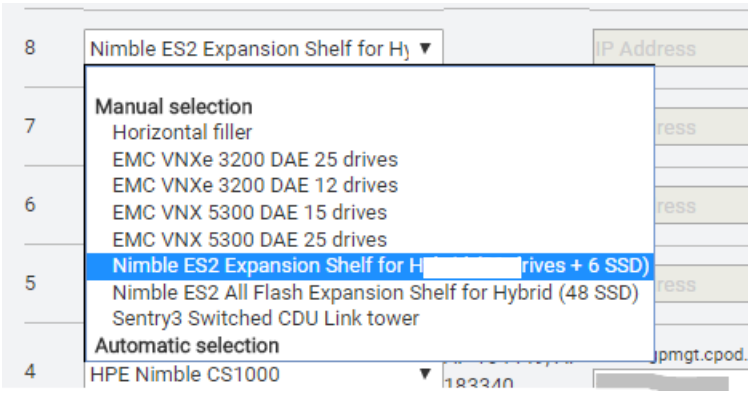


        iv. Enter port 5392 and the login credentials for the Nimble array. Then click **Detect hardware** to confirm acceptance and communication between AO and Nimble.

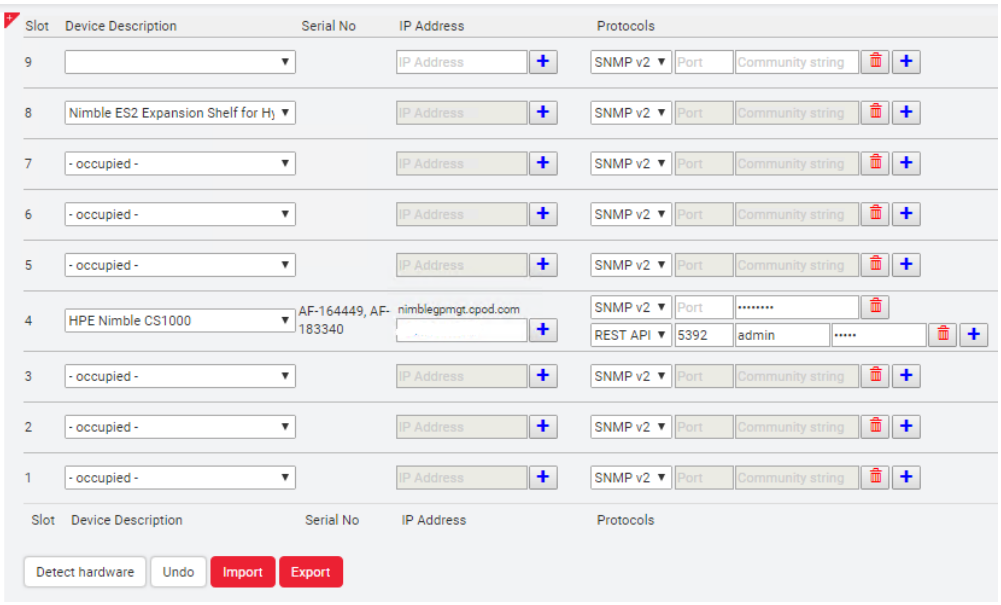


An information message appears if there is an extension module present on the Nimble array.

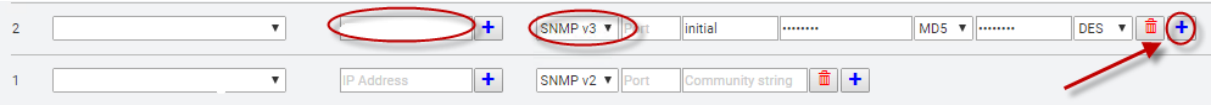
v. If an expansion unit is also being deployed in the same rack, locate the RMU of the upper-most row supporting the expansion location, and in the drop-down list, click the appropriate Nimble expansion device.



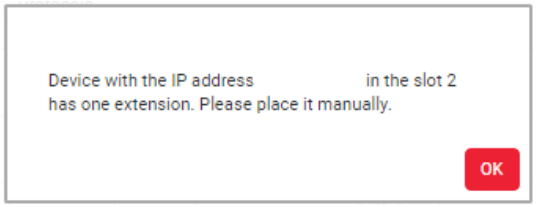
vi. Continue with the administration or click **Next**, and then click **Finish** to save administered values.
AO populates the subsequent slots to complete the physical representation of the device.



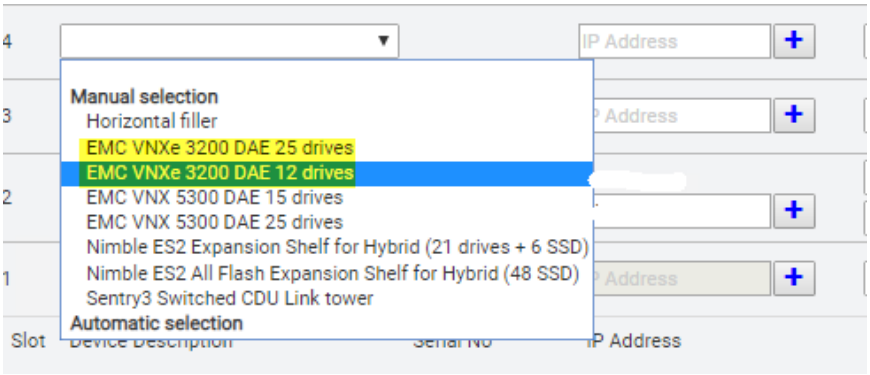
11. Do the following to administer EMC VNX 3200e:
    a. Locate the upper-most slot location for the EMC 3200 core. This is where the IP address is administered.
       The EMC device requires two API interfaces: SNMP and CLI.
    b. Administer the SNMP v3 interface first:
       I. In the **User name** field, type *initial.*
       II. In the **Authentication key** and **Privacy key** fields, type *avaya123*.
       III. In the **Authentication type** field, click **MD5**.
       IV. Click on the Privacy type, and then click AES.
       V. Click the + icon at the far-right end of the row to create a second entry interface.



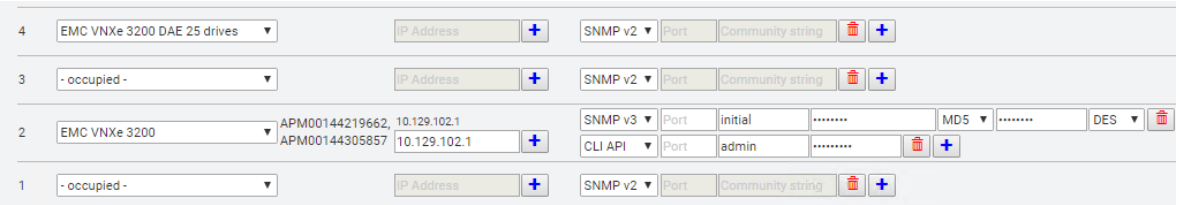
    c. In the second API drop-down list, click **CLI API**.
    d. In the **User name** and **Password** fields, type the login credentials for EMC 3200.
    e. Click **Discover hardware** to confirm device acceptance and communication between AO and the EMC 3200 device.
    f. If an expansion unit is present in the rack, an information message appears to alert the administrator to add it manually. There is no IP address associated with an expansion storage device.



g. Locate the upper-most slot location where the expansion unit is located, and then in slot filler drop-down list, click the EMC expansion device to be deployed.



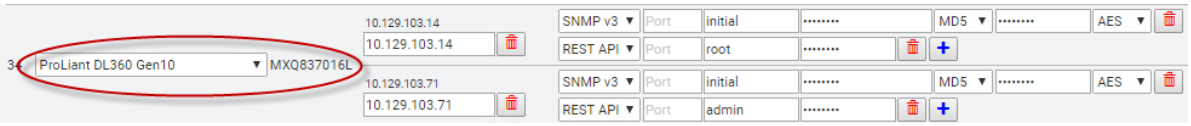
h. After you select the EMC expansion device, click **Next**, and then click **Finish** to complete and save the current administration.
AO populates the subseuqent slots to represent the physical location of the device.



12. Do the following to administer G450s:
    a. Locate the rack and slot where you want to place the G450s.
    b. Type the IP address for each device in the appropriate slot.
    c. In the **Community string** field, type *avaya123*.
    d. After all the G450 components are administered, click **Detect hardware** to confirm communication between AO and G450 devices.

13. After the devices are administered or if you want to temporarily stop the administration process, do not leave the AO administration process without saving the administered information.
    Do the following to enter and save the administered information in Avaya Orchestrator:
    - Click **Detect hardware**.

The hardware types and serial numbers are automatically detected and displayed in their corresponding slots.

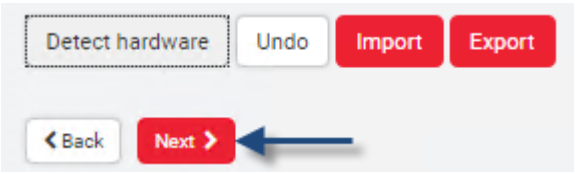


If there is undetectable administration entered, an error message appears.

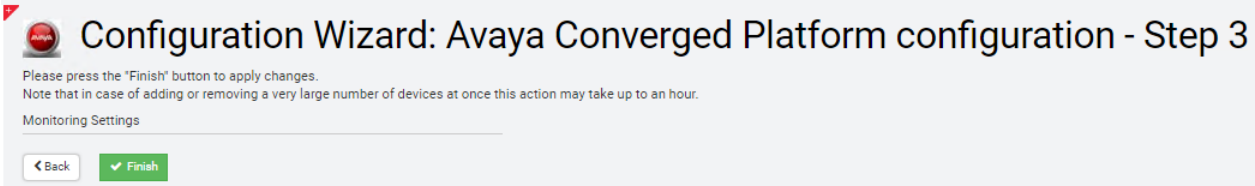
14. Do the following to identify failed entry fields:
    The fields that fail do not successfully detect the hardware type and serial number. The failed entries can be identified by the empty *Slot Device Description* fields alongside previously entered IP and SNMP information. If the administration error is known and can be rectified, do the necessary changes and click **Detect hardware** after each change until all devices are accepted.

15. Do the following to remove unwanted entries:
    After you click **Detect hardware**, any entry that is incorrect must be removed. For example, an incorrect IP address or a wrong slot administered. Press the space bar in the **IP address** field to remove the IP address, and then click **Detect hardware**. AO removes all associated entry data from the form.

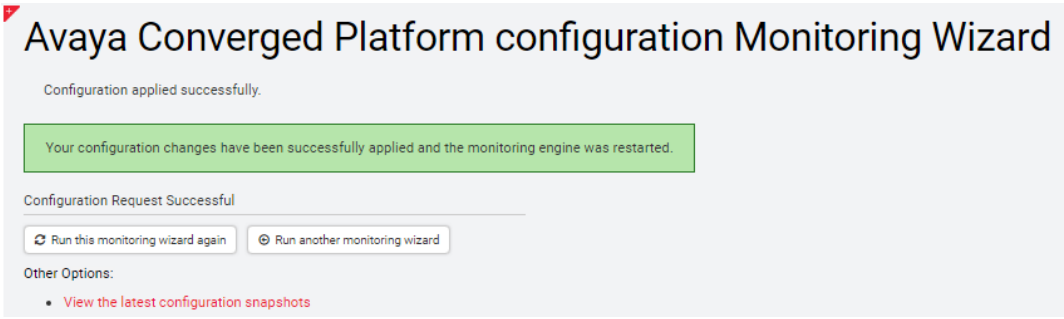
    a. After the hardware administration is complete and all hardware is successfully detected and/or removed as needed, click **Next**.



Step 3 of the configuration wizard appears.



b. Click **Finish** to save the administered information. Depending on the number of devices and racks administered, this process may take 30 seconds or up to 10 minutes. The following message appears on successful completion.



Protocol requirements for hardware components

The following table contains protocol requirements for hardware components.

HW Type	HW Model	SNMP v1	SNMP v2c	SNMP v3	REST API	CLI API
Media	G450		Yes			
PDU	Sentry 3 smart		Yes			
PDU	Sentry 4 PIPS		Yes			
Ethernet Switch	VSP 7254XSQ		Yes			
Ethernet Switch	VSP 4850GTS		Yes			
Ethernet Switch	VSP 7024XLS		Yes			
Server	HPE Gen 8, Gen 9 and Gen 10 *ESXi element*		Yes		Yes	
Server	HPE Gen 8, Gen 9 and Gen 10 *iLO element*		Yes		Yes	
Server	Lenovo RD540 (IMM)	Yes				Yes
Server	Lenovo RD540 (ESXi)	Yes			Yes	
Server	Lenovo RD340 (IMM)	Yes				Yes
Server	Lenovo RD340 (ESXi)	Yes			Yes	
Server	Lenovo RD530 (IMM)	Yes				Yes
Server	Lenovo RD530 (ESXi)	Yes			Yes	
Storage	HPE Nimble CS1000		Yes		Yes	
Storage	EMC VNX3200e			Yes		Yes
Storage	EMC VNX5300	Yes				Yes

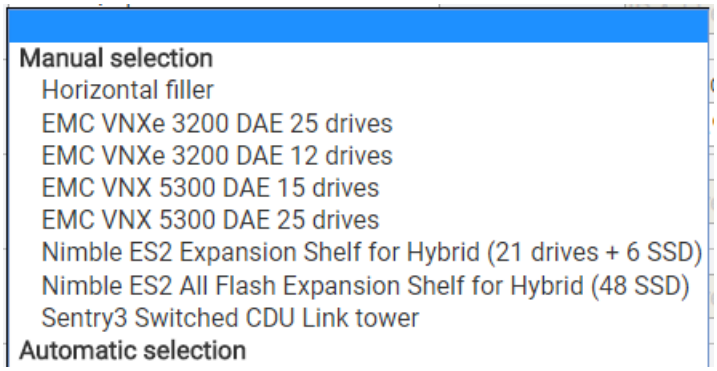
Managing rack devices

About this task

Along with adding new hardware elements, you might want to remove devices or edit the configuration. This topic contains information about additional editing options within the AO Configuration Wizard.

Procedure

1. Do the following to add a filler slot to the solution:
   a. Click **ACP Configuration Wizard**.
   b. Click the slot in the diagram that corresponds to a slot targeted for a filler label.
   c. To produce a filler panel, click the **Device Description** drop-down list to view the options.
      For reserving an empty slot for rack ventilation purposes or for future growth, click **Horizontal filler**.
      The other items noted are storage and PDU expansion elements that occupy slot space, but do not have their own IP addresses for event monitoring. After the primary/master devices are administered, AO shows a message that these partner devices must be administered manually.



   d. Click **Detect hardware**.
   e. Click **Next**, and then **Finish**.

      The hardware type and serial number of the element are automatically displayed based on the information that you provide.

      Note:

      The *Failed to get device type* message appears if an error occurs during hardware discovery. Go to the Wizard entry form to confirm the IP address and protocol information/credentials and make the necessary rectifications, and then click **Detect hardware**.

2. Do the following to delete an element from the solution:
   a. Locate the element in the list.
   b. Delete the associated IP address.
   c. Click **Detect hardware**.

      The system clears the **Device description** and **Serial No** fields.

3. Click **Next**, and then click **Finish**.

Chapter 5: Host and Service details

Overview

This chapter contains information about how to use the different features of the Avaya Orchestrator interface to view information about hosts and services. The **Details** menu offers different ways to view the status of the hosts and services. For example, in larger environments, users may want to view status by host or service group, but in smaller environments users may prefer to view status by device.

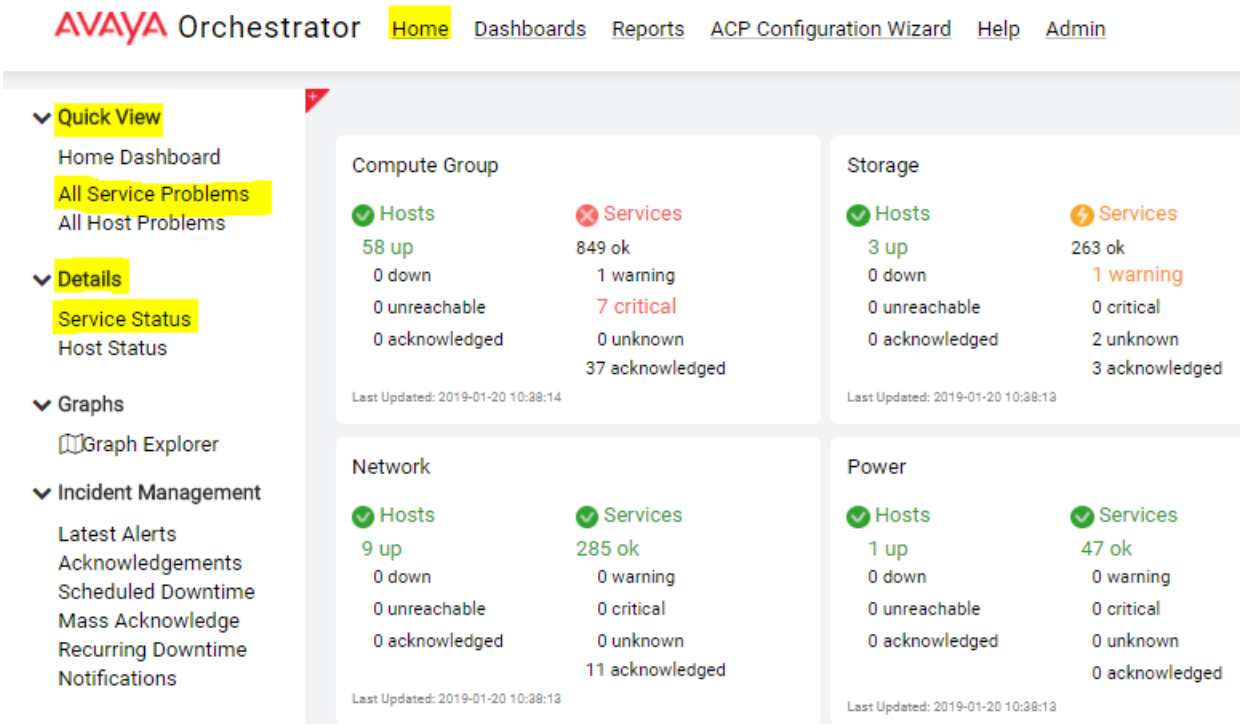
Avaya Orchestrator provides the following options to view host and service details:

- Individual hosts or services
- Host or service group summaries
- Host or service group overviews
- Host or service group grids

Service Status overview

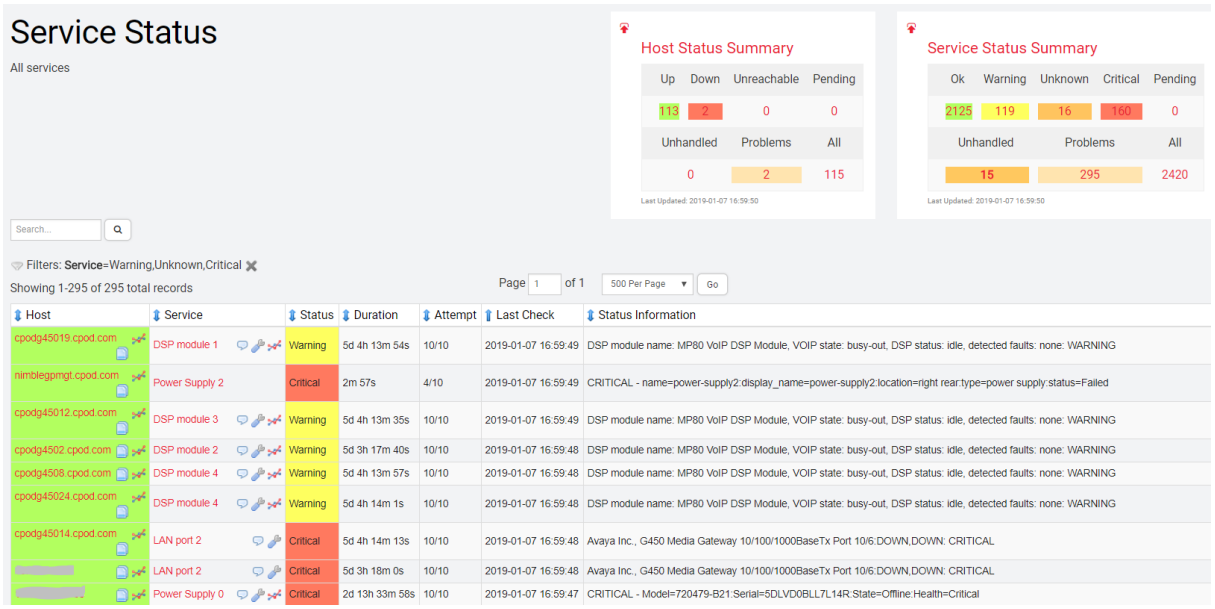
There are two high-level service related real-time reports.

- **Home** > **Quick View** > **All Service Problems**.
- **Home** > **Details** > **Service Status**.



All Service Problems

Purpose
This report provides a view only of all warnings and problems associated with the reported devices. There is no information provided for hosts services in an OK state.



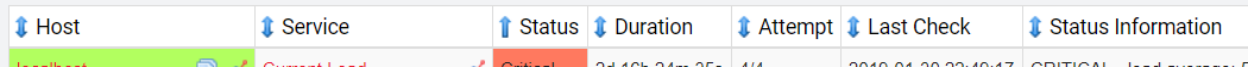
You can click the sort icon at top of the column to sort the alarms by the data in that column.

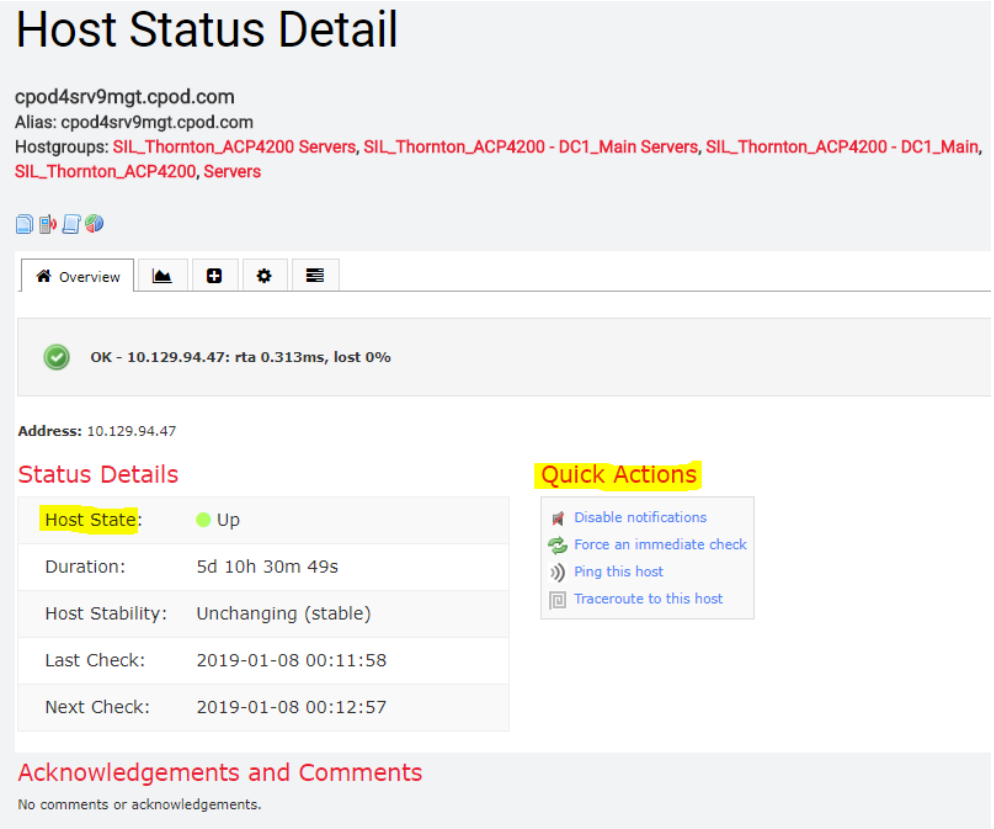
Service Problems

- **Host**: The specific device reporting an alarm event.
- **Service**: The specific function within the host that is reporting an alarm event.
- **Status**: Sort alarm events by “critical” events or “warning” events.
- **Duration**: Sort alarm events based on the length of time in the particular state.
- **Attempt**: List reports based on the number of successful checks and responses.
- **Last Check**: Sort alarms in sequence based on the last updated status.
- **Status Information**: Sort alarm events based on the type of service/host event reported.

You can click each host and service in the **Host** and **Service** columns respectively to view more information about that specific device or service. For example, if you click a host in the **Host** column, the **Host Status Detail** page for that host device appears.

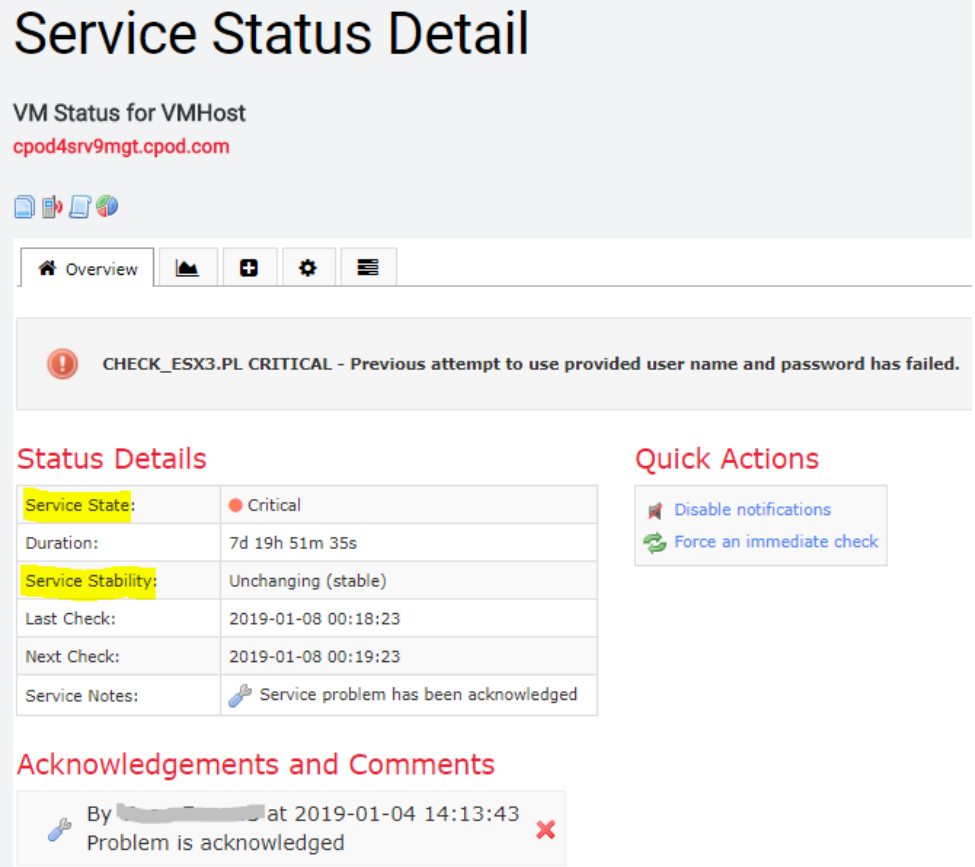
To determine how the specific view is sorted, look at the blue arrows corresponding to each of the sortable columns. The column with the single-direction arrow represents the sorted view. In the following example, the **Status** column represents the sorted view.





The **Host State** is **Up**, which confirms to the green (OK) status color of the host device. There are several **Quick Actions** available, as needed, to provide quick insight into potential problems with a host.

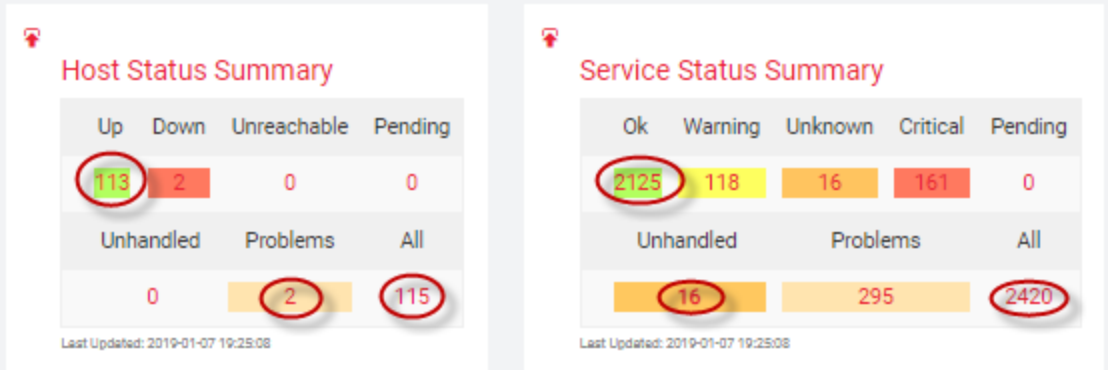
If you click a service in the **Service** column corresponding to the host, the **Service Status Detail** page for that service item appears.



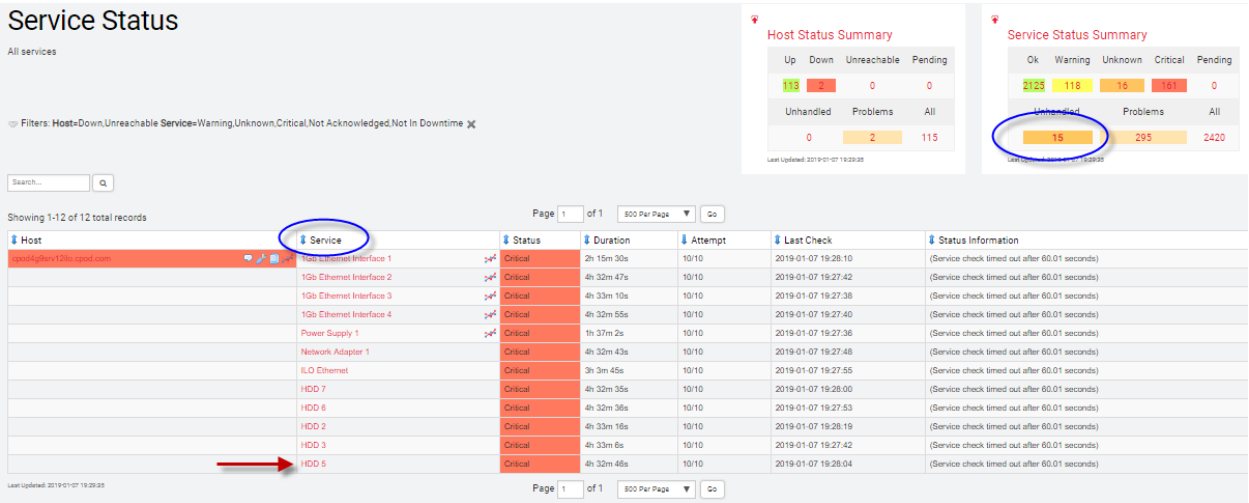
In the preceding screen shot, the **Service State** is Critical, confirming the corresponding red color of the service state on the primary report page. The **Service Stability** is Unchanging, indicating that the problem still exists for the AO tool. At the top of the detailed information, a description of the issue is provided. In the preceding example, Avaya Orchestrator is unable to access the ESXi host. The message “Previous attempt to use provided user name and password has failed” appears. You can resolve this problem by confirming and re-administering the proper host and/or service credentials in the ACP Configuration Wizard.

Additional views of all device states, including healthy device services, are available when you click the respective links. You can click the available links to become more familiar with how to navigate to the desired data points.

For example, in the upper-right corner of each report are the high-level Summary overviews of Hosts and Services. This is consistent across the host-related and service-related reports and provides the ability to navigate from this problem-related report page to a device-related summary that displays all service and host specific status, both alarming and healthy states.

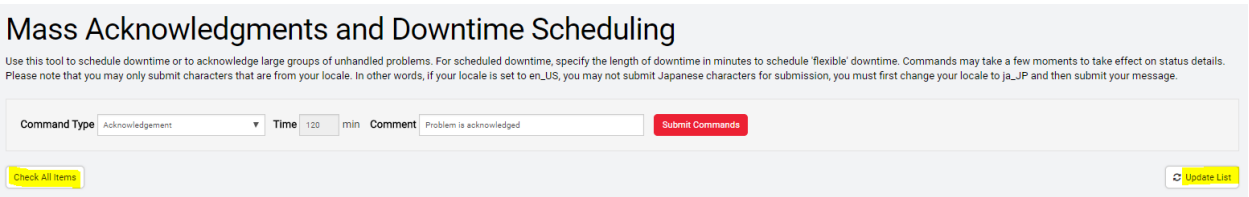


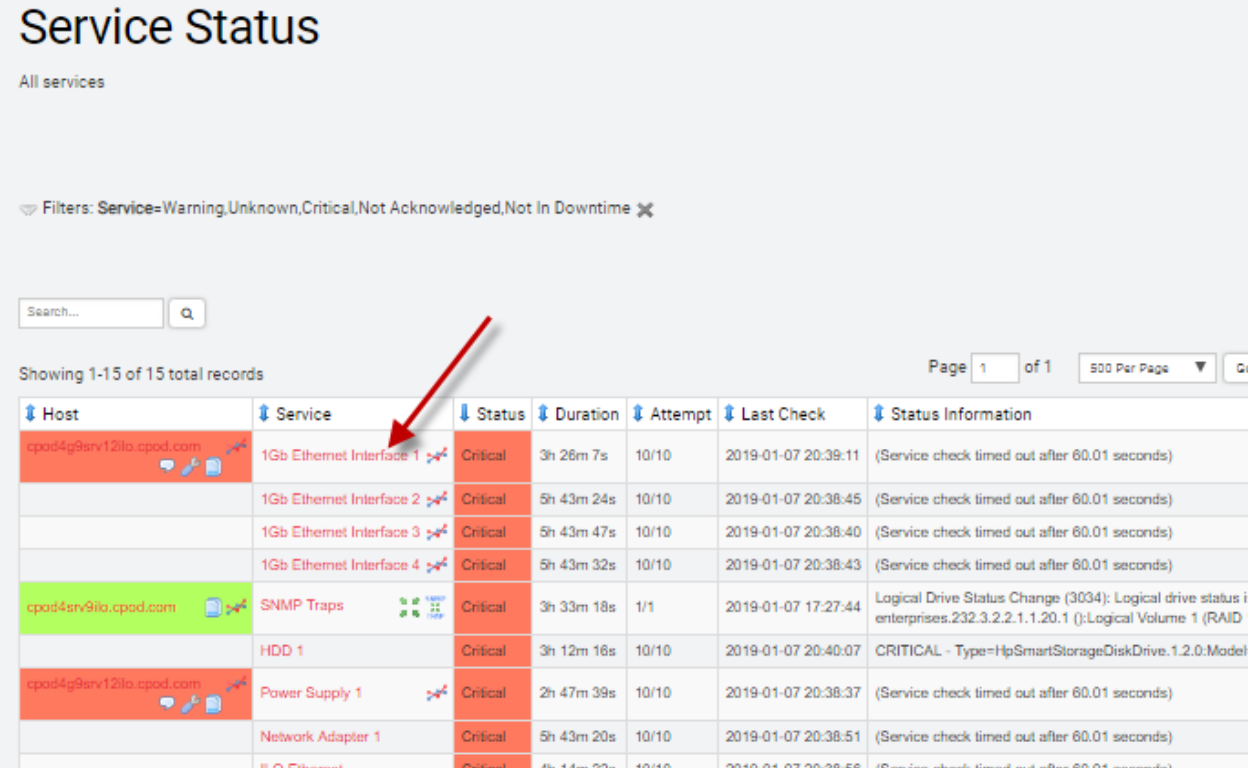
You can also click on any field/integer within the **Host Status Summary** and **Service Status Summary** areas for a more detailed view of the respective components. For example, in **Service Status Summary**, the **Unhandled** items represent those that are not yet acknowledged. You can click in the **Unhandled** area to view the Service Status for those reported items.



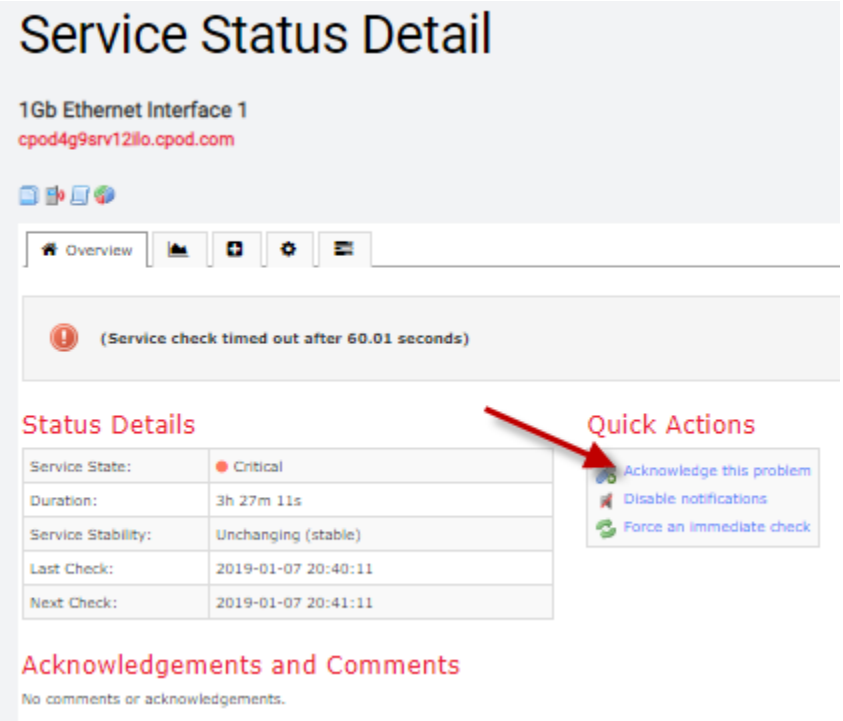
As each Service represented is acknowledged, the number of **Unhandled** items decrement.

Note:
If appropriate for the nature of a solution-wide outage and recovery, **Home** > **Incident Management** > **Mass Acknowledgement** allows you to acknowledge all problems at once from this screen.

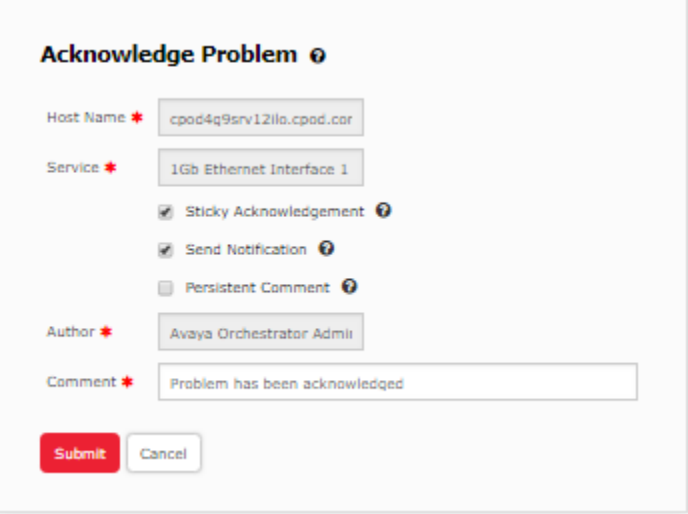


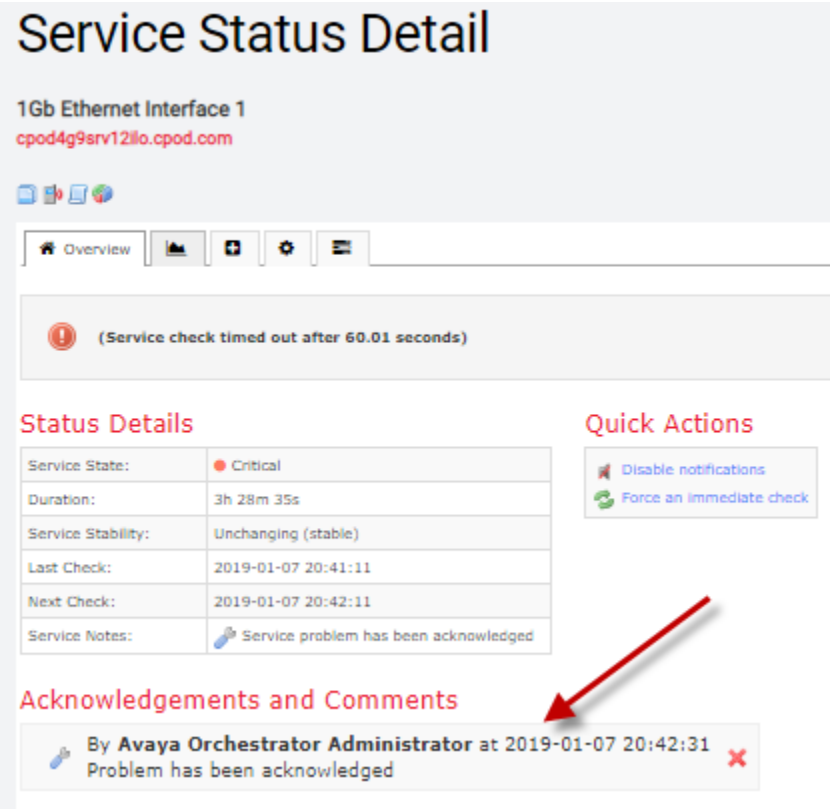


In the preceding screen shot, the *1Gb Ethernet Interface 1* is selected. After you click on that service, the service detail for that service is displayed.

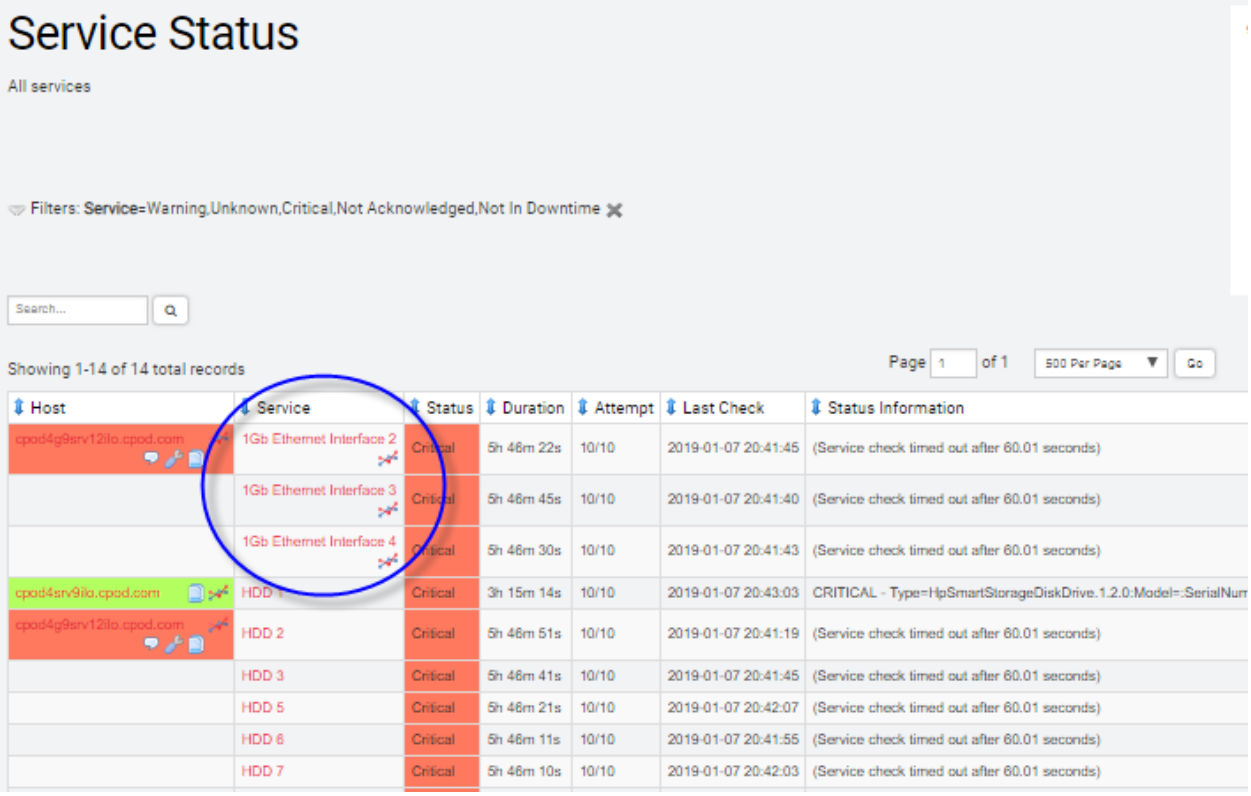


On the **Service Status Detail** page, click **Acknowledge this problem** to resolve the **Unhandled** state, if appropriate.





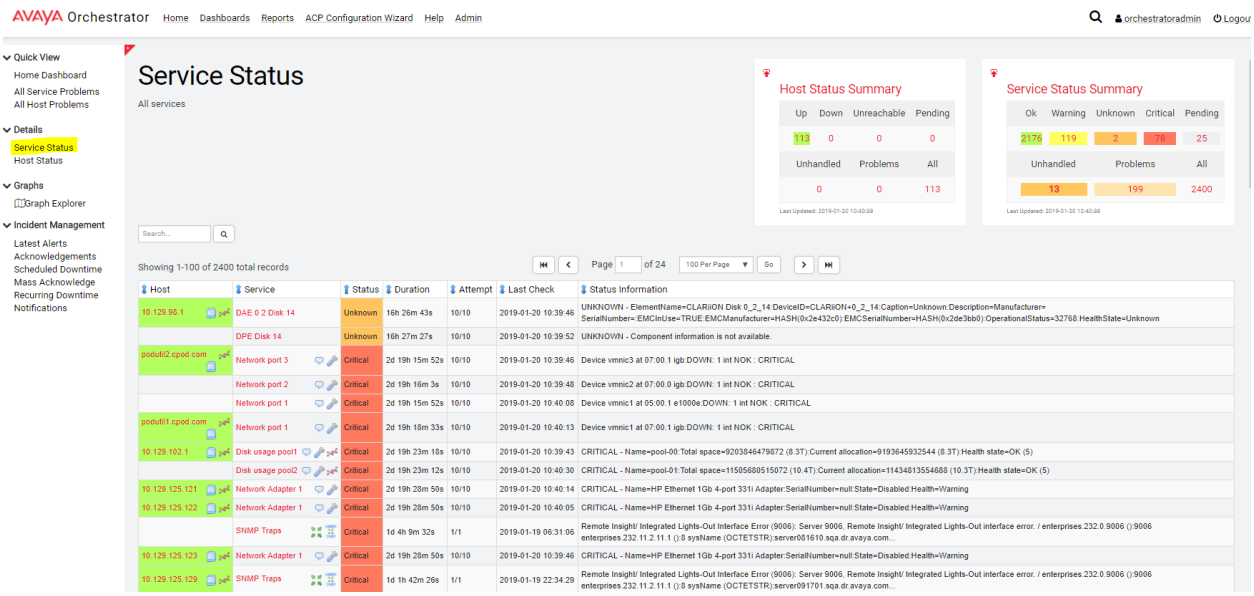
After you acknowledge the problem, AO reports the acknowledgement as a comment, decrements the **Unhandled** report value at that time, and the specific host's Service Status removes the previously reported unhandled service item.



The preceding screen shot shows how you can easily navigate from a high-level problem view to a specific device view, and with a third click, navigate to the specific service of a device.

Service Status

The **Service Status** option displays a complete list of all monitored services. Services are color-coded based on their current status. You can click an entry in the **Service** column to view detailed information about that service on the **Service Status Detail** page. You can click an entry in the **Host** column to view detailed information about that host on the **Host Status Detail** page.



Service Status Detail

The **Service Status Detail** page contains detailed statistical information about a service operating in the solution. To view this page, click a service on the **Service Status** page. The **Service Status Detail** page contains the following tabs:

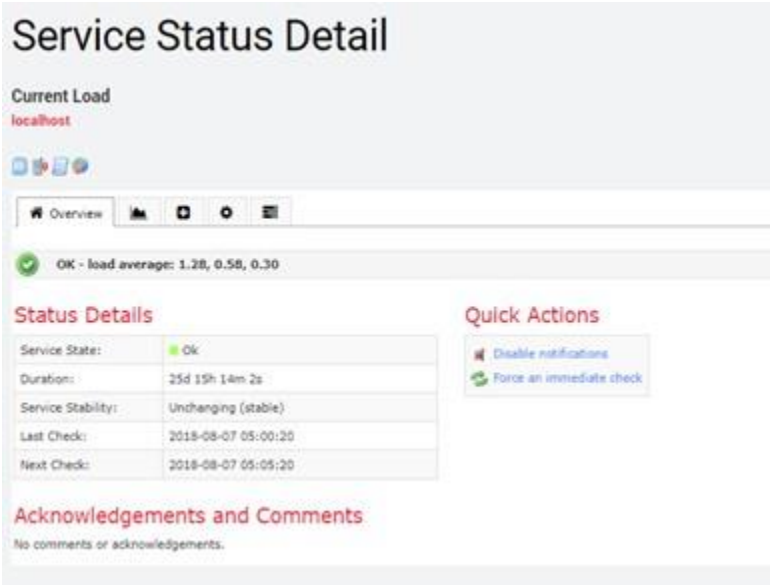
- Overview
- Performance Graphs
- Advanced
- Configure
- Free Variables

Overview

The **Overview** tab displays basic service information such as state, duration a service is in this state, stability, last checked time, and next check time.

You can use the links in **Quick Actions** to enable and disable notifications as well as force an immediate check. Other actions defined in the **Actions** component appear in this list.

Acknowledgments and comments also appear on this tab.



Performance Graphs

The **Performance Graphs** tab displays graphical information about the service. By default, information for the last 24 hours is displayed.

A Gauge is displayed if the performance data contains warning or critical thresholds.

The graph data is derived from the round robin database (RRD). The values are averaged if you generate performance graphs for larger time periods such as weeks and months.

The gauge data is derived from the last check result received by the service when it was populated into the RRD file. The data is in an accompanying XML file in the same directory where the RRD file resides.

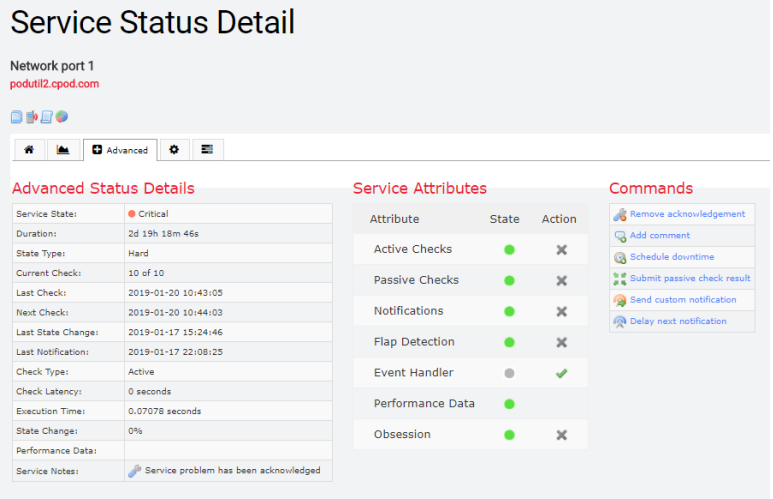
If the service does not produce performance data, the **Performance Graphs** tab still appears but no graphs are shown. Note that most services currently do not provide performance graphs. This function is more widely offered for Host detail reports.

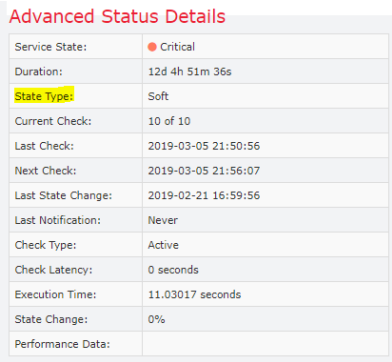
Advanced

The **Advanced** tab displays more detailed information about the service.

The **State** column of the **Service Attributes** area displays the current state of each attribute. You can click ✔ and ✖ in the **Action** column to enable or disable the attributes.

By changing any state here, you can significantly change the monitoring of your AO application. However, you must have administrative rights if you want to stop or start these processes to debug a problem.





The **State Type** can be either hard or soft and is shown in other reporting and display areas in AO.

Hard type: Represents an SNMP trap receipt. SNMP notifies only one time per issue. Hence, such alerts are considered hard, that is, confirmed. This is also the state available for proactive monitoring type alarms that are validated to be in the same state across 10 checks, of one per minute.

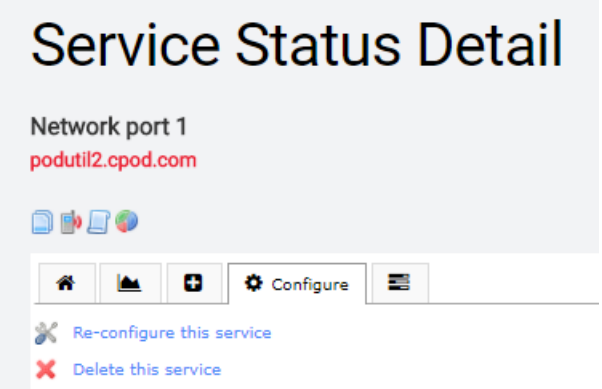
Soft type: Represents a proactive alarm that has not been in the same state for 10 checks.

Configure

The **Configure** tab allows you to re-configure or delete standard services.

If the service uses any advanced features, such as being assigned to multiple hosts, you cannot use either option.

When re-configuring a service, the options available are similar to a configuration wizard.



Free Variables

Free Variables is an advanced feature of Core that allows custom directives with values to be stored in a service object.

If your service has any free variables defined, the free variables appear here in a table for your reference.

Host Status

The **Host Status** option displays a complete list of all monitored hosts. Hosts are color-coded based on their current status. You can click an entry in the **Host** column to view detailed information about that host on the **Host Status Detail** page.

Host Status Detail

The **Host Status Detail** page contains detailed statistical information about a host operating in the solution. To view this page, click a host on the **Host Status** page. The **Host Status Detail** page contains the following tabs:

- Overview
- Performance Graphs
- Advanced

- Configure
- Free Variables

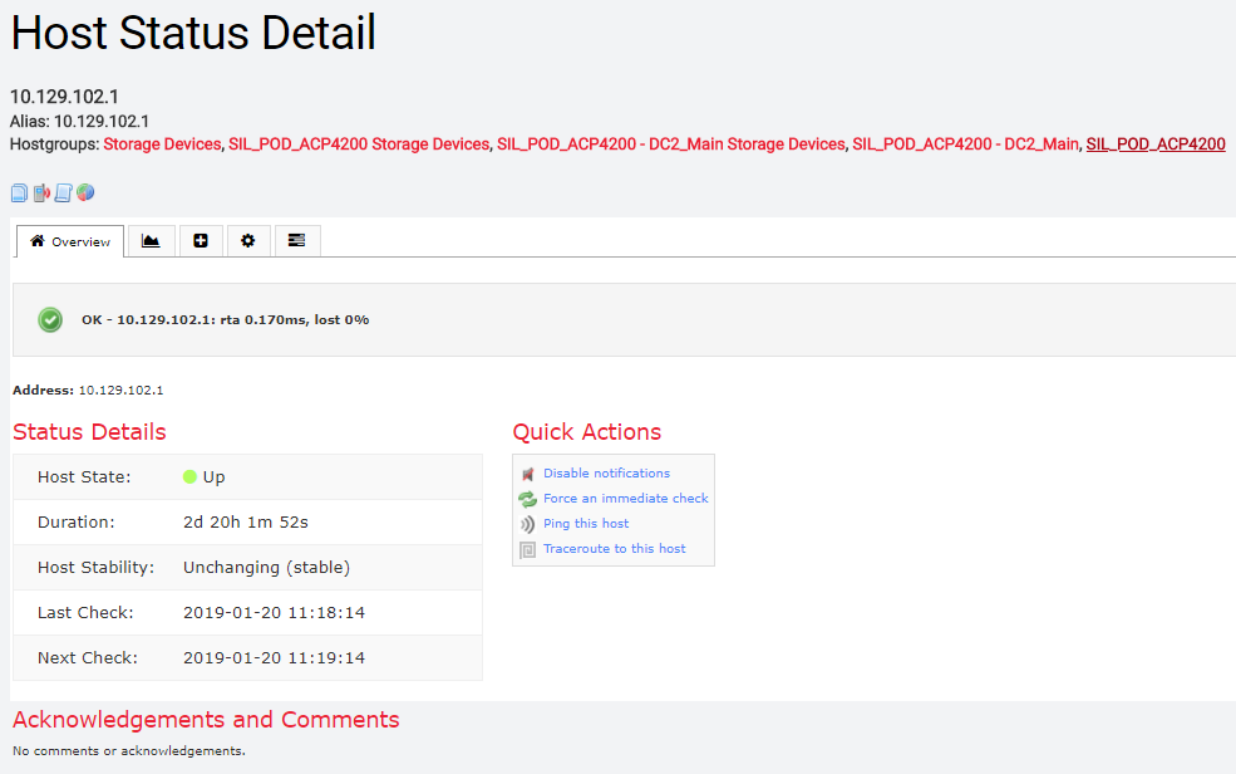
Overview

The **Overview** tab displays basic host information such as state, duration a host is in this state, stability, last checked time, and next check time.

The following host **Quick Actions** are available on this tab:

- Enable or disable notifications.
- Force an immediate check.
- Ping the host.
- Traceroute the host.

Acknowledgments or comments also appear on this tab.



Performance Graphs

The **Performance Graphs** tab displays graphs for the host object and the first four services for the host. By default, information for the last 24 hours is displayed. Use the link at the bottom for more performance graphs that allow you to browse through all the performance graphs of the services assigned to the host.

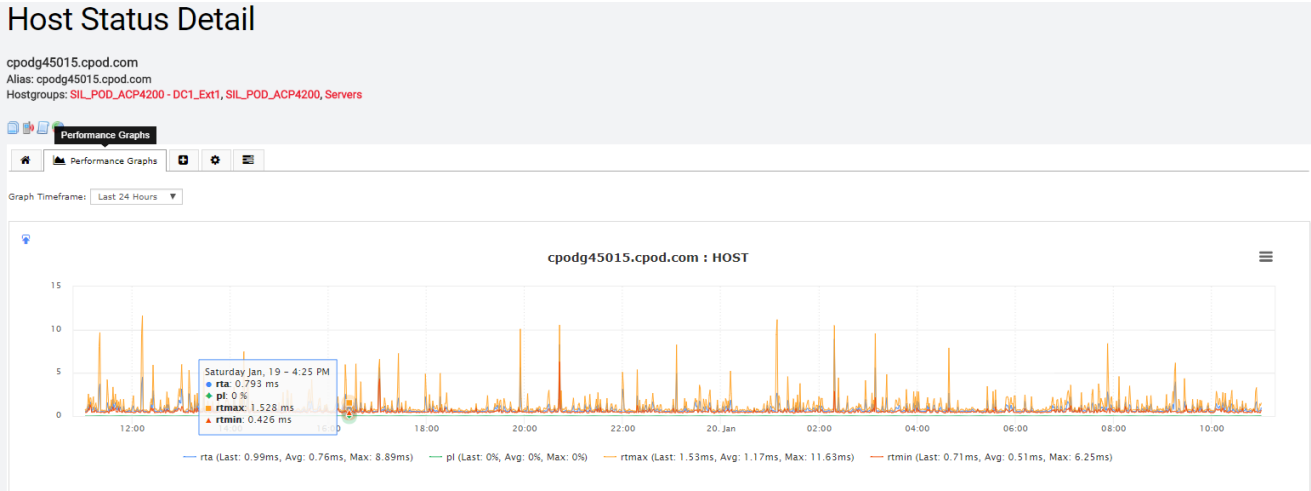
A gauge is displayed if the host object performance data contains warning or critical

thresholds.

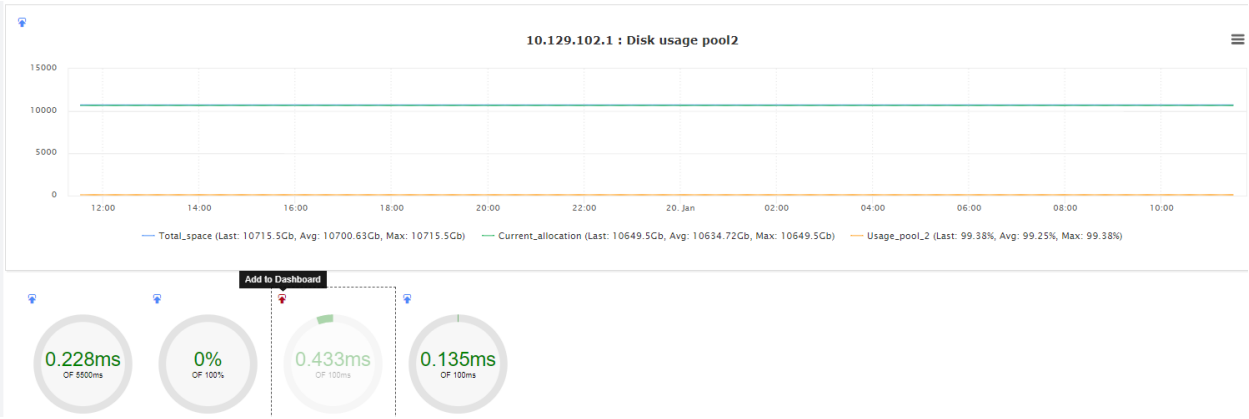
The graph data is displayed from the round robin database (RRD). The values are averaged if you generate performance graphs for larger time periods such as weeks and months.

The gauge data is derived from the last check result received by the host when it was populated into the RRD file. The data is in an accompanying XML file in the same directory where the RRD file resides.

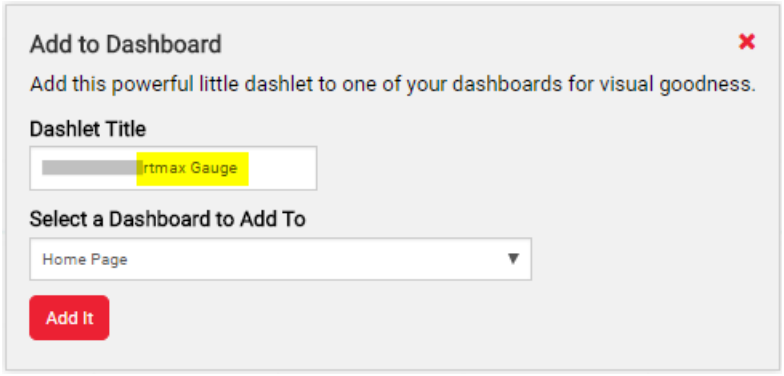
If the host does not produce performance data, the tab still appears but no host graphs are shown. The service graphs are shown if they exist.



Toward the bottom of the performance graphs are gauges. These provide the same information that is contained in the graphical format, but display it in a different visual reference form. You can click the blue icon located at the upper-left of each round gauge to place the item on a specific dashboard. These dashlets can be seen by all users, wherever they are placed.

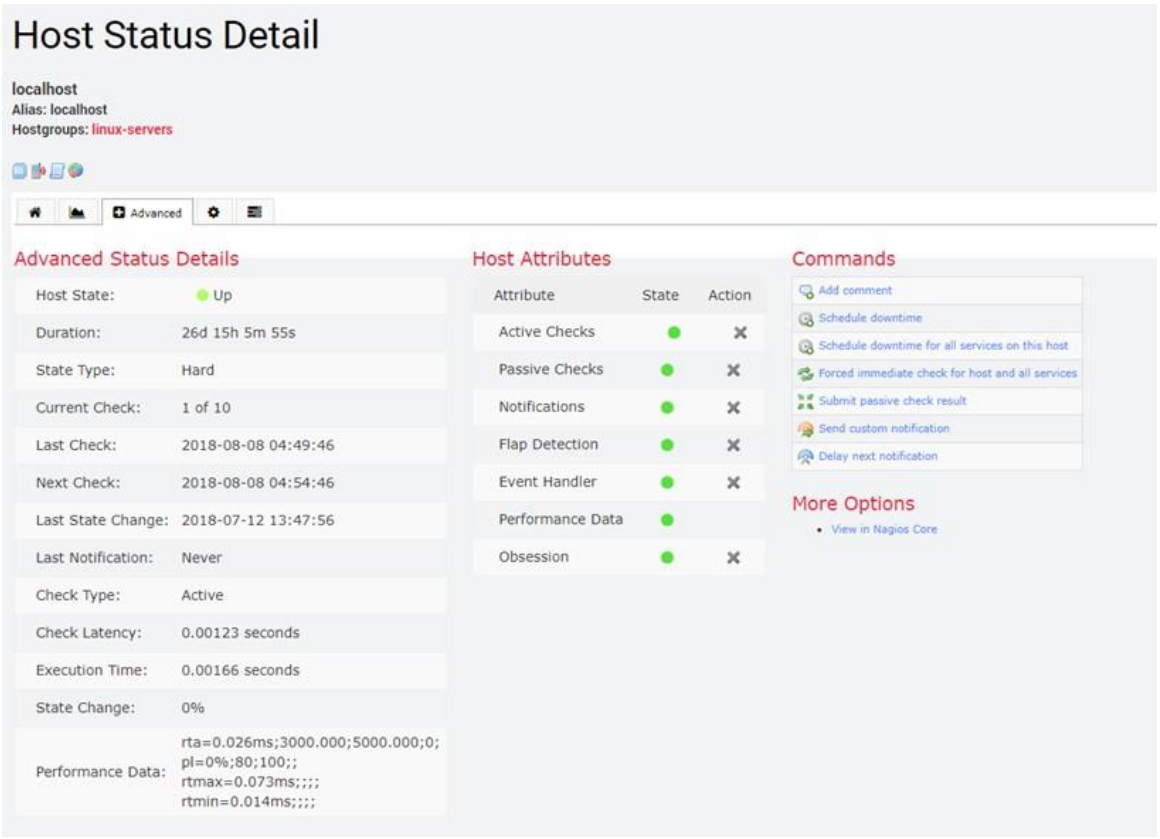


After you click the blue icon, the following dialog box appears. The **Dashlet Title** field shows the IP address associated with the Host dashlet along with the service source of the data. In the following example, the storage array is reporting *round trip max time gauge.*



Advanced

The **Advanced** tab shows more detailed information about the host.



The **Host Attributes** area displays the current state of each attribute and allows you to enable or disable the attributes.

In the **State** column:

- If an attribute is enabled, the circle is in green color. In the **Action** column, click to disable the attribute.
- If an attribute is disabled, the circle is in gray or red color. In the **Action** column,

click the check mark to enable the attribute.

The **Commands** table allows you to:

- **Add comment**

  The comment that you add appears on the **Overview** tab.

- **Schedule downtime**

  Define scheduled downtime for the host.

- **Schedule downtime for all services on this host**

  Define scheduled downtime for all the services on the host instead of defining it for each service individually.

- **Forced immediate check for host and all services**

  Force Avaya Orchestrator to immediately perform host check and all service checks.

- **Submit passive check result**

  Manually define the state of the host. This is most useful with Passive hosts. For an Active host, the check result that you submit is overwritten by the check results of the next host check interval.

- **Send custom notification**

  Send a custom notification to all the contacts that are configured to receive notifications for the host.

- **Delay next notification**

  Delay the next problem notification that is sent for the specified host. The notification delay is disregarded if the host changes state before the next notification is scheduled to be sent.

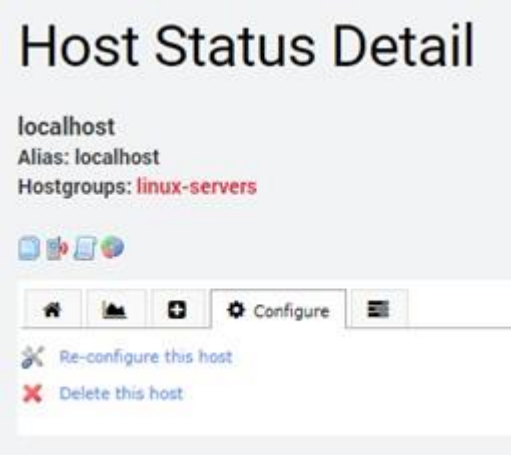
  This has no effect if the host is currently in an operational state.

Configure

The **Configure** tab allows you to re-configure or delete a host.

If the host uses any advanced features, you cannot use either option. You cannot delete a host object until all the services assigned to the host are deleted.

When re-configuring a host, the options available are similar to a configuration wizard.



Free Variables

Free Variables is an advanced feature of Core that allows custom directives with values to be stored in a host object.

If your service has any free variables defined, the free variables appear here in a table for your reference.

Chapter 6: Avaya Orchestrator dashboard deployment

Overview

This chapter contains information about assigning static dashboard views to different users.

Accessing the Avaya Orchestrator dashboard

Note:

In Avaya Orchestrator Release 1.4, there are limited options for customizing dashboards. The primary ACP Home Dashboard is the “go to” solution view for Release 1.4.

Procedure

1. Log in to the Avaya Orchestrator interface.
2. Click **Dashboards**.
   The Home page for the Dashboard canvas appears. This should not be confused with the ACP Home Dashboard page.
3. Click **Dashboard Tools** > **Deploy Dashboards**.

Deploying dashboard

About this task

Use this procedure to deploy your dashboard for other Avaya Orchestrator users.

Note:

There is no need to deploy dashboards for any users in AO Release 1.4. All users get all available dashboard views, unless restricted through the user level permissions by a system administrator.

This option will become more useful and meaningful in the next release of AO. If you feel a need to modify anything in this area, consult an Avaya services representative.

Before you begin

You must have administrative user rights to perform this task. The default login of *orchestratoradmin* provides this permission.

Procedure

1. On the Dashboard Deployment Tool page, in the **Dashboards to Deploy** area, select the dashboards that you want to deploy.

2. In the **Deploy to Users** area, select the users for whom you want to deploy the dashboards.
3. Click **Deploy Dashboards**.

Add Dashlets

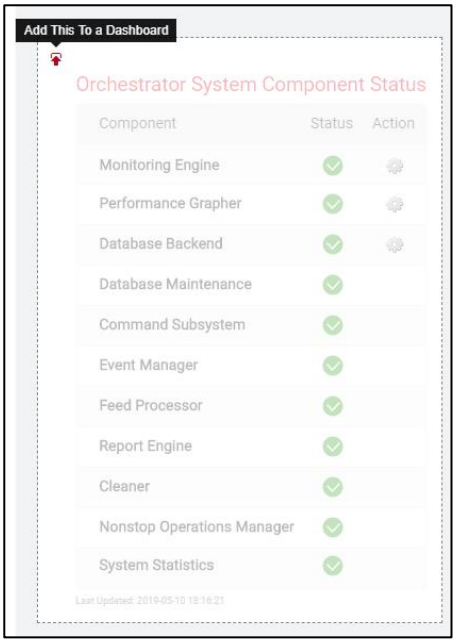
Use the information in this topic to build a Dashboard “home page” monitoring view.

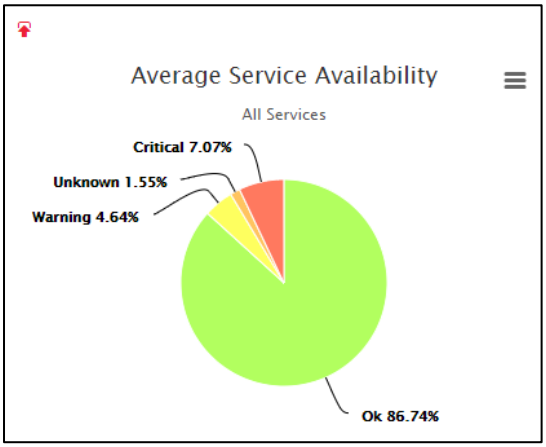
Note:

Dashboard customization will be officially provided and supported in the next release, which is Avaya Orchestrator Release 1.5. In AO Release 1.4, you can try out the available customization and become familiar with the options.

All dashboards are comprised of dashlets. A dashlet is easily recognized as a viewable reporting element that has a red arrow in the upper-left corner of its reporting screen. Dashlets can be found under a variety of menu options, such as the ACP Dashboard Home, Reports, and Admin submenus. In short, there is a wide variety of dashlet selections and not all of them are found under the **Dashboards** > **Add Dashlets** > **Available Dashlets** menu.

The following are some examples of dashlets found outside the Dashboard menu:





Adding Dashlets to a Dashboard

About this task

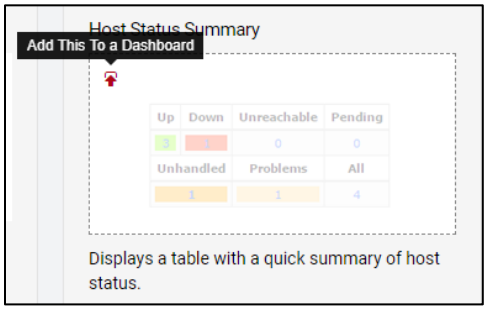
For AO Release 1.4, Avaya recommends that you do not make changes to the primary ACP Home Dashboard or add any additional dashlets. Instead, you can try a few different views on the blank Dashboard home page canvas.

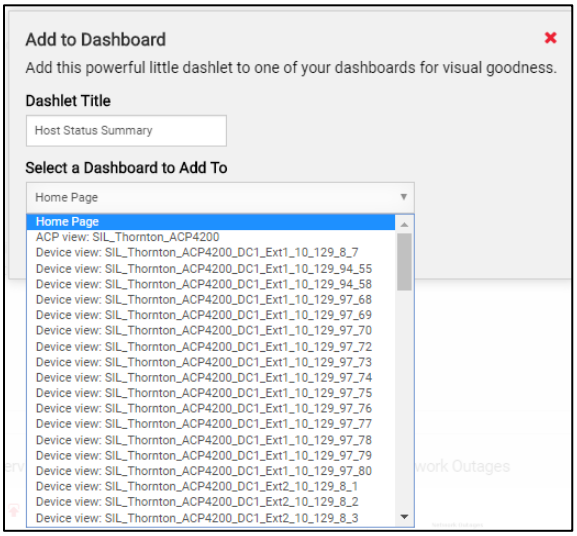
Procedure

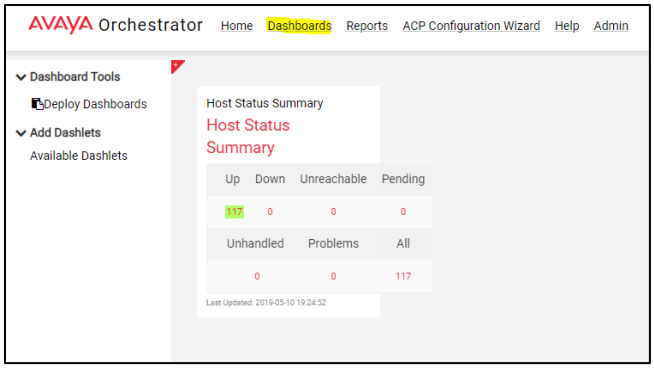
1. Click **Dashboards**
2. Click **Add Dashlets**, and then **Available Dashlets**.
3. Select a dashlet you want to try using in a customized dashboard format.
   You can also select any available dashlet from any other menu location.
4. Locate and click the red arrow associated with the dashlet you have selected.
5. Click on the drop-down selections to choose the desired options.

   In the example below, the Host Status Summary report was selected. The **Select a Dashboard to Add To** field displays the location where the dashlet can be added. For AO Release 1.4, Avaya recommends that you select “Home Page” and not “ACP view: <name given to the main dashboard environment>”. The “Home Page” does not represent the Home Dashboard, but rather the Dashboard home page, which is a blank page where you may experiment with the customization functionality.

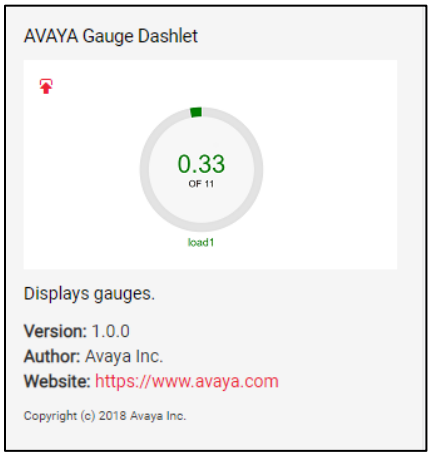
6. After selecting *Home Page,* the selected dashlet will be presented there.

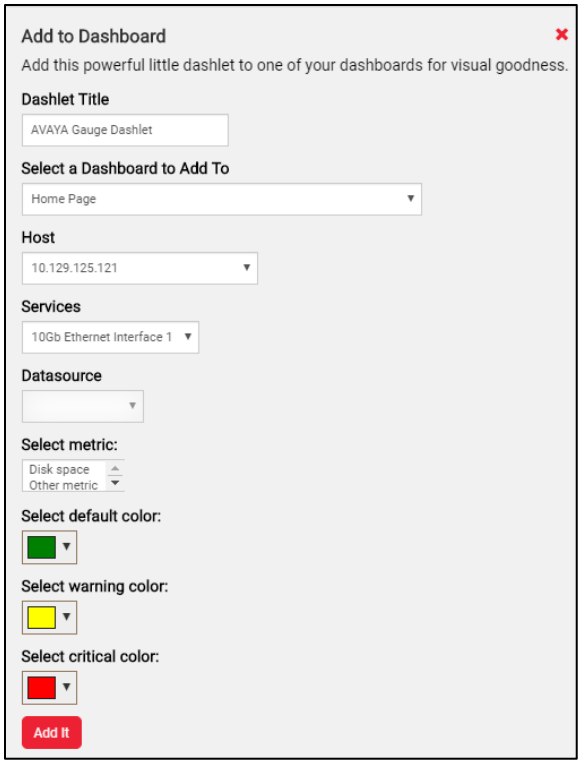






Some dashlets may require additional selected information. For example, a gauge dashlet can measure several different aspects of a host. After you select a specific host, you can select a related service from a list of options, and then select a subsequent Datasource and metric.




Add to Dashboard
Add this powerful little dashlet to one of your dashboards for visual goodness.
Dashlet Title
AVAYA Gauge Dashlet
Select a Dashboard to Add To
Home Page
Host
10.129.125.121
Services
10Gb Ethernet Interface 1
Datasource
Select metric:
Disk space
Other metric
Select default color:
Select warning color:
Select critical color:
Add It

Chapter 7: Maintenance and troubleshooting

Overview

This chapter contains information and procedures for maintaining and troubleshooting an Avaya Orchestrator instance.

Log files

This section contains information about the logs that are available for troubleshooting Avaya Orchestrator.

Standard log locations

The following locations contain alarm and application support activity logs in the Avaya Orchestrator server:

- `/var/log/orchestrator`
- `/var/log/snmptt`
- `/var`

These are system logs that provide helpful information when troubleshooting a problem in Avaya Orchestrator or within the server itself. By default, all the following logs are managed and rotated by rsyslog or by the system logger that the Avaya Orchestrator server is running.

Logs located in /var/log/orchestrator

```
[aoadmin@ao5 orchestrator]$ cd /var/log/orchestrator
[aoadmin@ao5 orchestrator]$ ls -ltr
total 2892
-rw-r--r--. 1 root   root         0 Jan 17 07:24 check_system_services.log
-rw-rw-r--  1 apache nagios 1164875 Jan 17 15:25 wizard-20190117.log
-rw-r--r--. 1 root   root       894 Jan 17 22:00 orchestrator_backup.log
-rw-rw-r--  1 apache nagios    3148 Jan 17 22:18 viewgen-20190117.log
-rw-rw-r--. 1 nagios nagios  943357 Jan 17 23:55 rediscovery-20190117.log
-rw-rw-r--  1 apache nagios     678 Jan 18 04:41 viewgen-20190118.log
-rw-rw-r--  1 nagios nagios    6407 Jan 18 07:15 rediscovery-20190118.log
-rw-r--r--. 1 nagios nagios  812347 Jan 18 07:15 orchestrator_rediscovery_cron.log
```

These are system logs that provide status details about the processes that support the administration wizard and the discovery of hardware in each of the designated racks.

Logs located in /var/log/snmptt

```
[aoadmin@ao5 snmptt]$ cd /var/log/snmptt
[aoadmin@ao5 snmptt]$ ls -ltr
total 6940
-rw-r--r--. 1 root   root    1384 Jan 17 15:04 snmpttsystem.log
-rw-rw-r--  1 snmptt root 7088318 Jan 18 07:39 snmptt.log
```

These are logs that collect the SNMP trap information received by Avaya Orchestrator. The information that passes into the snmptt.log file is often used to monitor real-time, incoming trap activities. The following screen shot contains an example:

Logs located in /var

These are system logs that provide helpful information when troubleshooting a problem in Avaya Orchestrator or the server itself. By default, all the following logs are managed and rotated by rsyslog or by the system logger that the Avaya Orchestrator server is running.

You must have root level privilege to view the following log files:

- `/var/log/messages`

  This is the system messages log. Most hardware-related errors, nrpe information, segfaults, kernel msg limits, ulimit errors, and so on appear here. If you suspect intermittent hardware problems, use this log or run **`dmesg`**.

- `/var/log/httpd/error_log`

  This is the Apache error log. Problems and bugs in the PHP, authentication problems, and problems with broken URLs are logged here. Because Avaya Orchestrator is a LAMP application, many issues are logged here. You can use this log for troubleshooting.

- `/var/log/httpd/access_log`

  This is the Apache access log. Failed authentications, Ajax requests, and page views are logged here.

- `/var/log/maillog`

  This file logs email sent through sendmail. It is only applicable to core contact "notify-*-by- email" notification handlers and sendmail tests.

System time configuration

Use the information and procedures in this section to configure the system date, time, and time zone for the server.

Configuring the system time zone

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **System Settings**.
4. On the **General** tab, in the **Timezone Settings** area, in the **Timezone** field, click the appropriate time zone.
5. Click **Update Settings**.

Verifying the configuration

About this task

Verify the system date and time configuration.

Procedure

1. Log in to the Avaya Orchestrator GUI.
2. Click **Admin** > **System Config** > **System Profile**.
3. On the System Profile page, click **View System Info**.

   Information about the system is displayed.
4. Locate the Date/Time section and verify that the information is correct.

Change passwords

Use the information and procedure in this section to change the password for an Avaya Orchestrator installation to ensure a safe and secure monitoring environment.

Default password considerations

All password changes are optional. Changing default passwords is a network security best practice that helps secure your Avaya Orchestrator installation from security threats and compromises.

Changing the Linux aoadmin (super user) password

About this task

Use the following procedure to change the password for the Linux `aoadmin` account. It is through this login that users can access the *root* account permissions.

Procedure

1. Log in to Avaya Orchestrator VM by using SSH.
2. Use the following credentials:

   User name: *aoadmin*

   Password: `Avaya123$`
3. At the aoadmin prompt $, type the **`passwd`** command.
4. Follow the next prompt and type the current password, and then press `Enter`.
5. Type the new password at the next command prompt and press `Enter`.
6. Re-enter the new password at the next command prompt and press `Enter`.

   A message appears that the password is successfully changed.

Configuring downtime

About this task

Use the following procedure to schedule downtime for a service, host, host group, or service group. You can schedule downtime to avoid receiving unnecessary or unwanted notifications during a period of expected service interruption.

You can configure a Fixed or Flexible downtime.

Note:

Fixed downtime starts and stops at the exact start and end time that is specified when the downtime is scheduled.

Flexible downtime is intended for an event when a host or service is unavailable for an amount of time, but the time when that event will start is not known. Avaya Orchestrator starts the downtime sometime between the scheduled start and end times. The duration lasts for the scheduled amount of time.

Flexible downtime assumes that the host or service for which you have scheduled the flexible downtime either goes down, becomes unreachable, goes into a non-operational state sometime between the start and end times that you specify. The time at which a host or service transitions to a problem state determines the time at which Avaya Orchestrator actually starts the downtime. The downtime lasts for the duration that you specify, even if the host or service recovers before the downtime expires.

Procedure

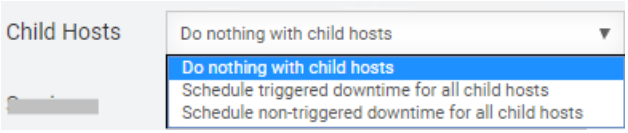
1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Home.**
3. In the left navigation pane, click **Incident Management** > **Scheduled Downtime**.
4. On the Scheduled Downtime page, click **Schedule Downtime**.
5. Do one of the following:
   a. Click **For Host(s)** if you want to schedule downtime for hosts.
   b. Click **For Service(s)** if you want to schedule downtime for services.

   Use the **Filter** field to filter host and service names in large deployments.
6. Click **Add Selected**.

   The **Author** field displays the login ID of the user who has logged in.
7. In the **Comment** field, type a comment indicating the purpose of the downtime.
8. In the **Triggered By** field, specify if the downtime is started by another scheduled downtime event.
9. In the **Type** field, click **Fixed** or **Flexible** depending on the type of downtime and provide the required information.
10. In the **Duration** field, specify a duration for the downtime.

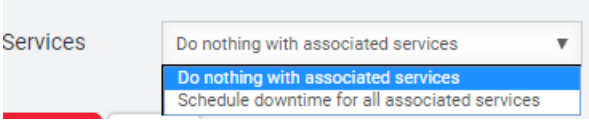
    The **Duration** field is available only when you schedule a Flexible downtime.
11. In the **Start Time** field, click the start time for the downtime.
12. In the **End Time** field, click the end time for the downtime.
13. In the **Child Hosts** field, click the child host behavior that matches the intended downtime situation.

    The **Child Hosts** field is available only when you schedule downtime for hosts.



14. In the **Services** field, click the effected services.

    The **Services** field is available only when you schedule downtime for hosts.



15. Click **Schedule**.

Configuring recurring downtime

About this task

Recurring downtime is useful when you have regular periods of downtime and you do not want to schedule those periods individually. You can configure recurring periods of downtime instead.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Home.**
3. In the left navigation pane, click **Incident Management** > **Recurring Downtime**.
4. On the Recurring Scheduled Downtime page, click the tab according to what you want to schedule the downtime for: **Hosts**, **Services**, **Hostgroups**, or **Servicegroups**.
5. Click **Add Schedule**.
6. On the **Add Recurring Downtime Schedule** page, do the following to schedule the recurring downtime:
   a. Specify the Host, Service, Hostgroup, or Servicegroup depending on the tab you have selected.
   b. If you are configuring a recurring downtime for hosts or hostgroups, select the check box corresponding to the **Services** field to include all services in the host or hostgroup.

      The check box is available only when you schedule recurring downtime for hosts and hostgroups.
   c. If you are configuring recurring downtime for services, in the **Services** field, type the associated services.

      The **Services** field is available only when you schedule recurring downtime for services.
   d. In the **Comment** field, type a comment that describes the recurring downtime.
   e. In the **Start Time** field, type a start time for the recurring downtime.

      Use a 24-hour time format.
   f. In the **Duration** field, type a duration, in minutes, for the recurring downtime.
   g. In the **Valid Months**, **Valid Weekdays**, and **Valid Days of Month** fields, specify the appropriate values for the recurring downtime.
7. Click **Submit Schedule**.

Scheduling downtime by using mass acknowledgement

About this task

You can use the *Mass Acknowledgments and Downtime Scheduling* page to schedule

downtime for hosts and services that are already in a non-operational state.

Procedure

1. Log in to Avaya Orchestrator.
2. Click **Home.**
3. In the left navigation pane, click **Incident Management** > **Mass Acknowledge**.
4. On the Mass Acknowledgments and Downtime Scheduling page, select all the hosts and services that you want to place in the scheduled downtime.
5. In **Command Type**, click **Schedule Downtime**.
6. In the **Time** field, specify the length of downtime in minutes to schedule flexible downtime.
7. In the **Comment** field, type a comment.
8. Click **Submit Commands**.

Notification configuration

This section contains information and procedures about how to configure and manage notifications. Notifications can be emails or SMS text messages and are sent to users when hosts and services change states. This keeps users updated on the health of their monitoring environment.

Users and contacts are two separate entities.

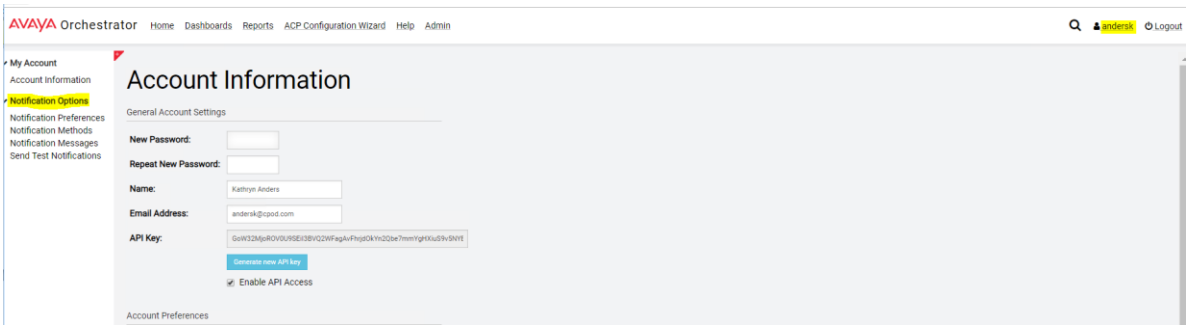
- Core process creates and uses contacts to send notifications.
  - When a user is created, a contact is created for it by the Core process.
  - Contacts are assigned to host and service objects. Core uses this information to track which contacts receive notifications.
  - In Avaya Orchestrator Release 1.4, end users cannot modify their notification preferences, such as the format of the email being sent or what type of notifications they receive.
- Avaya Orchestrator creates user accounts to receive notifications.
  - Provides an authentication mechanism so that end users can access Avaya Orchestrator.
  - Allows end users to define their notification preferences, such as the format of the email messages being sent, or the type of notifications they receive.
  - Allows end users to do other activities such as email reports.
  - Provide users with the ability to receive email and text notifications with different notification preferences for each method.

Note:
If you want to send notifications to the users that are imported from ADS/LDAP, ensure that the preceding notification configuration is completed.

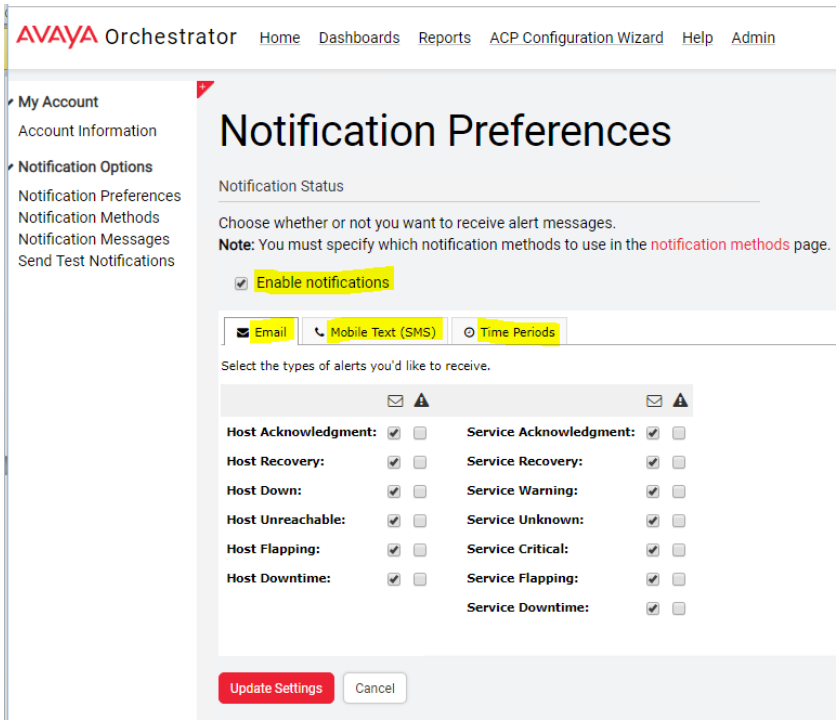
Configuring user notifications

Procedure

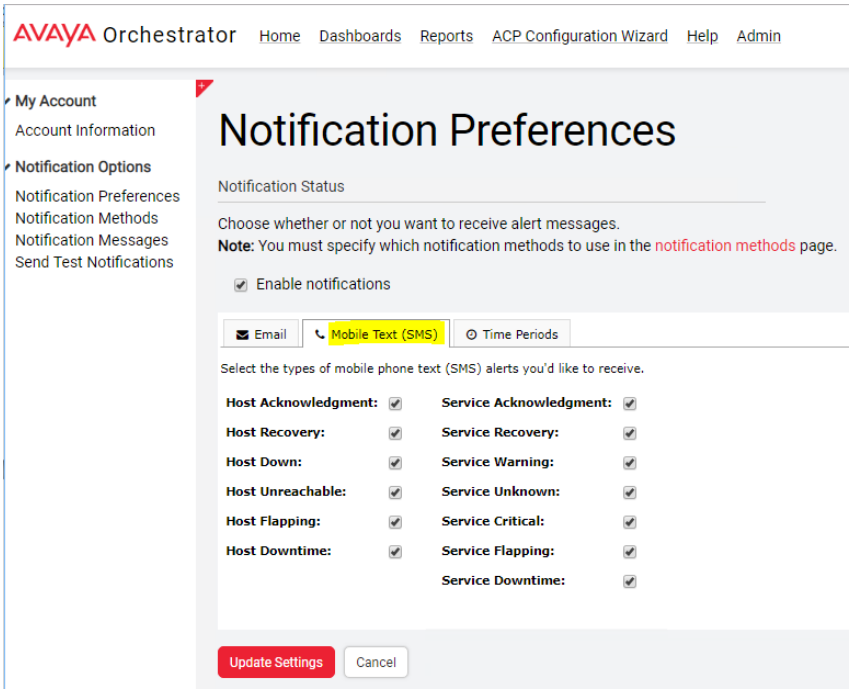
1. Log in to Avaya Orchestrator with the user credentials for which you want to configure user notifications.
2. Click the user name in the upper-right corner of the interface.



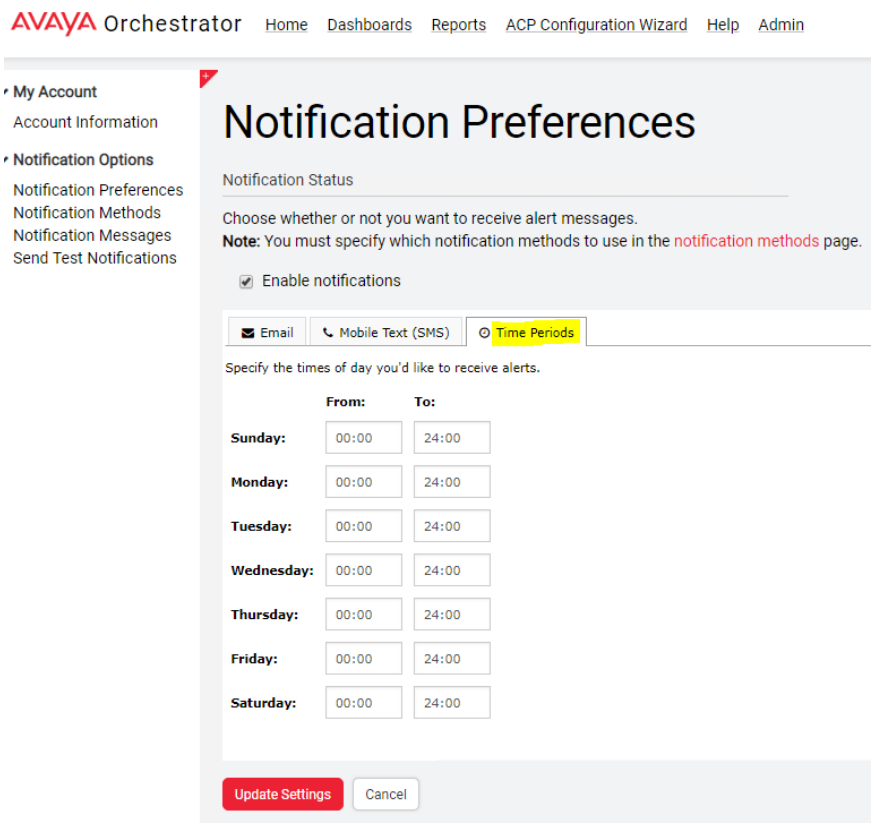
3. In the left navigation pane, click **Notification Options** > **Notification Preferences**.
4. On the Notification Preferences page, select the **Enable notifications** check box and do the following:
   a. On the **Email** tab, select the check boxes corresponding to the notifications that you want to enable.



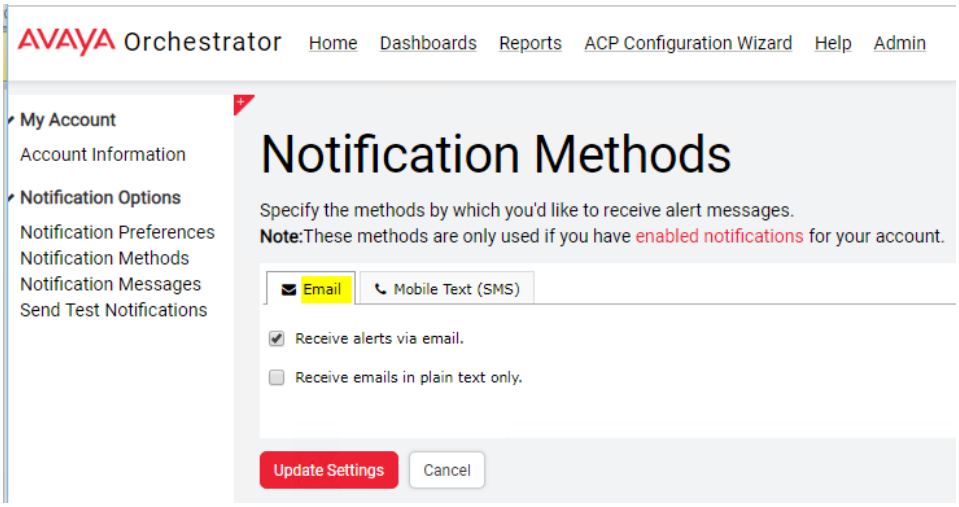
b. On the **Mobile Text (SMS)** tab, select the check boxes corresponding to the notifications that you want to enable.



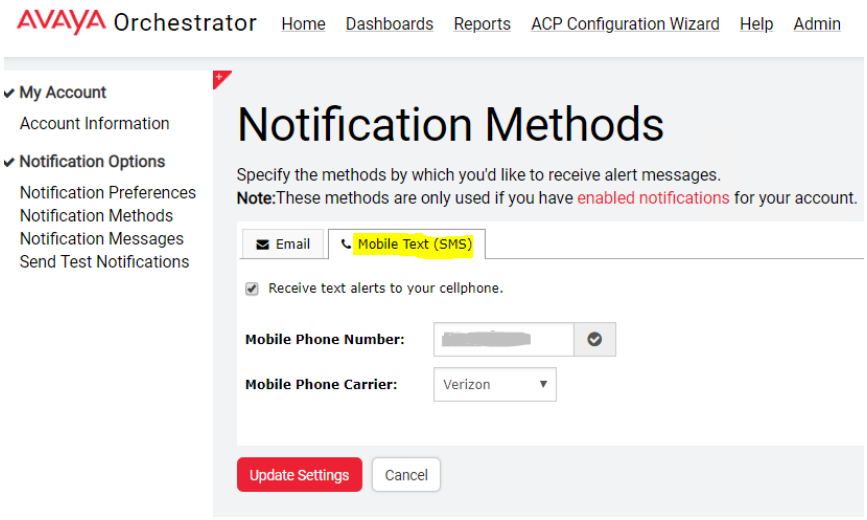
c. On the **Time Periods** tab, configure the time of the day and days of the week for receiving notifications.



5. In the left navigation pane, click **Notification Methods**.
6. On the Notification Methods page, do the following:
   a. On the **Email** tab, select the check box corresponding to the method by which you want to receive the notifications.



   b. On the **Mobile Text (SMS)** tab, select the **Receive text alerts to your cellphone** check box and specify the phone number and mobile phone carrier.



7. Click **Notification Messages**.
8. On the Notification Messages page, do the following:
   a. On the **Email** tab, configure the format of the email notifications.
   b. On the **Mobile Text (SMS)** tab, configure the format of the text notifications.
9. Click **Update Settings**.
10. **(Optional)** Avaya recommends that you use the **Send Test Notifications** option, located in the left navigation pane, to test the new notification settings.

Troubleshooting

Start with the bird's eye view

Home Dashboard Assessment

Start by viewing the Home Dashboard. This is where all bird's eye collective alarm information is presented. From here, you can drill down into many different reporting and action-oriented menus to learn more about problems and communicate status with other AO users who have opted to receive updates.

Host alarms

- The Host data in each category reflects the success or failure of AO to access the IP address of the administered devices.
- Alarms will be either *ok* or *critical.* Device ports will be either up or down.
- There is no need for *warning* level alarms for Hosts.
- *Unreachable* is not currently used in AO Release 1.4. It will be enabled in a future release and will relate to objects that are supported within a Host being monitored; for example, IP/SIP phones on a network host.

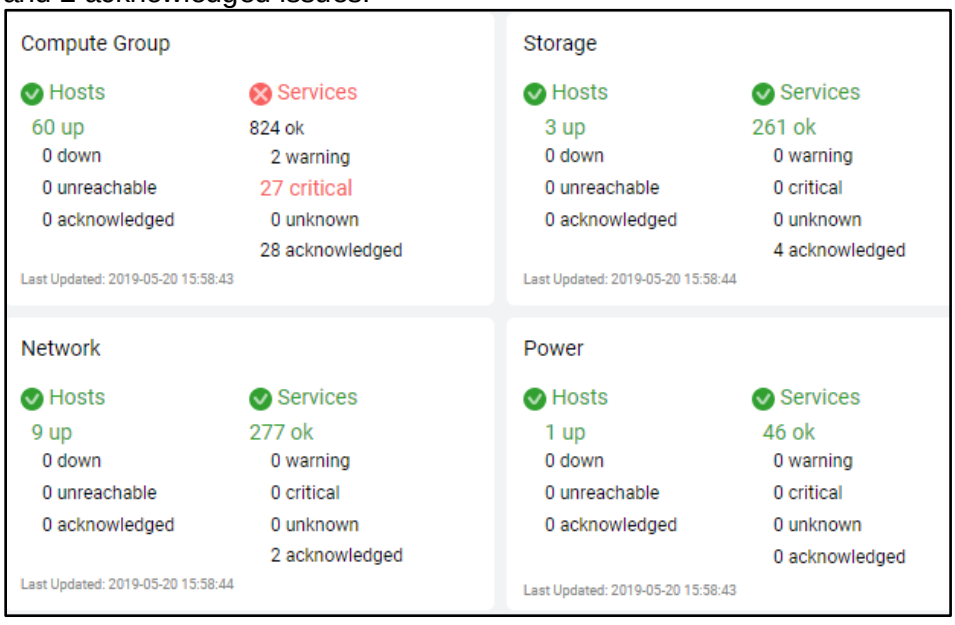
Service alarms

- Service data reflects the status of the monitored elements within each host.
- Alarms can be *ok, warning*, or *critical.*
- The *unknown* category reflects peg counts when hosts are down and reporting critical alarms. When a host is not accessible, AO cannot evaluate the internal services of that host. Therefore, the state of the services will be reported as *unknown.*

Acknowledged alarms

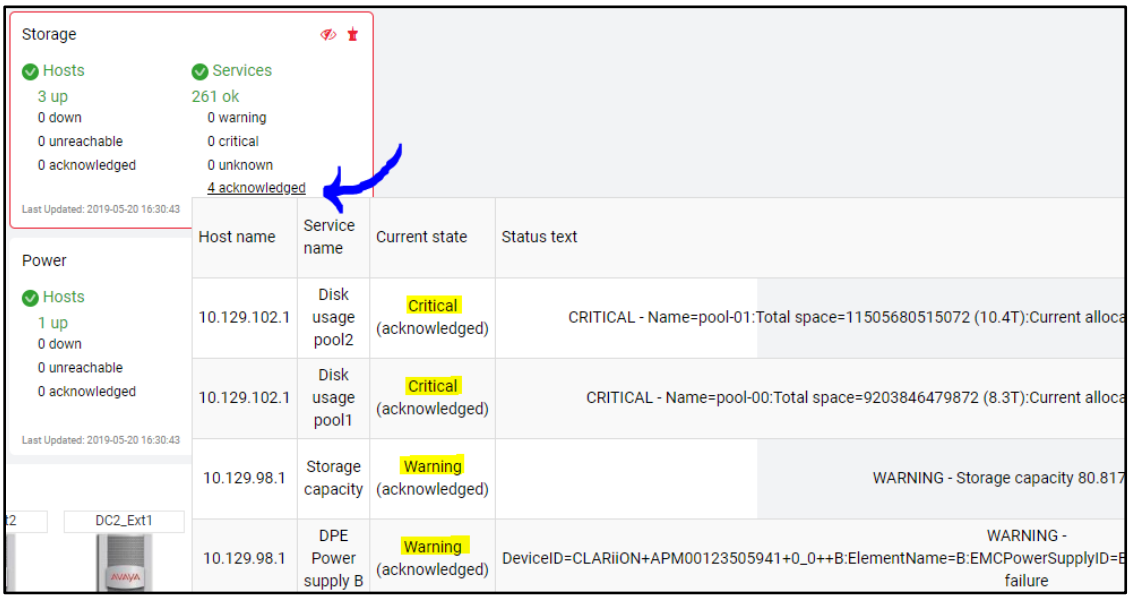
- When an administrative user has physically “acknowledged” an alarm in AO, alarm notification processing is stopped.
- On the Home dashboard view, as shown in the following screenshot, when an alarm is acknowledged, the associated *warning* or *critical* alarm is quiesced, or removed from this high-level view.
- An acknowledged alarm is the one already being attended and; therefore, should be removed from the collective alarm view to prevent potential visual distraction toward alarms already investigated. Removing such alarms states from the high-level overview allows the users who are monitoring the solution state of health to clearly view new alarms and new state changes.
- The acknowledged alarm(s) will remain present across all other reporting mechanisms, such as the Problems and Status reporting overviews, and they can be easily accessed by hovering over or clicking on the acknowledged link in each category.

In the following example, the *Storage* category reports no warnings and no critical alarms. There are 4 acknowledged alarms reported. A quick glance at this area would reveal no *new* issues. The same is true for the Network category, which reports no warnings, no critical alarms, and 2 acknowledged issues.



The following screenshot shows that hovering over the acknowledge issues reveals the true state of the services in each category. In this example, there are still 2 critical and 2 warning type alarms for the Storage array. They have not yet been resolved and can still be viewed but are not flagged as red and amber alarms. Should a new warning or critical alarm arrive for the

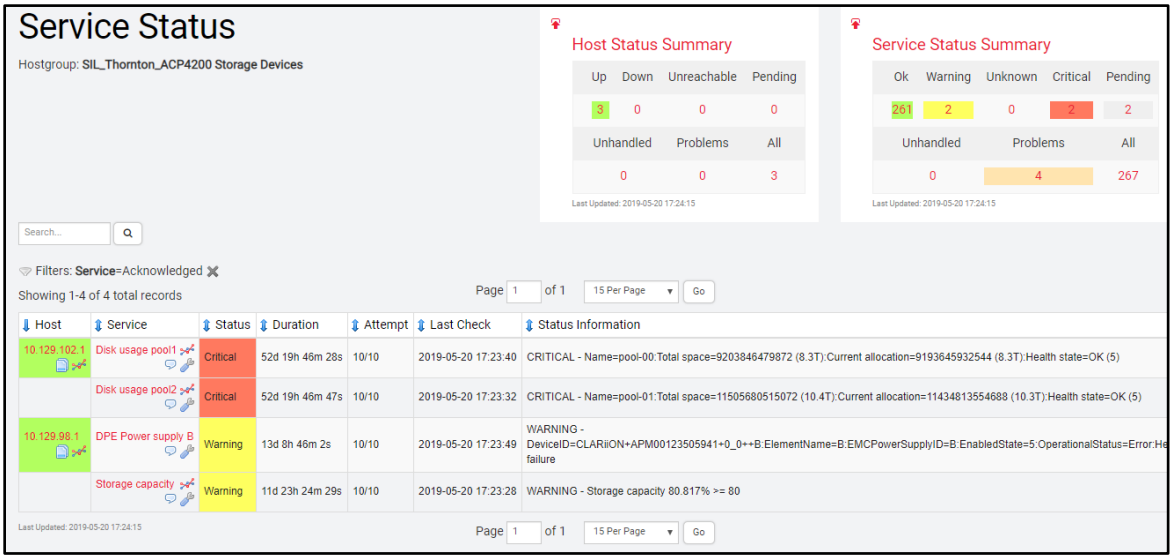
Storage area, the peg count in the warning or critical alarm area as well as the color change will grab the attention of those monitoring the solution.



Drilling down for information

Most elements in reports reveal information by hovering over fields and/or by drilling down into a specific area of concern.

In the following example, the Storage acknowledgement field was selected and clicked to drill down and view the details. The issues reported in the example represent the 2 critical and 2 warning alarms previously noted as being acknowledged.



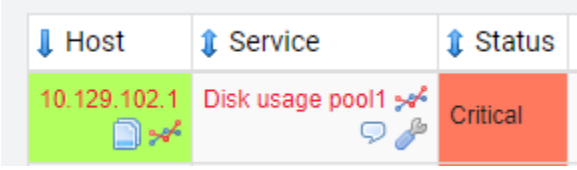
A closer look at the first item reveals icons communicating the other types of information available.

Under the Host column, the following icons are present:

- Stacked paper icon: To view the service status details.
- Graphical icon: To view the related performance graph for the associated host.[3]

Under the Service column, the following icons are present.

- Graphical icon: To view the related performance graph for the alarming service.
- Conversation bubble icon: Redirects you to the Service Status Detail page where there are acknowledgement comments noted.
- Wrench icon: This is present for all alarms that have been acknowledged (are being worked).

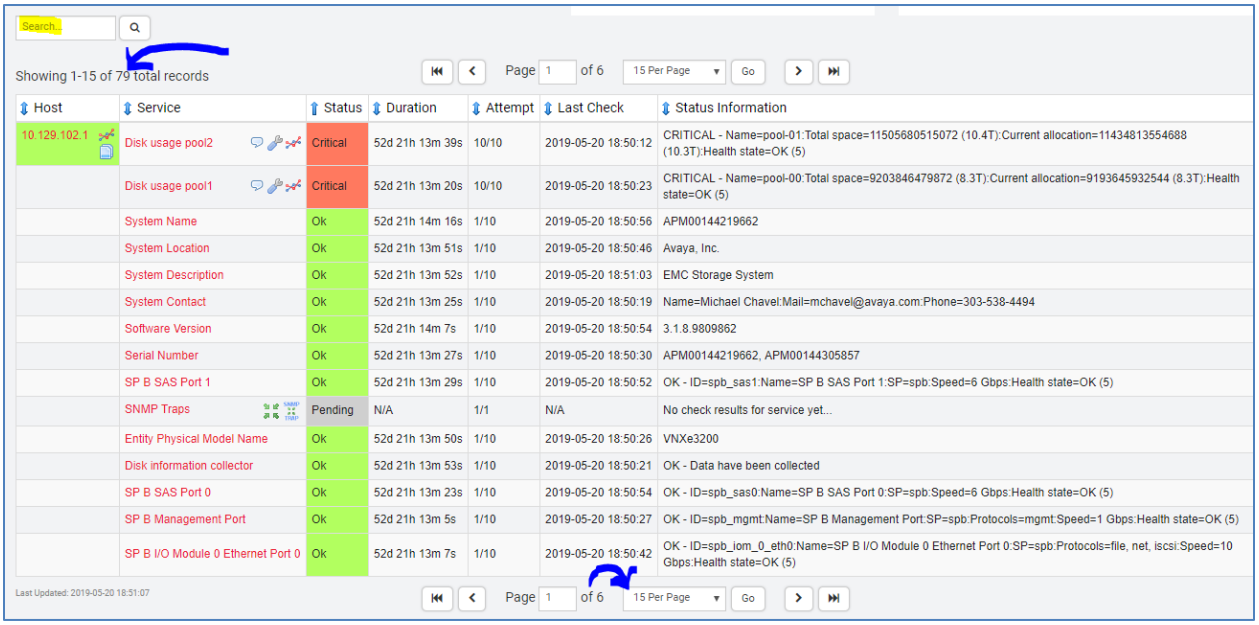


Service Status icon 

Drilling down into the paper stack displays the complete list of services associated with the host containing the services that are alarming, including those in a healthy state. This could provide needed insight into the source of a problem.

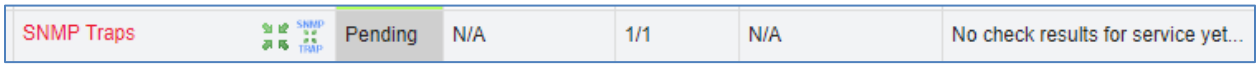
You may search for a specific service name for a specific sorted view or click on any of the blue arrows next to the column names for sorting according to that criteria. Verify the number of pages available and increase your view, as needed, at the bottom of each reporting page.

[3] Graphical representation is not often available for host elements.



From this report, you may drill down into more specific view of each Service or Host item, or into the same type of icons as previously available on the upper-level form.

An important item to note on this form is the SNMP Traps item, located somewhere at the middle of the page.



The two icons associated with the SNMP Traps items are:

- Inbound 4-corners arrows: Passive check only, indicating the only way this item will alarm is if a service on the host sends a trap to AO.
- SNMP Trap: A link to drill down to Service Status Detail for SNMP traps.

With critical alarms present for services within this host, you might be curious as to why the SNMP trap alarm is not reporting a critical or warning state, since the host should have sent an SNMP trap to AO in response to the state changes within the host.

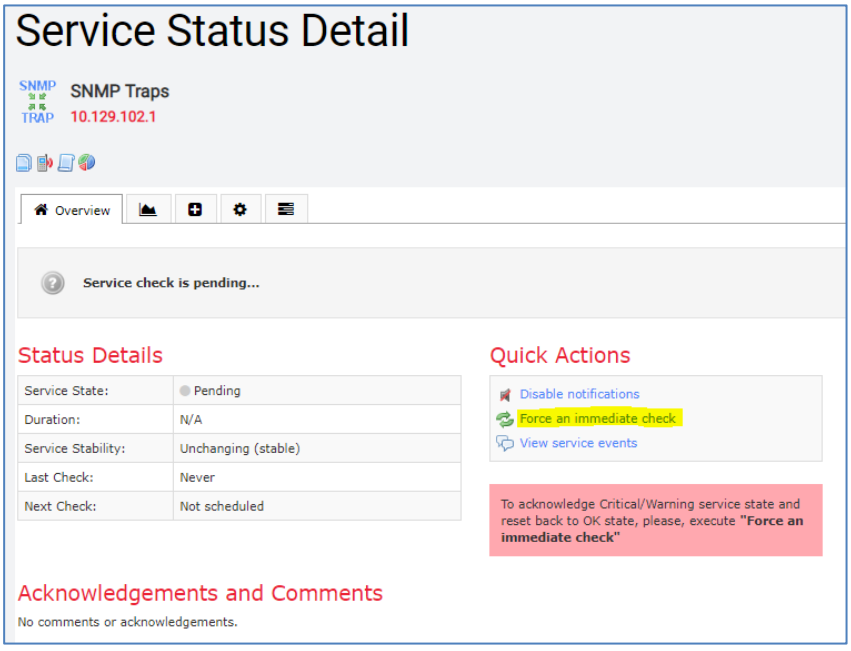
The current critical and warning alarms could also have been “learned” by AO through proactive monitoring. Still, SNMP should also be reporting an alarm state.

The reason this SNMP alarm is not reporting a critical or warning state is because it was reset to a “Pending” state, to await new SNMP trap information. It was cleared because the alarming state of the host was already reviewed and understood, each service alarm being “acknowledged” and cleared from the main solution view.

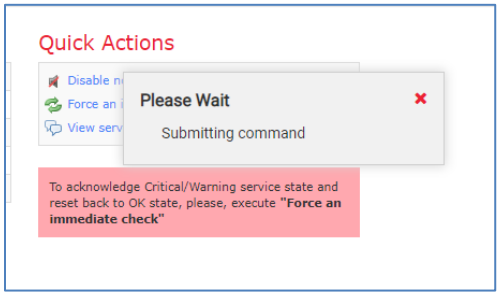
Important:
Clear the fields that are monitored after alarms are seen and understood.

After an alarm is acknowledged, AO clears the alarm status information from the main dashboard, creating a fresh view for new incoming alarms. You can perform the same kind of activity manually for the SNMP Trap element. After the SNMP alarm issues are recognized and are in the process of being resolved, you should clear the alarm field to identify new SNMP traps easily. Even if the issues are still open, they are tracked and monitored by proactive checks from AO.

To clear an SNMP Trap alarm, click on the SNMP Trap icon. You will be directed to the Service Status Detail page for SNMP Traps. The message in the red box instructs users how to reset the SNMP Trap field by selecting the **Force an immediate check** option in the **Quick Actions** area.



Clicking the **Force an immediate check** option, resets the SNMP Traps service field to a "Pending" state. When the next trap/alarm is sent to AO from the associated host, a state change will be reported.



Chapter 8: Event handlers

About event handlers

This chapter contains information about how to use event handlers in Avaya Orchestrator to take predefined actions when the hosts or services that you are monitoring change state. Avaya Orchestrator uses event handlers to automate processes when a specific host or service changes state. This reduces the amount of manual work when something changes in your environment.

Event handlers are optional system commands. They are scripts or executables that are run when a host or service changes state. These commands include, but are not limited to, restarting services, parsing logs, checking other host or service states, and making database calls. These scripts proactively run every five minutes on all hardware devices, providing alarms and state color changes for service and host problems.

Event handlers are called whenever a state change occurs. This includes HARD, SOFT, OK, WARNING, CRITICAL, and UNKNOWN states. When a state change occurs, the logic behind the executed action, if any, is performed by the script or executable that is called by Avaya Orchestrator when the state change occurs. The script can parse these states through macros passed to it by the event handler and is readable on various web pages.

Ensure that the ACP Configuration Wizard is properly administered for each rack with the necessary IP addresses and protocols. This is the core basis for Event Handlers to function properly.

Modifying Event Handlers is not supported in Avaya Orchestrator Release 1.4 because of the complexity involved, the required expertise in programming knowledge, and the required familiarity with Avaya Orchestrator. Customization of event handling will be supported in a future release.

Chapter 9: Backup and restore

Backup configuration

This chapter contains information and procedures about how to back up the Avaya Orchestrator configuration.

Backups are an important aspect of administration and maintenance of your system. They can and should be automated for nightly archiving. If the alarm and maintenance data is critical to maintain, it is recommended that you store the backups at a location other than the AO server location.

The backup script saves the archived information in the `/store/backups/orchestrator/` directory. Backup names correspond to the `AO_backup_yyyy-mm-dd_hh-ii.tar.gz` pattern, where `yyyy-mm-dd_hh-ii` is the year, month, day, hour, and minute of the backup creation date and time.

The backup script:

- Gathers all data files into a temporary directory in `/store/backups/orchestrator/`.
- Creates the backup `.tar.gz` file after collecting all stored AO data.
- Deletes all the files previously collected, during the gathering process, after successfully creating the `.tar.gz` file.

Important:

Ensure that there is enough free disk space in `/store/backups/orchestrator/` for the data collection and processing activities. If not, the backup process fails and the server runs out of disk space. Lack of disk space can also cause other issues for the Avaya Orchestrator server.

There is 20 GB of capacity allocated for backup storage. A large and active application is projected to require approximately 420 MB of storage for seven days. The capacity available is sufficient for approximately one year of local storage for most customer solutions.

Note:

The backup script restarts the service at the beginning of the backup to ensure that the `retention.dat` file is up to date with the latest information. There is a slight interruption to the monitoring process when the restart occurs.

You can create and schedule backups by using the web interface.

Creating a backup by using the web interface

About this task

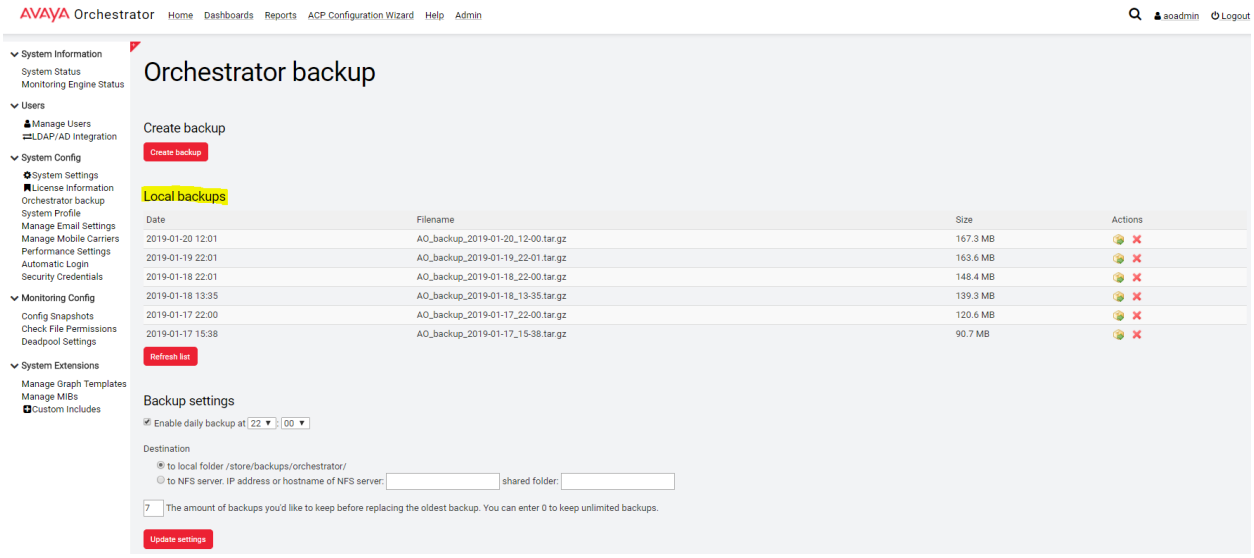
Use the following procedure to create a backup by using the Avaya Orchestrator web-based interface.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup**.
4. On the Orchestrator backup page, click **Create backup**.

Result

The new manually created backup file appears in *Local backups*.



Scheduling backups

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. Select the **Enable daily backup at** check box and in the corresponding fields, click the hour and minute at which the daily backup must start.

6. Click **Update settings**.

Configuring backup retention

About this task

Use the following procedure to configure the retention of backup files.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. In **The amount of backups you'd like to keep before replacing the oldest backup. You can enter 0 to keep unlimited backups** field, type the number of backup files that you want to retain.

   The oldest backup file is deleted when the maximum number of backup files is reached.

6. Click **Update settings**.

Storing backup files

About this task

Avaya recommends that you store the configuration backups at a location other than the one located within the Avaya Converged Platform 4200 series SAN. Remote storage ensures that configuration backups are available in all failure circumstances.

You can configure Avaya Orchestrator to save backup files to NFS server storage.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup.**
4. On the Orchestrator backup page, navigate to the **Backup settings** area.
5. In **Destination**, do one of the following:
   - Click **to local folder /store/backups/orchestrator/** to store the backup file on the locally allocated SAN storage of Avaya Orchestrator.
   - Click **to NFS server. IP address or hostname of NFS server** and specify the IP address or the hostname of the NFS server. In the **shared folder** field, type the shared folder name on

the NFS server.

6. Click **Update settings**.

Downloading the backup files

About this task

Avaya Orchestrator supports downloading of configuration backup files so that you can move the backup files to a remote location or alternate storage medium.

Procedure

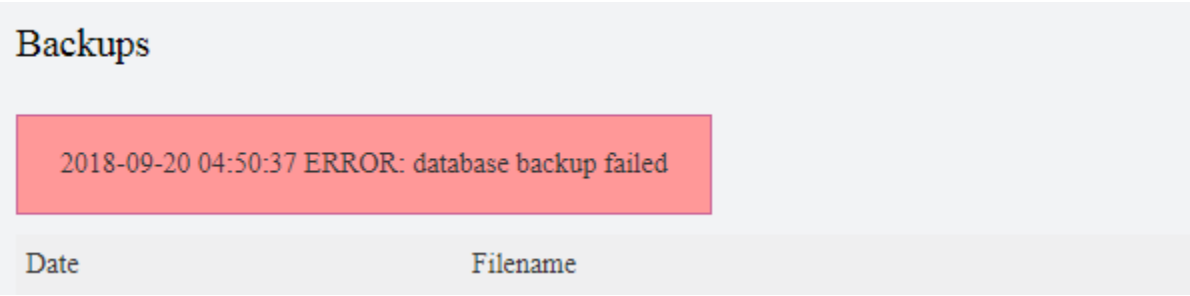
1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Orchestrator backup**.
4. On the Orchestrator backup page, navigate to the **Local backups** area.
5. Click the **Download** icon corresponding to the backup file that you want to download.
6. Move the backup file to a remote storage location or alternate storage medium. For example, the local computer.

Troubleshooting backups

The backup script writes high-level backup process information to the `/var/log/orchestrator_backup.log` log file.

An error message is displayed on the Backups page if an error occurred during the last backup. Click **Admin** > **Orchestrator backup** > **Backups** to navigate to the Backups page.

The following is an example of an error message:



Avaya Orchestrator system restore

The restore script for Avaya Orchestrator is used in the following scenarios:

- Restoring an Avaya Orchestrator server that has malfunctioned.
- Migrating Avaya Orchestrator between different server types.
  - Physical-to-physical
  - Physical-to-virtual
  - Virtual-to-virtual
  - Virtual-to-physical

In Avaya Orchestrator Release 1.4, restore functions are available only for exact matches between the software version of AO and the software version on the backup to be restored. For example, a backup of an AO application running load ABC can be restored to an AO application running load ABC.

Important: The restore script overwrites any existing configurations and data on the target server.

Restoring the system

Before you begin

Note:
Avaya recommends creating a VMware snapshot of the Avaya Orchestrator virtual machine before proceeding. This provides a fallback to the earlier image in case the outcome of any restoration results in undesired product behaviors.

Procedure

1. Log in to Avaya Orchestrator by using SSH and *aoadmin* credentials.
2. At the aoadmin admin prompt $, type ***su – root***, and then type the root password.
3. To restore a local backup, do the following:
   a. At the root # prompt, type the following command:

      cd /store/backups/orchestrator

   b. In the backup directory, identify the file that you want to restore and note the file name.

   c. Follow Step 5.
4. To restore a backup from an external device, do the following:
   a. From the remote backup media location, copy the backup file that you want to restore into the `/tmp` directory in Avaya Orchestrator.

   b. At the root # prompt, type the following command:

      cd /tmp

c. Follow Step 5.

5. At the root prompt, type the following command:

   restore_orchestrator <AO backup file name>

   The following messages appear indicating the start and completion of the restoration process.

```
[root@ao4 tmp]# restore_orchestrator AO_backup_2019-01-22_19-00.tar.gz
Log file is /var/log/orchestrator/restore_orchestrator.log
Restoration is started.
Restoration is completed.
[root@ao4 tmp]#
```

   Contact the Avaya Services Support team in case you come across any problems during the restoration process.

Export and Import ACP Configuration Wizard-Administration

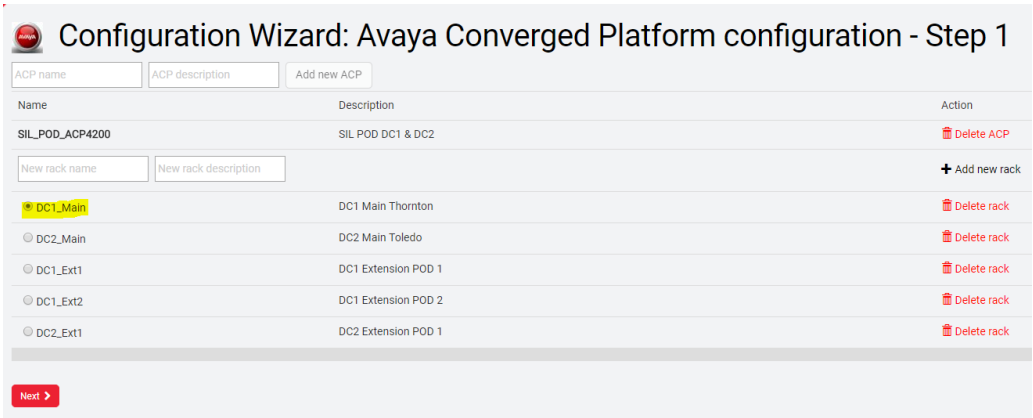
One of the most critical and time consumptive aspects of restoration is the administration of all solution components in the AO Wizard. This administration can be easily and quickly restored through this functionality. Any exports of the Wizard Administration, from an Avaya Orchestrator 1.4 software load, can be imported on to any AO 1.4 software load. An exact match of load software is not necessary for this activity, as long as both AO and the export file data are based on the same AO release, that is, 1.4.

This functionality is most often used after a redeployment of AO. For example, part of the upgrade process. However, it can be applied to existing systems once the items needing to be refreshed or restored with the import data have been removed.

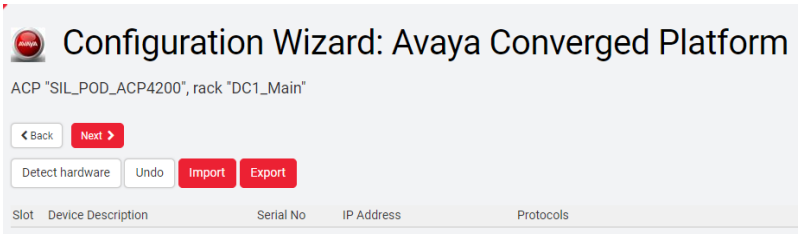
Exporting rack configuration

Procedure

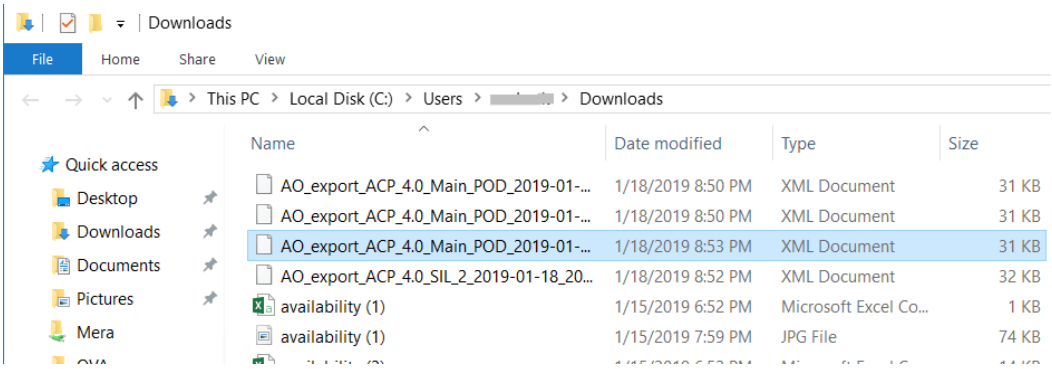
1. Log in to the Avaya Orchestrator web interface by using administrative credentials, and then click **ACP Configuration Wizard**.
2. On the Configuration Wizard: Avaya Converged Platform configuration – Step 1 page, select a rack, and then click **Next**.



3. On the Configuration Wizard: Avaya Converged Platform configuration – Step 2 page, click **Export.**



The Export function creates a file for the rack translations in the `Downloads` directory of the local machine.



4. Export each rack information one at a time.
   When finished, you can keep these files on the local computer, or copy them to other media or storage locations.

Importing rack configuration

About this task

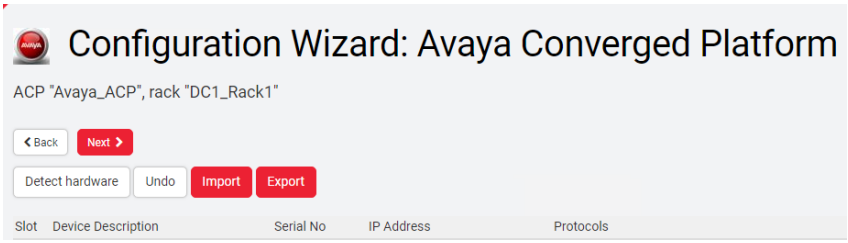
To import the configuration of a specific rack, the configuration of the rack must first exist.

Note:
The import process overwrites the configuration that is present in a rack.

Procedure

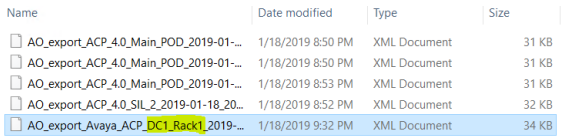
1. Log in to the Avaya Orchestrator web interface by using administrative credentials, and then click **ACP Configuration Wizard**.
2. On the Configuration Wizard: Avaya Converged Platform configuration – Step 1 page, select a rack.
   Ensure that the name of the rack that you select is the same as that of the exported XML data file that you want to import.
   The following screen shot provides an example of the XML file names:

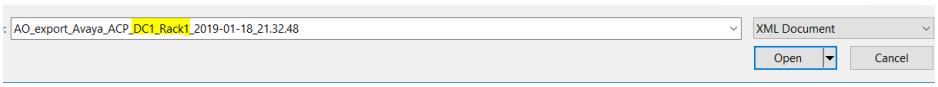
3. Click **Next**.
4. On the Configuration Wizard: Avaya Converged Platform configuration – Step 2 page, click **Import.**



   The `Downloads` directory on the local device is displayed.

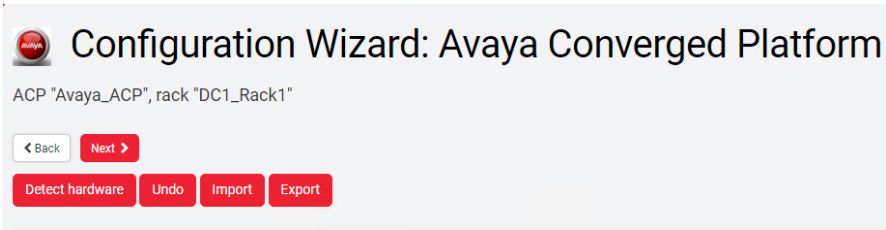
5. Browse to the file that you want to import, click the file, and then click **Open**.





The file is imported. Note that the **Detect Hardware** button is now red, indicating that the devices must be rediscovered.

6. Click **Detect Hardware**.



7. After hardware detection is complete, click **Next**.
8. Click **Finish** to complete the import and rediscovery process for the rack.
9. Repeat this procedure for all racks as needed.

Chapter 10: Users and contacts

About users and contacts

This chapter describes the relationships between users and contacts in Avaya Orchestrator. Users and contacts are closely related, although slightly different, and Avaya Orchestrator combines the functionality of both in Release 1.4.

Users vs. contacts

- Users correspond to user accounts that are used to log in to the Avaya Orchestrator web interface.
- A user is typically connected to a contact for both enabling notifications and obtaining permissions to view and modify hosts and services.
- Contacts are definitions in Core that are normally used for directing host and service alerts to specific individuals.
- Contacts do have a relationship with users, in order to ensure that the users can use the Avaya Orchestrator web interface.

Adding a user

Procedure

1. Log in to the Avaya Orchestrator web interface by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manage Users page, click **Add New User** to add a new user.
5. In the **General Settings** area, do the following:
   a. In the **Username** field, type a user name for the user to log in to Avaya Orchestrator.
   b. In the **Password** field, type a password for the user to log in to Avaya Orchestrator.
   c. In the **Repeat Password** field, retype the password.
   d. Select the **Force Password Change at Next Login** check box if you want the user to change the password when the user logs in the next time.
   e. Select the **Email User Account Information** check box to send the user's account

information to the user through an email message.

f. In the **Name** field, type the name of the user.

g. In the **Email Address** field, type the email address of the user.

h. In the **Phone Number** field, type the phone number of the user.

i. Clear the **Create as Monitoring Contact** check box.

j. Select the **Enable Notifications** check box if you want to send notifications to the user.

k. Select the **Account Enabled** check box to enable the user account and allow the user to log in to Avaya Orchestrator.

   If you clear this check box, the user cannot log in to Avaya Orchestrator by using the login credentials.

6. In the **Preferences** area, set the user preferences.

   For more information, see User preferences.

7. In the **Authentication Settings** area, set the authentication type for the user.

   For more information, see Linking existing Avaya Orchestrator users to Active Directory users and Linking existing Avaya Orchestrator users to LDAP users.

8. In the **Security Settings** area, set the security settings for the user.

   For more information, see User security settings.

9. Click **Add User**.

User preferences

Preference	Description
Language	The language preference of the user.
Date Format	The Date format preference of the user.
Number Format	The number format preference of the user.
Week Format	The week format preference of the user.

Relation of users to contacts

In normal operation, Avaya Orchestrator users are directly associated to Core contacts with a one-to-one relationship.

This direct correlation allows Avaya Orchestrator to manage alert notifications from the Core monitoring engine on a per-user basis. Avaya Orchestrator users can easily manage their notification preferences and methods by using the Avaya Orchestrator web interface.

When an Avaya Orchestrator user account is directly related to a Core contact, the user account is automatically granted permission to view and modify all hosts and services for which the underlying Core contact receives notifications.

Relationship configuration details

By default, Avaya Orchestrator allows users to manage their notification preferences, notification times, and notification messages through the web interface. This requires that each Avaya Orchestrator user has a direct relationship with a corresponding contact in Core.

The relationship between an Avaya Orchestrator user and a Core contact is established with the following configuration:

- There is a Core contact with the same short name as the user name of the Avaya Orchestrator user. For example, jdoe is the same short name for a contact and a user.
- The Core contact that corresponds to the user account must have the following properties:
  - Host notification command is: **`xi_host_notification_handler`**
  - Service notification command is: **`xi_service_notification_handler`**
  - Host and service notification time periods are both set to: **`<username>_notification_times`**
    For example, jdoe_notification_times

Chapter 11: User rights

User rights

This chapter contains information about Avaya Orchestrator user rights or permissions and how to effectively manage permissions to ensure security and obtain a web interface tailored to various individual needs.

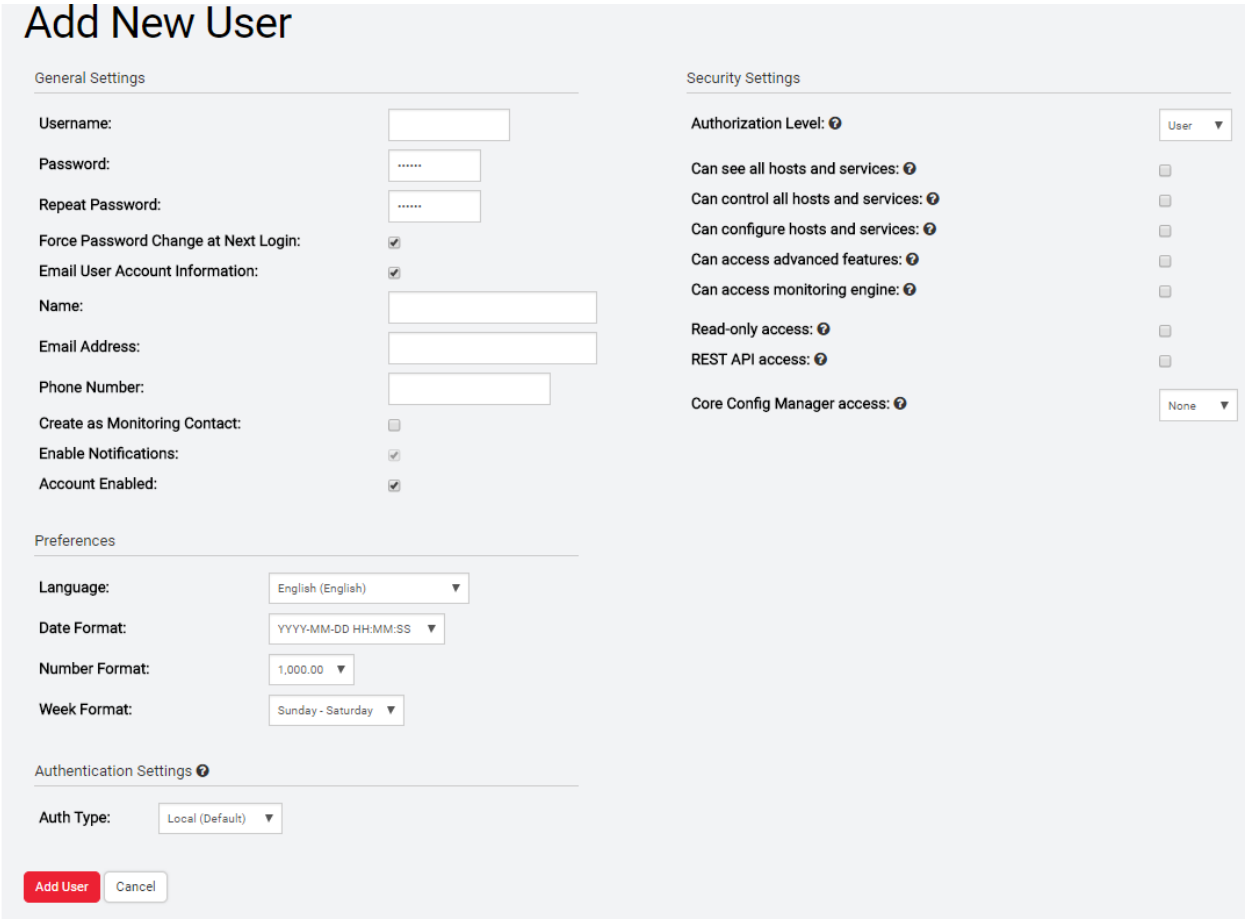
Managing permissions

About this task

You can configure permissions for individual users when adding a new user account to Avaya Orchestrator or modify the permission for an existing user on the Manage Users page.

Procedure

1. Log in to the Avaya Orchestrator web interface by using administrative credentials.
2. Click Admin.
3. In the left navigation pane, click Users > Manage Users.
4. On the **Manage Users** page, do one of the following:
   - Click the Edit  icon corresponding to the user that you want to edit.
   - Click **Add New User** to add a new user.



5. Set the permissions.

Note:

- Clear the **Create as Monitoring Contact** check box.
- The options that you select in the **Security Settings** area of the **Add New User** or **Edit User: *<user name>*** page determine the permissions.
  For more information, see User security settings.
- By default, **Authorization Level** is set to **User**. This is the most restrictive permission in Avaya Orchestrator.
- If you do not select any options, the user can only view the host and services that have the user defined as a contact.

Administrator privileges

Users with administrator privileges can access, add, and re-configure the following:

- Users
- Hosts
- Services
- Components
- Configuration wizards
- Dashlets
- Program settings
- Security credential

Notes:

You must enable the **Rest API access** option when you select the **Authorization Level** as **Admin**. Failure to do so results in undesirable configuration outcomes when changes are done in the ACP Configuration Wizard, which may require saved XML translations to be imported for resolution.

For more information, see Managing permissions.

User security settings

You can grant various levels of security settings to users depending on the requirements. The following table contains information about the security setting options:

Setting	Description
Authorization Level	The authorization level for the user. The options are: • **User**: Security settings for users. • **Admin**: Security settings for administrators. **Notes:** The **Admin** authorization level has all user rights except the **REST API access** right. By default, the **REST API access** option is not enabled for the **Admin** authorization level.
Can see all hosts and services	The user can see all hosts and services that ,are monitored and not just the ones they are a direct or indirect notification contact.

Can control all hosts and services	The user can: • Acknowledge problems • Schedule downtime • Toggle notifications • Force checks on all objects
Can configure hosts and services	The user can: • Run configuration wizards. • Delete from Detail page. • Re-configure from Detail page.
Can access advanced features	The user can: • Edit check command on the Re-configure Host/ service page. • Show the **Advanced tab** and commands on the Host/service page. • Allow setting host parents in wizards and on the Re-configure Host/service page.
Can access monitoring engine	The user can: • View the monitoring process icon on the navigation bar. • Control the monitoring engine. For example, shutdown or restart. • Allow access to the event logs.
Read-only access	This option restricts the user to a read-only role and overwrites other options preceding it.
REST API access	The Avaya Orchestrator REST API allows users to create/query to read, write, delete, and update data in the Avaya Orchestrator system by using commands that are authenticated through the Avaya Orchestrator API keys.
Core Config Manager access	Option to provide user access to Core Config Manager (CCM). Leave this option at the default state of **None**. • **None**: No access. CCM is not visible to the user. • **Login**: The user can view the CCM links and must log in with a CCM user account. • **Limited**: The user has integrated CCM access. The user can view the objects specified under this option. Select the objects to allow a user to add, edit, and remove the objects. • **Full**: The user has integrated CCM access. The user can access all objects with no administrative features.

Avaya Orchestrator API

Avaya Orchestrator API is a REST API that includes feature rich control over the Avaya Orchestrator system. The API allows you to read, write, delete, and update data in the Avaya Orchestrator system through commands that are authenticated by using Avaya Orchestrator API keys.

For the following settings, each user has a unique API key:

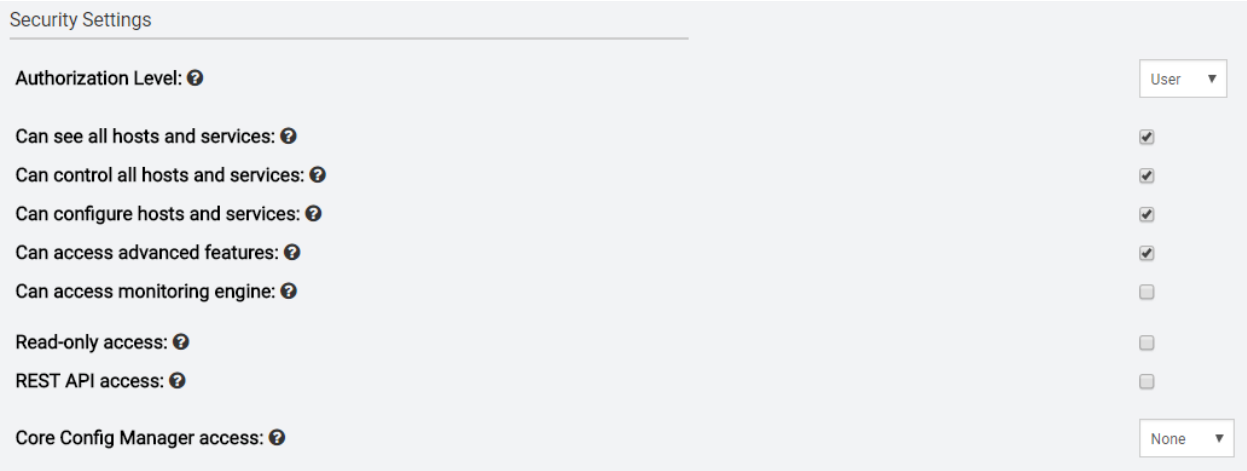
- Users have read access if the **REST API Access** setting is selected.
- Users can have access only to the **Objects API** endpoint and the relevant documentation.
- Administrators have full access to the API if the **REST API Access** setting is selected.

User privileges

Advanced user with change control

Common settings for an advanced user allow the user to view, control, and re-configure all existing hosts and services that are monitored, as well as, add new hosts and services to the monitoring configuration.

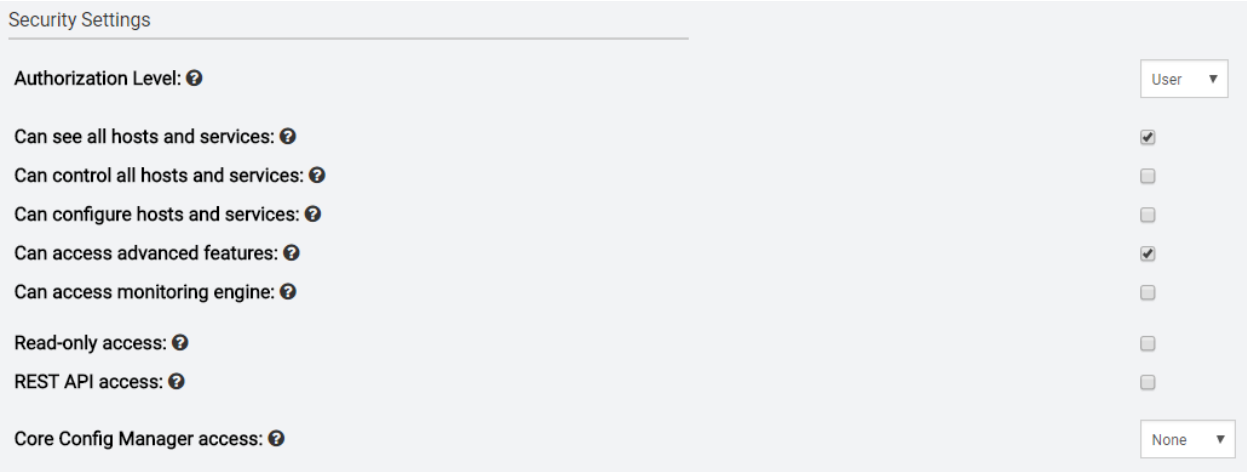
A user with these user rights has access to advanced information and commands related to hosts and services that are monitored. However, this user will not have access to control the monitoring engine. For example, shutdown and start the monitoring engine.



Basic read-only user

Common settings for a basic user allow the user to view all hosts and services that are monitored. However, the user cannot re-configure anything or submit commands to the monitoring engine.

These settings are often used when configuring user rights for IT managers or decision makers who need access only to view the monitoring information.



Chapter 12: Email configuration

Email configuration

This chapter contains information about how Avaya Orchestrator sends email messages and how to configure your email settings. Avaya Orchestrator uses email to send notifications and reports.

Accessing the email settings

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.

Web browser behavior

Important:

There are some web browser behaviors you should be aware of that can cause unwanted behaviors in ways that are not obvious to detect.

Different web browsers auto-complete and auto-populate fields on a web page when the web page loads. This usually occurs only when the web browser identifies a common field that does not have a value. The web browser has a saved value for that named field. Hence, the web browser populates the field with the saved value. Therefore, if you open the Manage Email Settings page in Avaya Orchestrator, the **Username** and **Password** fields are already populated, even when you visit the page for the first time after a fresh installation of Avaya Orchestrator.

However, this can actually cause confusion. For example, you might define SMTP settings that do not require a user name or password. If you click **Update Settings** when the **Username** and **Password** fields are populated with the values that the web browser auto-completes, authentication is attempted with those values, even though your receiving server does not require credentials. But, because the credentials are saved, they are used while sending email messages. As a result, sending of the email messages fails as the SMTP server is unaware about the credentials.

If you leave the **Username** and **Password** fields blank, and then click **Update Settings**, Avaya Orchestrator saves the settings and records that no user name or password is defined. However, when the web page refreshes, your web browser might re-populate those fields with the saved values.

Configuring the email address from which email messages are sent

About this task

Use the **Send Mail From** field to configure the email address from which email messages are sent. The format of the email address is: Plain Text Name <alias@your.email.domain>.

Note:

The brackets < > are required.

If you do not format the email address properly, the email is sent; however, in some circumstances the mail sending program switches to the system default. For example, Root User <root@localhost>.

If the receiver of the email message clicks the reply button in their email client, the reply is sent to the Root User <root@localhost>. Hence, ensure that you configure a valid email address.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in the **Send Mail From** field, type the email address from which you want to send the email messages.

Methods for sending emails

Avaya Orchestrator provides the following two methods for sending email messages:

- Sendmail / Postfix
- SMTP

Configuring Sendmail / Postfix as the method for sending email messages

About this task

This mail method uses Postfix to send email. It is referred to in the interface as **Sendmail** because this is historically the most common mail sending method. In the operating system, the **`sendmail`** command is actually the **`sendmail.postfix`** command that allows Postfix to accept **`sendmail`** commands.

The Avaya Orchestrator server uses the Sendmail method to send email messages directly to all the recipients. It contacts the email server for the email recipient and sends the message through SMTP port 25. This means that the message is sent by using plain text. Hence, network sniffing programs can easily view the contents of the email messages.

Problems can arise when you send email messages to recipients that have spam or virus detection software. The receiving mail server detects that the email message it received is not from the mail server that is the owner of that domain. The mail server either discards the email message or moves it to a junk mail folder. This behavior is obviously not desired as you want to make sure that notifications are received.

You need not configure additional settings if you select **Sendmail**, on the Manage Email Settings page, as your method to send email messages.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in **Mail Method**, click **Sendmail**.

Configuring SMTP as the method for sending email messages

About this task

You can use SMTP as the method for sending email messages if you want to configure Avaya Orchestrator to use an email server for mail delivery.

The email server can be:

- An internal email server in your organization, such as:
  - Microsoft Exchange
  - Postfix
- An external email server, such as:
  - Hosted email services
  - Internet service provider

Using an SMTP server for mail delivery is a more secure method of sending email messages. Also, the Avaya Orchestrator server can focus on monitoring activities and need not use computing resources for being an email server.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **System Config** > **Manage Email Settings**.
4. On the Mail Settings page, in the **General Mail Settings** area, in **Mail Method**, click **SMTP**.
5. In the **SMTP Settings** area, do the following:

a. In the **Host** field, type the network address of the SMTP server.

   You can specify the IP address or FQDN of the SMTP server.

b. In the **Port** field, type the network port that the SMTP server is listening on.

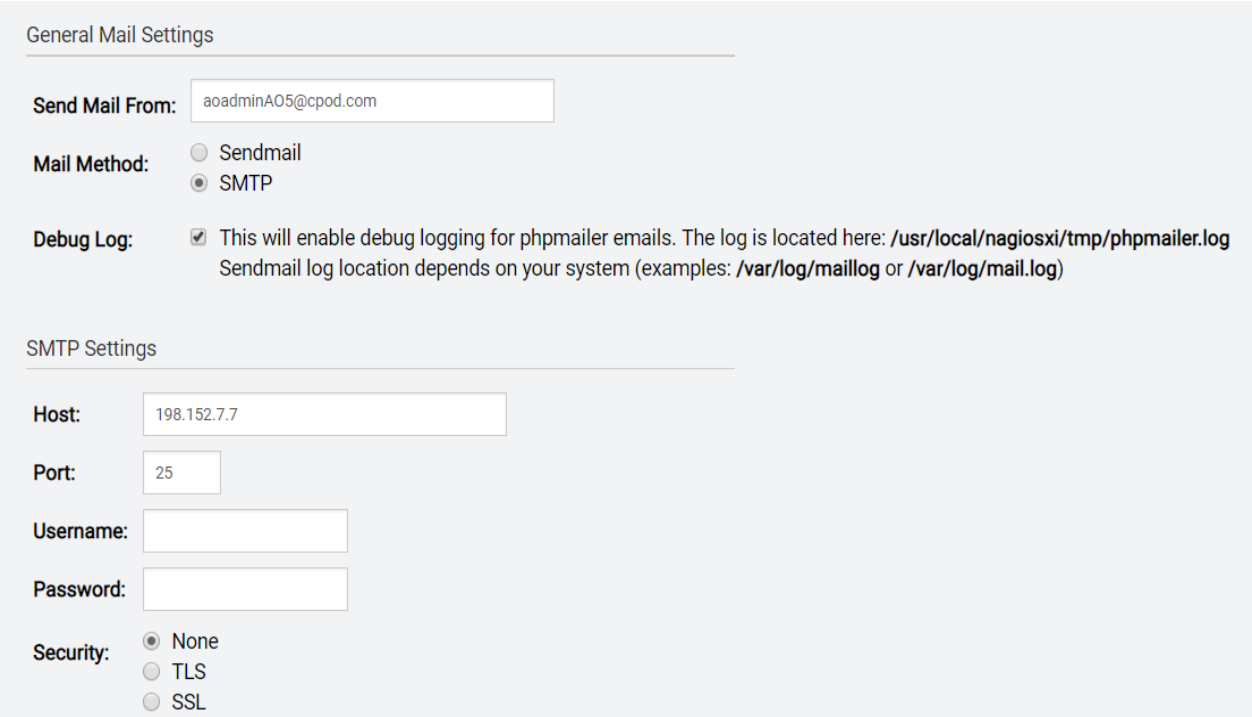
   Common port to use is 25.

Note:

- The **Username** and **Password** fields are used in Avaya Orchestrator Release 1.4. Hence, not required.
- TLS and SSL are not supported in Avaya Orchestrator Release 1.4.

Example:

In the following example, the SMTP server is a Microsoft Exchange server that allows connections from the Avaya Orchestrator server IP address. It does not require authentication and the **Security** option is set to **None**.



Chapter 13: User authentication and import

Authenticate and import users with Active Directory or LDAP

This chapter contains information about how to integrate Avaya Orchestrator with Active Directory (AD) or Lightweight Directory Access Protocol (LDAP) to allow user authentication and validation with an AD or LDAP infrastructure by using the Avaya Orchestrator interface.

This helps system administrators to simplify user management of large infrastructures and standardize credentials that are needed for Avaya Orchestrator by allowing users to authenticate with their AD or LDAP credentials.

Using a DNS server

About this task

This procedure assumes that the DNS settings for your Avaya Orchestrator server use DNS servers that are either of the following:

- Domain Controllers (DC) in your AD domain.
- Capable of resolving the DNS entries that are used to contact your LDAP servers.

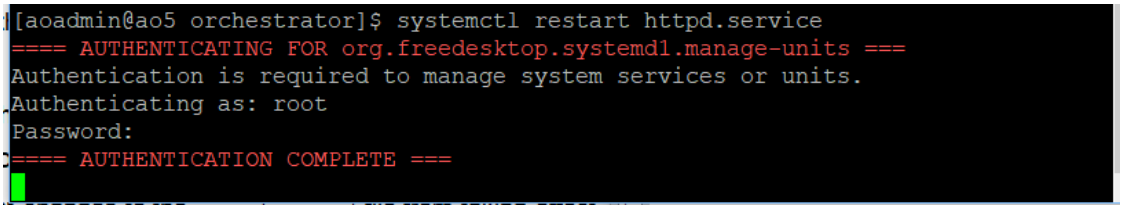
If you have problems with the DNS, use the following procedure to edit the `resolv.conf` file to use the DNS server within the AD infrastructure as the primary name server.

Procedure

1. Log in to Avaya Orchestrator by using SSH and the *aoadmin* login credentials.
2. Run the following command to edit the `resolv.conf` file in a text editor:
   sudo vi /etc/resolv.conf
3. Type the following before the lines that start with `nameserver`:

   i nameserver [DNS_server_IP] <ESC KEY>
   :wq!
   Caching options in PHP may prevent changes to the `resolv.conf` file from taking effect and require restarting the Apache service.
4. To edit the file, restart the Apache web server by running the following command:
   systemctl restart httpd.service

   The system prompts you to enter the root password to authenticate the permissions to perform this activity.



Note:

Be aware that the networking stack in RHEL can automatically overwrite the `/etc/ resolv.conf` file.

Configuring authentication servers

About this task

Use this procedure to configure the authentication server that Avaya Orchestrator must use.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **LDAP/AD Integration**.
4. To add an authentication server, click **Add Authentication Server**.
5. In the **Authentication Server Settings** area, select the **Enable this authentication server** check box.
6. In the **Connection Method** field, click one of the following:
   - **Active Directory**
   - **LDAP**
7. Do the following if you select **Active Directory** in the **Connection Method** field:
   a. In the **Base DN** field, type the LDAP formatted string where the users are located. For example Orchestrator user are on POD Organizational Unit

      For Example, OU=pod,DC=avaya,DC=com

   b. In the **Account Suffix** field, type the part of the full user identification that comes after the user name, in the format: @yourdomain.suffix.

      For example, `@avaya.com`.

   c. In the **Domain Controllers** field, type the domain controller servers that Avaya Orchestrator can use to authenticate against.

      This can be either IP addresses or fully qualified domain names.

      When you use SSL for security, this entry must match the Common Name (CN) in the SSL certificate that these domain controllers present to the Avaya Orchestrator server. TLS is not supported in Avaya Orchestrator Release 1.4.

For example, `dc1.avaya.com`

d. In the **Security** field, click the security method to connect to the server.

e. Click **Save Server**.

8. Do the following if you select **LDAP** in the **Connection Method** field:

a. In the **Base DN** field, type a LDAP formatted string where the users are located.

For example, `dc=avaya,dc=com`

b. In the **LDAP Host** field, type the IP address or the host name of the LDAP server that Avaya Orchestrator can use to authenticate against.

You can specify an IP address, short name, or fully qualified domain name. For example, `ldap01.avaya.com`

When you use SSL for security, this entry must match the Common Name (CN) in the SSL certificate that the LDAP server presents to the Avaya Orchestrator server.

For example, `ldap01.avaya.com`

c. In the **LDAP Port** field, type the TCP network port that you want to use to communicate with the LDAP server.

The default port is 389.

d. In the **Security** field, click the security method to connect to the LDAP server.

e. Click **Save Server**.

Importing users from Active Directory and LDAP

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manage Users page, click **Add Users from LDAP/AD**.
5. On the **LDAP / Active Directory Import Users** page, select the authentication server that you have defined and specify the user name and password to connect to the server.

   The account credentials that you provide are used only to authenticate against the Active Directory or LDAP to retrieve the directory contents. These credentials are not saved or used in the actual user authentication.
6. Click **Next**.

   After successful authentication, a node of your directory tree appears. This is relative to the Base DN that you specify.
7. Select the users that you want to import, and then click **Add Selected Users**.

8. Select the check boxes corresponding to the users for whom you want to configure the same preferences and security settings.
9. In the **Edit multiple** field, click **Preferences**.

   The **Preferences** dialog box appears.
10. Do the following to configure the preferences for the users:
    a. Clear the **Create as Monitoring Contact** check box.
11. In the **Edit multiple** field, click **Security Settings**.

    The **Security Settings** dialog box appears.
12. Configure the security settings for the users.

    For more information, see User security settingsUser security settings.
13. Click **Save**, and then click **Import**.

Result

After you import a user, Avaya Orchestrator queries the domain controllers or LDAP server to validate the credentials each time the user logs in.

Linking existing Avaya Orchestrator users to Active Directory users

About this task

If you have already created Avaya Orchestrator users, you can easily link these local accounts to Active Directory accounts.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manager Users page, click the **Edit** icon corresponding to the user that you want to link to Active Directory.
5. On the Edit User: *<user name>* page, in the **Authentication Settings** area, do the following:
   a. In the **Auth Type** field, click **Active Directory**.
   b. In the **AD Server** field, select the authentication server that you have defined.
   c. In the **AD Username** field, type the user name that is configured in Active Directory for the user.

      For example, `jane.doe`
6. Select the **Allow local login if auth server login fails** check box to allow the user to use the

local password that is created for the user.

Avaya Orchestrator uses the local login when the authentication server cannot be connected or times out, or the password provided is incorrect. This allows a secondary method of authentication if the authentication server is unreachable.

7. Click **Update User**.

Result

After these changes are made, the existing Avaya Orchestrator users can log in by using their Active Directory credentials.

Linking existing Avaya Orchestrator users to LDAP users

About this task

If you have created Avaya Orchestrator users, you can easily link these local accounts to LDAP accounts.

Procedure

1. Log in to Avaya Orchestrator by using administrative credentials.
2. Click **Admin**.
3. In the left navigation pane, click **Users** > **Manage Users**.
4. On the Manager Users page, click the **Edit** icon corresponding to the user that you want to link to LDAP.
5. On the Edit User: <*user name*> page, in the **Authentication Settings** area, do the following:
   a. In the **Auth Type** field, click **LDAP**.
   b. In the **LDAP Server** field, click the authentication server that you have defined.
   c. In the **User's Full DN** field, type the full distinguished name (DN) that is configured in LDAP for the user.

      For example, `uid=bobsmith,ou=People,dc=box293,dc=local`

   d. Select the **Allow local login if auth server login fails** check box to allow the user to use the local password that is created for the user.

      Avaya Orchestrator uses the local login when the authentication server cannot be connected or times out, or the password provided is incorrect. This allows a secondary method of authentication if the authentication server is unreachable.
6. Click **Update User**.

Result

After these changes are made, the existing Avaya Orchestrator users can log in by using their LDAP credentials.

LDAP account requirements

The following is an example of the required object classes and attributes that must exist for an LDAP user. If these attributes do not exist, it is likely that they do not appear in the list of users when you import from your LDAP server.

- dn: uid=bobsmith,ou=POD,dc=avaya,dc=com givenName: Bob
- sn: Smith
- cn: Bob Smith uidNumber: 10004
- gidNumber: 10004
- mail: bobsmith@avaya.com homeDirectory: /home/bobsmith objectClass: top
- objectClass: posixAccount objectClass: inetOrgPerson

Chapter 14: Resources

Documentation

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

Table continues…

Title	Description	Audience
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.
Using 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 104

Avaya Documentation Portal navigation on page 104

Finding documents on the Avaya Support website

Procedure

1. Go to https://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**.

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, Twitter, and GooglePlus.
- 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.

Training

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

Viewing Avaya Mentor videos

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

About this task

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

Procedure

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

    Note:
    Videos are not available for all products.

Support

Go to the Avaya Support website at 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 107

Using the Avaya InSite Knowledge Base

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

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

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

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

1. Go to https://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 106