Deploying Avaya Analytics™ for Avaya Oceana®

Release 4.3.1.1
Issue 1
March 2026

Notices

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

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

(HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

The purpose of this document is to provide information on how to prepare, install, and configure Avaya Analytics™.

This document is intended for the implementation personnel who install and configure Avaya Analytics™ at a customer site. The document also provides initial administration and mandatory post-installation procedures.

This document assumes that the user has working knowledge of the following:

- Avaya Oceana®
- Kubernetes (k8s)
- Docker
- VMware
- Grafana
- Prometheus
- Kibana
- Apache Kafka
- Red Hat Enterprise Linux
- Docker for Windows or Docker for Mac (offline installation)
- Windows PowerShell (offline installation)
- Istio
- Helm

New in this release

Avaya Analytics™ release 4.3.1.1 includes the following features and enhancements:

- Added support for Avaya Common Services Platform release 1.3.0.2.
- Added a banner to the login window that displays the expiration date for the platform cluster certificates.

- Added support for offline installation using Windows Subsystem for Linux (WSL).

Note:

Avaya Analytics™ release 4.3.1.1 requires more resources than previous releases, to implement the above features. For more information on new resource requirements, refer to Planning and preconfiguration on page 27.

Related links

Support for upgrading to Avaya Analytics 4.3.1.1 on page 10

Support for upgrading to Avaya Analytics™ 4.3.1.1

Upgrading from Avaya Analytics™ release 4.2 Patch 2, 4.3 Patch 2, and 4.3.1.0 to Avaya Analytics™ release 4.3.1.1 is supported.

Related links

New in this release on page 9

Expanding Cluster Control Manager node disk

About this task

Use this procedure to automatically expand the logical volume of `/var/avaya/artifactCache`, when you increase the disk size of **CCM node from vCenter**. This procedure is optional and must be performed only if you want to expand the disk size.

Procedure

1. Log in to vCenter using an account that has deployment permissions.
2. Click **Inventory Trees** > **VMs and Templates**.
3. Expand **VMs and Templates** to locate and select the target cluster.
4. Right-click the cluster and select **CCM node**.
5. Click **Power** > **Power Off**.
6. Click **Yes**.
7. Right-click the **CCM node** and select **Edit settings**.
8. Select **Virtual Disk (Hard Disk 1)**.
9. Enter the desired size for the hard disk.
10. Click **Ok**.
11. Righ-click the **CCM node** and select **Power** > **Power On**.

Chapter 2: Overview

Avaya Analytics™ overview

Avaya Analytics™ is a microservices-based reporting solution that collects events from Avaya Oceana®. These events are translated into Contact Center measures and stored in the reporting database. With these measures, you can create a suite of historical reports for Avaya Oceana®. Avaya Analytics™ is a reporting platform that provides the ability to view and analyze Avaya Oceana® data through historical interaction dashboards.

Avaya Analytics™ also offers a suite of measures for real-time dashboards to provide a view of the key Contact Center KPIs to supervisors and Contact Center managers.

With the new interface of Avaya Analytics™, you can:

- Streamline contact center operations
- Reduce operational costs
- Provide enhanced services to customers
- Get insights from interactions to enhance customer experience and agent performance
- Analyze interaction types that Avaya Oceana® supports

Avaya Analytics™ provides a simplified installation through the adoption of Avaya Common Services.

Avaya Common Services overview

Avaya Analytics™ is deployed as a product on Avaya Common Services (Common Services).

Common Services provides several common services for Avaya products, such as:

- logging
- alarming
- certificate management
- authentication
- eventing
- event monitoring

Common Services ensures ease of deployment and supports rolling upgrades, thereby simplifying the upgrade process. Every Avaya Analytics™ service is built according to microservices

architecture. Using Common Services, you can update a helm chart easily, which enables you to stage and deploy a new service or an updated service version.

You deploy the Common Services Cluster Control Manager (CCM) OVA in your virtual environment. You use CCM to install Avaya Analytics™, and during the install, CCM uses a pre-populated installation spreadsheet to apply your specified configuration, validate the data, configure all required virtual machines, deploy k8s clusters, and install all required services. All other required software is stored in an Avaya repository. You use your Avaya credentials to download this software during deployment. Avaya Analytics™ supports online and offline installs.

Each service has a helm chart, a collection of files that store K8s deployment data, configuration data, scripts, and software required for a successful install. Common Services uses these helm charts, contained in a helm repository, to deploy the Avaya Analytics™ solution.

Container technology

Common Services uses container technology to simplify deployment, configuration, and upgrades. Common Services uses Docker to build and run application containers within a data center. CCM can connect to the Avaya repository to obtain containers used to deploy services. Containers run on the kernel of a virtual machine and do not require a hypervisor. Each Avaya Analytics™ service runs in a container.

Kubernetes (k8s) is a container orchestrator that provides APIs and command lines to enable container deployment automation. CCM deploys a k8s cluster into your virtual environment, which runs on virtual machines (VMs). A cluster contains many nodes; a master node and worker nodes. Containers run on the k8s nodes as pods, and a pod can contain one or more containers deployed together.

Avaya Analytics™ on High Availability overview

In Avaya Analytics™, high availability (HA) is available by default.

The reporting database gets deployed automatically with a primary and standby instance. The Avaya Analytics™ measure processors are deployed as a primary and standby pair. The active and hot standby instances process all events with only the Active instance providing output to the database and Real-time topics. The HA switchover occurs at the application level. If any active application fails, the hot standby instance takes over.

Note:

You do not need to do a manual restore from backup after an HA event.

Avaya Analytics™ node HA

The vCenter HA manages the node detection and recovery. If a node fails, the pods running on that node is rescheduled to the other nodes in the cluster where pod anti-affinity rules permits. Anti-affinity indicates that no replica of a pod is co-located on a single node. The pods are relocated only if the available nodes have sufficient resources to meet the pod requirements.

Note:

The pods that Kubernetes cannot relocate gets redeployed only after the failed node is recovered.

Avaya Analytics™ host HA

The host recovery is based on vCenter assuming that all physical hardware, such as disk, CPU, RAM, or NIC are working. Any outages in these hardware component prevents the recovery of the host.

Avaya Analytics™ stream services

The streams services provide producers and measures to Avaya Workspaces for use in real-time reporting dashboards.

- By using Avaya Workspaces, you can view real-time reporting dashboards to monitor up-to-date statistics for your contact center and resources.
- By using the Avaya Analytics™ historical reporting interface, you can view and analyze historical interaction dashboards to enhance customer experience and agent performance.

Avaya Analytics™ HA caveats

Avaya Analytics™ HA is not based on an n+1 HA strategy due to footprint constraints. The current cluster consist of three master nodes on which the applications run. When a VM node or the EXSi host fails, Avaya Analytics™ relies on VMWare HA to recover the failed node or host.

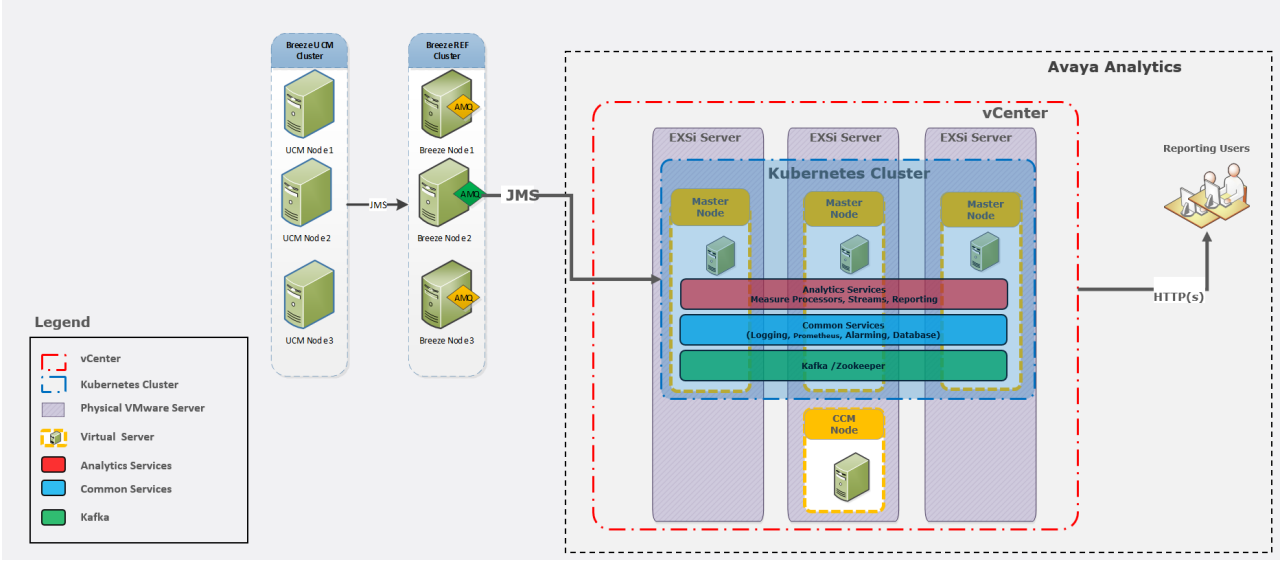
- During a node or host outage, Avaya Analytics™ runs at reduced capacity with potential loss of feature functionality depending on the node or host that failed.
- The remaining two node in the cluster do not have the resource capacity to host all the service that were originally running on the failed node.
- Kubernetes automatically spins up new instances of the failed service on the remaining two nodes, however; with limited resource capacity on these nodes not all service restarts.
- For restore, you must recover the failed node.
- After the node is recovered, the cluster remains unbalanced with most services running on the two nodes that remained running.
- Depending on the node that failed, recovery of the node outage can take up to 15 to 25 minutes.
- During node failure you do not lose any data, however, you might lose service continuity.
- After a node outage, the Real-time reports take several minutes to start updating.
- Historical reporting might not be available until the node recovers.
- After the node recovers, historical reporting services could take upto 45 minutes to revert to **Running** state and will continue to remain unavailable during this time.

For details about Avaya Analytics™ on non-HA, see the relevant chapter in this document.

Topology

Avaya Analytics™ for High Availability

The following diagram depicts the architecture for a High Availability Avaya Analytics™ reporting solution:



Chapter 3: Security Considerations for Avaya Oceana® and Avaya Analytics™ deployments

Introduction

Before you begin the deployment process, you must enable or configure the security layers using Avaya Oceana® and Avaya Analytics™ capabilities. Customers must engage the expertise of their security staff early in the implementation process. There are multiple configurations that turn OFF the security by default, with all other settings as ON. Customers can turn the Security settings OFF manually. The security staff must decide how to incorporate the system into the routine maintenance for virus protection, patches, and service packs.

Password policy

Every customer must create a password policy for their users. Administrators define a set of rules to maintain system security. Policies include rules for:

- Password syntax: The length and syntax.
- Password history: The number of unique passwords required before reuse of an old password.
- Password expiration and lockout: The validity, warning and grace period for expiration, and lockout rules.

Role-based access control

You can use roles to improve security and administration. Define administrative roles for your business using a role-based access control application.

Administrators can implement access control by grouping a set of privileges to a role. Roles are assigned to users. Some of the roles are: Agent, Supervisor, Manager, Quality Manager, and Administrator.

Data privacy

The Data Management utility allows you to handle data privacy requests from customers. For example, if a customer exercises the right to access information or their right to be forgotten, the Data Management utility provides a method to act on these requests.

SAL Policy Manager

Avaya SAL Policy Manager increases security and simplifies the management of authentication policies. Customers use SAL Policy Manager to set various policies to access managed devices

remotely. For example, the SAL Policy Manager comes with SSH proxy, which isolates the remote user from the connected device and prevents hosts from hopping during an SSH session.

Transport Layer Security

Transport Layer Security (TLS) is a cryptographic protocol used to increase security over computer networks.

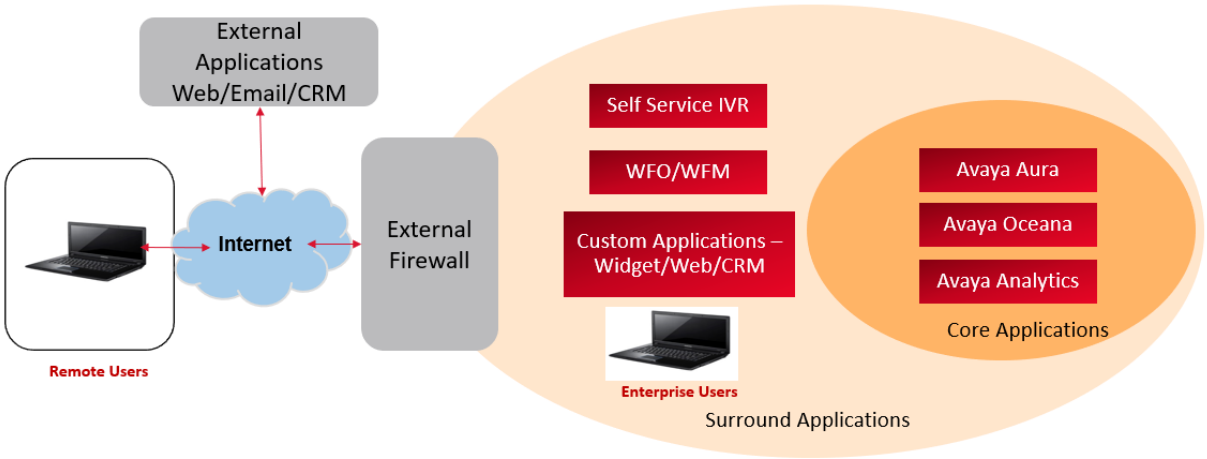
Setting TLS is a security requirement and required for internal communication and when you communicate with databases, and LDAP.

Important:

All clients must use TLS 1.2 to connect to any application in the cluster. TLS 1.0 is not supported.

Overview

The core applications of the solution must be secured at the core level, followed by the clients and applications, which connect securely to the inner core, and then the security at the entire enterprise level in the internet zone and beyond.



The inner layer of the solution contains the core applications, Avaya Aura® Core, Avaya Oceana® and the Avaya Analytics™ applications. The solution is secured by enabling the security between all the core applications. The applications outside of the core interact with the core applications. Security must be enabled for all communications and data exchange between these two layers. The applications and clients on the internet must access the contact center functionality in a secure and reliable manner.

This chapter describes the types of configurations, settings, and the techniques that the customer can use to secure all the areas, starting at the core, to the internet zone at the edge of company networks.

Core Applications Security

The operations require the three core applications to communicate with each other. Avaya Oceana® uses the Avaya Aura® Suite of applications comprising Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Communication Manager, Application Enablement Services, and Avaya Aura® Media Server to provide the voice platform for PSTN voice contacts. Avaya Oceana® is deployed with Avaya Analytics™ as it provides the reporting platform for real time and historical data.

You can secure communications and data transfer for the core applications using:

- Secure Communications with https and wss (web socket secure)
- Token Based Authorization
- TLS 1.2
- FQDNs
- A root CA certificate in conjunction with Identity Certificates to deliver a Server Authentication Model

Avaya Oceana® core applications are primarily Avaya Breeze® platform-based software applications called snap-ins or services. The software applications take the configuration data from configurable parameters called Attributes.

The following are examples of snap-in attributes related to security, which can be set on the Oceana Configuration Service, and automatically applied to all other Avaya Oceana® services:

- Secure Connections to Database - Default Value = True
- Toggle Secure Mode - Default Value = False (https on by default)
- Enable Tokenless Access - Default Value= False (Token required by default). All REST requests for these interfaces must contain a valid token within the request header or they are rejected.
- TLS version - Default Value = 1.2
- Enable Secure Communications - Default Value = True
- Authorization Required to Contact Service - Default Value = True
- Authorization Required for Service - Default Value = True

For all these attributes except the **Enable Tokenless Access** attribute, a value of `True` specifies that the web communications into these snap-ins are secure and also use token-based authorization. However, for enhanced security, Avaya recommends that all customers use the combination of Fully Qualified Domain Name (FQDN) and Domain Name Server (DNS) in conjunction with security certificates for all interfaces accessible in the solution. Avaya Oceana® Breeze Clusters must use an FQDN. After you configure all applications in the solution for security, all clients and applications can securely communicate with Avaya Oceana® and Avaya Analytics™.

Third-party certificates

There are three areas in the Avaya Analytics™ solution where third-party certificates can replace the default certificates:

- Avaya Oceana® connection through Reliable Eventing Framework (REF). See Creating certificates for connecting to Avaya Breeze Reliable Eventing Framework on page 176.
- Avaya Avaya Breeze® certificates for token validation. See Certificate authentication and token validation checklist on page 167.
- Certificates for externally facing interfaces. See Simplified process checklist: Using third-party identity certificates for external connections on page 193.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted entity that issues digital certificates and public-private key pairs. A CA verifies the identity of an individual or organization before issuing a digital certificate. A CA can be an external (public) or internal (private) entity configured inside an enterprise network. A Certificate Authority is a critical security service in a network.

Every Avaya Oceana® deployment has an Avaya Aura® System Manager deployed, and one of its functions is that of a CA. You can use System Manager's CA to secure the communications between the Avaya Aura® components, Avaya Oceana®, Avaya Breeze® platform, Avaya Analytics™ components, and all the other surrounding components in the solution.

Customers can implement a solution with their own Enterprise CA, either replacing System Manager as the CA or using it as a sub CA. Before attempting to make certificate changes in the deployed solution, you must have a solution level view to understand which network elements are affected. This requires planning and network audits before deploying new certificates.

A certificate change goes through the following four stages:

- Assessment: Identify and scope the migration work for your network.
- Planning: Plan and schedule the migration tasks.
- Migration: The actual migration which includes software upgrades, Trust Certificates deployment, and Identity Certificate deployment.
- Post-migration: Ongoing audits to avoid certificate expiration.

For public or private CA, the procedures for enabling security and applying the required certificates are almost identical. If you are using a third-party public CA, a third-party vendor certificates require time to be made available and the customer to work with the third-party to obtain the certificates after the correct information about their system is provided. When using third-party CA, configure client authentication and server authentication on the CA for Avaya Analytics™ configuration to work.

Using System Manager as a Root CA means the end customer can perform the certificate creation process themselves. For more details on System Manager as a CA, see the Avaya Aura® System Manager documentation suite.

Operating Systems

The solution comprises different Operating Systems (OS), such as Linux, Windows, and Windows server hosting the EDM Context Store database. There are different procedures for each OS type.

Omnichannel Database Server is one of the Windows-based OS applications in the core suite of products. This server runs the Omnichannel Database software, including the database that contains the digital channel media history information with the configuration items for digital channels.

For security, Avaya provides the following guidance and configuration instructions for this server:

- Secure Remote Access
- Antivirus Software Scanning Guidelines
- Firewall Guidelines

The other Windows-based server in the core solution is Avaya Control Manager. For more information about security guidelines and recommended security practices, see the respective product documentation. Communications from the Avaya Control Manager Server to the Avaya Oceana® component, Unified Contact Center Administration (UCA), are fully secured using https and token-based authorization.

Avaya Analytics™ is a core application suite on the core solution, running Linux-based OS application servers in a Kubernetes environment hosted on VMware.

Surround Applications and Client Security

Apart from the core applications, many optional surround applications communicate with the Avaya Oceana® and Avaya Analytics™ components. Different clients must interact and share information with the core components. Communications and information transport from these applications and clients must also be secured. Communications and data traffic from surrounding applications such as the IVR platform, the Avaya Experience Platform™ (Public Cloud Workforce Engagement) platform, and other value-added applications can all be secured using https, token-based authorization, and secure certificates. Avaya Oceana® and Avaya Analytics™ users use active directory/LDAP authentication with authorization tokens to secure sessions from the clients to the core applications.

Avaya Oceana® and Avaya Analytics™ users access their functionality through supported browsers. With a secure deployment, all communications from these clients are over https and trusted browser sessions.

These communications are within the contact center enterprise boundaries protected by the IT security infrastructure, such as firewalls. However, all contact centers must open their infrastructure to the outside Internet world securely if they are to provide contact center services to their end customers, which is the final layer of the solution.

EASG-based authentication of Web Administrative Interfaces for Avaya Analytics™

EASG overview

Enhanced Access Security Gateway (EASG) is a challenge-response authentication and authorization solution that service engineers can use to access Web-based applications of Avaya Analytics™. Avaya service engineers can access these applications without redirection to Avaya Breeze® Authorization Service or System Manager (SMGR). Using EASG-based authentication, service engineers can impersonate Avaya Analytics™ Historical Reporting customer accounts.

EASG configuration

EASG is already configured with SMGR and SSH-Login. You need to install Avaya Breeze platform with EASG enabled option.

EASG supports the following login IDs: `craft`, `init`, `inads`, and `sroot`.

Prerequisites for EASG authentication

- You should be able to log in to Avaya Analytics™ Historical Reporting.
- Authentication implementation must be compatible with Avaya SAL Policy Manager, which is based on point-to-point access to the end systems.

Using EASG to access Avaya Analytics Historical Reports

1. Open the SSH command .
2. Log in as `craft` to Cluster Control Manager over SSH.
3. Copy the **Product ID** and **Challenge** from the SSH terminal window to the corresponding fields on the EASG Web Mobile Response page. Use `craft` as **Login Name**.
4. Click **Query** to generate the Response token.
5. Click **Copy Response to Clipboard** and copy the response into the SSH terminal window to connect to CCM over SSH.
6. Run the **remoteDesktopSession** command to initiate a remote desktop connection, which provides a GUI to CCM.
7. Copy the URL and paste it in a web browser.
8. On the web browser, click **Firefox** to open a default webpage.
9. Click the **Historical Reporting** link to open the webpage that displays an Authorization token.
10. Copy the token, click the **modHeader** icon on the top right menu bar of the browser, and then click **Configure**.
11. Set the following parameters on the Simple Modify Headers page:
    - Enter a URL pattern in the **Url Patterns** field. For example:
      ```
      https://*/*
      ```
    - Create a new field named **EASG** and paste the token in it, including the string.
    - Create a new field named **EASG_USER_MAPPING** to set the name of the Avaya Analytics™ Historical Reporting user.
12. Click **Save** and then click the **Start** icon.
13. Navigate back to the **Cluster Control Manager** tab and click the **Click Here to Launch Historical Reporting page** link.

    If the EASG Authorization token is valid, you can access Avaya Analytics™ Historical Reporting.

Limitations

- You should have access to EASG Web Mobile.

- You must know the full URL path of the EASG login page.

Beyond the Enterprise Applications Security

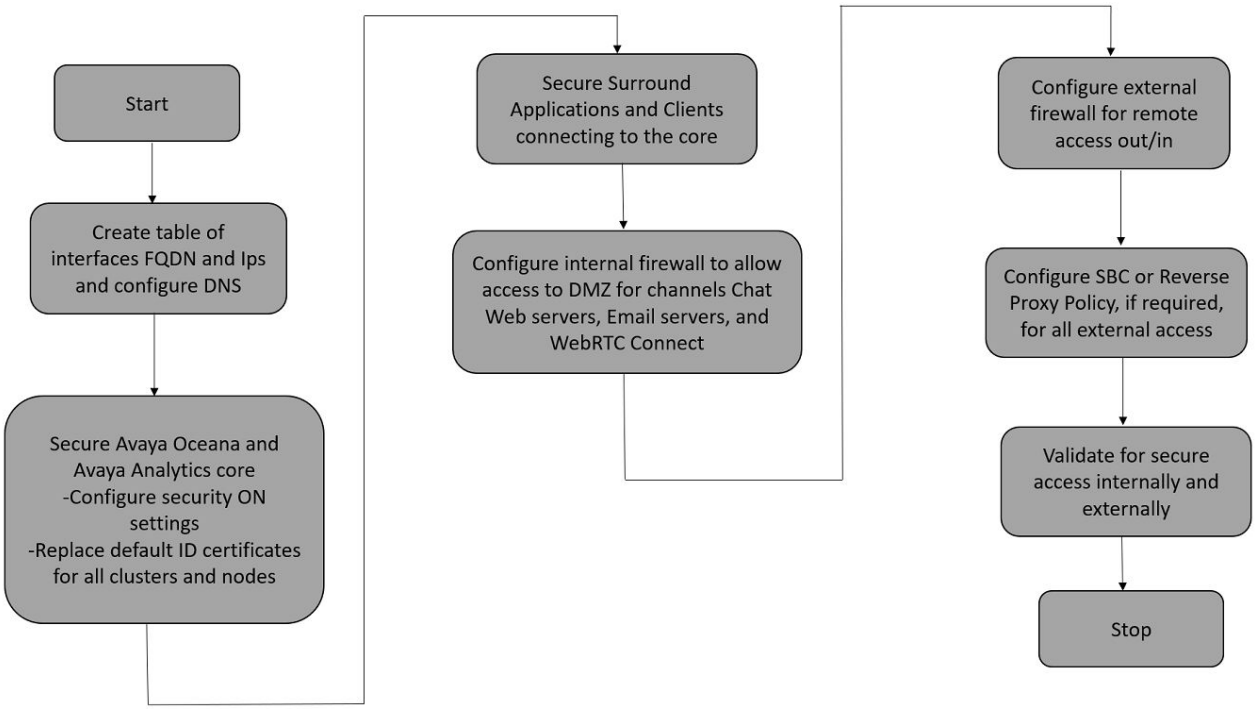
All Avaya Oceana® and Avaya Analytics™ deployments must be accessible to the Internet world. This access cannot be direct, but is allowed and made available in a secure manner through various security specific applications.

The following are examples of external access that are required for Avaya Oceana® and Avaya Analytics™ deployments:

- Avaya Oceana® Chat and Messaging customers require their communications to be securely routed in and out of the Avaya Oceana® core and surround applications including users' desktops and browser. Avaya Workspaces users require Internet access for messaging.
- Avaya Oceana® Email contacts require routing in and out of the Avaya Oceana® Email processing engine and its agent desktop client.
- Avaya WebRTC Connect customers using either voice and/or Video require their communications to be securely routed in and out of the Avaya Oceana® core and surround applications including users' desktop and browser.
- Other supported channels like SMS, Social and Generic, all require access from the Internet world in and out of the enterprise deployment.
- Remote users require secure access to all the functionality available inside the enterprise when they are working remotely.

Secure Solution Deployment

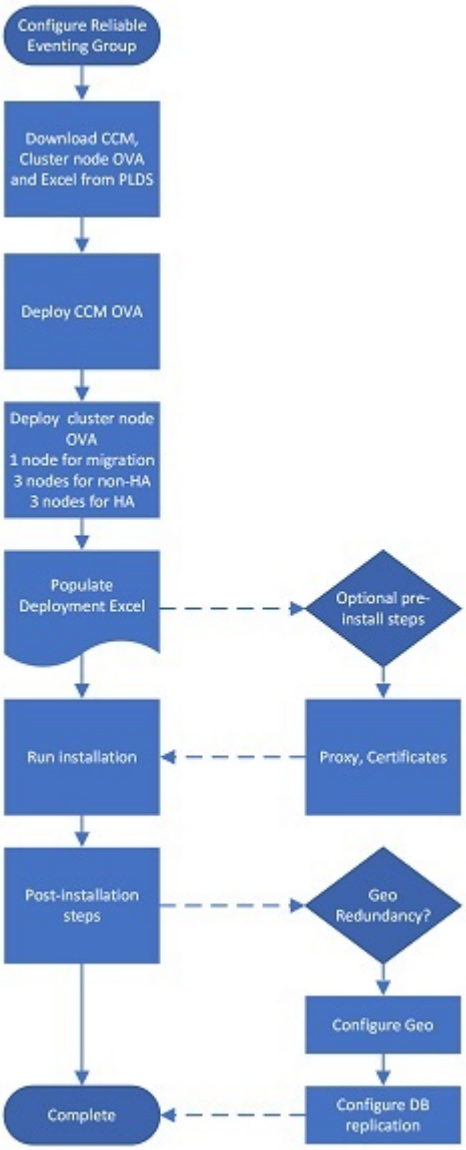
The flow chart displays the order in which Avaya Oceana® and the Avaya Analytics™ solution must be rolled out in a secure manner.


Start
Create table of interfaces FQDN and Ips and configure DNS
Secure Avaya Oceana and Avaya Analytics core
-Configure security ON settings
-Replace default ID certificates for all clusters and nodes
Secure Surround Applications and Clients connecting to the core
Configure internal firewall to allow access to DMZ for channels Chat Web servers, Email servers, and WebRTC Connect
Configure external firewall for remote access out/in
Configure SBC or Reverse Proxy Policy, if required, for all external access
Validate for secure access internally and externally
Stop

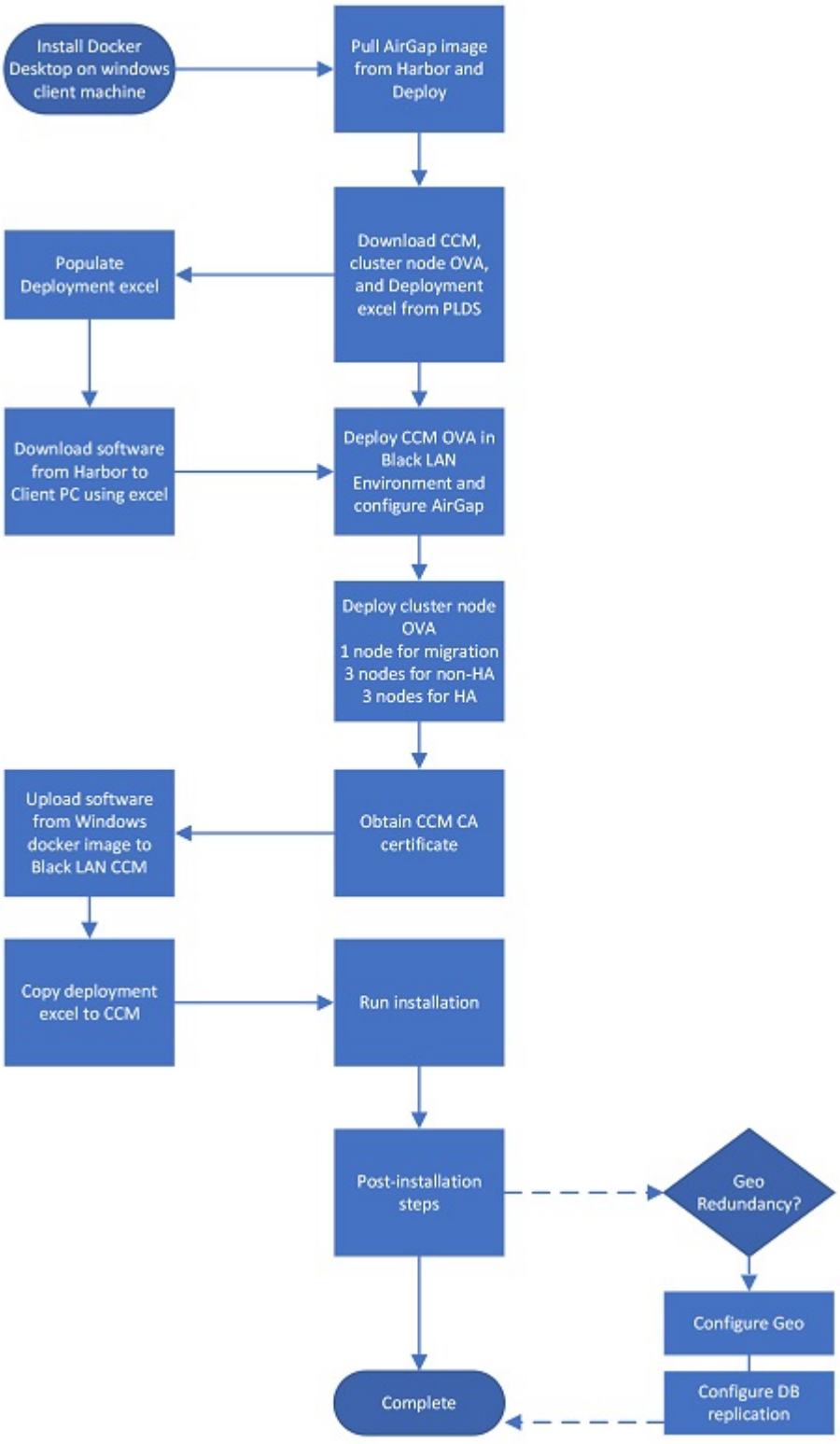
Chapter 4: Deployment process

Deployment process flow

The following task flow displays the sequence of procedures you must perform to deploy the Avaya Analytics™ solution in online mode:



The following task flow displays the sequence of procedures you must perform to deploy the Avaya Analytics™ solution in offline mode:


Install Docker Desktop on windows client machine
Pull AirGap image from Harbor and Deploy
Download CCM, cluster node OVA, and Deployment excel from PLDS
Populate Deployment excel
Download software from Harbor to Client PC using excel
Deploy CCM OVA in Black LAN Environment and configure AirGap
Deploy cluster node OVA
1 node for migration
3 nodes for non-HA
3 nodes for HA
Upload software from Windows docker image to Black LAN CCM
Obtain CCM CA certificate
Copy deployment excel to CCM
Run installation
Post-installation steps
Geo Redundancy?
Configure Geo
Configure DB replication
Complete

Deployment considerations and warnings

Consider the following when deploying the solution and after the deployment is complete.

vCenter restrictions after deployment

After cluster deployment, observe the following restrictions for any Common Services resources:

- Do not delete virtual machines in vCenter unless instructed to do so by a solution maintenance procedure.
- Do not rename the vCenter cluster object.
- VMware VM snapshots are supported for cluster nodes only when the nodes are powered off. Keep snapshots for a maximum of 72 hours. Over longer periods, snapshot files increase in size and can degrade performance of the virtual machine and the ESXi host.

Other solution considerations

- Reference the solution configuration spreadsheet for the proper resource allocations per cluster node. Modify the VM resources to match what is defined in the solution spreadsheet. These resources do not have to be applied with reservations. For more information, see the solution documentation.
- Do not delete a service unless instructed to do so by a troubleshooting or maintenance procedure. When a service fails, you must delete and reinstall the service before you can deploy another service.

Chapter 5: Planning and preconfiguration

Use the information in this chapter to plan the Avaya Analytics™ deployment with High Availability (HA). For detailed information on Avaya Analytics™ deployment with non-High Availability (HA), see the relevant chapter in this document.

Avaya Analytics™ hardware requirements for High Availability deployment

High Availability (HA) deployment

The following table provides information about the memory, storage, and vCPU requirements for each component of Avaya Analytics™ HA deployment without messaging:

You must install Avaya Analytics™ software on each master node. You must deploy each master node on separate physical servers. Cluster Control Manager (CCM) can reside on any physical server instance. You require a total of four virtual machines for an Avaya Analytics™ solution deployment, which includes HA.

The following table shows the default footprint sizes. Adding more feature capabilities, such as Routing Service by Group reporting, Async, or Agent Trace, increases these default footprint configurations.

Warning:

Do not delete nodes or VMs from your VMware.

Deployment size	Component	Number of physical servers	VMs	vCPU	RAM (GB)	IOPS	vCenter data store storage (GB)
100 agent	Totals	3	4	55	166.5	5000	3408
	CCM - server 1, 2, or 3		1	1	1.5	-	240
	Master node 1 - server 1		1	18	55	-	1584
	Master node 2 - server 2		1	18	55	-	1584
	Master node 3 - server 3		1	18	55	-	0
500 agent	Totals	3	4	61	187.5	5000	5746
	CCM - server 1, 2, or 3		1	1	1.5	-	240

Table continues…

Deployment size	Component	Number of physical servers	VMs	vCPU	RAM (GB)	IOPS	vCenter data store storage (GB)
	Master node 1 - server 1		1	20	62	-	2753
	Master node 2 - server 2		1	20	62	-	2753
	Master node 3 - server 3		1	20	62	-	0
1000 agent	Totals	3	4	73	226.5	5000	8064
	CCM - server 1, 2, or 3		1	1	1.5	-	240
	Master node 1 - server 1		1	24	75	-	3912
	Master node 2 - server 2		1	24	75	-	3912
	Master node 3 - server 3		1	24	75	-	0
2000 agent	Totals	3	4	85	274.5	10000	8424
	CCM - server 1, 2, or 3		1	1	1.5	-	240
	Master node 1 - server 1		1	28	91	-	4092
	Master node 2 - server 2		1	28	91	-	4092
	Master node 3 - server 3		1	28	91	-	0
4500 agent	Totals	3	4	97	382.5	10000	11,422
	CCM - server 1, 2, or 3		1	1	1.5	-	240
	Master node 1 - server 1		1	32	127	-	5591
	Master node 2 - server 2		1	32	127	-	5591
	Master node 3 - server 3		1	32	127	-	0

Important:

- You must create a data store specifically for Avaya Analytics™ usage. You can create additional data stores in vCenter for use by third-party applications. However you must ensure that the IOPS for the Avaya Analytics™ components are not affected.
- You can deploy your Avaya Analytics™ on the same VMware cluster as Avaya Oceana®. See VMware supported features as mentioned in this document.
- You can install a single Avaya Analytics™ deployment on a VMware cluster.
- VMware ESXi 8.0 is supported.
- You must enable VMware High Availability at the VMware cluster level.
- You must enable VMware DRS to ensure that the virtual machines are deployed on different physical hosts.

Note:

Disabling VMware DRS at the cluster level removes all the existing resource pools. Then these resource pools need to be manually added into the system again. VMware displays a warning to the administrator about the impacts of turning off DRS and resource pools with the option to save a *snapshot* if required.

- Avaya Analytics™ can be deployed using thin provisioning of the disk space. For the Avaya Analytics™ application, thin provisioning of the disk storage within VMware is supported for all agent configurations. For more information on specifics of thin provisioning, see Thin provisioning of disk storage in VMware on page 38.
- Avaya Analytics™ supports LDAP version 3.
- Solid State Drives (SSD) are supported in addition to SATA, 15000 RPM.
- Only external storage is supported for HA configurations.

  The external shared storage is a datastore that must be available for use during the installation of Avaya Analytics™. The automated deployment of Avaya Analytics™ for setting up volumes for the database uses external storage. The external storage is required to persist the historical data, logging, and kafka storage, located in the vCenter datastore. The external storage configured must be separate to the CCM and Kubernetes VM's disks.

Analytics and Messaging deployment

The following table provides information about the memory, storage, and vCPU requirements for each component of Avaya Analytics™ and Messaging deployment:

Deployment size	Component	VMs	vCPU	RAM (GB)	IOPS	vCenter data store storage (GB)
100 agent	Totals	4	61	175.5	5000	3440
	CCM - server 1, 2, or 3	1	1	1.5	-	240
	Master node 1 - server 1	1	20	58	-	1600
	Master node 2 - server 2	1	20	58	-	1600
	Master node 3 - server 3	1	20	58	-	0
500 agent	Totals	4	67	196.5	5000	5906
	CCM - server 1, 2, or 3	1	1	1.5	-	240
	Master node 1 - server 1	1	22	65	-	2833
	Master node 2 - server 2	1	22	65	-	2833
	Master node 3 - server 3	1	22	65	-	0
1000 agent	Totals	4	73	238.5	5000	8384
	CCM - server 1, 2, or 3	1	1	1.5	-	240
	Master node 1 - server 1	1	24	79	-	4072
	Master node 2 - server 2	1	24	79	-	4072
	Master node 3 - server 3	1	24	79	-	0
2000 agent	Totals	4	91	286.5	10000	9064
	CCM - server 1, 2, or 3	1	1	1.5	-	240
	Master node 1 - server 1	1	30	95	-	4412
	Master node 2 - server 2	1	30	95	-	4412

Table continues…

Deployment size	Component	VMs	vCPU	RAM (GB)	IOPS	vCenter data store storage (GB)
	Master node 3 - server 3	1	30	95	-	0
4500 agent	Totals	4	103	391.5	10000	12,862
	CCM - server 1, 2, or 3	1	1	1.5	-	240
	Master node 1 - server 1	1	34	130	-	6311
	Master node 2 - server 2	1	34	130	-	6311
	Master node 3 - server 3	1	34	130	-	0

Note:

The Messaging deployment is applicable for customers who deploy Avaya Analytics™ and Messaging on the same platform. It does not apply to the non-HA/Lab deployment of Avaya Analytics™.

For hardware requirement details of Avaya Analytics™ on non-High Availability (HA), see the relevant section in this document.

Supported browsers

Component	Microsoft Edge Chromium	Google Chrome (Windows and Apple MAC)	Mozilla	
			Firefox Standard	Firefox Enterprise
Avaya Workspaces for Avaya Oceana® • Supervisor and agent role Avaya Workspaces admin role • Customer Journey • Co-Browsing Snap-in agent role	144, 145	144, 145, 146	147, 148	140.8
Co-Browsing Snap-in customer	145	145, 146	148	140.8
Avaya Control Manager	145	145, 146	148	Not supported
Avaya Workspaces for Avaya Oceana® — Avaya WebRTC Connect Voice and Video agent	145 Video: Not supported Voice: supported	146	148	Not supported

Table continues…

Component	Microsoft Edge Chromium	Google Chrome (Windows and Apple MAC)	Mozilla	
			Firefox Standard	Firefox Enterprise
Customer Avaya WebRTC Connect application	145 Video: Not supported Voice: supported	146	148	Not supported
Avaya Analytics™ Release 4.x Real Time Reporting (using supervisor Avaya Workspaces for Avaya Oceana®)	144, 145	145, 146	147, 148	140.8
Avaya Analytics™ Release 4.x Historical Reporting	144, 145	145, 146	147, 148	140.8
Avaya Oceana® Multimedia Data Viewer & Avaya Oceana® Dashboard & Monitor	144, 145	145, 146	148	Not supported
Avaya Oceana® Administration Tool and OCMT	144, 145	145, 146 with Click Once Extension	148 with Click Once Extension	Not supported

Avaya Analytics™ virtual machine CPU requirements

In an Avaya Analytics™ solution, vCPU reservations are not required if the resources on the VMware host server are not overcommitted, and there is no contention for CPU resources.

- For processor selection purposes, the reference CPU is the Dual (2 Socket) E5-2697 V3 @ 2.6GHz processor. This is a 2 CPU socket configuration. Refer to this reference dual processor benchmark score available at https://www.cpubenchmark.net.
- Avaya Oceana® and Avaya Analytics™ VMware profiling uses a Dual 14-core Intel Xeon E5-2697 V3 2.60 GHz CPU as a reference CPU. This reference processor has 28 physical CPU cores. Each of the cores has an individual benchmark value that is one twenty-eighth of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select suitable VMware host hardware for Avaya Oceana® and Avaya Analytics™.
- The VMware CPU benchmark for the VMware physical host, which runs Avaya Oceana® and Avaya Analytics™, must be equal to or greater than 90% of the individual core benchmark and the reference dual processor.
- When selecting the distribution of cores per socket for the CCM virtual machine, use the VMware-provided defaults. For example, for 8 vCPUs, VMware sets a default selection of 1 core per socket across 8 sockets.

Do the following to ensure that your proposed VMware host CPUs meet the Avaya Analytics™ minimum requirements:

- Determine the individual core benchmark value for the reference CPU, Dual 14-core Intel Xeon E5-2697 V3 2.60GHz, by referring to the reference dual processor benchmark score available at https://www.cpubenchmark.net.
- Reference individual core benchmark value = Reference CPU benchmark from the website / Number of cores in the reference CPU. This processor has a minimum thread score of 1997 approximately. This is the minimum thread score that all CPU's used as hosts in an Avaya Oceana® and Avaya Analytics™ solution must be within 90%.
- Determine the individual core benchmark value for your chosen VMware physical host server CPU. Individual core benchmark value = Your chosen physical host server CPU benchmark from the website / Number of cores in the host server CPU.

Working example - CPU Model [Dual CPU] Intel Xeon Gold 6240R @ 2.40GHz 24 Core Processor for Avaya Oceana Breeze Virtual Machines

Procedure

1. To view the CPU Benchmark score for this processor, click https://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+Gold+6240R+%40+2.40GHz&id=3739&cpuCount=2

   Benchmark score = 54024

   Note:

   The benchmark scores change as they are updated regularly.

2. For this 24 Core Processor, divide the benchmark score 54024 by the total number of cores 48.

   Individual core rating = 1125.50 approximately.

3. To view the CPU Benchmark score for the Avaya reference processor, click https://www.cpubenchmark.net/cpu.php?cpu=Intel+Xeon+E5-2697+v3+%40+2.60GHz&id=2333&cpuCount=2

   Benchmark score = 30323

   Note:

   The benchmark scores change as they are updated regularly.

4. For a 14 Core Avaya reference processor, divide the benchmark score 30323 by the total number of cores 28.

   Individual core rating = 1082.96 approximately.

5. Compare the two values 1125.50 and 1082.92.

   The individual score for the 6240R processor is greater than the individual score for the 2697 processor, and therefore, is appropriate for use in an Avaya Oceana Breeze deployment.

   Important:

   - A processor that meets 90% of the Avaya reference processor is suitable for deployment. It does not have to be equal or greater than the individual core score for the Avaya reference processor.

     The following is a short list of suitable CPU types for physical hosts running the Avaya Oceana Breeze and Avaya Analytics CSP based virtual machines, currently in use by existing Avaya Oceana customers:

     - 14 core [Dual CPU] Intel® Xeon® Gold 6132 @ 2.60GHz
     - 16 core [Dual CPU] Intel® Xeon® Gold 5218 @ 2.30GHz
     - 24 core [Dual CPU] Intel® Xeon® Platinum 8280 @ 2.70GHz
     - 14 core [Dual CPU] Intel® Xeon® Gold 6132 @ 2.60GHz
     - 16 core [Dual CPU] Intel® Xeon® Gold 6226R 2.9GHz
     - 24 core [Dual CPU] Intel® Xeon® Gold 6240R @ 2.40GHz

   - Newer processors may not have a benchmark score rating and are not recommended for use in an Avaya Oceana and Analytics deployment.
   - High-specification processors with 32 or 48 cores or higher, and lower clock speeds (< 2.3 GHz), may not meet the specification required for Avaya Oceana and Analytics deployments.

VMware configuration

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
A single VMware cluster can be shared between Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. • The cluster contains virtual machines for both Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. • The cluster can also contain virtual machines of other applications without contention. **Note:** Avaya Oceana® 3.10.x and Avaya Analytics™ 4.2.x/4.3.x. can also be supported in separate clusters.	Yes For instructions on enabling affinity rules in a DRS-enabled VMware cluster, see PSN005416u located at https://downloads.avaya.com/css/P8/documents/101057845.	Yes For more information, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Cloning	No	No Avaya Analytics™ supports cloning cluster node VMs during the initial OVA deployment before they are powered up.
Distributed Resource Scheduler (DRS)	Yes For the documented guidelines in conjunction with affinity rules, see PSN005416u located at https://downloads.avaya.com/css/P8/documents/101057845.	Yes For the documented guidelines on HA and DRS rules for Avaya Analytics™ 4.x, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Storage DRS	No Avaya Oceana® does not support this feature. There are impacts to the datastores. The input or output load balancing occurring in production can cause outages.	No **Note:** Avaya Analytics™ 4.x does not support Storage DRS nor datastore clusters.
Distributed Power Management (DPM)	No	No

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
Distributed Switch (Network)	Yes • Requires VMware Enterprise Plus license. **Note:** Loss of vCenter indicates that you cannot manage data networks on the hosts. • If you use standard vSwitch, you can do the management from each host.	Yes • Requires VMware Enterprise Plus license. **Note:** Loss of vCenter indicates that you cannot manage the data networks on the hosts. • If you use standard vSwitch, you can do the management from each host.
Fault Tolerance	No	No
High Availability (HA)*	No • Avaya Oceana® does not support impacts to the virtual machines occurring in production. • For more information on configuring VMware HA in an Avaya Oceana® and Avaya Analytics™ single cluster deployment, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.	Yes • Mandatory for Avaya Analytics™ 4.x High Availability feature. • For the documented guidelines on HA and DRS rules for Avaya Analytics™ 4.x, see PSN005633u located at https://downloads.avaya.com/css/P8/documents/101067348.
Snapshots***	Partial • Yes, as part of maintenance window** procedures only for upgrades or patching. • You must remove all snapshots before putting the contact center back into production.	Partial • Yes, as part of maintenance window** procedures for upgrades or patching only for the following Avaya Analytics™ application: • Cluster Control Manager (CCM) - You must remove all snapshots before putting the contact center back into production. • Snapshots are supported for all the VMs in the cluster.

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ **Warning:** **Do not delete nodes or VMs from your VMware.**
Storage Thin Provisioning	Partial • Yes, for SAN storage. • No, for local hard disk storage.	Yes • Yes, for SAN storage. • No local storage supported. **Note:** Applicable only to Avaya Analytics™ on HA. • For more information on specifics of thin provisioning, see Thin provisioning of disk storage in VMware on page 38.
Suspend and Resume	No	No
Cold Migration	Yes • You can do a cold migration only on a virtual machine in a powered-off state. • Avaya Oceana® uses static IPs. Therefore, the new ESXI host(s) must have access to the original data network and datastore for the migrated virtual machines.	Yes • You can do cold migration only on a virtual machine in a powered-off state. • Avaya Analytics™ uses static IPs. Therefore Avaya Analytics™ virtual machines can only be migrated to hosts in the same VMware that has the same access to all elements in the cluster as existing hosts. When performing any cold migrations of Avaya Analytics™ virtual machines from host to host, see the *Considerations for upgrading Physical Hosts running Avaya Analytics™ virtual Machine* section in *Deploying Avaya Analytics™*.

Table continues…

VMware Feature	Avaya Oceana®	Avaya Analytics™ ⚠ **Warning:** **Do not delete nodes or VMs from your VMware.**
Reservations on vCPU and memory required to be enabled	Yes • Set to `Yes`. For production environments, Avaya Oceana® customers provide the VMware deployments wherever there is contention for resources. • Physical hosts running Avaya Oceana® virtual machines can have other virtual machines running and co-residing with the Avaya Oceana® virtual machines. • On Avaya Pod Fx systems, reservations are not required, because the Avaya supplied hardware is engineered not to be over provisioned.	No Avaya Analytics™ 4.x reservations on vCPU and memory are not mandatory, as long as the environment is not over provisioned and there is no contention for resources with other virtual machines.
Hyperthreading	No • Avaya Oceana® requires reservations. Therefore, Hyperthreading does not add any additional value. • You can enable on the VMware infrastructure for the other applications.	Yes

- * Avaya Oceana® provides its own HA mechanism.
- ** A maintenance window specifies a scheduled out-of-production window where the system does not process contacts, agents are all logged out, and queues are empty. This timeframe is dedicated to tasks such as patching, upgrades, and configuration.
  - During this timeframe, Avaya Oceana® and the applications such as Avaya Breeze® platform nodes, System Manager, Avaya Control Manager, and Omnichannel Database remain powered on and accessible on the customer network but do not process any contacts or operations.
  - During the creation of snapshots, you must power down Avaya Oceana® and the applications such as Avaya Breeze® platform nodes, Avaya Control Manager, and Omnichannel Database.
- *** You must delete snapshots from Avaya Oceana® virtual machines before placing Avaya Oceana® back into production. Snapshots must only be taken or deleted when the virtual machine is powered down.

Upgrading ESXi hosts running Avaya Oceana® or Avaya Analytics™ virtual machines

Hosts running virtual machines that are part of Avaya Oceana®, Avaya Analytics™ and/or Avaya Breeze® platform, must be kept up-to-date, including VMware ESXi.

Host software maintenance and updates must be planned into a maintenance windows where the contact center is not in service. In these maintenance windows, one or more physical hosts may be out of service, including all the virtual machines running on these hosts.

Important:

- Host maintenance must include consideration of all components of the customer solution. For example Avaya Analytics™, Avaya Breeze® platform and Avaya Oceana®. Refer to the relevant maintenance documents for each solution component:
- - The *VMware host maintenance* section in the *Maintaining and Troubleshooting Avaya Oceana®* manual.
  - The *Upgrading Avaya Analytics™ ESXI hosts* section in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* manual.
  - The *Maintaining and upgrading ESXi host software* section in the *Maintaining and Troubleshooting Avaya Breeze® platform* manual.

The following are important considerations when removing or adding physical hosts to the deployment:

- Do not remove or replace the physical VMware ESXi hosts running Avaya Analytics™ virtual machines from the VMware cluster during maintenance windows.
- You can add one or more physical hosts to the VMware cluster to facilitate host maintenance. Adding physical hosts enables migrating host virtual machines to a new host while the existing host is updated.
- You must propagate all the VMware permissions for the same user account used to deploy the Avaya Analytics™ cluster to the new host. You must perform this before removing the new host from maintenance mode and putting it into production. Avaya Analytics™ virtual machines cannot access resources on the new host if you fail to propagate VMware permissions.

Thin provisioning of disk storage in VMware

Avaya Analytics™ supports thin provisioning of disk storage in VMware for all agent configurations. Though this document specifies the required disk storage space for each agent configuration, you do not have to provision the entire disk space on day 1. You can add space as and when needed. No maintenance window is required.

Warning:

You must actively manage your VMware disk space and add more space before the application runs out of space.

Insufficient disk space provided to the system when operating with thin provisioning can result in disk write errors in the logs and data loss. Avaya bears no responsibility for errors and data loss.

To ensure efficient thin provisioning, do the following:

- Provision additional disk space whenever the remaining disk space is less than 0.25 TB, assuming that you can provision additional storage within an hour or less. You are accountable for the time required to provision additional disk storage before the system reaches its current limit.
- When the datastore capacity does not initially meet the requisite footprint, the minimum storage requirement for a deployment requires the datastore to be at least the size of disk 2 on cluster node 1 or 2.

  You can find this storage size in the spreadsheet on the Deployment Properties tab in the Footprint Summary table under Disk Storage Requirements for Cluster Node 1 or 2.

Adding additional disk space is a standard VMware operation.

Avaya Analytics™ deployment spreadsheet overview

During the install, you must configure Avaya Analytics™ and Common Services using a pre-populated Microsoft Excel spreadsheet. This spreadsheet uses macros, which you must enable before you start editing the worksheets. The minimum supported version of MS Excel is 2016.

Important:

Delete the spreadsheet from the Cluster Control Manager (CCM) after the deployment is complete. You must copy this spreadsheet and store it in a secure location, because the spreadsheet contains passwords and other configuration details that you entered in plain text.

This document includes configuration information for cluster deployment and Avaya Analytics™ software. The spreadsheet includes the following worksheets:

- **Instructions**: This worksheet provides you information on how to complete the deployment spreadsheet. This worksheet also displays the status of macros as `enabled` or `disabled`.

  Note:

  If the macros are disabled, then other worksheets are not visible. Therefore, you must enable the macros and restart the spreadsheet. To know how to enable macros in a spreadsheet, see the Microsoft help manual.

- **Password Policy**: This worksheet lists the password rules that you must follow when you create or change passwords for user logins. Ensure that the **Enforce Password policies** field is set to **TRUE**. This also ensures that users do not enter their login names as part of their passwords.
- **Deployment Properties**: Use this worksheet to configure vCenter FQDNs or IP addresses for use during virtual machine deployment.

Note:

Select the timezone in which your contact center is being deployed. Please ensure the timezone selected here matches the timezone of Oceana.

- **orca**: Use this worksheet to set the agent count and to configure Avaya Analytics™ solution data, such as Avaya Oceana® connection information.

  Important:

  DO NOT delete the product ORCA without consulting Avaya Support as you may lose your data and it may not be recoverable.

- **mstr**: Use this worksheet to configure Avaya Analytics™ Historical Reporting.

  Note:

  - Historical reporting will be configured with standard authentication on first install.
  - LDAP or SAML is configured as a post-install operation.
  - The standard and LDAP radio buttons will be available after LDAP is configured post-install.
  - The connection to the LDAP server must be secure.

You must edit the deployment spreadsheet using a Windows 10 client.

Important:

- See the guidance in the spreadsheet to update the required values. You must configure all of the values that are in an orange cell. Values in green cells are optional, and you can change these values if required. Do not modify any other values in the spreadsheet.
- You must set the solution agent count on the **orca** worksheet. Avaya Analytics™ hardware requirements vary depending on the selected agent count.
- Download the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file from PLDS. Use the Microsoft Edge browser to download the deployment spreadsheet. If you download the file using Chrome, the file name extension can change from `.xlsm` to `.zip`.

Avaya Analytics™ adopts latest Microstrategy

Avaya Analytics™ adopts the latest MicroStrategy 2025, platform updates and enhancement.

The existing Analytics 4.x customer will be able to upgrade from MSTR 2021 to current MSTR 2025 updates. Also, the customer will have the ability to preserve any custom reports built on MSTR 2021 during adoption of current MSTR 2025.

Avaya Analytics™ network requirements

When using the deployment spreadsheet to configure Avaya Analytics™, you must ensure that you adhere to the following networking requirements:

- All Avaya Analytics™ IP addresses must be on the same subnet.

- All DNS entries must use the same case.
- The returned DNS record is case-sensitive. Therefore, you must ensure the DNS entries exactly match each Avaya Analytics™ node.
- Avaya Analytics™ and Avaya Oceana® must use the same NTP server.

Note:

The following Avaya Analytics™ features are not supported when Avaya Breeze® platform nodes have `.local` domain name:

- Avaya Analytics™ kafka open interface is not supported. It affects WFO integration and custom applications.
- Avaya Analytics™ websocket open interface is not supported. It affects Agent Wallboard and other custom applications.
- GDPR feature is not supported.

Minimum VMware setup requirements

- VMware vCenter 8.0.
- VMware ESXi 8.0 with VMware vSphere Enterprise Plus license.
- VMware user permissions.

Create the following constructs in vCenter if they do not already exist:

- Data center.
- Cluster within the created data center with ESXi hosts added. CSP High Availability (HA) is the default. HA requires a minimum of three ESXi hosts, and VMware HA must be enabled. Consult your solution documentation to determine if additional hosts are required.
- Cluster with at least one datastore added. The VMware cluster used for Common Services must have access to a datastore. All ESXi hosts within the VMware cluster as well as the Cluster Control Manager and Common Services cluster node virtual machines must have access to the datastore.

  Additionally, the datastore used for the Common Services cluster must have hosts that are associated only to the cluster where the product is being deployed. It must be accessible from the Cluster Control Manager and from the Common Services cluster nodes. If the datastore is made up of one or more host resources, these hosts must have access to the VMware cluster where Cluster Control Manager and Common Services cluster nodes are being deployed.
- You can install a single Avaya Analytics™ deployment on a VMware cluster.

Note the following:

- Local datastores and datastore clusters are not supported.

- Solution deployment in VMware vApp is not supported.
- Suspending and resuming a virtual machine in VMware is not supported.
- You must have a VMware network switch. You can use a vSphere standard or distributed switch.
  - If you are using a vSphere standard switch, each ESXi host within the cluster must use the same name for the standard switch.
  - If you are using a distributed switch, each ESXi host must have access to the distributed switch.
  - The network used for the deployment should be under the datacenter.
- Using VMware Distributed Resource Scheduler (DRS) is optional.

  For HA CSP deployments, Avaya recommends to enable VMware DRS at the cluster level and set it to fully automatic. Use a conservative migration threshold when DRS is set to partially automatic or fully automatic.

  If VMware DRS is not enabled, then the High Availability Audit feature must be disabled. When prompted to configure the HA audit during installation, decline the audit if DRS is disabled.

  For information about hot migration (vMotion) support, see your solution documentation.
- Enable the NTP service and synchronize the time on all ESXi hosts in vCenter with an external time source. Configure Cluster Control Manager and Common Services nodes with the same external time synchronization source.

  Tip:

  To find the time stratum, run `chronyd -q -t 1 "server <ServerIP> iburst maxsamples 1"`, where `<ServerIP>` is the IP address of your NTP server.

HA audit requirements

To use the optional HA audit feature, you must provide a VMware read-only user and enable VMware Distributed Resource Scheduler (DRS). There are no other requirements for access to the vCenter.

If you are deploying with high availability enabled, you must create an anti-affinity rule in vCenter for the cluster nodes.

vCenter read-only user for HA audit

The optional High Availability Audit feature requires a VMware read-only user account.

Before you deploy an HA solution Avaya recommends creating the read-only user in vCenter with access to:

- vCenter (`propagate to children=false`)
- Datacenter (`propagate to children=false`)
- Cluster (`propagate to children=true`)

During cluster installation, provide this read-only user when prompted to enable the HA audit feature.

HA recommendations for VMware DRS

Using VMware Distributed Resource Scheduler (DRS) is optional.

If VMware DRS is not enabled, then the High Availability Audit feature must be disabled. When prompted to configure the HA audit during installation, decline the audit if DRS is disabled.

For HA CSP deployments, Avaya recommends to enable VMware DRS at the cluster level and set it to fully automatic. Use a conservative migration threshold when DRS is set to partially automatic or fully automatic.

vCenter password restrictions

About this task

Before installing Avaya Analytics™ in HA deployment, you must update the vCenter user account password. The following list of special characters cannot be used in the vCenter user account password provided during ccm install or ccm upgrade spec --infra:

` $ ( ) \ | ; : ' " < >

An exception to the above restriction is using a single $ symbol at the end of a password is allowed.

Warning:

Avaya Analytics™ installation can fail if the vCenter user account password consists special characters listed above. The vCenter account are disabled/locked due to multiple failed log in attempts in Avaya Analytics™.

Procedure

1. Log in to vCenter using your existing credentials
2. Run the following command to update vCenter user account password:

   ```
   ccm infra update-vcentercreds
   ```

   See section *Prerequisites for vCenter login credentials* in this chapter.

Real-time SAML support

Avaya Workspaces login uses Security Assertion Markup Language (SAML), if configured in Avaya Breeze® platform Authorization Service.

The Avaya Breeze® platform Authorization Service is used by real-time reporting of stream. If SAML integration is configured in the Avaya Breeze® platform Authorization Service, then:

- SAML authorization feature is used without any configuration required on the Avaya Analytics™ real-time stream pods (orca-streams-rest, orca-streams-data-publisher) or Avaya Breeze® Authorization service pods (orca-breeze-authorization-service).
- When attempting to access the Avaya Workspaces URL, unauthorized users are redirected to the Avaya Breeze® platform Authorization Service, which further redirects users to your identity provider (IdP), and prompts the user for credentials.
- After successful authentication, the Avaya Breeze® platform grants users authorization using an authorization token. If users have the correct permissions set in Avaya Control Manager, they can access Avaya Workspaces.
- When the dashboard icon in Avaya Workspaces is selected, this authorization token is passed to the Avaya Analytics™ real-time stream pods, which use the verification features of the Avaya Breeze® platform Authorization Service through orca-breeze-authentication-service to confirm that the user has a supervisor role. The user can see reports using the supervisor role.

For more information about SAML support, see *Configuring SAML Authentication* section in *Administering Avaya Breeze® platform* guide and *Avaya Workspaces single sign-on* in *Deploying Avaya Oceana® Solution* guide.

Data volume planning

Data volumes must be planned and managed for historical reporting data and also to ensure an ongoing performance of the Avaya Analytics solution. The volumes of data stored and transmitted by Avaya Analytics can be very large based on the configuration. Agents matched up against a large number of routing services can cause large data volumes. Avaya Analytics provides parameters to control and manage these data volumes, and these parameters must be monitored and updated to ensure that they match the requirements.

The following are the parameters required for managing the data volumes:

- Data Retention Limits: The default value for this parameter is defined in the *Avaya Analytics Data Dictionary*.
- Zero/Empty Row Suppression: This parameter can be enabled or disabled using the analytics script during an installation or upgrade. For more information, see *Maintaining and Troubleshooting guide*.

- Routing Service Group filters: This parameter can reduce the amount of routing service related events sent to Avaya Workspaces. For more information, see *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®*.

Planning tasks

- See the *Avaya Oceana® Solution Description* document.
- Perform all of the tasks described in *Deploying Avaya Oceana®*.
- Contact Avaya to ensure your credentials allow you to deploy the software successfully.

Chapter 6: Configuring Reliable Eventing group

Reliable Eventing group configuration overview

Reliable Eventing Framework (REF) provides a mechanism for delivering messages. It adopts Apache ActiveMQ that provides a rich set of capabilities such as reliability, asynchronous events, inter-node, and inter-cluster.

Reliable Eventing Framework provides the following features:

- Delivery of events across servers and clusters.
- Guaranteed event delivery with event persistence, acknowledgment, and durable subscriptions.
- Master and slave high availability with replicated persistent messages.

You can configure Reliable Eventing groups by using System Manager.

Important:

To edit or delete a Reliable Eventing group configuration, you must set the Avaya Oceana® Cluster 1 status in Avaya Oceana® to `Denying`. For more information, see the *Deploying Avaya Oceana®* document.

Creating a Reliable Eventing group

About this task

Create a Reliable Eventing group on Avaya Breeze® platform for persistent messages across servers and clusters.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. On the Reliable Eventing Groups page, click **New**.

3. On the Reliable Eventing Group Editor page, enter the following details:
   - **Cluster**: Select Avaya Oceana® Cluster 1.
   - **Group Name**: Assign a name to the Reliable Eventing group.
   - **Description**: Enter a brief description.
   - **Type**: Select **HA**.

     Note:

     You must select at least three Avaya Breeze® platform nodes or brokers. For example, the three Avaya Breeze® platform nodes of Avaya Oceana® Cluster 1.
4. In the **Unassigned Brokers** table, click **+** to assign the Avaya Breeze® platform nodes or brokers to the Reliable Eventing group.
5. Click the Associated clusters tab:
   a. In the **Unassigned associated clusters** table, click the **+** icon to add an associated cluster.
   b. In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.
6. Click **Commit**.

   The **Status** column displays one of the following:
   - Green check mark (✓) : Indicates that the status of the broker is up and running for subscription and event transfers.
   - Red cross mark (✗): Indicates that the status of the broker is down.
7. To view the status of the brokers, click the green check mark (✓).

Editing a Reliable Eventing group

About this task

You can modify the attributes of a Reliable Eventing group. For example, you can modify the group name, the REF type, or the assigned broker node.

Before you begin

To edit a Reliable Eventing group configuration, you must set the Avaya Oceana® Cluster 1 status in Avaya Oceana® to `Denying`. For more information, see the *Deploying Avaya Oceana®* document.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.

2. Select the **Reliable Eventing group** and click **Edit**.
3. Assign new brokers or remove existing brokers.
4. Click the Associated clusters tab:
    a. In the **Unassigned associated clusters** table, click the **+** icon to add an associated cluster.
    b. In the **Assigned associated clusters** table, click the **X** icon to remove an associated cluster.
5. Click **Commit**.

Deleting a Reliable Eventing group

Before you begin

To edit a Reliable Eventing group configuration, you must set the Avaya Oceana® Cluster 1 status in Avaya Oceana® to `Denying`. For more information, see the *Deploying Avaya Oceana®* document.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Dashboard**.
2. Select the **Reliable Eventing group** and click **Delete**.
3. In the Confirm Delete window, click **Continue**.

Viewing the status of Reliable Eventing destinations

About this task

You can use the Reliable Eventing destinations page to view whether the messages are enqueued, dequeued, dispatched, pending, inflight, or have expired.

Procedure

1. On System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.

    System Manager displays Broker Destination Status Page.
2. In the **Group** field, select the **Reliable Eventing group**.

    The Broker Destination Status page displays the destination status.

Deleting a Reliable Eventing destination

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **Reliable Eventing Administration** > **Destination Status**.
2. In the **Group** field, select the **Reliable Eventing group**.
3. On the Broker Destination Status Page, select a **Destination** and click **Delete/Purge**.
4. Click **Continue**.

   System Manager purges the messages and deletes the destination.

Running a maintenance test for a broker

About this task

In Avaya Breeze® platform, you can check whether Reliable Eventing Framework is functional or down.

Procedure

1. In System Manager, click **Elements** > **Avaya Breeze®** > **System Tools and Monitoring** > **Maintenance Tests**.
2. In the **Select Avaya Breeze to test** field, click the Avaya Breeze® platform instance that you want to test.
3. Select the **Test Reliable Eventing Framework** check box.
4. Click **Execute Selected Tests**.

   Avaya Breeze® platform displays one of the following statuses:

   - `Failure`: Indicates that Reliable Eventing is down and publishing and receiving messages by Reliable Eventing is failing.
   - `Success`: Indicates that Reliable Eventing is functional and publishing and receiving messages by Reliable Eventing is working.

Chapter 7: Deploying Cluster Control Manager

Cluster Control Manager overview

You must deploy the Avaya Common Services Cluster Control Manager (CCM) OVA in your virtual environment. During the deployment, you must enter configuration data using vCenter.

You must perform the procedures described in this chapter for both online and offline Avaya Analytics™ installs.

Note:

You must use new set of OVAs for CCM and node. For more information, see the Release Notes.

Required information for Cluster Control Manager deployment

The following information is required to deploy Cluster Control Manager:

Required information	Customer-specific values	Notes
Customer account login name		Login ID for the customer account.
Customer account login password		You are prompted to change the password at the time of the first customer login.
Enrollment password		Enter an Enrollment password. You must use the same enrollment password when deploying the CCM and when deploying the cluster nodes.
DNS server		A domain server IP address provided by your IT contact. Additional DNS servers can be added as a comma separated list.

Table continues…

Required information	Customer-specific values	Notes
Enhanced Access Security Gateway (EASG)		Use one of the following values: • 1 to enable EASG • 2 to disable EASG Avaya recommends enabling EASG.
Hostname		The FQDN of the Cluster Control Manager server.
Network domain search list		Domain search list separated by commas and provided by your IT contact.
NTP server		An NTP server in either IP address or DNS name format. This information is provided by your IT contact. Additional NTP servers can be added as a comma-separated list.
Public IPv4 address		The IPv4 address of the management interface. This information is provided by your IT contact.
Public IPv4 gateway		The IPv4 gateway for the management interface. This information is provided by your IT contact.
Public IPv4 netmask		The IPv4 netmask for the management interface. This information is provided by your IT contact.
Root account password		You are prompted to change the password at the time of the first root login.
Timezone		Time zone of Cluster Control Manager. **Note:** Select the timezone in which your contact center is being deployed. Please ensure the timezone selected matches with the timezone of Oceana.

Table continues…

Required information	Customer-specific values	Notes
Archive destination		You can set the archive destination to Local or Remote. If you set the archive destination to Remote, you must specify your remote server details. All solution backup files are stored in the configured archive destination. Application and Cluster Control Manager data is stored in this location. Avaya Analytics™ database also uses this archive destination for remote backups. Changing the remote server here overwrites it for Avaya Analytics™ remote database backup destination.
Scheduled backup		By default, scheduled backups are enabled. You must configure your scheduled backup settings. Consider how often you want scheduled backups to run.
Backup password		Ensure that you have your backup file password.

Installing the license file on System Manager

About this task

Use this procedure to install the Avaya Common Services license file.

Before you begin

Download the Avaya Common Services license file from Avaya PLDS.

Important:

After the 30-day licensing grace period elapses, the Common Services cluster is uninstalled. Product data is not preserved.

Procedure

1. On System Manager click **Services** > **Licenses**.

   System Manager displays the WebLM Home page.

2. On the left navigation pane, click **Install license**.
3. On the Install license page, browse to the location of the license file on your computer and click **Open**.
4. Click **Accept the License Terms & Conditions**.

5. Click **Install**.

Deploying Cluster Control Manager

About this task

The steps in this procedure use the vSphere web client connected to vCenter.

Before you begin

- Download the Cluster Control Manager OVA file to the workstation where you will be running the vSphere web client to configure the new virtual machine.
- Access to a minimum of 6 IP address or FQDNs registered in DNS.

Procedure

1. **(Optional)** If using vCenter 7.0 U2 or later, do the following.

   For more information about these substeps, see the VMware article at https://kb.vmware.com/s/article/84240.

   a. Download the OVF/OVA signing certificate chain from https://web.entrust.com/root-certificates/entrust_g2_ca.cer?_ga=2.204957712.1460439918.1633458407-705405935.1632328263.

      The following steps add the intermediate and root certificates to VECS store.

   b. Log in to vCenter as administrator.

   c. Click **Administration** > **Certificates** > **Certificate Management**.

   d. Click **Add** next to Trusted Root Certificates.

   e. Browse and select the certificates file downloaded in the first substep.

   f. Select the **Start Root certificate push to vCenter Hosts** check box.

2. Log in to vCenter using an account that has deployment permissions.
3. In the navigation pane, click **vCenter**.
4. Verify that the drs_lock attribute is not used.

   a. Click **Menu** > **Tags & Custom Attributes**.

   b. On the Tags & Custom Attributes page, click **Custom Attributes**.

   c. If the attribute drs_lock is present in the Attributes list, delete it by clicking the check box next to the attribute and clicking **DELETE**.

5. Click **Inventory Trees** > **Hosts and Clusters**.
6. Expand **Hosts and Clusters** to locate and select the target cluster.
7. Right-click the cluster and select **Deploy OVF Template**.

8. On the Select Template window, click **Local file** and navigate to the location where you downloaded the OVA.
9. Click **Open**.
10. Click **Next**.
11. On the Select name and location window, type a name for the Cluster Control Manager virtual machine.
12. Click the **Browse** tab and select the datacenter for the virtual machine.
13. Select your target deployment folder.
14. Click **Next**.
15. On the Select a resource window, click the **Browse** tab and select the cluster.
16. Click **Next**.
17. On the Review Details page, confirm the properties of the OVA file you selected and click **Next**.
    a. If using vCenter 7.0 U2 or later and you did not perform the optional first step, click **Ignore** next to the warning “The certificate is not trusted”.
    b. If using vCenter 7.0 U2 or later and you performed the optional first step, you can ignore “invalid certificate” in the Publisher field.
18. On the Accept license agreement window, click **Accept**.
19. Click **Next**.
20. On the Select storage window from the **Select virtual disk format** drop-down, select **Thin Provision**.
21. If you are given the option to select an encryption policy, set it to **None**.
22. Select the correct Datastore for your configuration.
23. Click **Next**.
24. On the Select networks window, change the **Public** field to a network appropriate for your configuration.
25. Click **Next**.
26. On the Customize template page, do the following:
    a. Enter a customer account login name.
    b. Enter a customer account password.

       You will be prompted to change the password at the first login.
    c. **(Optional)** Enter a root password.

       If you do not choose to create a root password at this time, you must contact Avaya support to enable the root account after deployment.
    d. Enable or disable the Enhanced Access Security Gateway.

e. Enter the enrollment password. This password must match the enrollment password used on the cluster nodes.

27. On the same screen under Network Settings, enter the following information:
    a. In **Hostname**, enter the host name of the Cluster Control Manager virtual machine.
    b. In **DNS Servers**, enter the IP addresses of up to 3 DNS servers, each separated by a comma.
    c. In **Network Domain Search List**, provide a list of domain searches separated by a comma.
    d. In **Public IPv4 Address**, enter the IP address for the host.
    e. In **Public IPv4 Gateway**, enter the gateway for the host.
    f. In **Public IPv4 Netmask**, enter the subnet mask for the host.
28. Complete the fields under HTTP(S) Proxy Settings (optional) to configure an outbound proxy.

    Leave fields that are not applicable to your proxy configuration blank.

    - **HTTPS Proxy Server**: If you are using an HTTPS proxy server, enter the IPv4 address or FQDN of the proxy server.
    - **HTTPS Proxy Port**: If you are using an HTTPS proxy server, enter the port number for the proxy server.
    - **HTTP Proxy Server**: If you are using an HTTP proxy server, enter the IPv4 address or FQDN of the proxy server.
    - **HTTP Proxy Port**: If you are using an HTTP proxy server, enter the port number for the proxy server.
    - **HTTP(S) Proxy Exclusion List**: Provide a comma-separated list of hosts that will not use the proxy server.

      A single asterisk (*) is not permitted.
    - **HTTPS CA Certificate**: If you are using an HTTPS proxy server, enter the CA certificate text in the base-64 format. Include the complete “BEGIN CERTIFICATE” and “END CERTIFICATE” tags.
29. From **Archive Destination**, select **Local** or **Remote**.

    Avaya Analytics™ database also uses this archive destination for remote backups. Changing the remote server here overwrites it for remote Avaya Analytics™ database backup destination.
30. If you selected **Remote**, configure the remote destination settings.
    a. In **FQDN/IP**, enter the FQDN or IP address of the remote destination.
    b. In **Port**, enter the port number for the remote destination.
    c. In **User Name**, enter the user name for your remote server.

d. In **Password**, enter the password for the remote server and confirm the password.

e. In **Base Directory**, enter the path to the directory where you want Cluster Control Manager and solution archives to be stored.

31. To schedule backups, complete the scheduled backup settings.

    a. In **Backup Recurrence**, select a recurrence interval.

       You can select **Daily**, **Weekly**, or **Monthly**.

    b. In **Backup Recurrence Multiple**, enter a number, which defines how often the backup runs in relation to the **Backup Recurrence** option you selected.

       For example, if you enter `3` and you set **Backup Recurrence** to:

       - **Daily**: The backup runs once every three days.
       - **Weekly**: The backup runs once every three weeks.
       - **Monthly**: The backup runs once every three months.

    c. In **Time of Day to Take Backup**, enter the time when you want the backup to run in the 24-hour time format.

       Use the hh:mm format to enter the time. For example, enter `19:00` if you want the backup to run at 7pm.

    d. If you set **Backup Recurrence** to **Weekly**, in **Day of Week to Take Backup**, select a day.

    e. If you set **Backup Recurrence** to **Monthly**, enter the day of the month when you want the backup to run.

       For example, enter `5` if you want the backup to run on the 5th of the month.

       If you enter `31` and the month only has 30 days, then the backup will run on the 30th. Similarly, if you enter `30`, then in February, the backup will run on the last day of the month.

    f. To enable the scheduled backup, set **Backup Enabled** to **True**.

32. In **Enter Backup Password**, enter the password for the backup file and confirm the password.

    The password must be at least 8 characters long and contain at least the following:

    - One upper case character
    - One lower case character
    - One number
    - One special character

33. Under System Time Settings, configure the NTP server and time zone settings.

    Enter the IP address or DNS name of up to three NTP servers.

    Select the time zone for Cluster Control Manager. Avaya recommends using the same time zone you defined in your solution configuration spreadsheet (Olson time zone format).

34. Click **Next**.
35. Click **FINISH** to complete the deployment and wait for the deployment to complete.
36. Locate your new VM in the inventory list and right-click it.
37. Click **Power** > **Power on**.
38. Click **Summary** > **Launch Console** to open a new console.

    The system displays the progress of the VM system initialization.
39. Using a utility, such as PuTTY, connect to the CCM node using SSH.
40. Log in using the Customer account login name and the customer account password entered during the OVA deployment.

    You will be prompted to reset the password.
41. If a root account was specified during OVA deployment, update the password for this account from the customer account login session, su – root.

    When prompted, update the root password. Exit from the root login when you have completed this step.

Chapter 8: Cluster node deployment

Required information for cluster node deployment

You require the following information to deploy cluster nodes:

Required information	Customer-specific values	Notes
Hard disk size		Hard disk size depends on the number of agents selected in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. For the first two cluster nodes, enter disk size value that must match the **Disk Storage Requirement(GB)** field value in deployment properties worksheet under `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. For the third cluster node enter 0. This shows as **hard disk 2** on the virtual machine summary.
Customer login settings		Enter a user name and password for ssh access to the cluster node. You will be prompted to change it on first login.
Root login		Enter a password. You will be prompted to change it on first login.
Enrollment password		Enter the same enrollment password that you established on the CCM during deployment.
Network settings		Enter the appropriate values for your Cluster Node VM: the IPV4 address (single NIC configuration), netmask, gateway, and fully qualified domain name.

Preparing the deployment spreadsheet

About this task

Use this procedure to install Avaya Analytics™ with High Availability (HA) configuration by using the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. You must enter the configurable values in the spreadsheet manually. The minimum supported version of MS Excel is 2016.

Before you begin

- Download the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file from PLDS.
- Enable the macros before you start editing the worksheets.
- Select the deployment types by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file. Complete the fields with the customer details that correspond to each deployment type, such as IP addresses and passwords.

Note:

The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Orca** tab.
3. In the **Number Of Agents** field, click one of the following options:
   - Agent 100
   - Agent 500
   - Agent 1000
   - Agent 2000
   - Agent 4500
4. Set the **Customize Processors to Install** field to `TRUE` to customize which measure processors get deployed.
   a. For **Routing Service Group Measure Processor**, set the **Install** field to `TRUE` if routing service real-time reporting is required.
   b. For **Agent Trace Measure Processor**, set the **Install** field to `TRUE` if agent trace historical reporting is required.

Note:

Enabling Routing Service Group Measure Processor and Agent Trace Measure Processor increases the cluster footprint resource, such as memory, CPU and disk storage, requirements.

During fresh installation or after migrating to Avaya Analytics™ 4.3.1.1 cluster, you must set the Agent Trace Measure Processor and Routing Service Group Processor to `TRUE` before deploying the Avaya Analytics™ 4.3.1.1 cluster.

5. Click the **Deployment Properties** tab.
6. Set **Node Affinity Enabled** to `TRUE`.
7. Complete the configurable fields in the spreadsheet.

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.
8. For enabling Cross-Origin Resource Sharing (CORS), in CORS field, enter a URL:

   The field value should be taken from the origin field of the HTTP request to the orca-streams-rest and orca-streams-data-publisher. For example, Go to **WORKSPACES** > **Chrome** > **Developer tools** > **Network** > **XHR** > **any orca-streams-rest URL**.

   Note:

   Once these fields are configured in deployment spreadsheet, there is no need to install CORS chrome plugin additionally.

Deploying cluster nodes

About this task

The steps in this procedure use the vSphere web client connected to vCenter.

Before you begin

- Deploy the Cluster Control Manager.
- Collect the required node information needed for deployment.

Procedure

1. Log in to vCenter using an account that has deployment permissions.
2. Access the target folder for deploying the cluster node virtual machines.
3. Use the Cluster Node OVA to deploy either one VM (for a non-HA single-node deployment) or three or more VMs (for an HA deployment with three master nodes).

   Use the values from the table of required node information that you collected.

   A centralized storage array with thin provisioning and no encryption is required.

   Note:

   After deploying one cluster node, if you have user permission in vCenter, you can clone and customize the second and third cluster nodes. For the third cluster node, the disk size must be set to 0 as only the 2 controller or master nodes require disk. If you

have used clone option, you need to delete the 2nd disk (360GB) associated with your third cluster node virtual machine.

4. Repeat the deployment instructions for the remaining cluster nodes, if applicable.

   CPU and Memory resource values can be found in deployment properties worksheet in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. Hard disk size depends on the number of agents selected in the deployment spreadsheet.

   You can manually set the resource footprint by editing the VM settings after OVA is deployed. Ensure cluster node 1 and 2 are deployed with correct disk size for disk 2. This value must match the Disk Storage Requirement(GB) value on the deployment properties sheet in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet.

   Important:

   Cluster Node 3 Disk 2 must be set to 0.

5. If you are deploying with high availability enabled, you must create an anti-affinity rule in vCenter for the cluster nodes.

   Create the anti-affinity rule before powering on the VMs after initial OVA deployment to prevent a hot migration.

   a. Navigate to your vCenter cluster.
   b. In the **Configure** tab, select **Configuration** > **VM/Host rules** > **Create VM/Host Rule**.
   c. Create a name for the anti-affinity rule.
   d. Select **enable rule**.
   e. Type `Separate Virtual Machines`.
   f. Add all the cluster nodes to the list.
   g. Click **OK**.

6. Power on all cluster node VMs.

   All CSP cluster node VMs are powered on and available for solution deployment.

Chapter 9: Deploying Avaya Analytics™ online

This chapter describes the procedures to install Avaya Analytics™ online.

Avaya Analytics™ on Avaya Common Services deployment overview

The Avaya Analytics™ solution on Avaya Common Services (Common Services) deployment, consists of four virtual machines; three master nodes HA and the Cluster Control manager (CCM) node as follows:

- Common Services and Avaya Analytics™ core services are deployed on the three master nodes.
- From the CCM node, you can download the software required to deploy the full solution on a Kubernetes (K8s) cluster consisting of three virtual machines (VMs).

Each master node is deployed on separate physical servers. The CCM can be deployed on any of the three physical servers containing the master nodes.

Important:

For more information, see Topology on page 14.

Pre-installation checklist

Download the following from PLDS before installing Avaya Analytics™ on Avaya Common Services (Common Services)

- Avaya Common Services license file
- `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm`

You must ensure that CCM has public internet access. Otherwise, you can deploy Avaya Analytics™ offline.

Preparing the deployment spreadsheet

About this task

Use this procedure to install Avaya Analytics™ with High Availability (HA) configuration by using the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. You must enter the configurable values in the spreadsheet manually. The minimum supported version of MS Excel is 2016.

Before you begin

- Download the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file from PLDS.
- Enable the macros before you start editing the worksheets.
- Select the deployment types by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file. Complete the fields with the customer details that correspond to each deployment type, such as IP addresses and passwords.

Note:

The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Orca** tab.
3. In the **Number Of Agents** field, click one of the following options:
   - Agent 100
   - Agent 500
   - Agent 1000
   - Agent 2000
   - Agent 4500
4. Set the **Customize Processors to Install** field to `TRUE` to customize which measure processors get deployed.
   a. For **Routing Service Group Measure Processor**, set the **Install** field to `TRUE` if routing service real-time reporting is required.
   b. For **Agent Trace Measure Processor**, set the **Install** field to `TRUE` if agent trace historical reporting is required.

Note:

Enabling Routing Service Group Measure Processor and Agent Trace Measure Processor increases the cluster footprint resource, such as memory, CPU and disk storage, requirements.

During fresh installation or after migrating to Avaya Analytics™ 4.3.1.1 cluster, you must set the Agent Trace Measure Processor and Routing Service Group Processor to `TRUE` before deploying the Avaya Analytics™ 4.3.1.1 cluster.

5. Click the **Deployment Properties** tab.
6. Set **Node Affinity Enabled** to `TRUE`.
7. Complete the configurable fields in the spreadsheet.

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.
8. For enabling Cross-Origin Resource Sharing (CORS), in CORS field, enter a URL:

   The field value should be taken from the origin field of the HTTP request to the orca-streams-rest and orca-streams-data-publisher. For example, Go to **WORKSPACES** > **Chrome** > **Developer tools** > **Network** > **XHR** > **any orca-streams-rest URL**.

   Note:

   Once these fields are configured in deployment spreadsheet, there is no need to install CORS chrome plugin additionally.

Setting up an outbound proxy

HTTP(S) outbound proxy configuration

You can configure an outbound HTTP or HTTPS proxy if your organization mandates the use of a proxy. Clients are configured to send requests to a proxy. The information in this section does not apply to an environment which either has no proxy or which uses an implicit proxy.

Cluster Control Manager configuration

You can configure the outbound proxy in one of the following ways:

- When deploying the Cluster Control Manager OVF by populating the HTTP(S) Proxy Settings section.
- Using the **`ccmNetSetup`** command on Cluster Control Manager.

The proxy exclusion list contains addresses with which Cluster Control Manager does not communicate through the proxy. If an HTTP or HTTPS proxy is configured, the proxy exclusion list includes `localhost,127.0.0.0/8` by default. As part of the cluster installation, the exclusion list is automatically populated with the Cluster Control Manager, vCenter, cluster FQDN, keepalived virtual IP address, and Kubernetes master host virtual IP address.

The format of the destination address can include an IP address prefix (1.2.3.4), a domain name, or a special DNS label (*). Note the following:

- A domain name can match other names and subdomains.

For example, with the domains `foo.example.com` and `example.com`, `example.com` matches both the `example.com` and `foo.example.com` domains. However, `.example.com` only matches `foo.example.com`.

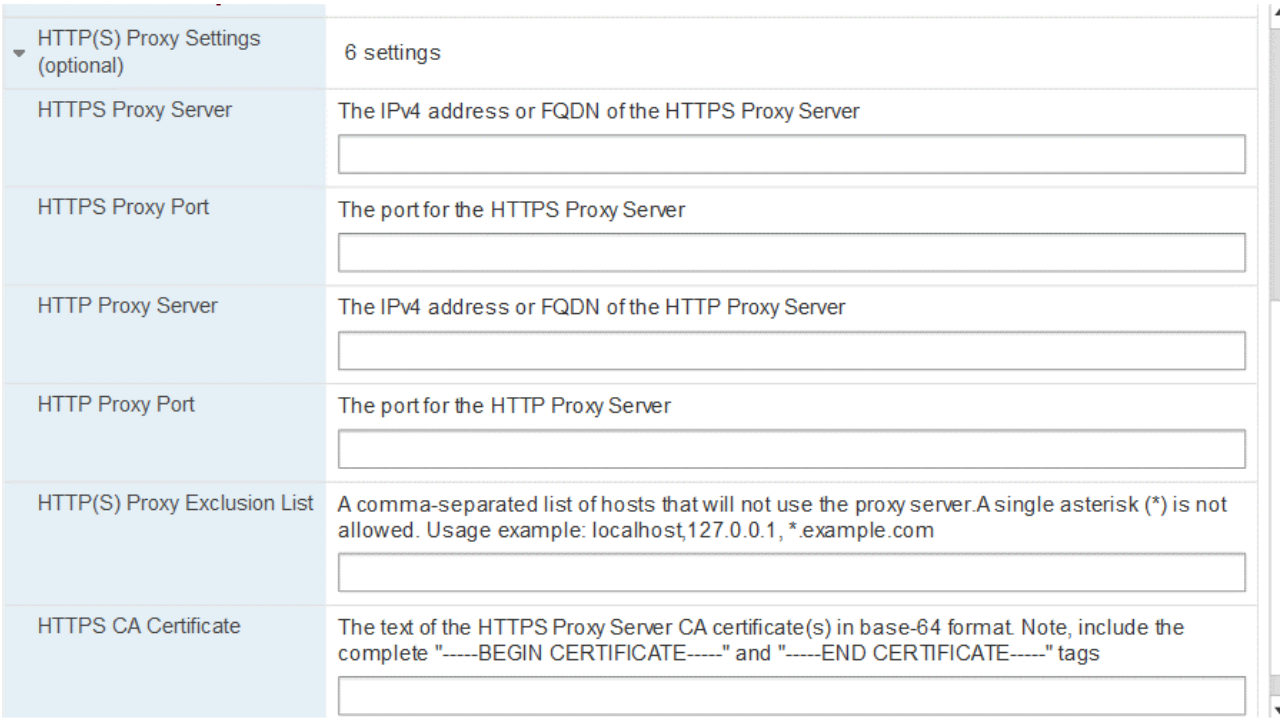
- A single asterisk (*) indicates that no proxying is needed.
- You can include a port number with IP address prefixes and domain names.

  An example of an IP address prefix with a port number is `1.2.3.4:80`, and an example of a domain name with a port number is `foo.example.com:80`.

Configuring proxy settings when deploying Cluster Control Manager

Procedure

Populate the following HTTP(S) proxy settings while deploying the Cluster Control Manager OVF.



Using the ccmNetSetup command to configure proxy settings

About this task

You can configure proxy settings using the `ccmNetSetup` command. You can use this command anytime to update Cluster Control Manager network attributes. For example, if the FQDN or IP address of the explicit proxy changes, you can run the `ccmNetSetup` command to reflect the new destination.

Before you begin

- If you are configuring an HTTPS proxy, ensure that you have the HTTPS proxy server CA certificate.
- Perform a full backup of Common Services and application data.

  For more information, see Backing up Common Services on page 69 and your solution documentation.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. For an HTTPS proxy, copy the HTTPS proxy server CA certificate to a directory on Cluster Control Manager, such as `/home/cust/`.
3. Run `ccmNetSetup` or `ccmNetSetup --collect-proxy-only`.
   - Running `ccmNetSetup` without any options prompts you to populate all Cluster Control Manager network attributes.
   - Running `ccmNetSetup --collect-proxy-only` prompts you to update proxy-related network attributes only.
4. When you see the prompt `Would you like to configure an HTTP proxy?`, enter `y`.
5. When prompted, provide the following information:
   - HTTPS proxy IP/FQDN
   - HTTPS proxy port
   - HTTP proxy IP/FQDN
   - HTTP proxy port
6. When prompted to enter the absolute file path of the HTTPS proxy server CA certificate, enter the path to the certificate file.

   For example, `/home/cust/<file name>`.
7. When prompted to confirm that the above information is correct, enter `y` if all the information you provided is correct.
8. To complete the proxy configuration, close the current command session and open a new one.

Installing Avaya Analytics™

About this task

To install Avaya Analytics™ on the Cluster Control Manager (CCM) server, select the required deployment type by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.

Before installing Avaya Analytics™, you must complete the fields with the customer details that correspond to each deployment type. Examples of customer details include IP addresses and passwords. The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

Use the screen utility while installing Avaya Analytics™. Screen is a Linux command with which you can detach from an SSH session and reattach at a later time. This avoids issues where the SSH session can disconnect after timing out, thereby interrupting the install.

Important:

Ensure that you are familiar with the screen utility. For detailed information about using screen, enter the **`man screen`** command.

Before you begin

- Configure CCM.
- Update the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
- Copy the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to the CCM server.
- For high availability, deploy 3 or more cluster nodes by setting values for CPU, memory, and disk. Refer to *Deploying Cluster Nodes* chapter in this guide.
- Modify the cluster node VMs running with the vCPU, memory, and disk allocation as stated in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. Cluster node VMs must be running with the vCPU memory and disk allocation as stated in the deployment spreadsheet.
- If you are deploying with high availability enabled (three master nodes) you must create an anti-affinity rule in your vCenter for your cluster nodes.

  If DRS is enabled, the vCenter administrator must create a DRS anti-affinity rule and include all master cluster node VMs in the rule.

  If DRS is disabled, the vCenter administrator must ensure that the VMs for the master cluster nodes are deployed on separate hosts if HA is required.

Procedure

1. Connect to the CCM server using the customer account log in.

   Important:

   If this is your first login after deploying CCM, you must change the password.

2. Copy the excel file to a location on the CCM server.
3. From the directory on CCM that contains the excel file, enter the following command: **`screen`**

   The screen utility allows the install to run in the background.

   Warning:

   Do not skip this step.

4. Run the following command: **`ccm install Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm`**
5. When prompted:
   a. Enter your Avaya SSO credentials.
   b. Accept the EULA.
   c. When prompted, either enable or do not enable the High Availability Audit feature.

      To enable the feature, respond `Y` to give the cluster deployment vCenter access.

      `Y` – Enable the High Availability Audit feature and grant deployment vCenter access for the cluster. The solution configuration spreadsheet must also set high_availability to `enabled`.

      `N` – Do not grant deployment vCenter access for the cluster, and do not enable the High Availability Audit feature.

      Example:

      ```
      The following features will be enabled if this cluster
      deployment is allowed vCenter access.
      - High Availability Audit

      Do you want to allow this cluster deployment vCenter access?
      (Y/N)
      ```

   d. Enter the vCenter user ID and password.
   e. Re-confirm the password.

   The installation starts downloading and installing the following:

   - The base cluster software
   - The common services platform software
   - The Avaya Analytics™ software

   The installation takes several hours to complete.
6. Run the following command in a separate window to monitor the progress of the install: **`tail -f /var/log/avaya/ccm/ccm-main.log`**

   During the installation folders and virtual machines are created on host machines visible in the host's vCenter.
7. If you want to disconnect from the SSH session and allow the install to continue in the background, do the following:
   a. Disconnect from the SSH session.
   b. When you want reconnect to the SSH session, start a new SSH session to CCM and connect using the customer account.
   c. Type **`screen -ls`** to retrieve the screen id of the session that is running the installation.

d. Type **`screen -dr <screen id>`** to reattach to the installation screen session.

See the following example command to reattach to the installation screen session:

```
[cust@examplelab ~]$ screen -ls
There is a screen on:
            9069.avaya.examplelab    (Detached)
1 Socket in /var/run/screen/S-cust.
[cust@examplelab ~]$ screen -dr 9069.avaya.examplelab
```

8. To check if the installation is successful, run the following command on the CCM console:

`ccm status`

The CCM console displays the status details as follows:

- If the Status column displays the status as `deployed`, it indicates that all the components are currently deployed to the cluster.
- If the Status column displays the status as `Staged` or `''`, it indicates that the software is staged on the system, but not deployed.

  The tools-policy and utility-services remain in a `staged` state.

  Note:

  You might see this status in the older versions of the software after a upgrade.
- If the Status column displays the status as `Error`, it indicates that the components failed to install.

Important:

If the installation fails, run the **`ccm install cancel`** command, resolve the issue causing the failure, and restart the installation procedure. For more information about troubleshooting installation failures, see *Maintaining and Troubleshooting Avaya Analytics™*.

9. Delete the spreadsheet from CCM after the deployment is complete. Ensure you keep a copy of the spreadsheet and store it in a secure location.

   This step is important to save the passwords and other configuration details that you entered as plain text for the deployment.

Backing up Common Services

About this task

Use this procedure to generate a backup file for Common Services. This backup does not contain product application data.

The following content is included in this Common Services backup:

- Local users for the system

- Product configurations
- Infrastructure configurations
- System certificates

You can run `ccm backup` on Cluster Control Manager to manually create a backup. You are automatically prompted to perform a backup during a major infrastructure or service change using the `ccm upgrade` or `ccm install` commands.

Avaya recommends taking a backup after any configuration changes to the system or deployed products.

Note:

Avaya Analytics™ database also uses this archive destination for remote backups. Changing the remote server here overwrites it for Avaya Analytics™ remote database backup destination.

Procedure

1. Log in to Cluster Control Manager.
2. To manually start a backup, run one of the following commands:
   - `ccm backup`: Stores the backup file in either the local or remote directory, depending on the archive destination you configured.

     The local directory location is `/var/avaya/artifactCache/ccmClusterBackup`. The remote location is `<base directory path>/ccmClusterBackup`.
   - `ccm backup --local`: Stores the backup file in the local directory at `/var/avaya/artifactCache/ccmClusterBackup`. This command overrides the configured archive destination.
   - `ccm backup --remote-server "<FQDN/IP> [-p <port>] -u <username> -d <directory path>"`: Stores the backup file in the remote directory you specify. This command overrides the configured archive destination.

     Include the double quotes as shown above for the `--remote-server` option. If you omit these quotes, the command will fail.

     You need to include `-p <port>` if you are using a port other than the default port 22.
3. When you are prompted to proceed with the backup, enter `y`.

   For local backups, confirm that the oldest backup file may be deleted.

   ```
   There are two backup archives located /var/avaya/artifactCache/
   ccmClusterBackup. The oldest one will be deleted
   Do you wish to proceed?
   Response [y, n] => y
   ```
4. If you used the `--remote-server` option in step 2, enter the remote server password when prompted.
5. If you did not configure a backup password, enter one when prompted.

This password is used to encrypt the generated backup file. You will need this password to perform restore operations.

The password must be at least 8 characters long and contain at least the following:

- One upper case character
- One lower case character
- One number
- One special character

6. Wait for the backup to complete.

   You will be notified of the location of the `.tgz` backup file.

7. If the backup file is in the local `/var/avaya/artifactCache/ccmClusterBackup` directory, copy it to a secure location and transfer it off of Cluster Control Manager.

   You are prompted when more than two backups are in the local directory.

   For scheduled backups, only the two most recent backup files are kept in the local directory.

8. **(Optional)** To free up space for future use, remove the backup file.

Chapter 10: Deploying Avaya Analytics™ offline

Avaya Analytics™ offline deployment overview

You can deploy Avaya Analytics™ using an offline client computer. However, the computer must not be connected to the public Internet and your environment must include an air gap network. An air gap network is an isolated network or closed system from any other public or generally accessible network for security related reasons. The use of an air gap network assists with securing and controlling physical access to servers and virus malware protection.

To move data between an air gap network and a public network, use an intermediate device. Use this device to connect to the public network to acquire the necessary Avaya install software. You can then use this intermediate device to deploy the Avaya Analytics™ software on to Cluster Control Manager (CCM) that is within the air gap network.

This chapter describes how to deploy new Avaya Analytics™ solution offline using Docker Desktop for Windows and Windows Subsystem for Linux. However, you must use only one method end-to-end. You can also use Docker for Mac to deploy Avaya Analytics™ offline.

Pre-installation checklist

Download the following from PLDS before installing Avaya Analytics™ on Avaya Common Services (Common Services)

- Avaya Common Services license file
- `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm`
- The Cluster Control Manager (CCM) batch script

Deploying Avaya Analytics™ offline using Docker Desktop for Windows

Planning and pre-configuration

Before deploying Avaya Analytics™ offline, you must do the following:

- Get a client computer with the following specifications:
  - Windows 10 Professional or Enterprise 64-bit operating system v1903 or later, or macOS Catalina 10.15.4

    Note:

    This deployment does not support Windows 10 Home and Windows PowerShell ISE.
  - 2 GB of available free memory
  - 1 available CPU of 2.0 GHz or higher
  - Available disk space:

    60 GB for a regular offline installation process when you run files directly from the client container to the Cluster Control Manager using the **`agn upload`** command.

    100 GB for a manual transfer, as the further steps require additional disk space. For more information about the manual transfer, see Air gap network: Uploading Avaya Analytics chart and images with restricted access to Cluster Control Manager on page 96.
- Get Windows or Mac local account administrator privileges to install Docker Desktop for Windows or Docker Desktop for Mac and add certificates to the trust store.
- Install Docker Desktop for Windows or Mac 2.2.0.3, or later on the client computer.
- Get basic knowledge of Windows Powershell, Linux, Docker, and Cluster Control Manager.
- Contact Avaya to ensure your SSO credentials allow you to deploy the software successfully.
- Get Docker Hub account credentials from https://hub.docker.com.
- Get external internet access to the Avaya repository and Docker Hub from the user's corporate network.
- If you are using a virtual machine with Windows 10, ensure that the BIOS-level hardware virtualization is enabled in the BIOS settings.

Getting access to Docker Hub

About this task

To install Docker Desktop for Windows, you must first sign up on Docker Hub and create a Docker ID. Your free Docker ID grants you access to Docker Hub repositories, and services, such as the Support Center, the Docker Forums, and the Docker Success portal.

Before you begin

Ensure that you have a valid email ID.

Note:

Docker sends an activation email to the specified email address.

Procedure

1. Signup for a free user account at: https://hub.docker.com/
2. Click **Sign up for Docker Hub**.
3. In the **Docker ID** field, enter a username.

   The username you enter is also your Docker ID. Your Docker ID must be between 4 and 30 characters long, and can only contain numbers and lowercase letters.
4. In the **Email** field, enter a valid email address.
5. In the **Password** field, enter a password.

   You can enter a password between 6 and 128 characters long.
6. Click **Sign up**.

   You receive an activation email in the specified email address.
7. Click the link in the email to verify your address.

   You can log in with your Docker ID only after you verify your email address.

Installing Docker Desktop for Windows

About this task

Docker is a development platform that you can use to build, run, and share containerized applications. Docker supports Docker Desktop for Windows, based on Microsoft support lifecycle for Windows 10 operating system.

Before you begin

Ensure that you have access to Docker Hub.

Procedure

1. Download Docker Desktop for Windows from Docker Hub.

   The installer file downloads to your `Downloads` folder.
2. To run the installer, double-click the **Docker Desktop Installer.exe** file.

   Tip:

   You can run the installer file from the recent downloads bar at the bottom of your web browser.

   The initial setup can take 5 to 10 minutes to complete.
3. On the `Configuration` page, do the following:
   a. Select the **Enable required Windows Features** check box.

b. Select the **Add shortcut to desktop** check box.

c. Clear the **Use Windows containers instead of Linux containers** check box.

By default, this check box is not selected.

d. Click **Ok**.

4. After the installation is complete, click **Close and restart**.

Result

Your desktop displays the Docker Desktop icon, which indicates that the application is now installed.

Starting Docker Desktop for Windows

About this task

Docker Desktop does not start automatically after installation. Use the following steps to start Docker Desktop.

Before you begin

Install Docker Desktop.

Procedure

1. On your taskbar, click the search icon, and type `Docker Desktop`.
2. Click the **Docker Desktop** app.
   - Windows displays the message that `Docker Desktop is starting`.
   - When you see that the whale icon in the status bar is steady, it indicates that Docker Desktop is running.
3. **(Optional)** If the whale icon is hidden in the Notifications area, click the up arrow on the taskbar to see it.
4. Close the Docker Welcome console.

Configuring Docker Desktop

About this task

Using the Docker Desktop menu, you can configure your Docker settings such as installation, updates, version channels, and Docker Hub login.

Before you begin

- Get access to Docker Hub.
- Install Docker Desktop for Windows.

Procedure

1. To open the Docker Desktop menu, click the Docker icon in the notifications area or on the system tray.

2. Click **Settings**.

   Docker displays the Settings page.

3. In the **General** tab, clear the following check boxes:

   - **Send usage statistics**
   - **Use containerd for pulling and storing images**

   Note:

   In Docker Desktop version 4.34.0 and later, the **Use containerd for pulling and storing images** check box is selected by default. Clear the check box for successful CSP Air Gap deployment.

4. In the **Resources** tab, click **FILE SHARING** and select the **C** check box.

   Note:

   The following steps applies only to software installed on the C drive.

5. Click **Apply & Restart**.
6. In the Start menu, navigate to `Windows PowerShell` folder and click **Windows PowerShell**.
7. On the Windows PowerShell console, enter `docker version`.

   The Docker console displays the docker client and server version information.

Obtaining the Cluster Control Manager air gap network controller container startup bat file

About this task

You must use the Cluster Control Manager (CCM) air gap network controller image to create the container on the client laptop or PC. You can use this container to pull Avaya Analytics™ software from the Avaya repository and then push the software onto CCM within the air gap environment.

Important:

For this procedure, we assume that you have configured the Docker Desktop file sharing resource to use the local Windows C:\ drive.

Before you begin

- Ensure that your Avaya SSO credentials allow you to download the software successfully.
- Obtain the available `ccm-ctl-agn-x.x.xxx.zip` from PLDS. For example; `ccm-ctl-agn-1.3.09.zip`

Procedure

1. On your taskbar, click the search icon and type `Windows PowerShell`.
2. Click the **Windows PowerShell** app.

3. To create the `cd C:\avaya` folder in Windows, run the following command on the Windows PowerShell console:

   `mkdir c:\avaya`

4. Copy the `ccm-ctl-agn-x.x.xxx.zip` that was downloaded from PLDS into the `c:\avaya` Windows folder.
5. In the `c:\avaya` folder in Windows, unzip the `ccm-ctl-agn-x.x.xxx.zip` file.

Starting the Cluster Control Manager air gap network container

About this task

You must start the Cluster Control Manager (CCM) air gap network container to complete the Avaya Analytics™ offline installation process. The first time the `ccm-ctl-agn-x.x.xxx.bat` script is run, the script creates a set of necessary folders, downloads the ccm-ctl-agn image, and starts the container. After the image is initially downloaded into the DockerDesktop cache, subsequent running of the batch script uses the cached ccm-ctl-agn image to start the container.

Important:

This procedure assumes that you have configured the Docker Desktop file sharing to use the Windows `c:\` drive.

Before you begin

- Confirm that Docker Desktop is running.
- Obtain the latest Cluster Control Manager air gap network controller container startup bat file `ccm-ctl-agn.bat`.

Procedure

1. On your taskbar, click the search icon, type `Windows PowerShell`.
2. Click the **Windows PowerShell** app.
3. On the Windows PowerShell console, type `C:\avaya\` and press **Enter**.
4. Run the `ccm-ctl-agn-x.x.xxx.bat script` that was earlier downloaded from PLDS.

   For example, type `.\ccm-ctl-agn-1.3.09.bat` and press **Enter**.
5. In the **Username** field, type your Avaya SSO username.
6. In the **Password** field, type your Avaya SSO password.

   Note:

   The script requests the Avaya SSO credentials only if the ccm-ctl-agn image is not downloaded earlier into the DockerDesktop cache.
7. When the prompt changes to a Linux prompt, type `agn` and press **Enter**.

   The Windows PowerShell console displays the **`agn`** command usage details.

Setting up an outbound proxy setup

You must download the Avaya Analytics™ charts and images to a laptop which uses an outbound proxy to access Avaya Harbor from a customer environment. To download the charts and images using the ccm-ctl-agn container, complete the following procedures:

Related links

[Adding the proxy CA certificates to the Windows truststore](#) on page 78
[Configuring Docker Desktop for outbound proxy](#) on page 78
[Configuring outbound proxy for the ccm-ctl-agn container](#) on page 79
[Adding the proxy CA certificate to the ccm-ctl-agn truststore](#) on page 80

Adding the proxy CA certificates to the Windows truststore

About this task

You can add the proxy certificates to the Windows truststore directly on your laptop or PC.

Procedure

1. On your taskbar, click the search icon, and type `Manage computer certificates`.
2. On the Certificates-Local Computer page, click **Trusted Root Certification** > **Certificates**.
3. Right-click the `Certificates` folder and click **All Tasks** > **Import**.
4. On the Certificate Import Wizard page, click **Next**.
5. To import the certificates file, click **Browse**.
6. On your local PC, click on the required certificate and click **Open**.
7. Click **Next**.
8. Select the **Place all certificates in the following** check box.
9. Ensure that the **Certificate store** field displays **Trusted Root Certification Authorities** and click **Next**.
10. Click **Finish**.

Related links

[Setting up an outbound proxy setup](#) on page 78

Configuring Docker Desktop for outbound proxy

About this task

You must configure Docker Desktop to use an outbound HTTP proxy.

Before you begin

- Install Docker Desktop.
- Keep the required proxy connection information handy.

Procedure

1. In your Windows system tray, right-click the Docker whale icon.
2. Click **Settings**.
3. On the Settings page, click **Resources** > **Proxies**.
4. Enable the **Manual proxy configuration** option.

   The proxy fields get automatically enabled.
5. Type the required information in the following proxy fields:
   - **Web Server (HTTP)**
   - **Secure Web Server (HTTPS)**
   - **Bypass proxy settings for these hosts & domains**: For example: *.domain.com or 127.0.0.0
6. Click **Apply & Restart**.

   Note:

   If your ccm-ctl-agn container is running, it stops automatically when Docker Desktop restarts.

Related links

Setting up an outbound proxy setup on page 78

Configuring outbound proxy for the ccm-ctl-agn container

About this task

You must configure the ccm-ctl-agn container to use an outbound HTTP proxy by including the proxy connection information in the following file:

`/avaya/proxy/config`

Note:

You must restart the ccm-ctl-agn container after you make any updates to the proxy configuration file.

Before you begin

- Install the ccm-ctl-agn container.
- Keep your proxy connection information handy.

Procedure

1. Start the ccm-ctl-agn container.
2. On the ccm-ctl-agn running container console, edit the `/avaya/proxy/config` file to replace the following variables on the right with your outbound HTTP proxy data:

   export http_proxy=<http_proxy>:<http_port>

   export https_proxy=<http_proxy>:<http_port>

export no_proxy=<excluded_proxy_connections>

3. Save the file.
4. Exit the ccm-ctl-agn container.
5. Restart the ccm-ctl-agn container.
6. **(Optional)** If the charts fail to download when you run the **`agn download`** command, you can troubleshoot the issue within the container.

   For more information, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.

Related links

Setting up an outbound proxy setup on page 78

Adding the proxy CA certificate to the ccm-ctl-agn truststore

About this task

You must add the proxy CA certificate to the ccm-ctl-agn container truststore for a secured connection. Add the proxy CA certificates in the `/avaya/cacerts` directory.

Note:

You must restart the ccm-ctl-agn container after making any CA certificate changes.

Before you begin

- Ensure that the ccm-ctl-agn container is running.
- Keep the proxy CA certificates information handy.

Procedure

1. In the ccm-ctl-agn running container console, copy your outbound HTTP proxy CA certificates in to the `/avaya/cacerts` directory.

   These files can be in Base64 or DER format.

   Alternately, you can also copy the proxy CA certificates to the Windows folder at `C:\avaya\caccerts`
2. Exit the ccm-ctl-agn container.
3. Restart the ccm-ctl-agn container.

Related links

Setting up an outbound proxy setup on page 78

Obtaining the Cluster Control Manager CA certificate

About this task

You must obtain the Cluster Control Manager (CCM) CA certificate and install the certificate into the Windows trust store.

Before you begin

- Get your CCM FQDN.
- Ensure that the CCM local Docker registry and ChartMuseum are running.
- Ensure that you have the local admin Windows user rights.

Procedure

1. Connect to your air gap network using your Windows PC or client laptop.
2. Using a browser, navigate to the CCM docker registry listening on port 5010 at `https://<ccm_fqdn.com>:5010/`, where <ccm_fqdn> is the FQDN of your CCM.
3. If you do not see a `Certificate error` message, skip the remaining steps.
4. If you see a `Certificate error` message, do the following:
   a. Click the Certificate error message.
   b. Click **View Certificate**.
   c. Click **Export to file**.
   d. Save the exported certificate.
5. On your taskbar, click the search icon, and type `Manage computer certificates`.
6. Click the **Manage computer certificates** control panel.
7. In `Certificates-Local Computer`, click **Trusted Root Certification**.

   The right-pane displays the `Certificates` folder.
8. Right-click **Certificates**.

   Windows displays the Certificate Import Wizard window.
9. Click **All Tasks** > **Import**.
10. On the Certificate Import Wizard page, select **Local Machine** and click **Next**.
11. Click **Browse**.
12. To import the Docker registry certificate that was exported earlier, select the file, and click **Open**.
13. Click **Next**.
14. Select the **Place all certificates in the following store** check box.
15. Ensure that in the **Certificate store** field, the specified location is `Trusted Root Certification Authorities`.
16. Click **Next**.
17. On the Completing the Certificate Import Wizard page, verify that the settings that you have selected are correct, and click **Finish**.

    The Certificate Import Wizard page displays the following message:

    `The import was successful`

18. In the Windows icon tray, click the Docker whale icon and click **Restart**.
19. Verify that the connection is successful with CCM local Docker registry. Run the following commands within the ccm-ctl-agn deployed container:
    a. To log in, run: `docker login < ccm fqdn >:5010`
    b. When prompted, enter the `Username` and `Password` of the CCM local Docker registry
    c. To log out, run: `docker logout < ccm fqdn >:5010`

    Log in and log out operations are successful.

Deploying Avaya Analytics™ offline using Windows Subsystem for Linux

Windows Subsystem for Linux setup

The following sections provide high-level setup information for Windows Subsystem for Linux (WSL) used in offline air-gap network deployments. WSL offers a lightweight Linux environment on Windows, enabling the execution of Linux-based tools and commands required for container and image management.

In this setup, WSL is used to run the `ccm-agn-wsl` environment and perform tasks such as handling container images, certificates, and related artifacts needed for offline deployments.

In an air-gap deployment, the target environment, including the Cluster Control Manager (CCM), does not have access to the public internet. A separate client system with internet access is used to download the required artifacts, which are then securely transferred to the air-gap environment.

The WSL environment facilitates these operations by providing a consistent Linux runtime for managing solution images, certificates, and container workflows. For more detailed procedures and configuration guidelines, see your solution documentation.

Planning and preconfiguration

Before configuring WSL, do the following:

- Ensure the following specifications are available on your computer:
  - Windows 10 or 11, Professional or Enterprise, 64-bit operating system.

    Note:

    WSL deployment does not support Windows 10 Home and Windows PowerShell ISE.
  - Free memory: 2 GB
  - CPU: 2.0 GHz or higher

- Available disk memory:
  - 100 GB for regular offline installation, when you run files directly from client container to the CCM using the `agn` upload command.
  - 140 GB for manual transfer, because further steps require additional disk space.
- Windows local account administrator privileges to install WSL for Windows.

- You must have basic knowledge of Windows PowerShell, Linux, Docker, and CCM.
- Contact Avaya to ensure you can deploy the software using your SSO credentials
- Ensure that the client computer has internet access to download artifacts from the Avaya repository.
- If you are using a virtual machine (VM) running on Windows 10 or 11, ensure that you enable the BIOS-level hardware virtualization in BIOS settings.
- On a VM, select **Hardware Virtualization**, from the **Edit Settings** > **CPU** drop-down list. Shut down the VM to change the option.

Preinstallation checklist

Download the following files from PLDS before installing Avaya Common Services (CSP) in an air-gap environment using WSL:

- The CCM AGN controller container startup WSL file (`ccm-ctl-agn-x.x.xx-wsl.zip`) from PLDS.

  Note:

  For example, `ccm-ctl-agn-1.3.09-wsl.zip`.

- The WSL distribution file (`ccm-agn-wsl-x.x.xx.tar`) from PLDS.

  Note:

  For example, `ccm-agn-wsl-1.3.07.tar`.

Installing Windows Subsystem for Linux (WSL)

About this task

You can install and configure Windows Subsystem for Linux (WSL2) to provide a light-weight Linux environment on Windows, which is required to run the CCM air-gap tooling and Docker within WSL.

Before you begin

Ensure the following specifications are available on your computer:

- Windows 10 or 11, Professional or Enterprise, 64-bit operating system.
- Local administrator privileges to enable Windows features.
- Hardware virtualization is enabled (required for WSL2).

- An active internet connection to download and update WSL components.

Procedure

1. Click **Windows Start** icon or **Windows Search** icon and search `Turn Windows features on or off`.
2. On the Windows Features pop-up, select **Virtual Machine Platform** and **Windows Subsystem for Linux**.
3. Click **OK**.
4. After the installation is complete, click **Restart Now**.

Configuring Windows Subsystem for Linux

About this task

You can configure WSL2 and import the CCM-provided WSL distribution image. The WSL configuration creates a Linux runtime environment on Windows, which is required to run the CCM air-gap tooling and container-based operations.

Before you begin

Ensure the following:

- You have local administrator privileges to run PowerShell commands.
- Download the CCM WSL distribution image (`ccm-agn-wsl-x.x.xx.tar`) from Avaya support PLDS.
- Windows features **Windows Subsystem for Linux** and **Virtual Machine Platform** are enabled.

Procedure

1. Click **Windows Start** icon or **Windows Search** icon and search `Windows PowerShell`.
2. In Windows PowerShell console, run `wsl --update` to update the WSL feature.
3. To verify successful completion of WSL 2 configuration, run `wsl --status`. Ensure that the output displays **Default Version: 2**.
4. To create a new directory, do the following:
   a. To navigate to the C drive, run `cd C:\`.

      You can use any drive available. In this procedure, C drive is used as an example.

   b. To create a new directory, run `mkdir "C:\avaya\ccm-wsl" -Force`.
5. Download and copy the `ccm-agn-wsl-x.x.xx.tar` CCM WSL distribution image file to the `C:\avaya\ccm-wsl` directory.
6. To change the directory to `C:\avaya\ccm-wsl\`, run `cd C:\avaya\ccm-wsl\ .`
7. To import the CCM WSL distribution image file (`ccm-agn-wsl-x.x.xx.tar`), run `wsl --import ccm-agn-wsl-x.x.xx C:\avaya\ccm-wsl\ .\ccm-agn-wsl-x.x.xx.tar --version 2`.

Note:

For example, `wsl --import ccm-agn-wsl-1.3.07 C:\avaya\ccm-wsl\ .\ccm-agn-wsl-1.3.07.tar --version 2`.

8. To verify the import of WSL image, run `wsl -l -v`.

Note:

A successful import displays the imported WSL distribution (for example, `ccm-agn-wsl-x.x.xx` with state as **Stopped** and **Version 2**.

Starting the ccm-agn-wsl image

About this task

To start the `ccm-agn-wsl` image, you have to first start with `ccm-agn-wsl` WSL distribution, which provides the Linux runtime environment required for executing the CCM air-gap commands and container operations

Before you begin

Ensure to import the `ccm-agn-wsl` WSL distribution.

Procedure

1. Click **Windows Start** icon or **Windows Search** icon and search `Windows PowerShell`.
2. In Windows PowerShell console, run `cd C:\avaya\` and then `wsl -d ccm-agn-wsl-x.x.xx`. For example, `wsl -d ccm-agn-wsl-1.3.07`

Note:

- The Windows drive is available under `/mnt` directory within the WSL console. For example, `/mnt/c`.
- Ignore the following warning displayed during WSL startup:

  "`wsl: Failed to start the systemd user session for 'root'. See journalctl for more details.`"

  This warning does not affect the `ccm-agn-wsl` environment functionality or CCM air-gap operations.

Stopping the ccm-agn-wsl image

About this task

Use this procedure to stop the `ccm-agn-wsl` WSL distribution when it is no longer required or before performing cleanup or maintenance activities. This step is optional and needed only when you want to end the active WSL session.

Procedure

In the `ccm-agn-wsl` WSL console, run `exit`.

The WSL session and the `ccm-agn-wsl` image stop.

Note:

To verify the status, run `wsl -l -v` in the PowerShell console.

Removing the ccm-agn-wsl image

About this task

Use this procedure to remove the `ccm-agn-wsl` WSL distribution when it is no longer required. This step is optional and you must perform it only if you want to clean up the environment or reinitialize the setup.

Procedure

In Windows PowerShell console, run `wsl --unregister ccm-agn-wsl-x.x.xx`. For example, `wsl --unregister ccm-agn-wsl-1.3.07`.

The `ccm-agn-wsl` WSL distribution is removed.

Note:

To verify the status, run `wsl -l -v` in the PowerShell console.

Adding proxy CA certificate to ccm-agn-wsl truststore

About this task

Use this procedure to install the required proxy and enterprise CA certificates in the `ccm-agn-wsl` truststore. Installing CA certificates ensures that the HTTPS communication with the Avaya Harbor registry is secure while using proxy or custom certificate authorities.

Before you begin

- Ensure that you install and start the `ccm-agn-wsl` distribution.
- Download the required proxy CA certificate files.
- Ensure that the certificates are in Base64 (.crt) or DER format.

Procedure

1. Copy the proxy CA certificates to `C:\avaya\cacerts` Windows directory
2. In the `ccm-agn-wsl` console, run `cp /mnt/c/avaya/cacerts/*.crt /etc/pki/ca-trust/source/anchors/` to copy the certificates to the truststore location.
3. To verify if the certificates copied successfully, run `ls /etc/pki/ca-trust/source/anchors/`.
4. To update the truststore, run `update-ca-trust extract`.
5. To restart the Docker service, run `systemctl restart docker`

Result

The proxy CA certificates are installed and the Docker securely communicates with external Avaya Harbor registries, within WSL.

Obtaining the ccm-ctl-agn image from Avaya Harbor

About this task

Download the `ccm-ctl-agn` container image from the Avaya Harbor registry to the Docker environment running within WSL. Use this image to start the CCM Air-Gap Network (AGN) container.

Procedure

1. To start the `ccm-agn-wsl` distribution image, run `wsl -d ccm-agn-wsl-x.x.xx`. For example, `wsl -d ccm-agn-wsl-1.3.07`.
2. In the `ccm-agn-wsl` console, run `docker login harbor.avaya.com` to log in to the Avaya Harbor registry.
3. In the **Username** field, enter your Avaya SSO username.
4. In the **Password** field, enter your Avaya SSO password.
5. In the `ccm-agn-wsl` console, run `docker pull harbor.avaya.com/flex/ccm-ctl-agn:x.x.xx`. For example, `docker pull harbor.avaya.com/flex/ccm-ctl-agn:1.3.09`.
6. To verify successful image download, run `docker image ls`.

Result

The `ccm-ctl-agn` image is cached in WSL Docker and is used to start the AGN container.

Obtaining Cluster Control Manager (CCM) Air-Gap Network controller container startup WSL file

About this task

Use the Cluster Control Manager air-gap network controller image to create the container on the client computer. You can use this container to pull Avaya CSP application from Avaya repository and later push it to CCM within the air-gap environment.

Before you begin

- Ensure you can download the application using your Avaya SSO credentials.
- Obtain the available `ccm-ctl-agn-x.x.xx-wsl.zip` file from PLDS. For example, `ccm-ctl-agn-1.3.09-wsl.zip`

Procedure

1. Copy the `ccm-ctl-agn-x.x.xx-wsl.zip` file PLDS to `C:\avaya` folder.

Note:

For Avaya™ products, download the script from PLDS associated with the Avaya™ product.

For example, Avaya Analytics™.

2. Extract the `ccm-ctl-agn-x.x.xx-wsl.zip` file contents to obtain the `ccm-ctl-agn-x.x.xx.wsl` file.

Starting Cluster Control Manager Air-Gap Network container

About this task

Use the startup script to start the CCM CTL AGN container inside WSL environment.

Note:

This procedure is executed on Windows C drive. Run the script on Windows drive where you have configured `ccm-agn-wsl`.

Procedure

1. To start the `ccm-agn-wsl` distribution image, run `wsl -d ccm-agn-wsl-x.x.xx`. For example, `wsl -d ccm-agn-wsl-1.3.07`.
2. To change Windows directory within WSL, run `cd /mnt/c/avaya`.

   Note:

   In WSL, Windows drives are available under `/mnt`.

   For example, `/mnt/c`.
3. Run the AGN startup script, `/mnt/c/avaya/ccm-ctl-agn-x.x.xx.wsl`. For example, `/mnt/c/avaya/ccm-ctl-agn-1.3.09.wsl`.

   Note:

   If AGN image is not available in the local Docker cache, the script prompts for Avaya SSO credentials to download the image.
4. When the container starts and the prompt changes, run the command `agn` to display the available AGN commands for managing Air-Gap operations.

Result

The CCM CTL AGN container successfully starts and is ready for use.

Obtaining Cluster Control Manager registry CA certificate for WSL distribution

About this task

In an offline air-gap deployment, secure communication with the CCM local Docker registry requires installing the registry's CA certificate within the WSL environment. This procedure extracts the certificate from the CCM registry and installs it in the Docker truststore within WSL.

Before you begin

Ensure the following:

- You complete the offline deployment setup on the CCM.
- ChartMuseum and Docker are running on CCM.
- You have access to the CCM registry host with **cust** user credentials.
- The `ccm-agn-wsl` distribution is running.

Procedure

1. Log in to the CCM registry host with `cust` user credentials.
2. To retrieve the certificate chain and save it as `ca.crt`, run `openssl s_client -connect <ccm-fqdn>:5010 -showcerts </dev/null | sed -n '/BEGIN CERTIFICATE/,/END CERTIFICATE/p' > ca.crt`.

   Note:

   The following OpenSSL warning can display after CSP cluster deployment due to internal or self-signed certificates:

   Warning:

   Unable to get local issuer certificate / unable to verify the first certificate.

   You can ignore the warning, as the `ca.crt` certificate generates successfully.
3. Copy the extracted certificate to `C:\avaya\cacerts` WSL Windows host folder.
4. If you are in the `ccm-ctl-agn` container shell, type `exit` to return to the WSL distribution shell.
5. To install the docker certificate in the WSL distribution shell, do the following:
   a. To create the Docker registry certificate directory, run `mkdir -p /etc/docker/certs.d/<ccm-fqdn>:5010`.
   b. To copy the certificate from Windows folder, run `cp /mnt/c/avaya/cacerts/ca.crt /etc/docker/certs.d/<ccm-fqdn>:5010/`.
6. To update the truststore, run `update-ca-trust extract`.
7. To restart the Docker service, run `systemctl restart docker`.
8. To verify access to the registry, run `docker login <ccm-fqdn>:5010`.

Note:

The login is successful, if the CCM registry CA certificate is correctly installed.

Next steps

If login is successful, the CCM registry CA certificate installs correctly and there is secure communication between the CCM registry and the Docker within WSL.

Preparing the deployment spreadsheet

About this task

Use this procedure to install Avaya Analytics™ with High Availability (HA) configuration by using the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. You must enter the configurable values in the spreadsheet manually. The minimum supported version of MS Excel is 2016.

Before you begin

- Download the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file from PLDS.
- Enable the macros before you start editing the worksheets.
- Select the deployment types by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file. Complete the fields with the customer details that correspond to each deployment type, such as IP addresses and passwords.

  Note:

  The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Orca** tab.
3. In the **Number Of Agents** field, click one of the following options:
   - Agent 100
   - Agent 500
   - Agent 1000
   - Agent 2000
   - Agent 4500

4. Set the **Customize Processors to Install** field to `TRUE` to customize which measure processors get deployed.
   a. For **Routing Service Group Measure Processor**, set the **Install** field to `TRUE` if routing service real-time reporting is required.
   b. For **Agent Trace Measure Processor**, set the **Install** field to `TRUE` if agent trace historical reporting is required.

   Note:

   Enabling Routing Service Group Measure Processor and Agent Trace Measure Processor increases the cluster footprint resource, such as memory, CPU and disk storage, requirements.

   During fresh installation or after migrating to Avaya Analytics™ 4.3.1.1 cluster, you must set the Agent Trace Measure Processor and Routing Service Group Processor to `TRUE` before deploying the Avaya Analytics™ 4.3.1.1 cluster.
5. Click the **Deployment Properties** tab.
6. Set **Node Affinity Enabled** to `TRUE`.
7. Complete the configurable fields in the spreadsheet.

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.
8. For enabling Cross-Origin Resource Sharing (CORS), in CORS field, enter a URL:

   The field value should be taken from the origin field of the HTTP request to the orca-streams-rest and orca-streams-data-publisher. For example, Go to **WORKSPACES** > **Chrome** > **Developer tools** > **Network** > **XHR** > **any orca-streams-rest URL**.

   Note:

   Once these fields are configured in deployment spreadsheet, there is no need to install CORS chrome plugin additionally.

Downloading Avaya Analytics™ chart and images

About this task

You must download the Avaya Analytics™ chart and images from Avaya to the Windows PC or client computer.

Important:

- This procedure and all the following procedures are applicable for both offline deployment methods, Docker desktop for Windows and WSL (Windows Subsystem for Linux).

- This procedure assumes that you have configured Docker Desktop file sharing for the `c:\` drive of your Windows client.

Before you begin

- Ensure that your Avaya SSO credentials allow you to download the software successfully.
- Get the `Avaya_Oceana_Application_Deployment.xlsm` file.
- Start the Cluster Control Manager air gap network container, ccm-ctl-agn, on your PC.

Procedure

1. On your Windows PC or client computer, save the `Avaya_Oceana_Application_Deployment.xlsm` file in `c:\avaya\downloads`.

   Note:

   Windows and the Cluster Control Manager Controller container share mount points, which are `c:\avaya\downloads` and `/root/downloads`, respectively.

2. In the ccm-ctl-agn container, run the following command:

   `cd /root/downloads`

3. Run the following command and verify that the page displays the excel file:

   `ls`

4. To download the Avaya Analytics™ charts and images from the Avaya repository, run the following command:

   `agn download Avaya_Oceana_Application_Deployment.xlsm`

5. In the **Avaya SSO User** and **Password** fields, enter your Avaya SSO credentials.

   The agn script processes the excel spreadsheet, and the Avaya Analytics™ charts and docker images start downloading. The ccm-ctl-agn container displays an Image Pull Report when the download is complete.

6. To view a list of the downloaded images, run the following command:

   `docker image ls`

7. To view a list of the downloaded charts, run the following command:

   `ls /root/downloads/*.tgz`

8. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-ctl-agn container at `/var/log/avaya/ccm/ccm-main.log`.

   For more information on possible issues and the respective troubleshooting solutions, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* doc.

Setting up Cluster Control Manager for Avaya Analytics™ offline deployment

About this task

You must set the username and password in the Cluster Control Manager (CCM) console to secure access to the CCM local docker registry and chartmuseum.

Before you begin

Install Cluster Control Manager (CCM) OVA in the air gap environment.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the following command:

   ```
   agn-ctl setup
   ```

3. At the prompt, enter an alpha-numeric username for the CCM local ChartMusem and Docker registry.
4. Enter an alpha-numeric password for the CCM local ChartMusem and Docker registry.
5. Re-enter the alpha-numeric password for the CCM local ChartMusem and Docker registry.
6. Note down the username and password for future use.

Starting ChartMuseum and Docker registry on Cluster Control Manager

About this task

Use this procedure to start the offline deployment repositories on Cluster Control Manager.

Before you begin

Set up Cluster Control Manager for offline deployment.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the **`agn-ctl start`** command.

Stopping ChartMuseum and Docker registry on Cluster Control Manager

About this task

Use this procedure to stop the offline deployment repositories on Cluster Control Manager.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the **`agn-ctl stop`** command.

Uploading Avaya Analytics™ chart and images with limited access to Cluster Control Manager

About this task

You must upload the Avaya Analytics™ chart and images from the Windows PC or client laptop to Cluster Control Manager (CCM).

Before you begin

- Depending on the offline deployment method used, Docker desktop or WSL, load the CCM CA certificates.
- Get the CCM hostname.
- Get the CCM local docker registry username and password that you noted down.
- Setup Cluster Control Manager for Avaya Analytics™ offline deployment.
- Start ChartMuseum and Docker registry on Cluster Control Manager.

Procedure

1. Connect to your air gap network using your Windows PC or laptop.
2. Start the ccm-ctl-agn container based on the deployment method used.
   - For Docker Desktop (Windows PowerShell):

     Run: `C:\avaya\ccm-ctl-agn.bat`.
   - For WSL-based deployment:

     Run the `ccm-ctl-agn` container from the WSL distribution using command: `/mnt/c/avaya/ccm-ctl-agn.wsl`.
3. Using the ccm agn deployed container, run the following command: **`agn upload <CCM FQDN>`**, where <*CCM FQDN*> is the FQDN of your CCM.
4. To access the CCM docker registry and ChartMuseum, enter the username when prompted.

5. Enter the password.
6. Re-enter the password.

   The agn command starts the following in a sequence:

   a. Processes the available chart and image data on the Windows PC or laptop.

   b. Starts uploading the charts and images to CCM. When the upload is complete, the console displays an image push report.
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-ctl-agn container at `/var/log/avaya/ccm/ccm-main.log`.

   For more information on possible issues and the respective troubleshooting solutions, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.
8. To copy the `Avaya_Oceana_Application_Deployment.xlsm` file, run the following command in the ccm-ctl-agn container:**`scp /root/downloads/Avaya_Oceana_Application_Deployment.xlsm <ccmUser>@<CCM FQDN>:`**, where <*ccmUser*> is the CCM customer login account and <*CCM FQDN*> is the FQDN of your CCM.

   Note:

   Do not skip the colon at the end of the command.
9. In the **Are you sure you want to continue connecting** field, type `yes` and press **Enter**.
10. At the prompt, enter the CCM user password.

    The ccm-ctl-agn container uploads the images and charts, which you earlier downloaded on the Windows PC or client laptop, into the local CCM docker registry and chartmuseum.

Confirming that the local Cluster Control Manager registry and ChartMuseum are running

About this task

You must confirming that the local Cluster Control Manager (CCM) registry and ChartMuseum are running before installing Avaya Analytics™ offline.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the following command:

   `agn-ctl status`
3. Verify that the following ports display the stats as `ACCEPT`:

   - ChartMuseum port 5011

- Registry port 5010

4. Verify that the CCM local registry status displays `UP`.

Air gap network: Uploading Avaya Analytics™ chart and images with restricted access to Cluster Control Manager

The following sections outline the steps to use the ccm-ctl-agn container to download the solution images to a computer and then save each image as a gzip file. On Cluster Control Manager, the `agn` command is used to load the solution's gzip images and charts onto the Cluster Control Manager local Docker registry and chart museum repository.

Note:

This procedure is optional, it is only applicable in an offline air gap network environment.

Saving the solution images as gzip files

About this task

Save each solution image as a gzip file. Perform this procedure using the `ccm-ctl-agn` container.

Before you begin

- Download the chart and images to the laptop using the Cluster Control Manager air gap network container.
- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

1. Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn save` command to save the downloaded images for the solution as a set of gzip images.
2. From the `/root/downloads` directory of the running `ccm-ctl-agn` container, run the `tar -zcvf downloads.tgz ../downloads` command.
3. Transfer the tar file to Cluster Control Manager using a thumb drive or a similar media device.

   The file path in Windows is `C:/Avaya/Downloads/downloads.tgz`.

Uploading the solution gzip images and charts onto Cluster Control Manager

About this task

Upload the solution gzip images and charts onto the Cluster Control Manager local Docker registry and chart museum using the `agn` command on Cluster Control Manager.

Before you begin

- Save each solution image as a gzip file.
- Transfer the solution `downloads.gzip` file to the `/var/avaya/artifactCache` directory on Cluster Control Manager.
- Set up Cluster Control Manager for offline deployment.
- Start ChartMuseum and Docker registry on Cluster Control Manager.

Procedure

1. On Cluster Control Manager, extract the Downloads tar file using `tar -zxvf downloads.tgz` to the `/var/avaya/artifactCache` directory if enough space is available.

   You can run `df -h` to see how much disk space is available. If the tar file is larger than half the disk space available, extract the file to a different server in the air gap network and then transfer it to Cluster Control Manager using an SCP client.

2. Run `agn load -d <full path to Downloads directory> -h <Cluster Control Manager FQDN>` to upload the solution gzip images and charts.

   The following is an example of this command:

   ```
   agn load -d /var/avaya/artifactCache/downloads -h ccm.server.example.com
   ```

3. When prompted, enter the user name and password to access the local Cluster Control Manager Docker registry and chart museum.

Result

After you upload all images and charts, the Cluster Control Manager local Docker registry and chart museum are staged for cluster deployment.

Removing the downloaded solution images from your computer

About this task

After you upload the images and charts to Cluster Control Manager, you can delete the downloaded images from your computer's Docker cache. Perform this procedure using the ccm-ctl-agn container.

Before you begin

- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn clean` command to delete the downloaded solution images.

This operation can take up to 5 minutes to complete.

Installing Avaya Analytics™ offline

About this task

You must upload the Avaya Analytics™ files from the Windows PC or laptop to Cluster Control Manager (CCM).

Use the Screen utility while installing Avaya Analytics™. Screen is a Linux command with which you can detach from an SSH session and reattach later. Using the Screen utility avoids issues where the SSH session can disconnect after timing out, thereby interrupting the install.

Important:

Ensure that you are familiar with the Screen utility. For detailed information about using Screen, enter the **`man screen`** command.

Before you begin

- Configure CCM.
- Update the macros-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to suit your deployment type.
- Copy the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to the CCM server.
- Confirm that the local CCM Docker registry and ChartMuseum are running.
- For high availability, deploy 3 or more cluster nodes by setting values for CPU, memory, and disk. Refer to *Deploying Cluster Nodes* chapter in this guide.
- Modify the cluster node VMs running with the vCPU, memory, and disk allocation as stated in the solution configuration spreadsheet. Cluster node VMs must be running with the vCPU memory and disk allocation as stated in the solution spreadsheet.
- If you are deploying with high availability enabled (three master nodes) you must create an anti-affinity rule in your vCenter for your cluster nodes.

  If DRS is enabled, the vCenter administrator must create a DRS anti-affinity rule and include all master cluster node VMs in the rule.

  If DRS is disabled, the vCenter administrator must ensure that the VMs for the master cluster nodes are deployed on separate hosts if HA is required.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. From the directory on CCM that contains the excel file, enter the following command:

   `screen`

   The Screen utility runs the install in the background.

   Warning:

   Do not skip this step.

3. Run the following command:

   ccm install Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm

4. At the prompt, do the following:

   a. Enter your Avaya SSO credentials.

      You must enter the CCM local registry username and password configured with the **agn-ctl setup** command earlier.

   b. Accept the EULA.

   c. When prompted, either enable or do not enable the High Availability Audit feature.

      To enable the feature, respond `Y` to give the cluster deployment vCenter access.

      `Y` – Enable the High Availability Audit feature and grant deployment vCenter access for the cluster. The solution configuration spreadsheet must also set high_availability to `enabled`.

      `N` – Do not grant deployment vCenter access for the cluster, and do not enable the High Availability Audit feature.

      Example:

      ```
      The following features will be enabled if this cluster
      deployment is allowed vCenter access.
      - High Availability Audit

      Do you want to allow this cluster deployment vCenter access?
      (Y/N)
      ```

   d. Enter the vCenter user ID and password.

   e. Re-confirm the password.

   The installation installs the following downloads:

   - The base cluster software
   - The common services platform software
   - The Avaya Analytics™ software

   Note:

   The installation takes several hours to complete.

5. Run the following command in a seperate window to monitor the progress of the install:

   tail -f /var/log/avaya/ccm/ccm-main.log

   During the installation, the software creates folders and virtual machines on the host machines that are visible in the vCenter of the host.

6. If you want to disconnect from the SSH session and want the install to continue in the background, do the following:
   a. Disconnect from the SSH session
   b. When you want to reconnect to the SSH session, start a new SSH session to CCM and connect using the customer account
   c. To retrieve the Screen ID of the session that is running the installation, type `screen -ls`
   d. To reattach to the installation Screen session, type `screen -dr <screen id>`

      See the following example command to reattach to the installation Screen session:

```
[cust@examplelab ~]$ screen -ls
There is a screen on:
            9069.avaya.examplelab    (Detached)
1 Socket in /var/run/screen/S-cust.
[cust@examplelab ~]$ screen -dr 9069.avaya.examplelab
```

7. To check if the installation is successful, run the following command on the CCM console:

   `ccm status`

   The CCM console displays the status details as follows:

   - If the Status column displays the status as `deployed`, it indicates that all the components are currently deployed to the cluster.
   - If the Status column displays the status as `Staged` or `''`, it indicates that the software is staged on the system, but not deployed.

     The tools-policy and utility-services remain in a `staged` state.

     Note:

     You might see this status in the older versions of the software after a upgrade.
   - If the Status column displays the status as `Error`, it indicates that the components failed to install.

   Important:

   If the installation fails, run the **`ccm install cancel`** command, resolve the issue causing the failure, and restart the installation procedure. For more information about troubleshooting installation failures, see *Maintaining and Troubleshooting Avaya Analytics™*.

8. Delete the spreadsheet from CCM after the deployment is complete. Ensure you keep a copy of the spreadsheet and store it in a secure location.

   This step is important to save the passwords and other configuration details that you entered as plain text for the deployment.

9. Stop the local CCM Docker registry and ChartMuseum. See section *Stopping ChartMuseum and Docker registry on ClusterControl Manager* in this section.

Chapter 11: Deploying Messaging

Deployment details for Messaging overview

Before commencing the installation process for Messaging, you must first have the following details:

Cloud Provider

A cloud provider account must be created for each customer to enable the delivery of messages to or from the end-user device. It acts as a gateway for messaging events.

The Avaya DevOps team provisions the cloud provider account with the following information:

- App ID
- Cloud Provider Key
- Cloud Security Key (Secret)

Avaya Oceana® details

You must have the following details specific to Avaya Oceana®:

- FQDN/IP address of Avaya Oceana® Cluster 3 where CustomerControllerService is installed
- System Manager Certificate Authority (CA)
- Avaya Oceana® Cluster Identity Certificate
- Credentials of a valid Avaya Breeze® user for file transfer

Avaya Common Services (Common Services) Cluster

Messaging is installed on the Avaya Common Services cluster. When you install Common Services, it creates and FQDN/IP address for inbound traffic into the cluster. You must obtain this FQDN/IP address to allow the cloud provider to send customer Messaging requests to the Async tool and Avaya Oceana®, so that the requests can be replied.

Based on your hardware configuration, you might also have an external load balancer that maps to the FQDN/IP address.

Note:

This Messaging deployment is applicable for customers who deploy Avaya Analytics™ and Messaging on the same platform. This deployment does not apply to the non-HA/Lab deployment of Avaya Analytics™.

Prerequisites

If you already deployed an older version of Messaging, you must log in to the Cluster Control Manager (CCM) console and remove the earlier version by running the following command:

```
ccm delete async
```

Ensure that you delete all instances of the earlier version of Messaging by running the following commands:

```
kubectl get pvc --all-namespaces | grep async
kubectl delete pvc file-transfer-tmp-dir-async-file-transfer-0 file-transfer-tmp-dir-async-file-transfer-1
```

To confirm that all instances of the earlier version of Messaging are deleted, run the following commands:

```
kubectl get pods --all-namespaces |grep async
kubectl get pvc --all-namespaces |grep async
kubectl get virtualservices --all-namespaces |grep async
kubectl get services --all-namespaces |grep async
```

Profanity message filter overview

The profanity filter helps you block the sending and receiving of responses to customers and agents if it contains profanity words. It is important to immediately identify the sensitive words used in the conversations and notify if they contain profanities.

The profanity filter works based on the value of the FilterEnabled flag. The filtering service scans the message and masks any text it does not want the destination party to see.

Note:

The adopting client is responsible for implementing the filtering service.

When the profanity filter is enabled, all messages sent from the end user to the contact center or from the agent to the end-user result in a call to the configured REST service. The following fields form part of the request:

- Message Text
- Channel Source
- Sender
- Destination

The filter service responds within the timeout window, set by default to 5 seconds. If the filter service is enabled and no response is received from the service call within the configured timeout period, each message raises an alarm. The Time out filter ensures the administrator is notified that the filtering service is unreachable or slow in responding.

After the timeout period, the async message is processed as normal and the original message is sent to the end-user or agent as normal.

A workrequestID is generated and sent to the profanity filter for all messages sent from EndUser to Agent. The sendWorkRequestID parameter is added to the deployment.yaml file in AsyncMsgConnector to enable or disable this functionality.

Configuring the Avaya Analytics™ deployment spreadsheet for Messaging

About this task

The deployment of Avaya Analytics™ is done through the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. To deploy Messaging, you must configure the values on the **Messaging** tab in the spreadsheet.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Deployment Properties** tab.
3. Set the **Install Async Messaging** field to `TRUE`.
4. On the Async tab, configure the following attributes for the Cloud Provider and Avaya Oceana®:

Attribute	Description
config:async-aggregator-interface:tenantmapping:aggregator:applicationId	The Application ID that is analogous with a Tenant ID. It is the Cloud Provider ID that is created with every new Messaging installation. The Avaya DevOps team provides this ID.
config:async-aggregator-interface:tenantmapping:aggregator:jwt:keyid	The Cloud Provider key. The Avaya DevOps team provides this key.
config:async-aggregator-interface:tenantmapping:aggregator:jwt:security	The Cloud security key. The Avaya DevOps team provides this key.
config:async-aggregator-interface:tenantmapping:aggregator:uri	The Cloud Provider API address zone. Using this attribute, you can determine at the time of installation whether the AWS instance is US data center or EU data center. You can select the data center in the deployment Excel file. Once you deploy it, you cannot change the data center. The default value is **US** data center.

Table continues…

Attribute	Description
config:async-oceana-adapter:oceana:clientcontroller:host	The FQDN of Avaya Oceana® cluster 3 where CustomerControllerService is installed. For example, your-cluster.async.oceana.com **Note:** • The FQDN must be all lowercase and must follow the valid FQDN guidelines. • You can explicitly specify a port number with the FQDN. For example, your-cluster.async.oceana.com:433. By default, the system uses the port number 443 for wss and port number 80 for ws.
config:async-oceana-adapter:oceana:contactPriority	The contact priority that you must set for every new contact in Async. Enter a value between `1` and `10`, in which 1 is the highest priority and 10 the lowest.
config:async-oceana-adapter:oceana:clientcontroller:protocol	The CustomerControllerService API provides the following two types of protocols based on the setup: • Secure web socket (wss) This protocol requires manual steps to configure System Manager Certificate Authority (CA) and Identity Certificates. • Non-secure (ws)
config:async-oceana-adapter:oceana:defaultAttributes	Default routing attributes for Messaging interactions.
config:async-oceana-adapter:service:reversedns:ip	The IP address of Avaya Oceana® cluster 3.
config:async-oceana-adapter:service:reversedns:hostnames[0]	The FQDN of Avaya Oceana® cluster 3. Ensure that the entries consist of lower case alphanumeric characters and "-" or ".". Also ensure that the entries start and end with an alphanumeric character.

Table continues…

Attribute	Description
config:async-file-transfer:filetransfer:oceana:storageEndpoint	The FQDN of Avaya Oceana® cluster 3 where CustomerControllerService is installed. For example, your-cluster.async.oceana.com **Note:** • The FQDN must be all lowercase and follow the valid FQDN guidelines. • You can explicitly specify a port number with the FQDN. For example, your-cluster.async.oceana.com:433. By default, the system uses the port number 443 for wss and port number 80 for ws.
config:async-file-transfer:filetransfer:oceana:user	The user name of the default user that authenticates file transfer uploads into Avaya Oceana®. The user must able to login to Avaya Workspaces. **Important:** Ensure that this user is created before the installation and is not shared by any other application.
config:async-file-transfer:filetransfer:oceana:password	The password of the default user that authenticates file transfer uploads into Avaya Oceana®.
config:async-file-transfer:filetransfer:oceana:publicStorageChannels	The list of social media channels.
config:async-aggregator-interface:tenantmapping:contactcenter:connectionLivelinessTimeout	Optional. The time in seconds, which sets the liveliness connection threshold between Async messaging services. This is an optional attribute.
config:async-aggregator-interface:tenantmapping:aggregator:deliveryFailure:message	The status message displayed when the application is down. For example: `Dear Customer, our services are currently unavailable. Please try again later.`
config:async-oceana-adapter:tryAgainLaterMessage	The status message displayed when the application cannot create a WebSocket because of the "too many open files" error. For example: `Dear Customer, our service is currently under a heavy load. Please try again later.`

Table continues…

Attribute	Description
config:async-oceana-adapter:profanityFilterService:endpoint	Endpoint for the Profanity Filter server that validates messages using a REST API call. The default value is: `http://localhost:8099/filter`
adapter:oceana:addIntegrationAttribute	Optional. If enabled, additional routing attribute is added for Messaging Interactions. This attribute includes information about channel from which message is received with `MessagingChannel` prefix. For example, `MessagingChannel.twitter` or `MessagingChannel.web`. Channel values are: `web - android - ios - messenger - whatsapp - twitter Switched off (false)` by default.
config:async-oceana-adapter:oceana:addIntegrationAttribute	Default value is false, optional. *Optional. If enabled, additional routing attribute is added for Messaging Interactions. This attribute includes information about channel from which message was received with “MessagingChannel” prefix. For example, “MessagingChannel.twitter”, “MessagingChannel.web”. The channel values are: • web • android • ios • messenger • whatsapp • twitter Switched off (false) by default.
config:async-oceana-adapter:Filter Service REST Url	Default value is Blank. Path to a filtering service that may be used to remove offensive text from messages. This is an optional field.

Table continues…

Attribute	Description
config:async-oceanaadapter:Filter Service Timeout	Default value is 5. Value is in seconds for the async-oceana-adapter to wait for a response from the filtering service. If no response is received within the timeout period, the original unfiltered message is used.
config:async-oceanaadapter: FilterEnabled flag	Default value is FALSE. The flag indicates if the filtering service should be called. True indicates the filtering service (if a URL is set) will be called. False (or no URL set) will bypass the filtering service.
config:async-oceanaadapter: SilentAlarms flag	Default value is TRUE. The flag indicates if an SNMP alarm shall be raised when the filter is enabled and the timeout period is exceeded. If TRUE, no alarm is raised but a log entry is created. If FALSE, an alarm is raised for each message where the timeout occurs.

5. In the **Product to Install** field, select **async (Async Messaging)**.
6. Continue with the installation steps of Avaya Analytics™.
7. If the cluster is already deployed, run the following command to add Messaging:

```
ccm upgrade spec
"Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm" --
products --force
```

Note:

Async pods start in a 0/1 Ready state by design. The force option skips this check and continues with the upgrade.

Post-installation configuration for Messaging

After deploying messaging, you must complete the post installation configuration by running a set of commands.

Configuring the System Manager Certificate Authority

About this task

Use this procedure to configure the System Manager Certificate Authority (CA).

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   `ccm release async updateSystemManagerCert.sh`
4. On the **SystemManager.pem CA** prompt, type the System Manager CA `.pem` file name.
5. At the prompt **Do you wish to add the SystemManager.pem to the file transfer facility Y/N:**, enter `y`

   If you enter `n`, the operation is terminated.

   Note:

   It is recommended to add System Manager certificate to the File Transfer pods to use the file transfer functionality in a secure way.

Configuring the Cloud Provider certificate

About this task

Use this procedure to configure the Cloud Provider certificate when calling the external public API, smooch.io.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   `ccm release async updateCooperateProxyCert.sh`
4. On the **CooperateProxyCert.pem** prompt, type the *`<Cloud Provider certificate>`*`.pem` file name.
5. At the prompt **Do you wish to add the CorporateProxyCert.pem to the file transfer facility Y/N:**, enter `y`

   If you enter `n`, the operation is terminated.

   Note:

   It is recommended to add Cloud Provider certificate to the File Transfer pods to use the file transfer functionality in a secure way.

Configuring a reverse DNS

About this task

Use this procedure to configure a reverse DNS if Avaya Oceana® is not on a DNS server and you are connecting over a secure WebSocket.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   ```
   ccm release async configureVendors.sh -r
   ```

4. On the **IP Address** prompt, type the address of the DNS entry.
5. On the **DNS Values** prompt, type the DNS entries in lower case separated by a space.

   Note:

   For **IP Address** and **DNS Values**, see the descriptions for **config:async-oceana-adapter:service:reversedns:ip** and **config:async-oceana-adapter:service:reversedns:hostnames[0]** attributes in Configuring the Avaya Analytics deployment spreadsheet for Messaging on page 103.

Verifying the status of the Messaging channel

About this task

Use this procedure to check whether the Messaging channel is operational. A successful result ensures that the Cloud Provider can access the new Messaging APIs using your external load balancer, or using the Avaya Common Services (Common Services) Cluster FQDN directly.

Important:

- Do not run this process from the Cluster Control Manager (CCM) console. Run it from another PC that has cURL installed and is on the customer's network.

Procedure

1. To check the health status of the Messaging channel:

   Run the following command, replacing *{Common Services.FQDN}* with the FQDN of the customer's Common Services cluster.

   ```
   curl -X GET http://{Common Services.FQDN}:31325/messaging/v1/health-check
   ```

   Verify the following response:

   ```
   {
       "alive": true
   }
   ```

2. To check the readiness of the Messaging channel:

   Run the following command, replacing *{Common Services.FQDN}* with the FQDN of the customer's Common Services cluster.

   curl -X GET http://{Common Services.FQDN}:31325/messaging/v1/ready

   Verify the following response:

```
{
    "5e46bd56cb011b001076c314": {
        "Aggregator": {
            "Name": "Smooch",
            "State": "200"
        },
        "ContactCenter": {
            "Name": "Oceana",
            "State": "READY"
        }
    }
}
```

(Optional) Manual configuration of Messaging parameters

If you do not want to configure the Messaging parameters through the Avaya Analytics™ deployment spreadsheet, you can configure them manually by running specific commands on the Cluster Control Manager (CCM) console.

Modifying digital connection account after installation

About this task

Use this procedure to modify the digital connection account details, if required, post installation.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   ccm release async configureVendors.sh -a

4. On the **profile** prompt, type `csp`.
5. On the **Aggregator URL** prompt, type `https://api.smooch.io/v1.1/apps/`.
6. On the **Aggregator App Id** prompt, type the Tenant ID that is specified in your digital connection application.
7. On the **Aggregator Key ID** prompt, type the Cloud Provider key that is specified in your digital connection application.

8. On the **Aggregator Security Key** prompt, type the Cloud security key that is specified in your digital connection application.
9. For the prompt to roll out the changes, enter `y`.
10. For the prompt to wait for the services to be restarted for changes to occur, enter `y`.

Configuring the Avaya Oceana® contact center

About this task

Use this procedure to configure the Avaya Oceana® contact center to establish a connection to Customer Controller WebSocket API.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   `ccm release async configureVendors.sh -c`

4. On the **profile** prompt, type `csp`.
5. On the **Protocol** prompt, type one of the following values:
   - `ws` for a non-secure connection.
   - `wss` for a secure connection.
6. On the **Oceana host** prompt, type the FQDN of Avaya Oceana® Cluster 3 where CustomerControllerService is installed.
7. On the **Default attributes** prompt, type the default routing attributes for Messaging interactions.
8. For the prompt to roll out the changes, enter `y`.
9. For the prompt to wait for the services to be restarted for changes to occur, enter `y`.

Configuring file transfer

About this task

Use this procedure to configure file transfer into Avaya Oceana®.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type su - and press **Enter**.
3. Run the following command:

   `ccm release async configureVendors.sh -f`

4. On the **Oceana Storage host** prompt, type the FQDN of Avaya Oceana® Cluster 3 where CustomerControllerService is installed.
5. On the **Breeze User** prompt, type the user name of the default user that authenticates file transfer uploads into Avaya Oceana®.
6. On the **Breeze Password** prompt, type the password of the default user that authenticates file transfer uploads into Avaya Oceana®.
7. On the **Breeze Authentication URI** prompt, type the URI for authenticating the default user that authenticates file transfer uploads into Avaya Oceana®.

   Note:

   If you use the file transfer feature to upload a file to Avaya Oceana®, you must install an ORCA stack on your cluster or an external cluster, so that you can leverage their orca-breeze-authentication service.

   If you point to an external cluster for your ORCA service, you must run the following command to trust the external cluster for the file transfer service:

   ```
   ccm release cert-manager crtmgr --add-trustcert
   filetransfertrustore $CERT_LOCATION
   ```

8. For the prompt to roll out the changes, enter `y`.
9. For the prompt to wait for the services to be restarted for changes to occur, enter `y`.

Chapter 12: Deploying Avaya Analytics™ for non-High Availability

Avaya Analytics™ non-High Availability deployment overview

Avaya Analytics™ supports the non-High Availability (HA) deployment option that you can use in lab and production environments with the following footprints:

- 100 agents
- 500 agents
- 1000 agents

The Avaya Analytics™ non-HA deployment option reduces the number of physical servers required from three to one. This deployment option eliminates the need for vSphere Enterprise Plus license, as Distributed Resource Scheduler (DRS) is not required. With this option, you can also reduce the footprint because you deploy one instance of each application pod.

Footprint details

This table provides the required memory, storage, and vCPU requirements for each component of Avaya Analytics™ non-HA deployment for the respective footprints:

Deployment size	Component	Platform	VMs	vCPU	RAM (GB)	HDD (GB)	IOPS
100 agent	All nodes	ESXi host	4	16	48128	1600	5000
500 agent	All nodes	ESXi host	4	16	53248	2833	5000
1000 agent	All nodes	ESXi host	4	18	62464	4072	5000

Important:

- See the Avaya Analytics™ High Availability hardware requirements table for the Cluster Control Manager and VM sizes.
- Deploy the non-HA configuration on a single physical server. For details on CPU requirements, see the Avaya Analytics™ virtual machine CPU requirements section in this chapter.
- Non-HA configuration supports SAN storage and local disks on Avaya Analytics™. Ensure to keep sufficient space available to meet the data store requirements.

- Async Messaging is not supported in Avaya Analytics™ non-HA deployment.

VMware licenses and configuration

You must deploy Avaya Analytics™ non-HA in a vCenter data center. The supported VMware version for non-HA deployment is:

- 8.x

The licenses required for non-HA deployments are:

- vCenter Server Standard
- vSphere Standard Edition

Caveats

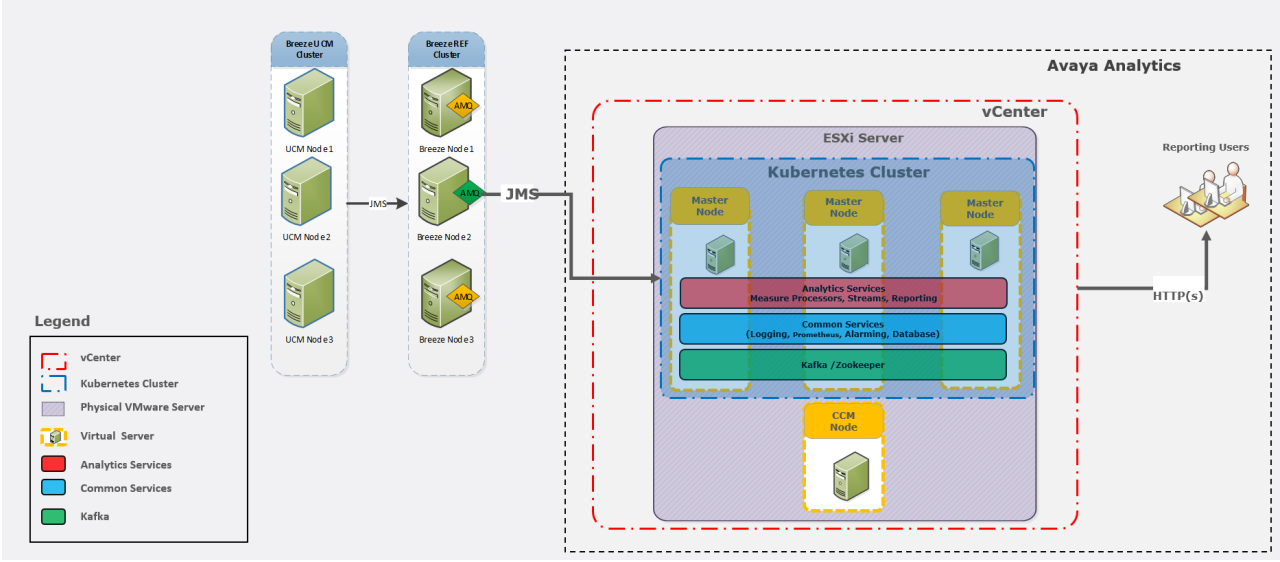
- Upgrading to Avaya Analytics™ requires a fresh Avaya Analytics™ on the HA footprint. You can back up and restore the data to the HA deployment.
- Downgrading from an Avaya Analytics™ HA to a non-HA configuration requires a fresh install of Avaya Analytics™ on the non-HA footprint.
- Avaya Analytics™ non-HA configuration does not support disaster recovery. It is a standalone configuration.
- Avaya Analytics™ non-HA configuration does not retain the data for the interval when a measure processor pod is restarted. This caveat is intended to reduce the impact on other measure processor pods.
- In an Avaya Analytics™ non-HA configuration, the real-time measures are reset to zero when you restart the interval controller pod.
- During a cluster node shutdown and restart in an Avaya Analytics™ non-HA configuration, the data produced by the measure processors on that node is not retained.
- In an Avaya Analytics™ non-HA configuration, historical data gets lost if the node with the database is shut down and not restarted within an hour.
- In an Avaya Analytics™ non-HA configuration, real-time reporting stops working if the data publisher service or Redis is running on the node that is restarted. Real-time reporting does not work until the node is fully recovered.
- You can install a single Avaya Analytics™ deployment on a VMware cluster.

Topology

The following diagram depicts the architecture for the deployment of an Avaya Analytics™ reporting solution in a non-High Availability (HA) environment:

Note:

In this configuration option, Distributed Resource Scheduler (DRS) and Avaya Analytics™ HA are in off mode, and VMware HA is on.



Avaya Analytics™ virtual machine CPU requirements

In an Avaya Analytics™ solution, vCPU reservations are not required if the resources on the VMware host server are not overcommitted, and there is no contention for CPU resources.

- The VMware CPU benchmark must, at a minimum, match a Dual (2 Socket) E5-2697 V3 @ 2.6GHz processor. This is a 2 CPU socket configuration. See the reference to dual-processor benchmark score and thread rating available at https://www.cpubenchmark.net.
- Avaya Oceana® and Avaya Analytics™ VMware profiling use a Dual 14-core Intel Xeon E5-2697 V3 2.60 GHz CPU as a reference CPU. This reference processor has 28 physical CPU cores. Each of the cores has an individual benchmark value that is one twenty-eight of the overall benchmark score of the reference processor. You use this individual core benchmark value to compare the cores from different processors and to select the suitable VMware host hardware for Avaya Oceana® and Avaya Analytics™.
- The VMware CPU benchmark for the VMware physical host, which runs Avaya Oceana® and Avaya Analytics™, must be equal to or greater than 90% of the individual core benchmark and thread value score for the reference dual-processor.
- While selecting the distribution of cores per socket for the CCM virtual machine, use the VMware-provided defaults. For example, for 8 vCPUs, VMware sets a default selection of 1 core per socket across 8 sockets.

Do the following to ensure that your proposed VMware host CPUs meet the Avaya Analytics™ minimum requirements:

- Determine the individual core benchmark value for the reference CPU, Dual 14-core Intel Xeon E5-2697 V3 2.60GHz by referring to the reference dual-processor benchmark score and thread rating available at https://www.cpubenchmark.net.

- Reference individual core benchmark value = Reference CPU benchmark from the website or Number of cores in the reference CPU. This processor has a minimum thread score of 1997, which is the minimum thread score that all CPUs used as hosts in an Avaya Oceana® and Avaya Analytics™ solution must achieve.
- Determine the individual core benchmark value for your chosen VMware physical host server CPU. Individual core benchmark value = Your chosen physical host server CPU benchmark from the website/Number of cores in the host server CPU.

Preparing the deployment spreadsheet

About this task

Use this procedure to prepare the deployment spreadsheet for installing Avaya Analytics™ in a non-High Availability environment.

Depending on the Avaya Analytics™ version, you can prepare the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` as follows:

- For a new installation, you must enter the values manually.

Before you begin

- Download the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file from PLDS.
- Enable the macros before you start editing the worksheets.
- Select the deployment types by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file. Complete the fields with the customer details that correspond to each deployment type, such as IP addresses and passwords.

Note:

The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Orca** tab.
3. In the **Number Of Agents** field, click one of the following options:
   - Agent 100
   - Agent 500
   - Agent 1000
4. On the **Deployment Properties** tab, in the **Node Affinity (HA) Enabled** field, select **FALSE**.

This step disables the following:

- Platform node affinity
- Avaya Analytics™ HA

5. Complete the configurable fields in the spreadsheet.

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.

Setting vCenter permissions

About this task

You must set the appropriate vCenter permissions to deploy Avaya Analytics™ non-High Availability to a single host.

Procedure

1. Perform the steps using the Option 3 category from the VMware permissions section.
2. To target a single host, set the **ccm-vms** for the desired ESXI host.

Installing Avaya Analytics™

About this task

Use this procedure to install Avaya Analytics™ in a non-High Availability (HA) environment through the screen utility.

Screen is a Linux command with which you can detach from an SSH session and reattach later. Using Screen, you can avoid any issues where the SSH session can disconnect after timing out, thereby interrupting the install.

Important:

Ensure that you are familiar with the screen utility. For detailed information about using screen, enter the **`man screen`** command.

Before you begin

- Select the required deployment type by selecting the agent footprints in the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
- Update the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.

  Complete the fields with the customer details that correspond to each deployment type. Examples of customer details include IP addresses and passwords. The spreadsheet includes descriptions of each configurable field to guide the installer during the configuration process.

- Modify the cluster node VM running with the vCPU, memory, and disk allocation as stated in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet. Cluster node VMs must be running with the vCPU memory and disk allocation as stated in the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet.

Procedure

1. Connect to the Cluster Control Manager (CCM) server using the customer account login.

   Important:

   If you are logging in for the first time after deploying CCM, you must change the password.

2. Copy the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to a location on the CCM server.
3. From the directory on CCM that contains the excel file, enter the following command: **`screen`**

   The screen utility allows the install to run in the background.

   Warning:

   Do not skip this step.

4. Run the following command: **`ccm install Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm`**
5. When prompted:
   a. Enter your Avaya SSO credentials.
   b. Accept the EULA.
   c. When prompted, either enable or do not enable the High Availability Audit feature.

      To enable the feature, respond `Y` to give the cluster deployment vCenter access.

      `Y` – Enable the High Availability Audit feature and grant deployment vCenter access for the cluster. The solution configuration spreadsheet must also set high_availability to `enabled`.

      `N` – Do not grant deployment vCenter access for the cluster, and do not enable the High Availability Audit feature.

      Example:

```
The following features will be enabled if this cluster
deployment is allowed vCenter access.
- High Availability Audit

Do you want to allow this cluster deployment vCenter access?
(Y/N)
```

d. Enter the vCenter user ID and password.

e. Re-confirm the password.

The installation starts downloading and installing the following:

- The base cluster software
- The common services platform software
- The Avaya Analytics™ software

The installation takes several hours to complete.

6. Run the following command in a separate window to monitor the progress of the install:

   `tail -f /var/log/avaya/ccm/ccm-main.log`

   During the installation, folders and virtual machines are created on host machines visible in the host's vCenter.

7. If you want to disconnect from the SSH session and allow the install to continue in the background, do the following:

   a. Disconnect from the SSH session.

   b. When you want to reconnect to the SSH session, start a new SSH session to CCM and connect using the customer account.

   c. Type **`screen -ls`** to retrieve the screen id of the session that is running the installation.

   d. Type **`screen -dr <screen id>`** to reattach to the installation screen session.

      See the following example command to reattach to the installation screen session:

```
[cust@examplelab ~]$ screen -ls
There is a screen on:
            9069.avaya.examplelab    (Detached)
1 Socket in /var/run/screen/S-cust.
[cust@examplelab ~]$ screen -dr 9069.avaya.examplelab
```

8. To check if the installation is successful, run the following command on the CCM console:

   `ccm status`

   The CCM console displays the status details as follows:

   - If the Status column displays the status as `deployed`, it indicates that all the components are currently deployed to the cluster.
   - If the Status column displays the status as `Staged` or `''`, it indicates that the software is staged on the system but not deployed.

     The tools-policy and utility-services remain in a `staged` state.

     Note:

     You might see the `Staged` or the `''` status in the older versions of the software after an upgrade.

- If the Status column displays the status as `Error`, it indicates that the components failed to install.

Important:

If the installation fails, run the **`ccm install cancel`** command, resolve the issue causing the failure, and restart the installation procedure. For more information about troubleshooting installation failures, see *Maintaining and Troubleshooting Avaya Analytics™*.

9. Delete the spreadsheet from CCM after the deployment is complete. Ensure you keep a copy of the spreadsheet and store it in a secure location.

   This step is important to save the passwords and other configuration details that you enter as plain text for the deployment.

Chapter 13: Upgrading Avaya Analytics™

Avaya Analytics™ upgrade overview

Avaya Analytics™ 4.3.1.1 release supports the following upgrade path:

- Avaya Analytics™ 4.2 Patch 2 and later to Avaya Analytics™ 4.3.1.1
- Avaya Analytics™ 4.3 Patch 2 and later to Avaya Analytics™ 4.3.1.1
- Avaya Analytics™ 4.3.1.0 to Avaya Analytics™ 4.3.1.1

Note:

When upgrading a DR environment, there should not be any traffic during an upgrade. If any schema changes happens on DC1 as a part of upgrade, they will propagate to DC2.

This chapter provides the steps for upgrading Avaya Analytics™ by using both online and offline methods.

To roll back to the previous release after an upgrade, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.

Avaya Analytics™ online upgrade

Preparing for the upgrade

About this task

Before starting the upgrade, complete the following activities in a service maintenance window.

Important:

- Avaya Analytics™ release 4.3.1.1 requires more resources than previous releases. For more information on new resource requirements, refer to Planning and preconfiguration on page 27.
- Before starting the upgrade, lab must be shut down and resources must be increased for node VMs.

Procedure

1. Take a full backup of the Avaya Analytics™ service data. For more information about taking backup, see *Avaya Analytics™ backups* and *Creating metadata backups* sections in *Maintenance and Troubleshooting Avaya Analytics™ for Avaya Oceana®* guide.

2. Note the scheduled database backups. You must create same backup schedules after the upgrade is complete. See *Avaya Analytics™ backups* and *Managing scheduled backups* sections in *Maintenance and Troubleshooting Avaya Analytics™ for Avaya Oceana®* guide.
3. Note the index patterns in use on the Kibana or the logging interface.
4. Using a utility such as WinSCP, transfer the updated Avaya Analytics™ deployment spreadsheet.
5. If the vCenter login password is expired, update the password before upgrading Avaya Analytics™ , run the following command:

   ```
   ccm infra update-vcentercreds
   ```

   Note:

   vCenter password must not contain the following special characters:

   ` $ ( ) \ | ; : ' " < >

   An exception to the above restriction is using a single $ symbol at the end of a password is allowed.

   This step is valid in HA environment only.

Preparing the deployment spreadsheet

About this task

Use this procedure to prepare the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet to upgrade from a previous version of Avaya Analytics™. The minimum supported version of MS Excel is 2016.

Important:

You must have minimum Avaya Analytics™ 4.2 Patch 2 version installed for the upgrade.

Record the updated CPU memory and hard disk values as compared to the previous deployment spreadsheet. This step is essential while increasing the resources before powering on the nodes.

Before you begin

- Copy the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to a location that you can access from your desktop.
- Enable the macros before you start editing the worksheets.
- The Routing Service by Group measure processor cannot be enabled during an upgrade. If you are upgrading to Avaya Analytics™ 4.3.1.1, to enable the Routing Service by Group measure processor, do the following:
  - Set the Routing Service by Group measure processor feature to `False` in the deployment spreadsheet and then upgrade to Avaya Analytics™ 4.3.1.1.
  - After the upgrade is completed, set the Routing Service by Group measure processor feature to `True` in the deployment spreadsheet. Follow the procedure in *Upscaling Avaya Analytics™* chapter in this document.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Deployment Properties** tab.
3. To copy your configuration from the previous version of the deployment spreadsheet click **Load Previous Configuration**.
4. To import the file from your local machine, browse for the file and click **Open**.
5. After the spreadsheet is updated, review all the configurable fields and update any value that is incorrect or missing.

   Note:

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.

Powering Off a cluster

About this task

Use this procedure to gracefully shut down your lab. Complete this procedure during a maintenance window.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Caution:

If you shut down your lab using a different method than what is described in this procedure, file corruption might occur.

Before you begin

- You must plan a maintenance window to perform this task.
- Stop call events across the solution.

  To stop all Avaya Oceana® traffic for an Avaya Analytics™ cluster, run the `kubectl scale deployment orca-ref-input-adaptor --replicas=0` command using an account with root privileges.
- Back up Common Services using the `ccm backup` command.

  If you do not perform a backup, you risk a full reinstallation of the solution.
- Back up product application data as described in your solution documentation.

Procedure

1. Log in to Cluster Control Manager with customer account and then switch to root user.
2. Run `ccm smoke-test` before starting any upgrade, migration, or reboot.

   Resolve any negative condition before starting any procedure.

3. Run the `pre-infra-upgrade` command to gracefully shut down the authorization service database.

   Wait for the command to complete before continuing. Ensure that this command is successful.

4. Determine which nodes contain the image registry pod using `kubectl get pods -n image-registry -o wide`.

   Note the cluster node IP/FQDN which has the image registry.

5. Determine which nodes contain a second disk and which nodes are diskless.

   Note the disk status of each node, for use when shutting down or powering on nodes.

   To identify a list of nodes that have a second disk, run the `checkInfra -Sd | grep LVM_THIN` command. The output lists the FQDNs of nodes containing a second disk.

   ```
   [cust@flex190-129 ~]$ checkInfra -Sd | grep LVM_THIN
   | pool_sds              | flex190-132.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |             |
   | pool_sds              | flex190-133.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |             |
   [cust@flex190-129 ~]$
   ```

   The other nodes in the cluster are diskless nodes. That is, node FQDNs not printed in the command output are diskless nodes.

6. Log in to vCenter as an administrator or with the account used to deploy the cluster.
7. Click the **VMs and Templates** tab.
8. Locate and click on each node virtual machine in the folder you designated during your cluster deployment.
9. Use the following steps to shut down each node:

   a. Right-click on diskless node and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.

   b. Right-click on disk bearing node 1 and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.

   c. Right-click on disk bearing node 2 and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.

Adding CPU, memory, and SDS disk size for nodes

About this task

Use this procedure to increase node CPU, memory resources, and SDS disk size.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Before you begin

- You must plan a maintenance window to perform this task.
- All the nodes are shut down using the procedure described above.

Procedure

In vCenter, on each cluster node VM, edit the settings to increase the CPU, memory resources, and SDS disk size as per deployment spreadsheet for the 4.3.1.1 release.

Result

After this procedure, the cluster nodes are updated with the new CPU and memory resource allocations.

Powering On a cluster

About this task

Use this procedure to gracefully power on your solution cluster. You can also use this procedure to power on after an unexpected power down. Complete this procedure during a maintenance window.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Procedure

1. Log in to vCenter as an administrator or with the account used to deploy the cluster.
2. Click the **VMs and Templates** tab.
3. Power on the disk bearing node that was previously running the image-registry pod from step 4 in the powering down procedure. If the registry was running on a diskless node, then power on disk bearing node 1. Wait for 5 minutes before proceeding.
4. Power on the remaining disk bearing node. Wait 5 minutes before proceeding.
5. Power on the diskless node last. Wait 5 minutes before proceeding.
6. Reconnect the SDS satellite pods.
   a. Run `kubectl exec --namespace=piraeus deployment/piraeus-op-piraeus-operator-cs-controller linstor node list`.

      Note:

      This lists the FQDNs of each node that are needed to complete the next step.

   b. Run `kubectl exec --namespace=piraeus deployment/piraeus-op-piraeus-operator-cs-controller linstor node reconnect <fqdn of node 1>`.

   c. Repeat the above step using the FQDN for node 2 and node 3. Wait 5 minutes before proceeding.

7. Start scaling up resources by first bringing up the Authorization pods using `post-infra-upgrade`. Wait for 20 minutes before continuing to the next step.
8. Proceed when pod state has stabilized (not all pods will be running at this point because they are dependent on the `orca-ref-input-adaptor` pods.
9. Scale up `orca` resource `orca-ref-input-adaptor`. Wait for another 90 minutes for the remaining pods to come up.

   Important:

   If pods are still not running, see the below note and do not delete pods.

   Note:

   Do not use `kubectl delete pod` command. If there is a PV volume attachment associated to the pod, the risk of PV mount failures when deleting a pod significantly increases. Instead of deleting pods, scale down resources by executing `kubectl scale <resource> <name> -n <namespace> --replicas=0`where resource=statefulset, deployment and name = exact resource to scale (Example mstr-srv). Wait for the pod(s) to delete and then run `kubectl scale <resource> <name> -n <namespace> --replicas=<former # of replicas>`. If for any reason the pod is not deleted, wait approximately for 30 minutes. If the pods are not yet deleted and do not disappear, then escalate to the next level service team. Additional steps are needed to clean up the volume attachments in the case a deleted pod does not fully exit.

   Note:

   Avaya Analytics™: If CSP cluster certificate rotation has to be executed:

   - Do not run ccm cluster-rotate-certificates outside of a screen session.
   - If the cluster certificate rotation fails for any reason, do not reboot the cluster.

10. Run `ccm smoke-test`.

    Resolve any negative condition before proceeding.

11. Perform basic sanity of Avaya Analytics™ to ensure it is working fine.

Prestaging the Cluster Control Manager upgrade artifact

About this task

Use this procedure to prestage the Cluster Control Manager upgrade artifact before upgrading Cluster Control Manager. Prestaging the upgrades does not disrupt service to Cluster Control Manager or cluster nodes.

Typical upgrade operations automatically download artifacts. While convenient, this can create lengthy maintenance windows. Prestaging upgrade artifacts helps minimize the duration of maintenance windows. Prestaging involves manually downloading the upgrade artifact to Cluster Control Manager before the upgrade operation.

Before you begin

Using a utility, such as WinSCP, transfer the updated solution spreadsheet and `upgrade-config.yaml` file, if one is provided, to Cluster Control Manager.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. In `/home/<customer account>`, create the CCM `upgrade-config.yaml` file.

   For example: `system: 1.3.0.2.242002` and `common_services_product_version: 1.3.0.2.242002`. For information about the version number to use, see the solution release notes.
3. Run the `ccm upgrade system <upgrade-config.yaml> --stage` command.
4. When prompted, enter your Avaya SSO credentials.
5. At the prompt to accept the terms of the EULA, enter `y`.

   You must accept the EULA for the upgrade to continue.
6. When prompted to take a backup after the CCM upgrade, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

Next steps

After the CCM artifact staging is complete, continue with the Upgrading Cluster Control Manager procedure.

Upgrading Cluster Control Manager

About this task

Use this procedure to upgrade Cluster Control Manager. The upgrade takes about 15 to 20 minutes to complete. When the upgrade completes, the upgrade utility exits and the Cluster Control Manager automatically reboots.

Before you begin

- Ensure that file integrity validation is disabled. You can check this by running `clusterFileIntegrity`. To disable file integrity validation, run `clusterFileIntegrity disable`.

  You can re-enable file integrity validation after the entire solution upgrade process is complete.
- Follow the procedures in your solution documentation to take a full backup of the solution service data, export metric data, and logs (if needed).
- Run `ccm report` to back up Elasticsearch data.

- Run `ccm release common-services exportPrometheusSnapshot` to back up solution metric (Prometheus) data.
- Using a utility, such as WinSCP, transfer the updated solution spreadsheet and `upgrade-config.yaml` file, if one is provided, to Cluster Control Manager.

  Unless instructed by your solution documentation, do not update the values on the cluster-config tab of the spreadsheet.
- If utilizing the Common Services High Availability Audit, verify that the vCenter credentials provided during the initial cluster installation are not expired. If these credentials are expired or close to expiring, update the credentials in vCenter and then update the credentials on Cluster Control Manager using the `ccm infra update-vcenter-creds` command.
- From the vCenter that is managing the solution cluster, take a virtual machine snapshot of Cluster Control Manager.

  Note:

  VMware VM snapshots are supported for cluster nodes only when the nodes are powered off. Keep snapshots for a maximum of 72 hours. Over longer periods, snapshot files increase in size and can degrade performance of the virtual machine and the ESXi host.
- (Optional): Prestage the CCM upgrade artifact.

  Prestaging artifacts is non-service impacting and can be completed outside of a maintenance window.

Procedure

1. Log in to Cluster Control Manager using the customer account login.
2. Create the `upgrade-config.yaml` file.

   Note:

   If an upgrade configuration YAML file has been provided by your solution, use that file and skip this step.

   a. Enter the `vi /home/<customer account directory>/upgrade-config.yaml` command.

   b. Enter the version string from your solution documentation.

   For example:

   ```
   common_services_product_version: 1.3.0.2.242002
   system: 1.3.0.2.242002
   ```

   For information about the GA version number to use, see your solution release notes.

   c. Save and exit the file.
3. From the directory on Cluster Control Manager that contains the `upgrade-config.yaml` file, enter the `screen` command.

   The screen utility enables the upgrade to run in the background.

4. To begin the upgrade, run the `ccm upgrade system upgrade-config.yaml` command.
5. When prompted, enter your Avaya SSO credentials.
6. Accept the EULA.

   You must accept the EULA for the upgrade to continue.

A snapshot warning displays indicating not to proceed with the upgrade if you have not taken a snapshot. A prompt also indicates that the system will reboot after the upgrade is applied.

7. At the `Do you wish to continue?` prompt, enter `y` to confirm that you have taken a snapshot and to acknowledge the reboot.

   Important:

   If a snapshot has not been taken, type `n` and return to the *Before you Begin* section to confirm that all prerequisites have been completed before continuing.

8. When prompted to take a backup after the CCM upgrade, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

9. **(Optional)** To detach from the upgrade SSH session, see Detaching from the upgrade SSH session on page 136.
10. **(Optional)** Monitor upgrade progress on the screen session or by viewing `/var/log/avaya/ccm/upgrade.log` using `tail -f` command.
11. **(Optional)** If the upgrade fails with an error, resolve the issue causing the failure and restart the upgrade by reverting to your snapshot and running the `ccm upgrade system upgrade-config.yaml` command.

    Contact Avaya support personnel if the problem persists.

12. Wait for the cluster node power-on process to complete.
13. Wait approximately 30 minutes, then run `ccm smoke-test` on Cluster Control Manager and confirm that all tests pass. If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.

Result

The system reboots after the upgrade is applied.

Verifying the Cluster Control Manager upgrade

About this task

After upgrading Cluster Control Manager, verify the upgrade.

Procedure

1. After the reboot, when Cluster Control Manager is reachable, log in using your customer account.
2. Verify that the software version of the Cluster Control Manager has been updated by running the `swversion` command.

   The Cluster Control Manager version that the `swversion` command reports should match the upgrade bundle in your solution documentation. This command reports the previous cluster version until you upgrade your cluster and services.
3. If you performed a backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.

Removing the previous version of Async Messaging

About this task

You must remove the previous version of Async Messaging before upgrading the cluster.

Note:

Skip this procedure if you do not have any previous version of Async Messaging in your solution.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. On the CCM console, run the following command:

   `ccm delete async`

   Ensure that you delete all instances of the earlier version of Messaging by running the following commands:

   `kubectl get pvc --all-namespaces | grep async`

   `kubectl delete pvc file-transfer-tmp-dir-async-file-transfer-0 file-transfer-tmp-dir-async-file-transfer-1`

   To confirm that all instances of the earlier version of Messaging are deleted, run the following commands:

   `kubectl get pods --all-namespaces |grep async`

   `kubectl get pvc --all-namespaces |grep async`

   `kubectl get virtualservices --all-namespaces |grep async`

   `kubectl get services --all-namespaces |grep async`

Prestaging the cluster node and solution upgrades

About this task

Use this procedure to prestage the cluster node and solution before upgrading them. Prestaging the upgrades does not disrupt service to Cluster Control Manager or cluster nodes.

Typical upgrade operations automatically download artifacts. While convenient, this can create lengthy maintenance windows. Prestaging upgrade artifacts helps minimize the duration of maintenance windows. Prestaging involves manually downloading the upgrade artifact to Cluster Control Manager before the upgrade operation.

Before you begin

Confirm the following are completed:

- The configuration spreadsheet values are correct and saved to the file.
- The solution configuration spreadsheet is transferred to Cluster Control Manager.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. To run the prestage in the background, at the CCM prompt run the `screen` command.
3. Run the `ccm upgrade spec <solution-spreadsheet> --stage --calculate-size` command to determine if Cluster Control Manager and the cluster registry have enough space to host the solution artifacts.
4. Run the `ccm upgrade spec <solution-spreadsheet> --stage` command to download and stage the flex-vsphere artifact, solution charts, and solution container images.

   The staging can take over 50 minutes depending on the size of the solution container images and the number of charts.
5. At the prompt to accept the terms of the EULA, enter `y`.

   You must accept the EULA for the upgrade to continue.

   The prestaging can take over 50 minutes depending on the size and number of charts.

   CCM upgrade
6. Run `ccm upgrade spec <solution-spreadsheet> --status` to verify that the prestaging is complete.

   Note:

   When prompted to create a backup after the CCM upgrade, enter `N` because a backup is created during prestaging.

Upgrading the cluster

About this task

The cluster upgrade takes a minimum of one hour. During the upgrade, folders and virtual machines are created on the host machines visible in the vCenter of the host.

Before you begin

- Remove the previous version of Async messaging.
- (Optional): Pre-stage the cluster node.

  Pre-staging artifacts is non-service impacting and can be completed outside of a maintenance window.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. To run the upgrade in the background, at the CCM prompt, type `screen`.

   When running the upgrade in the background, if you need to detach from the upgrade SSH session, see Detaching from the upgrade SSH session on page 136.
3. Run the `ccm upgrade spec <complete path>/<solution spreadsheet name>.xlsx --infra` command.

   The upgrade takes approximately one hour, and services take approximately one more hour to start.

   Tip:

   If the upgrade stalls and does not progress, then cancel the upgrade, run `ccm upgrade hard-reset` to clear the state, and retry the upgrade.
4. When prompted, enter your Avaya SSO credentials.
5. When prompted, type `y` to confirm the cluster node upgrade to the new version specified in the solution spreadsheet and to accept the warning reminding you to start a `screen` session.

   Only type `y` if you have already run `screen`. Do not continue with the upgrade until you do this.

   Failure to run the `screen` command exits the process and you have to start over.
6. When prompted, accept the EULA.

   Validation runs after accepting the EULA. If any part of the validation fails, you must address the detected issues and restart the upgrade.
7. When prompted to perform a backup, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the

archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

8. **(Optional)** To monitor the progress of the upgrade, run the `tail -f /var/log/avaya/ccm/ccm-main.log` command.

Verifying the cluster node upgrade

About this task

After you complete the cluster node upgrade, verify the operational state of the cluster before continuing with the solution service upgrade. Do not continue with the solution service upgrade unless all services, except for tools-policy and utility-service, are DEPLOYED and show RUNNING or COMPLETE.

Procedure

1. Run `swversion -c` to verify that the cluster version is updated and matches what is defined in the release notes.
2. Run the `ccm smoke-test` and `ccm status --pod-details` commands.

   The pods might not be operational immediately after the upgrade. Continue running these commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.
3. If you performed a local backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.

Solution upgrade

Use the following procedures to upgrade the solution and verify the status of the cluster. Perform the upgrade during a maintenance window.

Solution upgrade prerequisites

- Ensure that file integrity validation is disabled. You can check this by running `clusterFileIntegrity`. To disable file integrity validation, run `clusterFileIntegrity disable`.

  You can re-enable file integrity validation after the entire solution upgrade process is complete.
- Upgrade Cluster Control Manager and cluster nodes.
- If upgrading a multinode cluster, run the `checkInfra -p -cn <IPs-FQDNs>` command and verify that the cluster IOPS, network latency, and network bandwidth meet the minimum requirements.

  For **`<IPs-FQDNs>`** specify a comma-separated list of all cluster node IP addresses or FQDNs. This command can take over 15 minutes to complete.
- Confirm the following are completed:
  - The configuration spreadsheet values are correct and saved to the file.
  - The solution configuration spreadsheet is transferred to the Cluster Control Manager.

- Confirm the operational state of the cluster by running the `ccm smoke-test` and `ccm status --pod-details` commands before proceeding with the solution upgrade. The status of all services, except for tools-policy and utility-service, should be DEPLOYED. The status of all pods should be RUNNING or COMPLETE.

  When a service fails, you must delete and reinstall the service before you can deploy another service. If you require additional assistance, contact Avaya Support personnel.

  Note:

  `ccm smoke-test` shows a different value for the number of pods than what was reported for the previous version of Cluster Control Manager. If this command reports fewer pods than expected, then you must resolve this issue before you proceed. For example, if it reports 55 out of 60 pods, then you must investigate and resolve this issue.
- Take note of the index patterns in use on the logging service (Kibana). You will need to manually recreate them after the upgrade process is complete.
- (Optional): Prestage the solution.

  Prestaging artifacts is non-service impacting and can be completed outside of a maintenance window.

Upgrading solution services

About this task

Upgrade the services in the solution(s).

Before you begin

Ensure that the Cluster Control Manager and cluster nodes are upgraded before proceeding with the services upgrade.

Do not continue with the solution service upgrade unless all services, except for tools-policy and utility-service, are DEPLOYED and show RUNNING or COMPLETE.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. To run the upgrade in the background, at the CCM prompt, type `screen`.

   When running the upgrade in the background, if you need to detach from the upgrade SSH session, see Detaching from the upgrade SSH session on page 136.
3. Run the `ccm upgrade spec <complete path>/<solution spreadsheet name>.xlsx --products` command.
4. When prompted, type `y` to confirm the requested products to upgrade to the new versions specified in the solution spreadsheet and to accept the warning reminding you to start a `screen` session.

   Only type `y` if you have already run `screen`. Do not continue with the upgrade until you do this.

   Failure to run the `screen` command exits the process and you have to start over.

5. When prompted, accept the EULA.

   Validation runs after accepting the EULA. If any part of the validation fails, you must address the detected issues and restart the upgrade.

6. When prompted to perform a backup, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

7. **(Optional)** To monitor the progress of the upgrade, run the `tail -f /var/log/avaya/ccm/ccm-main.log` command.

8. **(Optional)** If the upgrade exits with an error, run the `ccm upgrade spec <solution spreadsheet name>.xlsm --products --force` command again.

9. Wait approximately 30 minutes, then run `ccm smoke-test` on Cluster Control Manager and confirm that all tests pass. If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.

10. Log in to the Cluster Control Manager (CCM) console as the customer user.

11. Switch to being the root user by entering the command `su`.

12. After the upgrade is completed, restart database pods by running the following command and wait till the database pods are in running state:

```
kubectl get pod --no-headers -o custom-columns=":metadata.name" | grep analyticsdb-node- | xargs kubectl delete pod
```

Verifying the solution service upgrade

About this task

Verify the upgrade of the solution services.

Procedure

1. Run the `ccm smoke-test` and `ccm status --pod-details` commands to ensure that the products are upgraded to the same version specified in the solution spreadsheet.

   The pods might not be operational immediately after the upgrade. Continue running these commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.

2. Run the `swversion -c` and `ccm swhistory` commands to verify that the installed software versions match the software versions specified in the deployment spreadsheet.

3. If you performed a backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.

4. **(Optional)** Delete previous backups.

Detaching from the upgrade SSH session

About this task

If you are running an upgrade in the background, use this procedure to detach from the SSH session.

Procedure

1. Start a new SSH session to Cluster Control Manager and log in with your customer account.
2. Type `screen -ls` to retrieve the screen ID of the session that is running the upgrade.
3. Type `screen -d <screen id>` to detach the session from the SSH session.
4. Close the SSH session.

   The upgrade continues to run in the background.

Reattaching to the upgrade SSH session

About this task

After detaching from the upgrade SSH session, you can use this procedure if you want to reopen the SSH session.

Procedure

1. Log in to Cluster Control Manager using your customer account.
2. At the CCM prompt, type `screen -ls` to retrieve the screen ID of the session.

   If no screen IDs are listed, the upgrade is complete.
3. Type `screen -r <screen id>` to reattach to the upgrade session.

Avaya Analytics™ offline upgrade

Avaya Analytics™ supports two methods for offline upgrade, Docker desktop for Windows and Windows Subsystem for Linux (WSL). For more information on these methods, refer to Avaya Analytics offline deployment overview on page 72

Air gap network: Downloading and uploading chart and images

If your environment is in an air gap network, then perform the following procedures under this section:

- *Air gap network: Downloading and uploading the Cluster Control Manager upgrade image using a gzip file*
- *Air gap network: Uploading Avaya Analytics™ chart and images with restricted access to Cluster Control Manager*

Downloading the Cluster Control Manager upgrade Docker image

About this task

Download the upgrade Docker image to your computer and then upload the image onto Cluster Control Manager. Use the ccm-ctl-agn container for the downloading and uploading process.

Before you begin

You must have:

- Valid Avaya SSO credentials.
- A functional ccm-ctl-agn container on your computer.
- The Cluster Control Manager `upgrade-config.yaml` file or the latest version of the ccmupgrade image.

Procedure

1. On the command line of the ccm-ctl-agn container, change the directories to the download directory at `cd /root/downloads`.
2. Create an image directory at `mkdir images`.
3. Change to the images directory at `cd images`.
4. To log in to harbor.avaya.com, run the `docker login harbor.avaya.com` command.
5. Run the `docker pull harbor.avaya.com/flex/ccmupgrade:<ccm-upgrade-version>` command.

   `<ccm-upgrade-version>` is the version of the ccmupgrade package.
6. To log out from harbor.avaya.com, run the `docker logout harbor.avaya.com` command.

Setting up Cluster Control Manager for Avaya Analytics™ offline deployment

About this task

You must set the username and password in the Cluster Control Manager (CCM) console to secure access to the CCM local docker registry and chartmuseum.

Before you begin

Install Cluster Control Manager (CCM) OVA in the air gap environment.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the following command:

   `agn-ctl setup`
3. At the prompt, enter an alpha-numeric username for the CCM local ChartMusem and Docker registry.

4. Enter an alpha-numeric password for the CCM local ChartMusem and Docker registry.
5. Re-enter the alpha-numeric password for the CCM local ChartMusem and Docker registry.
6. Note down the username and password for future use.

Starting ChartMuseum and Docker registry on Cluster Control Manager

About this task

Use this procedure to start the offline deployment repositories on Cluster Control Manager.

Before you begin

Set up Cluster Control Manager for offline deployment.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the **`agn-ctl start`** command.

Stopping ChartMuseum and Docker registry on Cluster Control Manager

About this task

Use this procedure to stop the offline deployment repositories on Cluster Control Manager.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the **`agn-ctl stop`** command.

Obtaining the Cluster Control Manager CA certificate

About this task

You must obtain the Cluster Control Manager (CCM) CA certificate and install the certificate into the Windows trust store.

Before you begin

- Get your CCM FQDN.
- Ensure that the CCM local Docker registry and ChartMuseum are running.
- Ensure that you have the local admin Windows user rights.

Procedure

1. Connect to your air gap network using your Windows PC or client laptop.
2. Using a browser, navigate to the CCM docker registry listening on port 5010 at `https://<ccm_fqdn.com>:5010/`, where <ccm_fqdn> is the FQDN of your CCM.
3. If you do not see a `Certificate error` message, skip the remaining steps.
4. If you see a `Certificate error` message, do the following:
    a. Click the Certificate error message.

b. Click **View Certificate**.
c. Click **Export to file**.
d. Save the exported certificate.

5. On your taskbar, click the search icon, and type `Manage computer certificates`.
6. Click the **Manage computer certificates** control panel.
7. In `Certificates-Local Computer`, click **Trusted Root Certification**.

   The right-pane displays the `Certificates` folder.
8. Right-click **Certificates**.

   Windows displays the Certificate Import Wizard window.
9. Click **All Tasks** > **Import**.
10. On the Certificate Import Wizard page, select **Local Machine** and click **Next**.
11. Click **Browse**.
12. To import the Docker registry certificate that was exported earlier, select the file, and click **Open**.
13. Click **Next**.
14. Select the **Place all certificates in the following store** check box.
15. Ensure that in the **Certificate store** field, the specified location is `Trusted Root Certification Authorities`.
16. Click **Next**.
17. On the Completing the Certificate Import Wizard page, verify that the settings that you have selected are correct, and click **Finish**.

    The Certificate Import Wizard page displays the following message:

    `The import was successful`
18. In the Windows icon tray, click the Docker whale icon and click **Restart**.
19. Verify that the connection is successful with CCM local Docker registry. Run the following commands within the ccm-ctl-agn deployed container:
    a. To log in, run: `docker login < ccm fqdn >:5010`
    b. When prompted, enter the `Username` and `Password` of the CCM local Docker registry
    c. To log out, run: `docker logout < ccm fqdn >:5010`

    Log in and log out operations are successful.

Confirming that the local Cluster Control Manager registry and ChartMuseum are running

About this task

You must confirming that the local Cluster Control Manager (CCM) registry and ChartMuseum are running before installing Avaya Analytics™ offline.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Run the following command:

   `agn-ctl status`

3. Verify that the following ports display the stats as `ACCEPT`:
   - ChartMuseum port 5011
   - Registry port 5010
4. Verify that the CCM local registry status displays `UP`.

Uploading the Cluster Control Manager upgrade Docker image

About this task

Upload the Cluster Control Manager upgrade image into the Cluster Control Manager local Docker registry.

Before you begin

- Load the Cluster Control Manager CA certificates:
  - For Docker Desktop, install the certificates in the Windows trust store.
  - For WSL-based deployment, install the certificates in the WSL truststore. See Obtaining Cluster Control Manager registry CA certificate for WSL distribution on page 89.
- Get the Cluster Control Manager hostname
- Start the Cluster Control Manager air gap network container
- Download the Cluster Control Manager upgrade Docker image
- Setup Cluster Control Manager for offline deployment.
- Note the Cluster Control Manager local docker registry username and password
- Start ChartMuseum and Docker registry on Cluster Control Manager
- Connect to your air gap network using your Windows PC or laptop

Procedure

1. Using the ccm agn deployed container, to tag the upgrade Docker image for the Cluster Control Manager registry, do the following:
   a. To obtain the name of the ccm upgrade Avaya Harbor tagged image for re-tagging, run the `docker images --format '{{.Repository}}:{{.Tag}}' | grep ccmupgrade` command.

b. To apply the new tag, run the `docker tag <harbor-tag> <ccm-tag>` command.

Note:

- The tag is in the following format: `<RegistryFQDN:PORT>/flex/image:version`. If the port is 443, you can omit typing the port number.
- `<harbor-tag>` is part of the Avaya Harbor Docker Registry, which is `harbor.avaya.com/flex/<image:version>`

  This tag is the name you obtained in the previous step.
- `<ccm-tag>` is part of the local CCM Docker Registry, which is `<CCM-FQDN>:5010/flex/<image:version>`

2. To obtain the CCM tagged images to push to the CCM registry, run the `docker images --format '{{.Repository}}:{{.Tag}}' | grep :5010 | grep ccmupgrade` command.
3. To get a Docker login for the CCM local Docker registry, run the `docker login <CCM-FQDN>:5010` command.
4. To push the CCM tagged images to the CCM registry, run the `docker push <image-tag-name>` command.
5. When prompted, enter the username and password of the agn-ctl setup.
6. Log out from Docker using the `docker logout <CCM-FQDN>:5010` command.
7. **(Optional)** To remove the Avaya Harbor tagged images, run the `docker rmi <harbor-tag>` command.

   <harbor-tag> is part of the Avaya Harbor Docker Registry, which is `harbor.avaya.com/flex/<image:version>`.

Prestaging the Cluster Control Manager upgrade artifact

About this task

Use this procedure to prestage the Cluster Control Manager upgrade artifact before upgrading Cluster Control Manager. Prestaging the upgrades does not disrupt service to Cluster Control Manager or cluster nodes.

Typical upgrade operations automatically download artifacts. While convenient, this can create lengthy maintenance windows. Prestaging upgrade artifacts helps minimize the duration of maintenance windows. Prestaging involves manually downloading the upgrade artifact to Cluster Control Manager before the upgrade operation.

Before you begin

Using a utility, such as WinSCP, transfer the updated solution spreadsheet and `upgrade-config.yaml` file, if one is provided, to Cluster Control Manager.

Procedure

1. Log in to Cluster Control Manager with your customer account.

2. In `/home/<customer account>`, create the CCM `upgrade-config.yaml` file.

   For example: `system: 1.3.0.2.242002` and `common_services_product_version: 1.3.0.2.242002`. For information about the version number to use, see the solution release notes.

3. Run the `ccm upgrade system <upgrade-config.yaml> --stage` command.
4. When prompted, enter your Avaya SSO credentials.
5. At the prompt to accept the terms of the EULA, enter `y`.

   You must accept the EULA for the upgrade to continue.

6. When prompted to take a backup after the CCM upgrade, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

Next steps

After the CCM artifact staging is complete, continue with the Upgrading Cluster Control Manager procedure.

Powering Off a cluster

About this task

Use this procedure to gracefully shut down your lab. Complete this procedure during a maintenance window.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Caution:

If you shut down your lab using a different method than what is described in this procedure, file corruption might occur.

Before you begin

- You must plan a maintenance window to perform this task.
- Stop call events across the solution.

  To stop all Avaya Oceana® traffic for an Avaya Analytics™ cluster, run the `kubectl scale deployment orca-ref-input-adaptor --replicas=0` command using an account with root privileges.

- Back up Common Services using the `ccm backup` command.

  If you do not perform a backup, you risk a full reinstallation of the solution.

- Back up product application data as described in your solution documentation.

Procedure

1. Log in to Cluster Control Manager with customer account and then switch to root user.
2. Run `ccm smoke-test` before starting any upgrade, migration, or reboot.

   Resolve any negative condition before starting any procedure.
3. Run the `pre-infra-upgrade` command to gracefully shut down the authorization service database.

   Wait for the command to complete before continuing. Ensure that this command is successful.
4. Determine which nodes contain the image registry pod using `kubectl get pods -n image-registry -o wide`.

   Note the cluster node IP/FQDN which has the image registry.
5. Determine which nodes contain a second disk and which nodes are diskless.

   Note the disk status of each node, for use when shutting down or powering on nodes.

   To identify a list of nodes that have a second disk, run the `checkInfra -Sd | grep LVM_THIN` command. The output lists the FQDNs of nodes containing a second disk.

   ```
   [cust@flex190-129 ~]$ checkInfra -Sd | grep LVM_THIN
   | pool_sds              | flex190-132.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |             |
   | pool_sds              | flex190-133.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |             |
   [cust@flex190-129 ~]$
   ```

   The other nodes in the cluster are diskless nodes. That is, node FQDNs not printed in the command output are diskless nodes.
6. Log in to vCenter as an administrator or with the account used to deploy the cluster.
7. Click the **VMs and Templates** tab.
8. Locate and click on each node virtual machine in the folder you designated during your cluster deployment.
9. Use the following steps to shut down each node:
   a. Right-click on diskless node and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.
   b. Right-click on disk bearing node 1 and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.
   c. Right-click on disk bearing node 2 and click **Power** > **Shut Down Guest OS** to shut down the node. Wait for the node to shut down.

Adding CPU, memory, and SDS disk size for nodes

About this task

Use this procedure to increase node CPU, memory resources, and SDS disk size.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Before you begin

- You must plan a maintenance window to perform this task.
- All the nodes are shut down using the procedure described above.

Procedure

In vCenter, on each cluster node VM, edit the settings to increase the CPU, memory resources, and SDS disk size as per deployment spreadsheet for the 4.3.1.1 release.

Result

After this procedure, the cluster nodes are updated with the new CPU and memory resource allocations.

Powering On a cluster

About this task

Use this procedure to gracefully power on your solution cluster. You can also use this procedure to power on after an unexpected power down. Complete this procedure during a maintenance window.

Note:

Skip this procedure if you are upgrading from 4.3.1.0

Procedure

1. Log in to vCenter as an administrator or with the account used to deploy the cluster.
2. Click the **VMs and Templates** tab.
3. Power on the disk bearing node that was previously running the image-registry pod from step 4 in the powering down procedure. If the registry was running on a diskless node, then power on disk bearing node 1. Wait for 5 minutes before proceeding.
4. Power on the remaining disk bearing node. Wait 5 minutes before proceeding.
5. Power on the diskless node last. Wait 5 minutes before proceeding.
6. Reconnect the SDS satellite pods.
   a. Run `kubectl exec --namespace=piraeus deployment/piraeus-op-piraeus-operator-cs-controller linstor node list`.

      Note:

      This lists the FQDNs of each node that are needed to complete the next step.

b. Run `kubectl exec --namespace=piraeus deployment/piraeus-op-piraeus-operator-cs-controller linstor node reconnect <fqdn of node 1>`.

c. Repeat the above step using the FQDN for node 2 and node 3. Wait 5 minutes before proceeding.

7. Start scaling up resources by first bringing up the Authorization pods using `post-infra-upgrade`. Wait for 20 minutes before continuing to the next step.
8. Proceed when pod state has stabilized (not all pods will be running at this point because they are dependent on the `orca-ref-input-adaptor` pods.
9. Scale up `orca` resource `orca-ref-input-adaptor`. Wait for another 90 minutes for the remaining pods to come up.

Important:

If pods are still not running, see the below note and do not delete pods.

Note:

Do not use `kubectl delete pod` command. If there is a PV volume attachment associated to the pod, the risk of PV mount failures when deleting a pod significantly increases. Instead of deleting pods, scale down resources by executing `kubectl scale <resource> <name> -n <namespace> --replicas=0`where resource=statefulset, deployment and name = exact resource to scale (Example mstr-srv). Wait for the pod(s) to delete and then run `kubectl scale <resource> <name> -n <namespace> --replicas=<former # of replicas>`. If for any reason the pod is not deleted, wait approximately for 30 minutes. If the pods are not yet deleted and do not disappear, then escalate to the next level service team. Additional steps are needed to clean up the volume attachments in the case a deleted pod does not fully exit.

Note:

Avaya Analytics™: If CSP cluster certificate rotation has to be executed:

- Do not run ccm cluster-rotate-certificates outside of a screen session.
- If the cluster certificate rotation fails for any reason, do not reboot the cluster.

10. Run `ccm smoke-test`.

    Resolve any negative condition before proceeding.
11. Perform basic sanity of Avaya Analytics™ to ensure it is working fine.

Upgrading Cluster Control Manager

About this task

Use this procedure to upgrade Cluster Control Manager. The upgrade takes about 15 to 20 minutes to complete. When the upgrade completes, the upgrade utility exits and the Cluster Control Manager automatically reboots.

Before you begin

- Download the CCM upgrade Docker image to your laptop or PC
- Upload the CCM upgrade Docker image to CCM
- If an upgrade configuration yaml is provided by your solution, transfer the CCM `upgrade-config.yaml` file to Cluster Control Manager by using a file transfer utility, such as WinSCP.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Create the upgrade configuration yaml.

   Note:

   If an upgrade configuration yaml is provided by your solution, use that file and skip this step.

   a. Type `vi /home/<customer account directory>/upgrade-config.yaml`

   b. Enter the version string from your solution documentation.

   For example;

   ```
   common_services_product_version: 1.3.0.2.242002
   system: 1.3.0.2.242002
   ```

   For more information about the GA version number, see your solution release notes.

   c. Save and exit the file.
3. Change the directory to `/home/<customer account directory>`.
4. Run the following command:

   `screen`

   The screen utility runs the upgrade in the background.
5. To begin the upgrade, run the following command:

   `ccm upgrade system upgrade-config.yaml`
6. After the prompt to perform a backup, enter `y`.
   - Entering `n` cancels the operation.
   - Entering `y` runs a backup after the upgrade is complete.

   The backup takes approximately 5 to 10 minutes to complete. The backup file is located at `/var/avaya/artifactCache/`
7. To restore the operation, enter the password when prompted.
8. When prompted, enter your Avaya SSO credentials.

   You must enter the CCM local registry username and password configured with the **`agn-ctl setup`** command earlier.

9. **(Optional)** If the official Release Notes state that you must install a patch after the CCM upgrade, run the following command:

   `patchReleases`

10. Accept the EULA.
11. Confirm the warning regarding the recommendation of a snapshot for reversion and acknowledgment that CCM restarts after the upgrade is applied.

    Important:

    If a snapshot has not been taken, enter `no` and return to the Before you begin section to confirm all steps is complete before continuing.

    The restart takes about 2 minutes after the upgrade completes.

12. **(Optional)** Detach from the upgrade SSH session.

    For the steps to detach a session, see the Detaching from the upgrade SSH session on page 136

13. **(Optional)** If the upgrade fails with an error, resolve the issue causing the failure and restart the upgrade by reverting to your snapshot and running the **`ccm upgrade system upgrade-config.yaml`** command.

    For more information about troubleshooting installation failures, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.

Verifying the Cluster Control Manager upgrade

About this task

After upgrading Cluster Control Manager, verify the upgrade.

Procedure

1. After the reboot, when Cluster Control Manager is reachable, log in using your customer account.
2. Verify that the software version of the Cluster Control Manager has been updated by running the `swversion` command.

   The Cluster Control Manager version that the `swversion` command reports should match the upgrade bundle in your solution documentation. This command reports the previous cluster version until you upgrade your cluster and services.

3. If you performed a backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.

Preparing the deployment spreadsheet

About this task

Use this procedure to prepare the macro-enabled `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` spreadsheet to

upgrade from a previous version of Avaya Analytics™. The minimum supported version of MS Excel is 2016.

Important:

You must have minimum Avaya Analytics™ 4.2 Patch 2 version installed for the upgrade.

Record the updated CPU memory and hard disk values as compared to the previous deployment spreadsheet. This step is essential while increasing the resources before powering on the nodes.

Before you begin

- Copy the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file to a location that you can access from your desktop.
- Enable the macros before you start editing the worksheets.
- The Routing Service by Group measure processor cannot be enabled during an upgrade. If you are upgrading to Avaya Analytics™ 4.3.1.1, to enable the Routing Service by Group measure processor, do the following:
  - Set the Routing Service by Group measure processor feature to `False` in the deployment spreadsheet and then upgrade to Avaya Analytics™ 4.3.1.1.
  - After the upgrade is completed, set the Routing Service by Group measure processor feature to `True` in the deployment spreadsheet. Follow the procedure in *Upscaling Avaya Analytics™* chapter in this document.

Procedure

1. Open the `Avaya_Oceana_Application_Deployment_<ReleaseNumber>.xlsm` file.
2. Click the **Deployment Properties** tab.
3. To copy your configuration from the previous version of the deployment spreadsheet click **Load Previous Configuration**.
4. To import the file from your local machine, browse for the file and click **Open**.
5. After the spreadsheet is updated, review all the configurable fields and update any value that is incorrect or missing.

   Note:

   The key configurable fields are marked in orange in the spreadsheet. The corresponding rows describe the information that you must enter in the respective fields.

Downloading Avaya Analytics™ chart and images

About this task

You must download the Avaya Analytics™ chart and images from Avaya to the Windows PC or client computer.

Important:

- This procedure and all the following procedures are applicable for both offline deployment methods, Docker desktop for Windows and WSL (Windows Subsystem for Linux).
- This procedure assumes that you have configured Docker Desktop file sharing for the `c:\` drive of your Windows client.

Before you begin

- Ensure that your Avaya SSO credentials allow you to download the software successfully.
- Get the `Avaya_Oceana_Application_Deployment.xlsm` file.
- Start the Cluster Control Manager air gap network container, ccm-ctl-agn, on your PC.

Procedure

1. On your Windows PC or client computer, save the `Avaya_Oceana_Application_Deployment.xlsm` file in `c:\avaya\downloads`.

   Note:

   Windows and the Cluster Control Manager Controller container share mount points, which are `c:\avaya\downloads` and `/root/downloads`, respectively.

2. In the ccm-ctl-agn container, run the following command:

   `cd /root/downloads`

3. Run the following command and verify that the page displays the excel file:

   `ls`

4. To download the Avaya Analytics™ charts and images from the Avaya repository, run the following command:

   `agn download Avaya_Oceana_Application_Deployment.xlsm`

5. In the **Avaya SSO User** and **Password** fields, enter your Avaya SSO credentials.

   The agn script processes the excel spreadsheet, and the Avaya Analytics™ charts and docker images start downloading. The ccm-ctl-agn container displays an Image Pull Report when the download is complete.

6. To view a list of the downloaded images, run the following command:

   `docker image ls`

7. To view a list of the downloaded charts, run the following command:

   `ls /root/downloads/*.tgz`

8. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-ctl-agn container at `/var/log/avaya/ccm/ccm-main.log`.

   For more information on possible issues and the respective troubleshooting solutions, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* doc.

Uploading Avaya Analytics™ chart and images with limited access to Cluster Control Manager

About this task

You must upload the Avaya Analytics™ chart and images from the Windows PC or client laptop to Cluster Control Manager (CCM).

Before you begin

- Depending on the offline deployment method used, Docker desktop or WSL, load the CCM CA certificates.
- Get the CCM hostname.
- Get the CCM local docker registry username and password that you noted down.
- Setup Cluster Control Manager for Avaya Analytics™ offline deployment.
- Start ChartMuseum and Docker registry on Cluster Control Manager.

Procedure

1. Connect to your air gap network using your Windows PC or laptop.
2. Start the ccm-ctl-agn container based on the deployment method used.
   - For Docker Desktop (Windows PowerShell):

     Run: `C:\avaya\ccm-ctl-agn.bat`.
   - For WSL-based deployment:

     Run the `ccm-ctl-agn` container from the WSL distribution using command: `/mnt/c/avaya/ccm-ctl-agn.wsl`.
3. Using the ccm agn deployed container, run the following command: **`agn upload <CCM FQDN>`**, where <*CCM FQDN*> is the FQDN of your CCM.
4. To access the CCM docker registry and ChartMuseum, enter the username when prompted.
5. Enter the password.
6. Re-enter the password.

   The agn command starts the following in a sequence:

   a. Processes the available chart and image data on the Windows PC or laptop.
   b. Starts uploading the charts and images to CCM. When the upload is complete, the console displays an image push report.
7. **(Optional)** If you see a docker pull error, you can view or retrieve the logs within the ccm-ctl-agn container at `/var/log/avaya/ccm/ccm-main.log`.

   For more information on possible issues and the respective troubleshooting solutions, see the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* document.
8. To copy the `Avaya_Oceana_Application_Deployment.xlsm` file, run the following command in the ccm-ctl-agn container:**`scp /root/downloads/`**

`Avaya_Oceana_Application_Deployment.xlsm <ccmUser>@<CCM FQDN>:`, where *<ccmUser>* is the CCM customer login account and *<CCM FQDN>* is the FQDN of your CCM.

Note:

Do not skip the colon at the end of the command.

9. In the **Are you sure you want to continue connecting** field, type `yes` and press **Enter**.
10. At the prompt, enter the CCM user password.

    The ccm-ctl-agn container uploads the images and charts, which you earlier downloaded on the Windows PC or client laptop, into the local CCM docker registry and chartmuseum.

Air gap network: Downloading and uploading the Cluster Control Manager upgrade image using a gzip file

In an offline air gap network environment, before upgrading Cluster Control Manager, you must download the Cluster Control Manager upgrade image to your computer and then upload the image to Cluster Control Manager. This section describes the process of using the ccm-ctl-agn container to download the Cluster Control Manager upgrade image, save it as a gzip file, and then upload it to Cluster Control Manager.

Note:

This procedure is optional, it is only applicable in an offline air gap network environment.

Downloading the Cluster Control Manager upgrade image

About this task

Use this procedure to download the Cluster Control Manager upgrade image. Perform this procedure using the command line of the ccm-ctl-agn container.

Before you begin

- You must have valid Avaya SSO credentials.
- You must have the version number of the latest released Cluster Control Manager `ccmupgrade` package.
- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

1. Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn ccm-upgrade download <CCM upgrade version>` command to download the Cluster Control Manager upgrade package.

   Replace `<CCM upgrade version>` with the version number of the latest released Cluster Control Manager `ccmupgrade` package.

   Example: `agn ccm-upgrade download 1.3.0.2.242002`
2. When prompted, enter the Avaya SSO user name and password associated with Avaya Harbor.

Result

The upgrade image is downloaded to the Docker cache on your computer.

Saving the Cluster Control Manager upgrade image as a gzip file

About this task

Save the Cluster Control Manager upgrade image as a gzip file using the ccm-ctl-agn container.

Before you begin

- Download the Cluster Control Manager upgrade image to the Docker cache on your computer.
- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

1. Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn ccm-upgrade save <CCM upgrade version>` command to save the downloaded Cluster Control Manager upgrade image as a gzip file.

   Replace `<CCM upgrade version>` with the version number of the Cluster Control Manager `ccmupgrade` image.

   Example: `agn ccm-upgrade save 1.3.0.2.242002`

2. After saving the upgrade image as a gzip file, from the `/root/downloads` directory of the `ccm-ctl-agn` container, run the `tar -zcvf downloads.tgz ../downloads` command.
3. Transfer the tar file to Cluster Control Manager using a thumb drive or a similar media device.

   The file path in Windows is `C:/Avaya/Downloads/downloads.tgz`.

Uploading the Cluster Control Manager upgrade gzip image onto Cluster Control Manager

About this task

Upload the Cluster Control Manager upgrade gzip image file onto the Cluster Control Manager local Docker registry using the `agn` command. Run the `agn` command on Cluster Control Manager.

Before you begin

- Save the Cluster Control Manager upgrade image as a gzip file.
- Transfer the solution downloads.tgz file to the `/var/avaya/artifactCache` directory on Cluster Control Manager.
- Set up Cluster Control Manager for offline deployment.
- Start ChartMuseum and Docker registry on Cluster Control Manager.

Procedure

1. On Cluster Control Manager, extract the Downloads tar file using `tar -zxvf downloads.tgz` to the `/var/avaya/artifactCache` directory if enough space is available.

   You can run `df -h` to see how much disk space is available. If the tar file is larger than half the disk space available, extract the file to a different server in the air gap network and then transfer it to Cluster Control Manager using an SCP client.

2. Run `agn ccm-upgrade load -d <full path to Downloads directory> -h <Cluster Control Manager FQDN>` to upload the Cluster Control Manager upgrade gzip file.

   The following is an example of this command:

   ```
   agn ccm-upgrade load -d /var/avaya/artifactCache/downloads -h
   ccm.server.example.com
   ```

3. When prompted, enter the user name and password to access the local Cluster Control Manager Docker registry.

Next steps

Upgrade Cluster Control Manager.

Air gap network: Uploading Avaya Analytics™ chart and images with restricted access to Cluster Control Manager

The following sections outline the steps to use the ccm-ctl-agn container to download the solution images to a computer and then save each image as a gzip file. On Cluster Control Manager, the `agn` command is used to load the solution's gzip images and charts onto the Cluster Control Manager local Docker registry and chart museum repository.

Note:

This procedure is optional, it is only applicable in an offline air gap network environment.

Saving the solution images as gzip files

About this task

Save each solution image as a gzip file. Perform this procedure using the `ccm-ctl-agn` container.

Before you begin

- Download the chart and images to the laptop using the Cluster Control Manager air gap network container.
- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

1. Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn save` command to save the downloaded images for the solution as a set of gzip images.

2. From the `/root/downloads` directory of the running `ccm-ctl-agn` container, run the `tar -zcvf downloads.tgz ../downloads` command.
3. Transfer the tar file to Cluster Control Manager using a thumb drive or a similar media device.

   The file path in Windows is `C:/Avaya/Downloads/downloads.tgz`.

Uploading the solution gzip images and charts onto Cluster Control Manager

About this task

Upload the solution gzip images and charts onto the Cluster Control Manager local Docker registry and chart museum using the `agn` command on Cluster Control Manager.

Before you begin

- Save each solution image as a gzip file.
- Transfer the solution `downloads.gzip` file to the `/var/avaya/artifactCache` directory on Cluster Control Manager.
- Set up Cluster Control Manager for offline deployment.
- Start ChartMuseum and Docker registry on Cluster Control Manager.

Procedure

1. On Cluster Control Manager, extract the Downloads tar file using `tar -zxvf downloads.tgz` to the `/var/avaya/artifactCache` directory if enough space is available.

   You can run `df -h` to see how much disk space is available. If the tar file is larger than half the disk space available, extract the file to a different server in the air gap network and then transfer it to Cluster Control Manager using an SCP client.
2. Run `agn load -d <full path to Downloads directory> -h <Cluster Control Manager FQDN>` to upload the solution gzip images and charts.

   The following is an example of this command:

   ```
   agn load -d /var/avaya/artifactCache/downloads -h ccm.server.example.com
   ```
3. When prompted, enter the user name and password to access the local Cluster Control Manager Docker registry and chart museum.

Result

After you upload all images and charts, the Cluster Control Manager local Docker registry and chart museum are staged for cluster deployment.

Removing the downloaded solution images from your computer

About this task

After you upload the images and charts to Cluster Control Manager, you can delete the downloaded images from your computer's Docker cache. Perform this procedure using the ccm-ctl-agn container.

Before you begin

- Start the Cluster Control Manager air gap network container (`ccm-ctl-agn`) on the laptop.

Procedure

Using the `ccm-ctl-agn` deployed container on the laptop, run the `agn clean` command to delete the downloaded solution images.

This operation can take up to 5 minutes to complete.

Removing the previous version of Async Messaging

About this task

You must remove the previous version of Async Messaging before upgrading the cluster.

Note:

Skip this procedure if you do not have any previous version of Async Messaging in your solution.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. On the CCM console, run the following command:

   `ccm delete async`

   Ensure that you delete all instances of the earlier version of Messaging by running the following commands:

   `kubectl get pvc --all-namespaces | grep async`

   `kubectl delete pvc file-transfer-tmp-dir-async-file-transfer-0 file-transfer-tmp-dir-async-file-transfer-1`

   To confirm that all instances of the earlier version of Messaging are deleted, run the following commands:

   `kubectl get pods --all-namespaces |grep async`

   `kubectl get pvc --all-namespaces |grep async`

   `kubectl get virtualservices --all-namespaces |grep async`

   `kubectl get services --all-namespaces |grep async`

Solution upgrade

Solution upgrade prerequisites

- Ensure that file integrity validation is disabled. You can check this by running `clusterFileIntegrity`. To disable file integrity validation, run `clusterFileIntegrity disable`.

You can re-enable file integrity validation after the entire solution upgrade process is complete.

- Upgrade Cluster Control Manager and cluster nodes.
- If upgrading a multinode cluster, run the `checkInfra -p -cn <IPs-FQDNs>` command and verify that the cluster IOPS, network latency, and network bandwidth meet the minimum requirements.

  For **<IPs-FQDNs>** specify a comma-separated list of all cluster node IP addresses or FQDNs. This command can take over 15 minutes to complete.
- Confirm the following are completed:
  - The configuration spreadsheet values are correct and saved to the file.
  - The solution configuration spreadsheet is transferred to the Cluster Control Manager.
- Confirm the operational state of the cluster by running the `ccm smoke-test` and `ccm status --pod-details` commands before proceeding with the solution upgrade. The status of all services, except for tools-policy and utility-service, should be DEPLOYED. The status of all pods should be RUNNING or COMPLETE.

  When a service fails, you must delete and reinstall the service before you can deploy another service. If you require additional assistance, contact Avaya Support personnel.

  Note:

  `ccm smoke-test` shows a different value for the number of pods than what was reported for the previous version of Cluster Control Manager. If this command reports fewer pods than expected, then you must resolve this issue before you proceed. For example, if it reports 55 out of 60 pods, then you must investigate and resolve this issue.
- Take note of the index patterns in use on the logging service (Kibana). You will need to manually recreate them after the upgrade process is complete.
- (Optional): Prestage the solution.

  Prestaging artifacts is non-service impacting and can be completed outside of a maintenance window.

Restarting the local ChartMuseum and Docker registry on Cluster Control Manager

About this task

Use this procedure to restart the offline upgrade deployment process of Avaya Analytics™ on Cluster Control Manager (CCM).

Before you begin

Set up CCM for the Avaya Analytics™ offline deployment process.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To stop the local Docker registry and ChartMuseum processes, run the following command:

   agn-ctl stop

3. To restart the local Docker registry and ChartMuseum processes, run the following command:

   agn-ctl start

Upgrading the cluster

About this task

The cluster upgrade takes a minimum of one hour. During the upgrade, folders and virtual machines are created on the host machines visible in the vCenter of the host.

Before you begin

- Remove the previous version of Async messaging.
- Restart the CCM local Docker registry and ChartMuseum processes.

Procedure

1. Log in to Cluster Control Manager with your customer account.
2. Use a utility, such as WinSCP, to transfer the solution configuration spreadsheet to the `~/artifacts` directory.
3. To run the upgrade in the background, at the CCM prompt, type `screen`.

   When running the upgrade in the background, if you need to detach from the upgrade SSH session, see Detaching from the upgrade SSH session on page 136.
4. Go to the directory where solution spreadsheet is copied and run the **ccm upgrade spec <solution spreadsheetname>.xlsm --infra --force** command.
5. When prompted, enter your Avaya SSO credentials.
6. When prompted, type `y` to confirm the cluster node upgrade to the new version specified in the solution spreadsheet and to accept the warning reminding you to start a `screen` session.

   Only type `y` if you have already run `screen`. Do not continue with the upgrade until you do this.

   Failure to run the `screen` command exits the process and you have to start over.
7. When prompted, accept the EULA.

   Validation runs after accepting the EULA. If any part of the validation fails, you must address the detected issues and restart the upgrade.
8. When prompted to perform a backup, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local, the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

9. **(Optional)** To monitor the progress of the upgrade, run the `tail -f /var/log/avaya/ccm/ccm-main.log` command.
10. Check status of the **pgo-client** pod, it must be up and running.

Verifying the cluster node upgrade

About this task

After you complete the cluster node upgrade, verify the operational state of the cluster before continuing with the solution service upgrade. Do not continue with the solution service upgrade unless all services, except for tools-policy and utility-service, are DEPLOYED and show RUNNING or COMPLETE.

Procedure

1. Run `swversion -c` to verify that the cluster version is updated and matches what is defined in the release notes.
2. Run the `ccm smoke-test` and `ccm status --pod-details` commands.

   The pods might not be operational immediately after the upgrade. Continue running these commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.
3. If you performed a local backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.

Upgrading solution services

About this task

The cluster upgrade takes a minimum of one hour. During the upgrade, folders and virtual machines are created on the host machines visible in the vCenter of the host.

Before you begin

Restart the CCM local Docker registry and ChartMuseum processes.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2.
3. Use a utility, such as WinSCP, to transfer the solution configuration spreadsheet to the `~/artifacts` directory.

   Note:

   This spreadsheet is the file you used to download the Avaya Analytics™ software artifacts to the PC or laptop.
4. To run the upgrade in the background, at the CCM prompt, type `screen`.

   When running the upgrade in the background, if you need to detach from the upgrade SSH session, see Detaching from the upgrade SSH session on page 136.

5. Run the `ccm upgrade spec <solution spreadsheet name>.xlsm --products --force` command.
6. At the prompt, enter your vCenter credentials.
7. At the prompt, enter your Avaya SSO credentials.

   Note:

   You must enter your CCM local registry username and password that you earlier configured with the **`agn-ctl-setup`** command.
8. At the prompt, confirm the cluster upgrade to the new version specified in the solution spreadsheet.
9. When prompted, accept the EULA.

   Validation runs after accepting the EULA. If any part of the validation fails, you must address the detected issues and restart the upgrade.
10. To take a backup, enter `y`.
    - Entering `n` cancels the operation.
    - Entering `y` runs a backup after the upgrade is complete.

    The backup takes approximately 5 to 10 minutes to complete. The backup file is located at `/var/avaya/artifactCache/`
11. To restore the operation, enter the password when prompted.
12. **(Optional)** To monitor the progress of the upgrade, run the following command:

    `tail -f /var/log/avaya/ccm/ccm-main.log`
13. **(Optional)** If the upgrade exits with an error, run the following command again: `ccm upgrade spec <solution spreadsheet name>.xlsm --products --force`
14. Stop the local CCM Docker registry and ChartMuseum. See section *Stopping ChartMuseum and Docker registry on ClusterControl Manager* in this section.
15. Log in to the Cluster Control Manager (CCM) console as the customer user.
16. Switch to being the root user by entering the command `su`.
17. After the upgrade is completed, restart the database pods by running the following command and wait till the database pods are in running state:

```
kubectl get pod --no-headers -o custom-columns=":metadata.name" | grep
analyticsdb-node- | xargs kubectl delete pod
```

Verifying the solution service upgrade

About this task

Verify the upgrade of the solution services.

Procedure

1. Run the `ccm smoke-test` and `ccm status --pod-details` commands to ensure that the products are upgraded to the same version specified in the solution spreadsheet.

   The pods might not be operational immediately after the upgrade. Continue running these commands periodically at 10 minute intervals until all pods are running. If these tests continue to fail after 30 minutes, contact Avaya support personnel for assistance.
2. Run the `swversion -c` and `ccm swhistory` commands to verify that the installed software versions match the software versions specified in the deployment spreadsheet.
3. If you performed a backup, navigate to the latest backup file and transfer the file off of Cluster Control Manager.
4. **(Optional)** Delete previous backups.

Detaching from the upgrade SSH session

About this task

If you are running an upgrade in the background, use this procedure to detach from the SSH session.

Procedure

1. Start a new SSH session to Cluster Control Manager and log in with your customer account.
2. Type `screen -ls` to retrieve the screen ID of the session that is running the upgrade.
3. Type `screen -d <screen id>` to detach the session from the SSH session.
4. Close the SSH session.

   The upgrade continues to run in the background.

Reattaching to the upgrade SSH session

About this task

After detaching from the upgrade SSH session, you can use this procedure if you want to reopen the SSH session.

Procedure

1. Log in to Cluster Control Manager using your customer account.
2. At the CCM prompt, type `screen -ls` to retrieve the screen ID of the session.

   If no screen IDs are listed, the upgrade is complete.
3. Type `screen -r <screen id>` to reattach to the upgrade session.

Migration to a larger agent configuration

Checklist for migrating to a larger agent configuration

No	Task	Description	✔
1	Backup the Crunchy database and the Historical Reporting metadata present on the source system.	See “Configuring database backups” and “Creating metadata backups” in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* guide.	
2	Perform a fresh install procedure for a higher deployment option with Async messaging turned on. Ensure that the software patch level is identical on both source and target systems.	Installing Avaya Analytics for a higher deployment option on page 161	
3	Restore the Crunchy database and Historical Reporting metadata on the target system.	See “Restoring the database” and “Creating metadata backups” in the *Maintaining and Troubleshooting Avaya Analytics™ for Avaya Oceana®* guide.	

Installing Avaya Analytics for a higher deployment option

About this task

This procedure describes the migration process from 500 agents deployment to 2000 agent deployment. Use this procedure for migration, regardless of the deployment size.

Before you begin

Ensure to take a complete backup of the system before performing the migration procedure. The backup includes a backup of the application database and the Historical Reporting metadata.

Procedure

1. Delete the cluster.
2. Perform a fresh installation with the target agent deployment configuration.

   For example, 2000 agent deployment using the same software version as previously installed on the source environment.
3. Perform the post installation tasks. See Post upgrade task on page 161.
4. Restore the backup taken before the migration process.

   Upgrade to the latest release, if applicable.

Post upgrade task

Perform the following task after completing an Avaya Analytics™ upgrade. This procedure is applicable to both online and offline upgrades.

Reconfiguring SNMP alarm destinations

About this task

After upgrading the Avaya Analytics™ to latest release, you must reconfigure alarms with Avaya™ Services as a destination as it was configured in previous release.

For reconfiguring you need to remove destinations from Avaya Analytics™ SNMP configuration and then add it again.

Before you begin

Ensure that you have Passwords of the SNMPv3 user configured for the NMS, Authentication passwords and Privacy passwords for the existed at the current configuration SNMP destinations.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. To select the **SNMP** option, enter the corresponding number.
5. To select the **List the current destination for sending SNMP alarms** option, enter the corresponding number.
6. Copy and save the result list of destinations to a file.
7. Return to the previous page by entering `b`.
8. To select the **Delete configured destination address** option, enter the corresponding number.
9. In the **Proceed with SNMP Destination deletion** field, type **y**.

   Entering `n` cancels the operation.
10. Enter the **Destination IP address**, which needs to be deleted from destinations configuration
11. Return to the previous page by entering `b`.
12. Repeat the above deletion steps to delete all the destinations mentioned in the saved list of destinations.
13. Add all the SNMP destinations using the saved list of destinations.

Verifying the upgrade

About this task

Use this procedure to verify that the upgrade is successful and the Avaya Analytics™ components are running.

Before you begin

Complete the post installation verification steps mentioned in this document.

Procedure

1. To verify that Historical Reporting is running, do the following:
   a. Log in to Historical Reporting.
   b. Run one or more reports.
2. To verify Real Time reporting is running, do the following:
   a. Initiate voice or multimedia contact.
   b. Log in to Avaya Workspaces and verify that the real-time reports are updating.
3. Create the index patterns from the note you recorded while preparing for the upgrade in the Kibana or the logging interface.
4. Remove the CCM Virtual Machine snapshot taken at the beginning of the upgrade procedure.

   Warning:

   Failure to remove the snapshot can result in performance degradation of the CCM virtual machine and the ESXi host.

Reverting a failed upgrade to the previous release

About this task

After a failed upgrade, use this procedure to downgrade or revert back to the previous release of Avaya Common Services.

Before you begin

Ensure that you have:

- The original solution configuration spreadsheet used to install the previous release to which you are reverting back.

Procedure

1. Run `ccm uninstall --force` to uninstall the cluster and services as required.

   If the cluster uninstall fails, contact Avaya support personnel for assistance.
2. In vCenter, revert Cluster Control Manager to the snapshot image taken before the upgrade.
3. Log in to the restored snapshot of Cluster Control Manager and run the `ccm uninstall-cluster --force` command.

   If the node removal fails, contact Avaya support personnel for assistance. Manual cleanup might be required.
4. On Cluster Control Manager, type `screen` to run the installation in the background.

5. Using the original solution configuration spreadsheet, which is compatible with the release you are reverting back to, run the `ccm install <solution spreadsheet name>.xlsx` command.
6. Restore application data using the information in your solution documentation.

Chapter 14: Post installation tasks

Post installation overview

Perform the following mandatory tasks after deploying Avaya Analytics™ on Avaya Common Services. To perform these tasks, log in to the Cluster Control Manager (CCM) console as a cust user and then switch to a root user. Root user access might not be required for some steps as indicated in the respective procedures.

To complete some of these procedures you require access to:

- Cluster Control Manager IP address
- System Manager IP address
- Authorization Service Avaya Breeze® node SIPs
- Avaya Oceana® Cluster 1 Avaya Breeze® Node SIPs
- Avaya Control Manager

Note:

The post-install script might take some time to display the options after you run the **`ccm release orca analytics`** command or might display the following message: `Failed to get auth token`. Wait for some time or type the command again.

Linking LDAP to a group

About this task

Use this procedure only if you configured LDAP while installing Avaya Analytics™ by using the `Avaya_Oceana_Application_Deployment.xlsm` spreadsheet. This procedure manually links your LDAP groups to the corresponding Avaya Analytics™ groups with the appropriate user privileges assigned to the respective groups.

Before you begin

You must create three groups on LDAP to add users into for linking them to the respective groups with the appropriate user privileges in Avaya Analytics™.

For example:

- Consumer
- Basic

- Advanced

Note:

You must create supervisors and supervisor groups on or below the search root path. You can store them at a location that is one or more levels below the search root folder. The search root path must include both supervisors and supervisor groups.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Historical Reporting** by pressing the corresponding number.
5. Select the **LDAP Configuration** option by entering the corresponding number.
6. Select the **Link LDAP to a Group** option by entering the corresponding number.
7. In the **Proceed to LDAP groups config** field, enter `y`.

   Entering `n` cancels the operation.

   The CCM console displays the options to create a link between the users and groups in the LDAP directory and in Avaya Analytics™.
8. In the **basicLDAPLINK DN** field, type the input parameter for linking the Basic group to the LDAP group and press **Enter**.

   For example, `CN=Basic,CN=Users,DC=CCQPUNE,DC=AVAYA,DC=COM`
9. In the **advancedLDAPLINK DN** field, type the input parameter for linking the Advanced group to the LDAP group and press **Enter**.

   For example, `CN=Advanced,CN=Users,DC=CCQPUNE,DC=AVAYA,DC=COM`
10. In the **consumerLDAPLINK DN** field, type the input parameter for linking the Consumer group to the LDAP group and press **Enter**.

    For example, `CN=Consumer,CN=Users,DC=CCQPUNE,DC=AVAYA,DC=COM`
11. Return to the previous page by entering `b`.
12. Quit the current page by entering `q`.
13. Return to the main menu by entering `m`.

Certificate authentication and token validation checklist

The following procedures provide a worked example of using System Manager for signing a Certificate Signing Request (CSR) file. To complete the certificate authentication and token validation for Avaya Oceana®, maintain the sequence in the following table:

- If an intermediate Certificate Authority (CA) signs your CSR, use the full certificate chain in a single `.pem` file.
- If you have separate files, such as signed certificate, intermediate CA, and root CA, combine these files into a single `.pem` file before importing them into the keystore.

Note:

Ensure to maintain the following order of the certificates in the above instances in the `.pem` file:

1. Signed certificate
2. Intermediate certificate
3. Root certificate

No.	Task	Notes	✔
1	Get the AuthorizationService node and cluster information.	See, Obtaining AuthorizationService node and cluster information on page 168	
2	As a root user, to rename the current ssl directory, run the following command: **`mv /home/cust/ssl /home/cust/ssl4001`**	This step is required only for upgrades from version 4.0.0.1. Ensure that the name of the folder containing the new certificates is different from `/home/cust/ssl4001`.	
3	Create Certificate Signing Request for Avaya Oceana® authentication.	See, Creating Certificate Signing Request for Avaya Oceana Authentication on page 169	
4	Get the `.csr` file signed.	Getting the Certificate Signing Request file signed on page 170	
5	Get identity token.	See, Getting identity token on page 172	
6	Import signed certificate for Avaya Oceana® authentication.	See, Importing signed certificate for Avaya Oceana authentication on page 173	
7	Retrieve the identity certificates.	See, Retrieving the identity certificates on page 174	
8	Create Avaya Breeze® keystore.	See, Creating Avaya Breeze certificates keystore on page 175	

Table continues…

No.	Task	Notes	✔
9	Restart the relevant services.	See, • Restarting Avaya Breeze Authentication on page 181 • Restarting Streams REST on page 182 • Restarting Data Publisher on page 182 • Restarting Reliable Eventing Framework Input Adapter on page 183 • Restarting the Open Kafka interface on page 184	

Obtaining AuthorizationService node and cluster information

About this task

Perform the following procedure to obtain information about the Avaya Breeze® platform nodes and clusters that AuthorizationService is installed on. This information is required during certificate configuration.

Procedure

1. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Service Management** > **Services**.
2. Click **AuthorizationService**.
3. From the **Service Status** list, note the names of the nodes where the AuthorizationService is installed and the cluster information for those nodes.
4. On the System Manager web console, click **Elements** > **Avaya Breeze®** > **Cluster Administration**.
5. Expand the cluster where the AuthorizationService SVAR is installed.
6. Click on each Avaya Breeze® platform node and note their SIP Entity IP addresses.

Creating Certificate Signing Request for Avaya Oceana® Authentication

About this task

A Certificate Signing Request (CSR) file is an encoded text file that contains information about the organization and the domain that you want secure. This file is required for the activation of a digital SSL certificate and is generated on the server where you plan to install the certificate. A CSR is submitted to the Certificate Authority (CA) and used to generate the certificate. Use this procedure to create CSR for Avaya Oceana® authentication.

Note:

Avaya does not endorse the use of wildcard certificates.

Before you begin

Obtain AuthorizationService node and cluster information.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Deployment** by pressing the corresponding number.
5. Select the **Create Certificates for authentication and token validation** option by entering the corresponding number.

   The CCM console displays the following options:

   a. `Create keystore for Oceana Authentication`

   b. `Create Breeze Certs keystore to validate tokens`
6. Select the **Create keystore for Oceana Authentication** option by entering the corresponding number.
7. To create CSR for Oceana authentication, select the **Create Certificate Signing Request (CSR) for Oceana Authentication** option by selecting the corresponding number.
8. In the **Proceed to csr creation** field, enter `y`.

   Entering `n` cancels the operation.
9. In the **Enter the path location on CCM to store the CSR that will be created** field, enter the desired location.

   The default location is `/home/cust/ssl`
10. Configure the following parameters according to their descriptions mentioned in the table and press **Enter**:

Parameter	DN field	Description	Example or To Do
COUNTRY	**Country**	The two-letter ISO abbreviation for your country.	IE
STATE	**State or Province**	The state or province where your organization is legally located. Do not use an abbreviation.	Connacht
CITY	**City or Locality**	The city where your organization is legally located.	Galway
ORGANIZATION	**Organization Name**	The exact legal name of your organization.	AVAYA
ORG_UNIT	**Organizational Unit Name**	The section of the organization.	Analytics
MACHINE_NAME	**Common Name**	Your name or the hostname of the server.	ccm13940.apclab.com
SANS	Subject Alternative Name	Define alternative names or specify additional host names for a single SSL certificate. If multiple, separate with space.	ccm130100 10.134.139.100 If not applicable leave blank.
YOUR_EMAIL	**Email Address**	Your email address.	If not applicable leave blank.
[ ]	—	A challenge password.	Leave blank
[ ]	—	An optional company name.	Leave blank

11. At the prompt for **Please enter a password that will be used to encrypt the Private Key**, enter a new password to encrypt the private key of the certificate.

    The CCM console displays a message that the CSR and certificate are generated.

12. Check that the CSR file is available in your selected directory.

Next steps

1. Get the CSR file signed.
2. Add the signed certificate to System Manager to obtain an identity token.

Getting the Certificate Signing Request file signed

About this task

You must get your Certificate Signing Request (CSR) file signed. The steps in this procedure are a working example of getting the CSR file signed by System Manager.

For information on getting CSR file signed by third party CA, refer to *Certificate Management* section in this document.

Procedure

1. To get the `.csr` file signed, copy the `.csr` file onto your local machine.
2. To create an end entity in System Manager, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Add End Entity**.
3. On the Add End Entity page, do the following:

DN field	Description	Example or To Do	
End Entity Profile	The unique end entity profile.	Click **EXTERNAL_CSR_PROFILE**	
Username	Your username.	Galway	
Password or Enrollment Code	New REF certificate password.	Galway	
Confirm Password	New REF certificate password.		
SANS	Subject Alternative Name	Define alternative names or specify additional host names for a single SSL certificate If multiple, separate with a space	ccm130100 10.134.139.100 If not applicable leave blank.
Email Address	Your email address.	abc@avaya.com	
CN, Common Name	The FQDN of the CCM server.	ccm13940	
CN, Common Name	The server host name or your name.	ccm13940	
O, Organization	The exact legal name of your organization.	AVAYA	
C, Country (ISO 3166)		IE	
OU, Organizational Unit	The section of the organization.	Analytics	
L, Locality	-	Galway	
ST. State or Province	-	Galway	

4. Leave the other fields blank and click **Add**.
5. To create a PEM file using end entity in System Manager, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Public** > **Web** > **Create Certificate from CSR**.

6. On the Certificate enrollment from a CSR page, do the following:
   - Enter the username.
   - Enter the enrollment code.
   - Choose the `.csr` file
   - In the **Result type** field, select **PEM - certificate only**.
7. Click **OK**.
8. To get the System Manager PEM file, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Public Web** > **Fetch CA Certificates** > **Download as PEM**.
9. Copy both the PEM files on to CCM into the directory that was created in the previous script as a root user. For example, `/home/cust/ssl`

   You can also copy the files to another location and then move the files into the `/home/cust/ssl` directory by using the command line.

Next steps

Use the signed certificate to get the identity token.

Getting identity token

About this task

To get the identity token, you must add the signed certificate to System Manager.

Before you begin

Ensure to get the CSR signed

Procedure

1. Log in to System Manager.
2. Click **Elements** > **Avaya Breeze®** > **Configuration** > **Authorization**.
3. On the Authorization Configuration page, click **New**.
4. On the New External Authorization Client page, do the following:
   a. In the **Name** field, enter the name of your client.
   b. In the **Certificate** field, browse to the location of the signed CSR certificate file.

      System Manager generates a clientkey.
   c. Note down the key ID details.

Note:

You must use the same key ID later when you are create your secrets. The clientKey is later used when you complete the second part of the script for certificates for authentication and token validation.

For example, OCEANA.authenticationService.server1clientKey=6DutVilZQLi3YA_tHMFZgw

Importing signed certificate for Avaya Oceana® authentication

About this task

You must import the signed certificate to Cluster Control Manager and in the directory that you used while creating Certificate Signing Request (CSR) for Avaya Oceana® authentication.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Deployment** by pressing the corresponding number.
5. Select the **Create Certificates for authentication and token validation** option by entering the corresponding number.

   The CCM console displays the following options:

   a. `Create keystore for Oceana Authentication`.

   b. `Create Breeze Certs keystore to validate tokens`.
6. Select the **Create keystore for Oceana Authentication** option by entering the corresponding number.
7. To import signed certificate, select the **Import signed certificate for Oceana Authentication** option by selecting the corresponding number.
8. In the **Proceed to import cert** option, enter `y` and press **Enter**.

   Entering `n` cancels the operation.
9. In the **Please confirm that you saved the signed cert and root cert files to the CCM and in the directory that was used in the first option 'Create Certificate Signing Request (CSR) for Oceana Authentication'** field enter `y`.

   Entering `n` cancels the operation.

10. In the **Enter the path location on CCM where the csr file was created from the option 'Create Certificate Signing Request (CSR) for Oceana Authentication'** field, enter the required location.

    The default location is `/home/cust/ssl`.

11. In the **Please enter the file name of the signed certificate** field, enter the required file name.

    For example, `signed.pem`.

12. In the **Please enter the file name of the root CA certificate** field, enter the required file name.

    For example, `SystemManagerCA.pem`.

13. In the **Please enter a password for the Oceana Authentication cert keystore that will be created** field enter the password and re-enter the password at the prompt.
14. At the prompt for **Please enter the password used for encrypting the Private Key**, enter the password you used to encrypt the private key.
15. In the **Please enter SMGR IP address** field, enter the SMGR IP address.
16. Enter SIP Entity IP address for Avaya Breeze® node 1, where the AuthorizationService is installed.
17. Enter SIP Entity IP address for Avaya Breeze® node 2, where the AuthorizationService is installed.
18. Enter SIP Entity IP address for Avaya Breeze® node 3, where the AuthorizationService is installed.

    Leave this field blank if not applicable.

19. Enter the Avaya Breeze® node port.

    The default port is 443.

Retrieving the identity certificates

About this task

You must retrieve the identity certificates from System Manager and save files to your CCM server to the same location where you saved the certificate creation scripts.

Before you begin

Procedure

1. On System Manager, navigate to **Services** > **Inventory** > **Manage Elements**.
2. Select the first Avaya Breeze® node that the authentication service uses.
3. Click **More Actions** and select **Manage Identity Certificates**.

4. Click **Authorization** > **Export**.
5. Select the second Avaya Breeze® node that is used by the authentication service.
6. Click **More Actions** and select **Manage Identity Certificates**.
7. Click **Authorization** > **Export**.
8. Select the third Avaya Breeze® that is used by the authentication service.

   The third Avaya Breeze® node is available only on the 100 agents footprint configuration.
9. Click **More Actions** and select **Manage Identity Certificates**.
10. Click **Authorization** > **Export**.
11. Rename the `.pem` files.

    Important:

    Avoid spaces while renaming the files, for example, `identity-cert-4496.pem`
12. Copy the `.pem` files to the directory created to hold the certificates in the *Creating Certificate Signing Request for Avaya Oceana® Authentication* section in this document.

    The default location is `/home/cust/ssl`.

Creating Avaya Breeze® certificates keystore

About this task

You must create Avaya Breeze® certificates keystore for validating tokens.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Deployment** by pressing the corresponding number.
5. Select the **Create Certificates for authentication and token validation** option by entering the corresponding number.

   The CCM console displays the following message:

   `Select which keystore you would like to configure.`

   a. `Create keystore for Oceana Authentication.`

   b. `Create Breeze Certs keystore to validate tokens.`

6. In the **Please select the type of certs you would like to create** field, enter the number corresponding to the **Create Breeze Certs keystore to validate tokens** option.
7. To confirm that you saved the renamed identity-cert PEM files to CCM and in the directory that was used in the **Create Certificate Signing Request (CSR) for Oceana Authentication** option, enter `y`.

   Entering `n` cancels the operation.
8. To store the certificates this procedure creates, enter the location of the path on CCM.

   The default path is `/home/cust/ssl`.
9. At the prompt, enter the name of the Avaya Breeze® node 1 identity certificate.

   For example, `identity-cert-1.pem`.
10. At the prompt, enter the name of the Avaya Breeze® node 2 identity certificate.

    For example, `identity-cert-2.pem`.
11. At the prompt, enter the name of the Avaya Breeze® node 3 identity certificate.

    For example, `identity-cert-3.pem`. If not applicable, leave blank.
12. Enter the password for the Avaya Oceana® Authentication cert keystore.

    The CCM console displays the message that the certificate was added to the keystore.
13. Enter the full URL for the Avaya Oceana® Avaya Breeze® 1 TokenEndpoint.
14. Enter the full URL for the Avaya Oceana® Avaya Breeze® 2 TokenEndpoint.
15. For 100 agents footprint configuration, enter the full URL of the Avaya Oceana® Avaya Breeze® 3 TokenEndpoint, if applicable.
16. Enter the Avaya Oceana® clientKey. For example, `MFyaFHFyRAKXXTiH9Ss6uA`.

    Wait for the CCM console to create the breeze-security secret and restart the orca-breeze-authentication pod.
17. Quit the current page by entering `q`.

Creating certificates for connecting to Avaya Breeze® Reliable Eventing Framework

About this task

Connections to the Reliable Eventing Broker (ActiveMQ) use TLS authentication. External clients, other than snap-ins, require an identity certificate issued by the System Manager CA for that connection.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. Select **Deployment** by pressing the corresponding number.
5. Select the **Create Certificates for connecting to REF** option by entering the corresponding number.
6. In the **Please enter the value for the type of certs you would like to create** field, enter the number corresponding to the **Create a Certificate Signing Request for connecting to REF** option.
7. To store the CSR that this procedure creates, enter the location on CCM. The default location is `/home/cust/sslRef`.
8. Configure the following parameters according to their descriptions mentioned in the table:

Parameter	DN field	Description	Example or To Do
COUNTRY	**Country**	The two-letter ISO abbreviation for your country.	`IE`
STATE	**State or Province**	The state or province where your organization is legally located. Do not use an abbreviation.	`Galway`
CITY	**City or Locality**	The city where your organization is legally located.	`Galway`
ORGANIZATION	**Organization Name**	The exact legal name of your organization.	`AVAYA`
ORG_UNIT	**Organizational Unit Name**	The section of the organization.	`Analytics`
MACHINE_NAME	**Common Name**	The FQDN of the CCM server.	`ccm13940`
SANS	Subject Alternative Name	Define alternative names or additional host names for a single SSL certificate. Separate multiple entries with spaces. If not applicable leave blank.	`ccm130100 10.134.139.100`
YOUR_EMAIL	**Email Address**	Your email address	
Extra attribute	—	A challenge password	Enter a password
Extra attribute	—	An optional company name	Enter an optional company name

The CCM console creates the `.csr` file in the specified location.

9. At the prompt for **Please enter a password that will be used to encrypt the Private Key**, enter a new password to encrypt the private key of the certificate.
10. To confirm that the `.csr` file is available in the specified directory, run the following command: **`ls -l <path>`** where `<path>` is the directory you specified in step 7.
11. Quit the current page by entering `q`.
12. To get the `.csr` file signed, copy the `.csr` file onto your local machine.

Create end entity in System Manager

About this task

Using this procedure to create an end entity in System Manager. The following steps are a worked example of using System Manager as the CA.

Procedure

1. In System Manager, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Add End Entity**.
2. On the Add End Entity page, do the following:

DN field	Description	Example or To Do
End Entity Profile	The unique end entity profile.	Click **EXTERNAL_CSR_PROFILE**
Username	Your username.	`Galway`
Password or Enrollment Code	New REF certificate password.	`Galway`
Confirm Password	New REF certificate password.	
SANS	Subject Alternative Name	Define alternative names or additional host names for a single SSL certificate. Separate multiple entries with spaces. If not applicable leave blank. `ccm130100 10.134.139.100`
Email Address	Your email address.	`abc@avaya.com`
CN, Common Name	The FQDN of the CCM server.	`ccm13940`
CN, Common Name	The server host name or your name.	`ccm13940`
O, Organization	The exact legal name of your organization.	`AVAYA`
C, Country (ISO 3166)		`IE`
OU, Organizational Unit	The section of the organization.	`Analytics`
L, Locality	-	`Galway`
ST. State or Province	-	`Galway`

3. Leave the other fields blank and click **Add**.
4. To create a PEM file using the end entity in System Manager, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Public** > **Web** > **Create Certificate from CSR**.
5. On the Certificate enrollment from a CSR page, do the following:
   - Enter the username.
   - Enter the enrollment code.
   - Choose the `.csr` file
   - In the **Result type** field, select **PEM - certificate only**.
6. Click **OK**.
7. To get the System Manager PEM file, click **SMGR** > **Services** > **Security** > **certificates** > **Authority** > **Public Web** > **Fetch CA Certificates** > **Download as PEM**.
8. Copy both the `.pem` files on to CCM into the directory that was created in the previous script as a root user. For example, `/home/cust/sslRef`.

   You can also copy the files to another location and then move the files into the `/home/cust/sslRef` directory by using the command line.

   Note:

   Ensure to maintain the following order of the certificates in the `.pem` files:

   a. Signed certificate
   b. Intermediate certificate
   c. Root certificate

Import the signed PEM file and root CA PEM file into your keystore

About this task

In the following steps, you can import the signed `PEM` file and `root CA PEM` file into your keystore.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`

4. Select **Deployment** by pressing the corresponding number.
5. Select the **Create Certificates for connecting to REF** option by entering the corresponding number.

   The CCM console displays the following message:

   a. `Create a Certificate Signing Request for connecting to REF.`

   b. `Import the signed PEM file and root CA PEM file into your keystore.`
6. In the **Please enter the value for the type of certs you would like to create** field, enter the number corresponding to the **Import the signed PEM file and root CA PEM file into your keystore** option.
7. To confirm that you saved the signed `PEM` file and `root CA PEM` file to CCM and in the directory that was used for creating the CSR file earlier, type `y` and press **Enter**.
8. To store the certs that are created, enter the location on CCM.

   The default path is `/home/cust/sslRef`.
9. Enter the file name of the signed pem. For example, `signed.pem`.
10. Enter the file name of the ROOTCA pem. For example, `SystemManagerCA.pem`.
11. At the prompt for **Please enter the password used for encrypting the Private Key**, enter the password you used to encrypt the private key.
12. Enter the password for the `ref-input-adaptor.jks` keystore.

    Important:

    This password must match the password of the **config:orca-ref-input-adaptor:oceana:certificate:password** field that you entered in the spreadsheet before installing Avaya Analytics™.

    Wait for the CCM console to create the oceana-ref secret.
13. Quit the current page by entering `q`.

Creating certificates for Avaya Workspaces clients

About this task

Create security certificates that you can use to secure the connection between Avaya Workspaces and Avaya Analytics™.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.

3. To create a certificate for Avaya Workspaces client, do the following:
   a. Run the Avaya Analytics™ Administration script using the following command:

      ccm release orca analytics

   b. Enter a number corresponding to the **Deployment** option.
   c. Enter a number corresponding to the **Create Certificate for Workspaces client** option.
   d. The **Proceed to Workspaces client cert creation? [y/n]** message displays. Enter **y**.
   e. Enter the path of the location on which CCM stores the extracted certificate. The default path is `/home/cust/ssl`.
4. Copy the `myFlexRootCA.pem` file to the windows machine on which the Workspaces client is running.
5. Connect to the Windows client on which the Avaya Workspaces browser is running and run the following command: **certmgr.msc**
6. Select **Trusted Root Certificate Authorities**.
7. Right-click the `Certificate` folder and click **All Tasks** > **Import**.
8. Select **Local Machine**.
9. Select `myFlexRootCA.pem` and click **Import**.

Note:

You can deploy the Avaya Workspaces certificate to all Windows clients using Group policy or logon script.

Restarting Avaya Breeze® Authentication

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To run the `Analytics Administration` script, use the following command:

   ccm release orca analytics

3. Select **Deployment** by pressing the corresponding number.
4. Select **Service Restart Options** by pressing the corresponding number.
5. To restart the Avaya Breeze® Authentication service, select the **Restart Breeze Authentication** option by entering the corresponding number.
6. In the **Proceed with Breeze Authentication restart** field, type `y`.

   Entering `n` cancels the operation.

   Wait for the service to start running.

7. Return to the previous page by entering `b`.
8. Quit the current page by entering `q`.
9. Return to the main menu by entering `m`.
10. To check the status of Breeze Authentication, run the following command as the root user:

    `kubectl get pods | grep breeze-auth`

Restarting Streams REST

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
3. Select **Deployment** by pressing the corresponding number.
4. Select **Service Restart Options** by pressing the corresponding number.
5. To restart the Streams Rest service, select the **Restart Streams Rest** option by entering the corresponding number.
6. In the **Proceed with Streams Rest restart** field, enter `y`.

   Wait for the service to start running.
7. Return to the previous page by entering `b`.
8. Quit the current page by entering `q`.
9. Return to the main menu by entering `m`.
10. To check Streams REST status, run the following command as a root user:

    `kubectl get pods | grep streams-rest`

Restarting Data Publisher

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
3. Select **Deployment** by pressing the corresponding number.

4. Select **Service Restart Options** by pressing the corresponding number.
5. To restart the Data Publisher, select the **Restart Data Publisher** option by entering the corresponding number.
6. In the **Proceed with Data Publisher restart**, enter `y`.

   Entering `n` cancels the operation.

   Wait for the service to start running.
7. Return to the previous page by entering `b`.
8. Quit the current page by entering `q`.
9. Return to the main menu by entering `m`.
10. To check the Data Publisher status, run the following command as a root user:

    `kubectl get pods | grep data-publisher`

Restarting Reliable Eventing Framework Input Adapter

About this task

You must restart the Reliable Eventing Framework Input Adapter to restart the Breeze authentication service.

Before you begin

To check if the admin-data service status is displayed as running, use the following command on the Cluster Control Manager (CCM) console:

`kubectl get pods | grep admin-data`

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
3. Select **Deployment** by pressing the corresponding number.
4. Select **Service Restart Options** by pressing the corresponding number.
5. To restart the Reliable Eventing Framework Input Adaptor service, select the **Restart Ref Input Adaptor** option by entering the corresponding number.
6. In the **Proceed with REF Input Adaptor restart** field, enter `y`.

   Entering `n` cancels the operation.

   Wait for the service to start running.
7. Return to the previous page by entering `b`.

8. Quit the current page by entering `q`.
9. Return to the main menu by entering `m`.
10. To check the status of Reliable Eventing Framework Input Adaptor, run the following command as the root user:

    `kubectl get pods | grep ref-input`

Restarting the Open Kafka interface

Before you begin

Check if the admin-data service status is displayed as running by using the following command on the Cluster Control Manager (CCM) console: **`kubectl get pods | grep open-interface-kafka`**

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
3. Select **Deployment** by pressing the corresponding number.
4. Select **Service Restart Options** by pressing the corresponding number.
5. To restart the Open Kafka interface, select the **Restart Open Interface Kafka Interface** option by entering the corresponding number.
6. In the **Proceed with Kafka interface restart** field, enter `y`.

   Entering `n` cancels the operation.

   Wait for the service to start running.
7. Return to the previous page by entering `b`.
8. Quit the current page by entering `q`.
9. Return to the main menu by entering `m`.

Configuring SAML authentication for Historical Reporting

About this task

Use this procedure to configure SAML authentication post-installation of Avaya Analytics™. You can use this procedure to configure and generate the SAML files on Historical Reporting linking to profile created on an Identity Provider (IDP).

Before you begin

- You must create the following three groups on Active Directory and Identity Provider and add Avaya Analytics™ reporting supervisors into these groups:
  - Consumer
  - Basic
  - Advanced

  These groups link Avaya Analytics™ reporting supervisors to the respective groups with appropriate user privileges in Avaya Analytics™.
- You must create a relying party trust (ADFS) profile on your IDP. For more information refer to *Creating a relying party trust* section in *Avaya Analytics™ maintenance and troubleshooting guide*.
- Note the relying party trust identifier and the relying party SAML SSO service URL.

  The relying party trust identifier is the unique identifier of the web application. The relying party configured SAML SSO service URL is the URL that IDP sends and receives in SAML requests and responses.
- The `/saml/SSO` is removed from the end of the URL.
- Export the IDP metadata.xml and make it available on the CCM.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. To select the **Historical Reporting** option, enter the corresponding number.
5. To select the **SAML** option, enter the corresponding number.
6. To select the **Enable SAML** option, enter the corresponding number.
7. Enter the full path and file name to the **IDP Metadata XML** file on CCM for the web.
8. Enter the full path and file name to the **IDP Library Metadata XML** file for the library.
9. Enter the **Unique Identifier of the web application** that recognizes the IDP.

   For example, **AnalyticsWebHome**.
10. Enter the **Web URL** from which IDP sends and receives SAML requests and responses.

    For example, https://cluster.fqdn/AvayaAnalytics.
11. Enter **Unique identifier of the library application** to be recognized by the IDP. Leave it blank if not applicable.

    For example, **AnalyticsLibHome**.
12. Enter **Library URL** from which IDP sends and receives SAML requests and responses. Leave it blank if not applicable.

For example, `https://cluster.fqdn/MicroStrategyLibrary`.

Note:

The above mentioned example library URL is applicable for release 4.3.1.0 and later. For older releases, use the Library URL - `https://cluster.fqdn/AvayaAnalytics/library`.

13. Set **SAML behind a proxy** to `True`.
14. Enter **SAML signature algorithm**. For example, SHA256WITHRSA.
15. If, SAML encryption key is required, set **Generate SAML encryption key** as `True`. Otherwise, set it to `False`.
16. In the **User display name** attribute, enter `DisplayName`.
17. In the **User email address** attribute, enter `EMail`.
18. In the **User distinguished name** attribute, enter `DistinguishedName`.
19. In the **User group attribute**, enter `Groups`.
20. In the **Group attribute format**, enter `Simple`.
21. In the **Groups** (Advanced, Basic, Consumer) that can access Web Administrator page. Leave it blank if not applicable.
22. Enter **Authentication method** when accessing an admin page. Set to `1` to use standard authentication or `2` to protect with SAML Authentication.

    Note:

    If set to 2, a group needs to be entered in the step. Enter the groups (Advanced, Basic, Consumer) that can access Web Administrator.

23. Confirm the following settings (y/n):

    SAML configuration

    IDP Metadata XML file: `/home/cust/IDPMetadata.xml`

    IDP Library Metadata XML file(blank if not applicable): `/home/cust/IDPMetadata.xml`

    Unique identifier of the web application: `AnalyticsWebHome`

    URL the IDP sends and receive SAML requests: `https://cluster.fqdn/AvayaAnalytics`

    Unique identifier of the library application:`AnalyticsLibHome`

    Library URL,(blank if not applicable):`https://cluster.fqdn/AvayaAnalytics/library`

    Use Proxy,(blank if not applicable): `true`

    SAML signature algorithm: `SHA256WITHRSA`

Generate SAML encryption key: `false`

DisplayName: `DisplayName`

Email: `EMail`

DistinguishedName: `DistinguishedName`

Groups: `Groups`

Group format: `Simple`

Admin Groups: `Advanced`

Authentication method: `1`

The SAML authentication for historical reporting is configured.

Map SAML users to Historical Reporting local or LDAP users

About this task

Use this procedure to map SAML users to Historial reporting local or LDAP users.

Before you begin

SAML is enabled for Historical reporting.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. To select the **Historical Reporting** option, enter the corresponding number.
5. To select the **SAML** option, enter the corresponding number.
6. To select **Map SAML users to Historical reporting**, enter the corresponding number.
7. To **Map a single SAML user to Historical reporting**, enter the corresponding number.
   a. Enter **Username** of the local or LDAP user.
   b. Enter **Name ID** of the SAML user from the SAML assertion.

      The entered SAML user is mapped with Historical reporting local or LDAP user.

8. To map the list of SAML users to Historical reporting local users, do the following:
    a. To select the **Generate a user list that can be imported to map SAML users to Historical Reporting**, enter the corresponding number.

       A list of SAML users is generated using user information stored in Avaya Analytics™ metadata. This file is stored in a path, such as, `/home/cust/saml_user_list_2022-02-17_13-49.scp`.

    b. Open the user file in the new terminal window to review and make necessary corrections.

       Note:

       The SAML Name ID must be correct to map SAML users to Historical reporting local users.

       For example,

       `cat /home/cust/saml_user_list_2022-02-17_13-49.scp`

       Alter USER "username1" TRUSTEDLOGIN "**username1**";

       Alter USER "username2" TRUSTEDLOGIN "**username2**";

       Alter USER "username3" TRUSTEDLOGIN "**username3**";

       Here, you can review the Name IDs in bold letters and correct them if necessary.

    c. Return to the previous terminal window where the menu is still open.

    d. To return to the previous page, type `b` and press **Enter**.

    e. To select **Import user list for mapping SAML users to Historical Reporting**, enter the corresponding number.

    f. Enter the file path of the user's list.

       For example, `/home/cust/saml_user_list_2022-02-17_13-49.scp`.

    The SAML users are mapped to Historical reporting local users.

9. To verify if the SAML users are mapped to Historical reporting local users, perform the following steps:
    a. To select the **Historical Reporting** option, enter the corresponding number.

    b. To select the **SAML** option, enter the corresponding number.

    c. To select **Map SAML users to Historical reporting**, enter the corresponding number.

    d. To **List mapped SAML users with Historical reporting**, enter the corresponding number.

Copying Historical Reporting SPMetadata.xml to CCM

About this task

Use this procedure to copy Historical Reporting Service Provider SPMetadata.xml to CCM and add its encryption certificate to Identity Provider relying party trust.

Before you begin

A relying party trust is created on the Identity Provider.

The SAML configuration procedure is completed.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. To switch to the root user, type **su** and press **Enter**.
3. To run the Analytics Administration script, use the following command:

   ```
   ccm release orca analytics
   ```

4. To select the **Historical Reporting** option, enter the corresponding number.
5. To select the **SAML** option, enter the corresponding number.
6. To select the **Show SAML configuration** option, enter the corresponding number.

   SAML configuration status is displayed.
7. To select **Export SPMetadata.xml file for SAML**, enter the corresponding number.
8. The SPMetadata.xml is exported to `/var/avaya/artifactCache/saml/ directory` and date and time are appended.
9. WinSCP the SPMetadata.xml from the CCM onto the Identity provider server.
10. Add the **Signing certificate to relying party trust** using, following steps:
    a. Using notepad or another editor, open SPMetadata.xml and copy the certificate into a new file. The signing certificate is identified by the tag **`<md:KeyDescriptor use="signing">`**.

       Note:

       Copy the data between the **`<ds:X509Certifcate>`** tags but not the tags.

    b. Save the file as a .cer file type.
    c. Select properties to edit the relying party trust and navigate to the **Signature** tab.
    d. Select **Add** and navigate to the location where the `.cer` file is saved.
    e. Select the certificate and **Open** to import.
    f. Click **Ok**.

11. To add the **Encryption certificate to relying party trust** use the following steps:
    a. Using notepad or another editor, open SPMetadata.xml and copy the certificate into a new file. The encryption certificate is identified by the tag **<md:KeyDescriptor use="encryption">**.

       Note:

       Copy the data between the **<ds:X509Certifcate>** tags but not the tags.

    b. Save the file as a `.cer` file type.
    c. Select properties to edit the relying party trust and navigate to the **Encryption** tab.
    d. Select **Browse** and navigate to the location where the `.cer` file is saved.
    e. Select the certificate and Open to import.
    f. Click **Ok**.

Disable SAML authentication for Historical Reporting

About this task

Use this procedure to disable SAML authentication for Historical Reporting.

Before you begin

SAML authentication is enabled on Historical Reporting.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   ccm release orca analytics
4. To select the **Historical Reporting** option, enter the corresponding number.
5. To select the **SAML** option, enter the corresponding number.
6. To select the **Disable SAML**, enter the corresponding number.

Configuring SNMP alarm destinations

About this task

You must configure alarms with Avaya™ Services as a destination.

To receive notifications on security or fault-related events, configure the details of your Network Management System (NMS), such as the authentication protocol configured for NMS and listening port of the configured NMS.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To run the `Analytics Administration` script, use the following command:

   `ccm release orca analytics`
4. To select the **SNMP** option, enter the corresponding number.
5. To select the **Configure a destination for sending SNMP alarms** option, enter the corresponding number.
6. In the **Proceed with SNMP Desctination config** field, type **y**.

   Entering `n` cancels the operation.
7. In the **Hostname/IP of the configured NMS destination** field, type the hostname or IP address of your NMS and press **Enter**.
8. In the **Listening port of the configured NMS** field, enter the port number of your NMS.

   The default option is `162`.
9. In the **Username of the SNMPv3 user configured for the NMS** field, type the username of an SNMP user that can access the NMS and press **Enter**.
10. In the **Password of the SNMPv3 user configured for the NMS** field, type the password of an SNMP user that can access the NMS and press **Enter**.
11. In the **Authentication protocol configured for NMS** field, type the NMS authentication protocol in use and press **Enter**.

    The options are:

    - `SHA`
    - `MD5`
12. In the Privacy protocol configured for NMS, type the NMS privacy protocol in use and press **Enter**.

    The options are:

    - `AES`
    - `DES`
13. In the **Authentication password** field, type the NMS privacy protocol password and press **Enter**.

    Leave this field blank if you do not have a password.
14. In the **Privacy password** field, type the NMS authentication password and press **Enter**.

Leave this field blank if you do not have a password.

The CCM console displays the new NMS settings.

15. Review the NMS settings.
16. If you are satisfied with the settings, in the **Please confirm your settings** field, type `y` and press **Enter**.

    This CCM console adds the SNMP destination and displays the alarm details.
17. Return to the previous page by entering `b`.
18. Quit the current page by entering `q`.
19. Return to the main menu by entering `m`.
20. To view the list of the current destinations for sending SNMP alarms, select the **List the current destination for sending SNMP alarms** option by entering the corresponding number.
21. Return to the previous page by entering `b`.
22. Quit the current page by entering `q`.
23. Return to the main menu by entering `m`.
24. To send a test SNMP alarm to a destination, select the **Send a test SNMP alarm to destination** option by entering the corresponding number.

    Avaya Analytics™ sends a test alarm to the configured destination.
25. Return to the previous page by entering `b`.
26. Quit the current page by entering `q`.
27. Return to the main menu by entering `m`.

Certificate management

Certificate Manager is an Avaya Common Services service that runs in a cluster and manages the identity and trust certificates for Cluster Control Manager and for the services that are deployed in the cluster.

When Avaya Common Services is deployed, it automatically installs Certificate Manager. When other services are deployed, the service chart provides Certificate Manager with the necessary information to process and create trusted stores and identity certificates.

In addition, Certificate Manager:

- Imports third-party certificates.
- Securely stores certificates generated by Certificate Manager or third-party Certificate Authorities (CAs).
- Adds, removes, and replaces certificates in a trusted store.

- Provides its CA for download to be installed on an external device's trusted store.
- Monitors certificates for expiration.

  Certificate Manager regenerates certificates that are about to expire. It also raises alarms when third-party certificates have expired or are about to expire.

  For information on replacing Default Breeze Node Identity Certificates, see section “How to replace Default Breeze Node Identity Certificates” in *Deploying Avaya Oceana® Solution* document.

Related links

[Customizing .CSR file](#) on page 194
[Downloading the Certificate Manager CA certificate](#) on page 198
[Replacing an identity certificate with an internally signed CA certificate (optional)](#) on page 199
[Rotating certificates](#) on page 200
[Deleting a CA certificate from a trusted store](#) on page 200

Simplified process checklist: Using third-party identity certificates for external connections

The following checklist outlines the basic process for working with third-party certificates:

Note:

When using third-party CA, configure client authentication and server authentication on the CA for Avaya Analytics™ configuration to work:

No.	Task	Notes	✔
1	Generate Certificate Signing Requests (CSRs).	See [Generating CSRs](#) on page 194.	
2	Provide the CSRs to the third-party CA to sign.	This produces third-party signed identity certificate PEM files. Name the PEM files using the format `<serviceId>.pem`.	
3	Import the third-party CA certificate and identity certificates.	You can perform this task using a single procedure. See [Importing a third-party CA certificate and identity certificates simultaneously](#) on page 196. Options are also available to import a third-party CA certificate and identity certificates separately if required.	

Note:

- If your CSR was signed by an intermediate Certificate Authority (CA), use the full certificate chain in a single `.pem` file.
- If you have separate files, such as signed certificate, intermediate CA, and root CA, combine these files into a single `.pem` file before importing into the keystore. The order

of the combined `pem` file should have the signed certificate first at the top of the file, followed by the intermediate certificate, and then the root CA.

Generating CSRs

About this task

Use this procedure to create CSRs. The third-party CA uses these CSRs to generate identity certificates to import back into Certificate Manager.

Before you begin

Determine whether you want to:

- Use the system-generated default set of identity certificates for externally facing interfaces. If you choose this default option, no further action is required.
- Manually specify the identity certificates for external and internal interfaces to be used to generate CSRs. For more information, see *Specifying the identity certificates used for generating CSRs* section in *Maintenance and Troubleshooting Avaya Analytics™* guide.

Procedure

1. Log in to Cluster Control Manager.
2. If you are using the default set of identity certificates for externally facing interfaces, run the following command:

   ```
   ccm release cert-manager third-party-certs --generate-service-csr
   --output-dir <output-directory>
   ```

Result

The generated CSRs are available in the output-directory. The CSR files are in the `<serviceID>.csr` format.

Warning:

ccm-identity_v2.pfx-ccm-identity_v2.pfx.csr when created needs to be ignored.

Customizing .CSR file

About this task

Use this procedure to customize a .csr file generated for the default set of identity certificates for externally-facing interfaces. You can customize the following fields of the certificate: C (Country), ST (State), L (Locality), O (Organization), and OU (Organization Unit).

Procedure

1. Log in to Cluster Control Manager.
2. To create default .csr files, run the following command:

   ```
   ccm release cert-manager third-party-certs --generate-service-csr --output-dir
   <output-directory>
   ```

   Eight default .csr files are created.

3. To open each of the seven default .csr files and to verify its subject and subjectAltName (Subject Alternative Name) values, run the following commands:

```
openssl req -text -noout -verify -in ccm-identity.pfx-ccm-identity.pfx.csr
openssl req -text -noout -verify -in ingressgateway-certificate-default-
ingressgateway-idcert.csr
openssl req -text -noout -verify -in eventing-kafka-cp-zookeeper-
kafkaconnectidcert.csr
openssl req -text -noout -verify -in eventing-kafka-cp-kafka-
kafkaexternalidcert.csr
openssl req -text -noout -verify -in egressgateway-certificate-default-
egressgateway-idcert.csr
openssl req -text -noout -verify -in orca-dbmgr-analyticsdb-primary-idcert.csr
openssl req -text -noout -verify -in orca-dbmgr-analyticsdb-replica-idcert.csr
```

4. To create a file called `CertInfoFile` template, run the following commands:

```
# create the "Cert Info" File template
rm -rf ./template.txt;
echo '{' >> ./template.txt;
echo ' "keyAlgorithm": "RSA"' >> ./template.txt;
echo '}' >> ./template.txt;
```

5. To create individual `CertInfoFiles` for service IDs, run the following commands:

```
# create the certInfoFiles
cp template.txt CCM-IGRESS-GATEWAY.certInfoFile;
cp template.txt CCM-EVENTING-KAFKA.certInfoFile;
cp template.txt CCM-EGRESS-GATEWAY.certInfoFile;
cp template.txt CCM-IDENTITY.certInfoFile;
cp template.txt CCM-EVENTING-KAFKA-ZOOKEEPER.certInfoFile;
cp template.txt ANALYTICSDB-PRIMARY.certInfoFile;
cp template.txt CCM-ALANYTICS-REPLICA.certInfoFile;
```

6. Update the subject and subjectAltName information in each individual `CertInfoFile`.

   The following is a sample command for the `CCM-IGRESS-GATEWAY.certInfoFile` file:

```
{
"subject": "C=US, ST=Colorado, L=Thornton, O=Avaya, CN=certmgmt-loadbalancer-
service",
"subjectAltName": "dNSName=certmgmt-loadbalancer-service",
"keySize": "2048",
"keyAlgorithm": "RSA"
}
```

7. To regenerate the .csr files using the updated individual `CertInfoFile`, run the following commands:

```
ccmcertmgr --generate-service-csr ingressgateway-certificate-default-
ingressgateway-idcert CCM-IGRESS-GATEWAY.certInfoFile > CCM-IGRESS-GATEWAY.csr;
ccmcertmgr --generate-service-csr eventing-kafka-cp-kafka-kafkaexternalidcert CCM-
EVENTING-KAFKA.certInfoFile > CCM-EVENTING-KAFKA.csr;
ccmcertmgr --generate-service-csr egressgateway-certificate-default-egressgateway-
idcert CCM-EGRESS-GATEWAY.certInfoFile > CCM-EGRESS-GATEWAY.csr;
ccmcertmgr --generate-service-csr ccm-identity.pfx-ccm-identity.pfx CCM-
IDENTITY.certInfoFile > CCM-IDENTITY.csr;
ccmcertmgr --generate-service-csr eventing-kafka-cp-zookeeper-kafkaconnectidcert
CCM-EVENTING-KAFKA-ZOOKEEPER.certInfoFile > CCM-EVENTING-KAFKA-ZOOKEEPER.csr;
ccmcertmgr --generate-service-csr orca-dbmgr-analyticsdb-primary-idcert
ANALYTICSDB-PRIMARY.certInfoFile > ANALYTICSDB-PRIMARY.csr;
ccmcertmgr --generate-service-csr orca-dbmgr-analyticsdb-replica-idcert
ANALYTICSDB-REPLICA.certInfoFile > ANALYTICSDB-REPLICA.csr;
```

8. To verify that the Subject and Subject Alternative Name information is updated in all the seven default .csr files, run the following commands:

```
openssl req -text -noout -verify -in CCM-IGRESS-GATEWAY.csr
openssl req -text -noout -verify -in CCM-EVENTING-KAFKA.csr
openssl req -text -noout -verify -in CCM-EGRESS-GATEWAY.csr
openssl req -text -noout -verify -in CCM-IDENTITY.csr
openssl req -text -noout -verify -in CCM-EVENTING-KAFKA-ZOOKEEPER.csr
openssl req -text -noout -verify -in ANALYTICSDB-PRIMARY.csr;
openssl req -text -noout -verify -in ANALYTICSDB-REPLICA.csr;
```

Related links

Certificate management on page 192

Importing a third-party CA certificate and identity certificates simultaneously

About this task

Use this procedure to simultaneously import a third-party CA certificate into Certificate Manager trust stores and the associated identity certificates signed by the third-party CA.

Before you begin

- Obtain the PEM file of the third-party CA.
- Obtain identity certificate PEM files signed by the third-party CA. Ensure that the name of the PEM files uses the `<serviceID>.pem` format.
  - To see the contents of a `pem` file, use the command:

    `openssl x509 -in certificate.pem -text`

  - To see the contents of a `csr` file, use the command:

    `openssl req -in mycsr.csr -noout -text`
- Determine whether you want to:
  - Use the system-generated default set of trust stores for externally facing interfaces. If you choose this default option, no further action is required.
  - Manually specify the trust stores for external and internal interfaces, the third-party CA certificate is added to. For more information, see *Specifying trust stores for adding a third-party CA certificate* section in *Maintenance and Troubleshooting Avaya Analytics™ guide*.

    Tip:

    If you specify identity certificates before generating CSRs, you should also specify trust stores for the third-party CA certificate.
- The signed identity certificates must have ExtendedKeyUsages of serverAuth and clientAuth. You can check the ExtendedKeyUsages values on the signed identity certificate by running the following command and verifying its output:

```
$ openssl x509 -noout -text -in <signed_cert>.pem
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
```

Procedure

1. Log in to Cluster Control Manager.
2. Transfer the third-party CA PEM file to the `/home/<customer account>/<third-party-CA_PEM_filename>` directory using a file transfer utility, such as WinSCP.
3. Transfer the identity certificate PEM files to the `/home/<customer_account>/id-cert-files` directory using a file transfer utility, such as WinSCP.
4. Navigate to the `/home/<customer_account>` directory.
5. If you are using the default set of trust stores for externally facing interfaces, do the following to import the third-party CA certificate and identity certificate PEM files:

```
ccm release cert-manager third-party-certs --add-certs --ca-cert-file \
<third-party-CA_PEM_filename> --id-cert-dir /home/<customer_account>/id-cert-files
```

Importing a third-party CA certificate separately (optional)

About this task

For most deployments, you would import a third-party CA certificate and identity certificates simultaneously.

Only use this procedure if you need to import the third-party CA certificate to a Certificate Manager trust store separately. This procedure does not import the signed identity certificates.

Before you begin

- Obtain the PEM file of the third-party CA.
- Determine whether you want to:
  - Use the system-generated default set of trust stores for externally facing interfaces. If you choose this default option, no further action is required.
  - Manually specify the trust stores for external and internal interfaces, the third-party CA certificate is added to. For more information, see *Specifying trust stores for adding a third-party CA certificate* section in *Maintenance and Troubleshooting Avaya Analytics™* guide.

    Tip:

    If you specified identity certificates before generating CSRs, then you should also specify trust stores for the third-party CA certificate.

Procedure

1. Log in to Cluster Control Manager.
2. Transfer the third-party CA PEM file to the `/home/<customer_account>/<third-party-CA_PEM_filename>` directory using a file transfer utility, such as WinSCP.
3. Navigate to the `/home/<customer_account>` directory.

4. If you are using the default set of trust stores for externally facing interfaces, run the following command to import the third-party CA certificate:

```
ccm release cert-manager third-party-certs --add-trustcert --ca-cert-file <third-party-CA_PEM_filename>
```

Importing third-party identity certificates separately (optional)

About this task

For most deployments, you would import a third-party CA certificate and identity certificates simultaneously. Only use this procedure if you need to import third-party identity certificates separately.

Before you begin

- Import your third-party CA certificate into the appropriate trust stores for the affected services.
- Obtain identity certificate PEM files signed by the third-party CA. Ensure that the name of the PEM files uses the `<serviceID>.pem` format.
  - To see the contents of a `pem` file, use the command:

    `openssl x509 -in certificate.pem -text`
  - To see the contents of a `csr` file, use the command:

    `openssl req -in mycsr.csr -noout -text`

Procedure

1. Log in to Cluster Control Manager.
2. Transfer the identity certificate PEM files to the `/home/<customer_account>/id-cert-files` directory using a file transfer utility, such as WinSCP.
3. Run the following command:

```
ccm release cert-manager third-party-certs --import-identity-cert-pem \
--id-cert-dir /home/<customer_account>/id-cert-files
```

Downloading the Certificate Manager CA certificate

About this task

Use this procedure to download a Certificate Manager CA certificate. Load this certificate onto an external server that accesses services in the cluster.

Before you begin

Record the cluster FQDN of the target cluster. The cluster FQDN is recorded in the solution deployment spreadsheet.

Procedure

1. Open a browser and navigate to `https://<cluster-FQDN>/ejbca/retrieve/ca_certs.jsp`.

2. On the EJBCA page, refer to **CertManagerCA**.
3. Click **Download as PEM**.

   The Certificate Manager CA certificate `CertManagerCA.pem` file downloads.
4. Install this Certificate Manager CA certificate on an external server that accesses services installed on the cluster.

Related links

Certificate management on page 192

Replacing an identity certificate with an internally signed CA certificate (optional)

About this task

Use this procedure to replace an existing identity certificate for a service with one signed by the internal CA. This procedure generates and replaces an identity certificate with the attributes specified in the file called `certInfoFile`.

Procedure

1. Log in to Cluster Control Manager.
2. Create a file called `certInfoFile` using the provided subject, commonName, keySize (mandatory), keyAlgorithm (mandatory), and subjectAltName values.

   If the subject is provided and includes a CN value, the CN value overrides the commonName value if it is provided.

   Any value that is not specified in `certInfoFile` is not included in the certificate.

   For example:

   ```
   {
     "subject": "C=US, ST=Colorado, L=Thornton, O=Avaya, CN=certmgmt-loadbalancer-
   service"
     "keySize": "2048",
     "keyAlgorithm": "RSA",
     "subjectAltName": "dNSName=certmgmt-loadbalancer-service",
   }
   ```
3. Store this file on Cluster Control Manager in one of the following directories:

   - `/home/<customer account>`
   - `/tmp`
4. To replace the certificate, run the `ccmcertmgr --replace-service-identity-cert <serviceId> <certInfoFile>` command.

Related links

Certificate management on page 192

Rotating certificates

About this task

Use this procedure to rotate certificates managed by Certificate Manager.

For clusters using certificates generated by Certificate Manager, this task instructs Certificate Manager to regenerate those certificates and instructs the cluster to use these certificates.

For clusters using third-party certificates, this task instructs the cluster to use the third-party certificates that have been imported into Certificate Manager.

Before you begin

- You must plan a maintenance window to perform this task.
- If the cluster is to use third-party certificates, you must import the third-party certificates into Certificate Manager before performing this task.

Procedure

1. Log in to Cluster Control Manager.
2. Run the `ccm rotate-cluster-certificates` command.

   This command can take more than 60 minutes to complete.
3. Wait approximately 30 minutes, then run `ccm smoke-test` on Cluster Control Manager and confirm that all tests pass. If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.

Related links

Certificate management on page 192

Deleting a CA certificate from a trusted store

About this task

Use this procedure to delete a CA certificate from a trusted store.

Before you begin

At a minimum, you require the service ID of the trust store from which you are deleting the CA. You can run `ccm release cert-manager getcerts -ts | grep serviceId` to find a list of service IDs.

Procedure

1. Log in to Cluster Control Manager.
2. To find the certificate ID, run the `ccmcertmgr --trusted-certs <serviceId> | grep certificateId` command.
3. To delete the certificate, run the `ccmcertmgr --delete-trustcert <serviceId> <certificateId>` command.

Related links

Certificate management on page 192

Certificate revocation

You can configure Certificate Manager to add revocation-related extensions to identity certificates issued by its internal CA. By default, certificates issued by Certificate Manager do not contain revocation-related extensions. You can enable or disable revocation for certificates issued by the Certificate Manager CA during a fresh installation or upgrade. When revocation is enabled, certificates contain extensions related to Certificate Revocation List (CRL) distribution, Online Certificate Status Protocol (OCSP) authority information access, or both. If Certificate Manager is configured to add CRL-related extensions to certificates, it issues a CRL every 24 hours with a validity of 7 days. You can download the CRLs from `http://<cluster_FQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DCertificate+Manager+CA%2cO%3DAvaya`.

Enabling revocation information

About this task

Use this procedure to enable revocation information in identity certificates issued by the Certificate Manager CA. You can do this during a fresh installation or upgrade.

When revocation is enabled, certificates contain extensions related to CRL, OCSP, or both. If Certificate Manager is configured to add CRL-related extensions to certificates, it issues a CRL every 24 hours with a validity of 7 days. You can download the CRLs from `http://<cluster_FQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DCertificate+Manager+CA%2cO%3DAvaya`.

Procedure

On the cert-manager tab of the solution configuration spreadsheet, add `config:certmgmt-service:service:ProvideRevocationInfo=` with one of the following values:

Value	Description
BOTH	Certificate Manager adds both CRL and OCSP information to certificates issued post-installation or post-upgrade.
CRL_ONLY	Certificate Manager only adds CRL information to certificates issued post-installation or post-upgrade.
OCSP_ONLY	Certificate Manager only adds OCSP information to certificates issued post-installation or post-upgrade.

For example, if you want both CRL and OCSP information to be included in certificates, add `config:certmgmt-service:service:ProvideRevocationInfo=BOTH` in the solution configuration spreadsheet.

If you change the value of `config:certmgmt-service:service:ProvideRevocationInfo` while upgrading, changes to revocation information only affect new certificates that are issued after the upgrade.

Disabling revocation information

About this task

Use this procedure to disable revocation information in identity certificates issued by the Certificate Manager CA. You can do this during a fresh installation or upgrade.

Procedure

On the cert-manager tab of the solution configuration spreadsheet, add `config:certmgmt-service:service:ProvideRevocationInfo=NONE`.

`NONE` indicates that Certificate Manager does not add any CRL or OCSP information to certificates issued after the installation or upgrade.

If you change the value of `config:certmgmt-service:service:ProvideRevocationInfo` while upgrading, changes to revocation information only affect new certificates that are issued after the upgrade.

Revoking a certificate

About this task

Use this procedure to manually revoke a certificate issued by the Certificate Manager CA.

Procedure

1. Log in to the Certificate Manager EJBCA web console at `https://<CLUSTER_FQDN>/ejbca/adminweb/` with the certmanagerrasuperadmin role.
2. Click **RA Functions** > **Search End Entities**.
3. From the **Search end entities with status** drop-down list, click **All** and then click **Search**.
4. Click **View_Certificates** for the relevant entities.
5. Look at the fingerprint ID or serial number to confirm which certificate you want to revoke.
6. Select the certificate number you want to revoke.
7. Select the reason for revocation and then click **Revoke**.

Generating a CRL manually

About this task

If Certificate Manager is configured to add CRL-related extensions to certificates, it issues a CRL every 24 hours with a validity of 7 days. You can download the CRLs from `http://<cluster_FQDN>/ejbca/publicweb/webdist/certdist?cmd=crl&format=PEM&issuer=CN%3DCertificate+Manager+CA%2cO%3DAvaya`.

Use this procedure to manually generate a CRL immediately.

Procedure

1. Log in to the Certificate Manager EJBCA web console at `https://<CLUSTER_FQDN>/ejbca/adminweb/`.
2. Navigate to **CA Functions** > **CA Structure & CRLs**.
3. From the Basic Functions section, click **Create CRL** to create a newly updated CRL.

Chapter 15: Post-installation verification

Verifying the Avaya Analytics™ installation

About this task

You can verify the status of the different Avaya Analytics™ pods collectively or individually after the installation is complete. If any of the services are not working as described in the respective steps in this procedure, contact your system administrator or Avaya support.

Procedure

1. Log in to the Cluster Control Manager (CCM) console as the customer user.
2. Switch to being the root user by entering the command `su`.
3. To check the status of Cluster Control Manager (CCM), run the following command:

   `ccm status`

   The page displays the following:

   - The status of all the staged products on CCM. For a successful installation, the status must be `DEPLOYED` for all the products, and all the pods must be running.
   - The current and previous versions of the Avaya Analytics™ components.
4. **(Optional)** To check only the current versions of Avaya Analytics™ components, run the following command:

   `swversion`
5. To check the status for all pods, run the following command:

   `kubectl get pods -A`

   The page displays information about the respective pods with the following columns:

   - READY: Indicates the number of pods running for the respective pod. For a particular pod status to be successful, all the instances for the pod must be running. For example, 2/2 indicates that the status is running as expected. While 1/2 indicates an error in the status, even if the STATUS column displays `Completed` or `Running`.

     Note:

     The Async messaging service will show a Running state with 1/2 by design.
   - STATUS: Indicates whether the pod is running or completed. If the pod has any errors, the column displays `Error`.

- RESTARTS: Indicates the number of times the pod has restarted.
- AGE: Indicates the duration for which the pod runs. The format is `d:h:m:s`, where *d* is the number of days, *h* is the number of hours, *m* indicates the time in minutes and *s* is time in seconds.

6. To check the status of the Breeze authentication and token validation certificates, run the following command:

   `kubectl get secrets| grep breeze-security`

   Ensure that the page displays the TYPE as `Opaque`.

7. To check the status of Breeze authentication, run the following command:

   `kubectl get pods| grep breeze-auth`

   The page displays the following information for each column:

   - READY: 1/1
   - STATUS: `Running` or `Completed`.
   - RESTARTS: The number of times the pod is restarted. This column can also be blank or `0`.
   - AGE: The duration for which the pod is running.

8. To check the status of Streams REST, run the following command:

   `kubectl get pods| grep streams-rest`

   The page displays the following for each column:

   - READY: 1/1
   - STATUS: `Running` or `Completed`.
   - RESTARTS: The number of times the pod is restarted. This column can also be blank or `0`.
   - AGE: The duration for which the pod is running.

9. To check the status of Data Publisher, run the following command:

   `kubectl get pods| grep data-publisher`

   The page displays the following for each column:

   - READY: 1/1
   - STATUS: `Running` or `Completed`.
   - RESTARTS: The number of times the pod is restarted. This column can also be blank or `0`.
   - AGE: The duration for which the pod is running.

10. To check the status of Ref Input Adaptor, run the following command:

    `kubectl get pods| grep ref-input`

The page displays the following for each column:

- READY: 1/1
- STATUS: `Running` or `Completed`.
- RESTARTS: The number of times the pod is restarted. This column can also be blank or `0`.
- AGE: The duration for which the pod is running.

11. To check the status of the Historical Reporting pods, run the following command:

    `kubectl get pods -n mstr`

    The page displays the following for each column:

    - READY: 1/1
    - STATUS: `Running` or `Completed`.
    - RESTARTS: The number of times the pod is restarted. This column can also be blank or `0`.
    - AGE: The duration for which the pod is running.

Chapter 16: Upscaling Avaya Analytics

Upscaling Avaya Analytics™

An administrator can perform upscaling of a cluster in Avaya Analytics™ to accommodate changes to the existing configuration. Upscaling is increasing the VMware node resources for the Avaya Common Services cluster by allocating additional CPU, memory, and disk storage.

Avaya Analytics™ supports upscaling from release 4.3.1.1 onward. Customers who use an older release must upgrade to Avaya Analytics™ 4.3.1.1 to perform an upscale. Avaya Analytics™ upscaling supports the following:

- Increasing the active agent count for Avaya Analytics™ without redeploying the Avaya Analytics™ application.
- Adding capacity to deploy new features such as asynchronous messaging, real-time routing service group reporting, and historical agent trace reporting without impacting the deployed applications.

The administrator can use the deployment spreadsheet to manage the upscaling process. The spreadsheet pre-calculates the additional CPU, memory, and disk storage requirements based on the updated configuration.

Note:

- Avaya Analytics™ does not support upgrading and upscaling simultaneously.
- Avaya Analytics™ does not support upscaling and downscaling from non-HA to HA deployment.

Adding CPU and memory to a node

About this task

Use this procedure to increase node CPU and memory resources when not also increasing SDS disk size or a upgrading software. For example, when adding a product.

Before you begin

- You must plan a maintenance window to perform this task.

Procedure

1. Open the same deployment spreadsheet that is configured to install or upgrade the cluster in the Avaya Analytics™ 4.3.1.1 release.

2. Make a note of the current SDS disk, CPU and Memory requirement for the installed cluster.
3. For increasing the agent count of the cluster, select the **New deployment size** from the dropdown menu on the **orca** tab.
4. For adding a new feature such as Async or historical agent trace reporting, enable the feature on the respective tab.
5. Compare the new footprint values with the old values and make note of any differences in the SDS disk, CPU and Memory. If there is no need to increase the disk size, skip the *Increasing SDS disk size for a node* section and ensure an infrastructure upgrade is not performed as a part of the CPU and Memory increase as this will result in a failure.
6. Power off the cluster nodes.

   See Powering off a cluster on page 208.
7. In vCenter, on each cluster node VM, edit the settings to increase the CPU and memory resources as required.
8. Power on the cluster nodes.

   See Powering on a cluster on page 210.
9. Log in to Cluster Control Manager with your customer account.
10. Copy the deployment spreadsheet to the CCM server.

Result

After this procedure, the cluster nodes are running with the new CPU and memory resource allocations.

Related links

Powering off a cluster on page 208
Powering on a cluster on page 210
Rebalancing Analytics pods on page 212

Powering off a cluster

About this task

Use this procedure to gracefully shut down your solution cluster. Complete this procedure during a maintenance window.

Caution:

If you shut down your cluster using a different method than what is described in this procedure, file corruption might occur.

Before you begin

- You must plan a maintenance window to perform this task.
- Stop call events across the solution.

To stop all Avaya Oceana® traffic for an Avaya Analytics™ cluster, run the `kubectl scale deployment orca-ref-input-adaptor --replicas=0` command using an account with root privileges.

- Back up Common Services using the `ccm backup` command.

  If you do not perform a backup, you risk a full reinstallation of the solution.
- Back up product application data as described in your solution documentation.

Procedure

1. Log in to vCenter as an administrator or with the account used to deploy the cluster.
2. Click the **VMs and Templates** tab.
3. Locate and click on each node virtual machine in the folder you designated during your cluster deployment.
4. Log in to Cluster Control Manager.
5. Run the `pre-infra-upgrade` command to gracefully shut down the authorization service database.

   Wait for the command to complete before continuing. Ensure that this command is successful.
6. Run `ccm version -k` to determine role of each node: either worker or controller-worker.

   Note the node roles, for use when shutting down or powering on nodes.
7. Run `kubectl get pods -n image-registry -o wide` as a root user.

   Note the cluster node hosting the image registry.
8. Determine which nodes contain a second disk and which nodes are diskless.

   Note the disk status of each node, for use when shutting down or powering on nodes.

   To identify a list of nodes that have a second disk, run the `checkInfra -Sd | grep LVM_THIN` command. The output lists the FQDNs of nodes containing a second disk.

   ```
   [cust@flex190-129 ~]$ checkInfra -Sd | grep LVM_THIN
   | pool_sds              | flex190-132.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |            |
   | pool_sds              | flex190-133.dr.example.com | LVM_THIN |
   vg_sds/sds_thinpool |   341.00 GiB |    464.76 GiB | True
   | Ok    |            |
   [cust@flex190-129 ~]$
   ```

   The other nodes in the cluster are diskless nodes. That is, node FQDNs not printed in the command output are diskless nodes.
9. Log in to vCenter as an administrator or with the account used to deploy the cluster.
10. Click the **VMs and Templates** tab.

11. Locate and click on each node virtual machine in the folder you designated during your cluster deployment.
12. Power off worker and controller-worker nodes.

    Caution:

    You must shut down the guest OS of the worker nodes before shutting down the controller-worker nodes.

    You must gracefully shut down the guest OS on nodes without a second disk (diskless nodes) before shutting down nodes containing a second disk.

    a. Right-click on each worker node and then click **Power** > **Shut Down Guest OS**.
    b. Wait until the worker node has completely powered down before continuing to the next node. Check VM status in the vCenter.
    c. Right-click on the controller-worker node without a second disk and then click **Power** > **Shut Down Guest OS**.
    d. Wait until the worker node has completely powered down before continuing to the next node. Check VM status in the vCenter.
    e. Right-click on each controller-worker node containing a second disk and then click **Power** > **Shut Down Guest OS**.

    Note:

    Power these off relatively together. No wait time is needed between the nodes.
13. Power off Cluster Control Manager.
    a. Click the **VMs and Templates** tab.
    b. Locate and click on Cluster Control Manager in the folder you designated for the cluster.
    c. Right-click Cluster Control Manager and then click **Power** > **Shut Down Guest OS**.

Related links

Adding CPU and memory to a node on page 207

Powering on a cluster

About this task

Use this procedure to gracefully power on your solution cluster. You can also use this procedure to power on after an unexpected power down. Complete this procedure during a maintenance window.

Procedure

1. Log in to vCenter as an administrator or with the account used to deploy the cluster.
2. Click the **VMs and Templates** tab.

3. Power on Cluster Control Manager.
   a. Locate and click Cluster Control Manager in the folder you designated for the cluster.
   b. Right-click Cluster Control Manager and then click **Power** > **Power On**.
   c. Wait until the VM has initialized and you can log in to Cluster Control Manager before proceeding to the next step.
4. Locate and click on each node virtual machine in the folder you designated during your cluster deployment.
5. Power on the image-registry controller-work node first and then the controller-worker and worker nodes.

   Caution:

   You must power on the controller-worker nodes before powering on the worker nodes.

   You must power on the nodes containing a second disk before powering on nodes without a second disk.

   a. Right-click on the controller node containing the second disk that was running the image-registry pod and then click **Power** > **Power On**
   b. Wait until login screen is present on VM console before proceeding with next VM.
   c. Right-click on the other controller node containing a second disk and then click **Power** > **Power On**
   d. Wait until login screen is present on VM console before proceeding with next VM.
   e. Right-click on each controller-worker node without a second disk and then click **Power** > **Power On**
   f. Right-click each worker node and then click **Power** > **Power On**.
6. Wait approximately 8 minutes for all nodes to power on before proceeding to the next step.
7. If you ran the **`pre-infra-upgrade`** command and gracefully shut down the cluster nodes, then run the **`post-infra-upgrade`** command to start the authorization service database.

   Skip this step if the cluster was unexpectedly powered down.
8. Wait approximately 7 minutes for pods to come up and for storage to sync.
9. For Avaya Analytics™, if you stopped all Avaya Oceana® traffic then run the following command to start data flow to the cluster.

   Skip this step if the cluster was unexpectedly powered down.

   Note:

   This step requires an account with root privileges.

   - For non-HA Avaya Analytics™:

     ```
     kubectl scale --replicas=1 deployment orca-ref-input-adaptor
     ```

- For HA Avaya Analytics™:

  ```
  kubectl scale --replicas=2 deployment orca-ref-input-adaptor
  ```

  Wait for the command to complete before continuing. Ensure that the command is successful.

10. Run `ccm smoke-test` to verify the operational state of the cluster.

    If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.

Related links

Adding CPU and memory to a node on page 207

Rebalancing Analytics pods

About this task

You must rebalance the analytics pods after powering on a cluster.

Before you begin

- Check the status of the pods using `ccm smoke-test`.
- Check the pod distribution across the nodes. Use the command **`kubectl describe nodes`** and check the value displayed for non-terminated pods against each node.

Procedure

1. Run the command **`ccm release orca analytics`** and choose from the following options in the below order:

   a. Option 6 Troubleshooting

   b. Option 4 General

   c. Option 4 Restart Standby pods

2. Wait for the pods to restart.
3. Run the command `ccm smoke-test` to check the status of the pods.
4. Run the command **`kubectl describe nodes`** and check the value displayed for **non-terminated pods:** against each node.

   Verify that the pods are evenly distributed between the nodes.

Related links

Adding CPU and memory to a node on page 207

Increasing SDS disk size for a node

About this task

This procedure increases the Software-Defined Storage (SDS) disk size for all disk nodes in the cluster. You cannot decrease SDS disk size.

Note:

vCenter does not enable you to resize SDS disks on virtual machines that have snapshots. To resize an SDS disk, remove any virtual machine snapshots before proceeding with this procedure.

Procedure

1. Resize the SDS disk in vCenter.

   This step can be done without powering off the cluster nodes.

2. Log in to Cluster Control Manager with an account that has root privileges.
3. On Cluster Control Manager, run the following command:

   ```
   kubectl exec --namespace=piraeus deployment/piraeus-op-piraeus-operator-cs-controller -linstor sp l
   ```

4. Note the nodes that have a storage pool of `pool_sds`.
5. Open the VMware Infrastructure client and log in to vCenter or the ESX host machine.
6. Right-click the cluster node VM from the output above.
7. Click **Edit settings**.
8. Select **Virtual Disk**.

   This is Hard Disk 2, with a size similar to the SDS Disk Size in current solution spreadsheet.

9. Enter the new size for the virtual hard disk based on the footprint summary table in the updated deployment spreadsheet.
10. Run the `ccm upgrade spec <solution spreadsheet name>.xlsx --infra` command.
11. Wait approximately 30 minutes, then run `ccm smoke-test` on Cluster Control Manager and confirm that all tests pass. If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.
12. To verify the new disk size, run the `checkInfra -Sd` command and review the SDS capacity.

    ```
    . . .
    Storage pools:
    +-------------------------------------------------------------------------------------------------------------------------------------------------------------
    --------------+
    | StoragePool          | Node                   | Driver   | PoolName           | FreeCapacity | TotalCapacity | CanSnapshots |
    State | SharedName |
    |
    =============================================================================================================================================================
    ==============|
    | DfltDisklessStorPool | flex190-78.example.com | DISKLESS |                    |              |               | False        |
    Ok    |            |
    ```

```
| DfltDisklessStorPool | flex190-79.example.com | DISKLESS |                    |              |               | False        |
Ok    |            |
| DfltDisklessStorPool | flex190-80.example.com | DISKLESS |                    |              |               | False        |
Ok    |            |
| DfltDisklessStorPool | flex190-94.example.com | DISKLESS |                    |              |               | False        |
Ok    |            |
| pool_sds             | flex190-78.example.com | LVM_THIN | vg_sds/sds_thinpool |   521.02 GiB |    599.70 GiB | True         |
Ok    |            |
| pool_sds             | flex190-79.example.com | LVM_THIN | vg_sds/sds_thinpool |   526.18 GiB |    599.70 GiB | True         |
Ok    |            |
+------------------------------------------------------------------------------------------------------------------------------------------------
--------------+
. . .
```

Result

After the upgrade completes, the cluster nodes have access to the increased SDS disk capacity.

Upgrading to add a service and increase capacity

About this task

Use this task to perform a product upgrade to increase the capacity of each service in the cluster and also add a new service or feature.

Before you begin

Obtain a copy of the cluster configuration spreadsheet and revise it as instructed by your solution documentation.

Procedure

1. Log in to Cluster Control Manager using your customer account.
2. Use a utility, such as WinSCP, to transfer the solution configuration spreadsheet to the `~/artifacts` directory.
3. Enter the `screen` command to run the upgrade in the background.
4. Enter the `ccm upgrade spec <cluster-config>.xlsx --products --force` command and wait for upgrade to complete successfully.
5. When prompted, type `y` to confirm the requested products to upgrade to the new versions specified in the solution spreadsheet and to accept the warning reminding you to start a `screen` session.

   Only type `y` if you have already run `screen`. Do not continue with the upgrade until you do this.

   Failure to run the `screen` command exits the process and you have to start over.
6. When prompted, accept the EULA.

   Validation runs after accepting the EULA. If any part of the validation fails, you must address the detected issues and restart the upgrade.
7. When prompted to perform a backup, enter `y` or `n`.

   If you enter `y`, a backup runs after the upgrade is complete. The backup takes approximately 5 to 10 minutes to complete. If the archive destination is set to Local,

the backup file is located at `/var/avaya/artifactCache/ccmClusterBackup`. If the archive destination is set to Remote, the `ccmClusterBackup` folder, which contains the backup file, is located in the base directory you specified.

8. **(Optional)** To monitor the progress of the upgrade, run the `tail -f /var/log/avaya/ccm/ccm-main.log` command.
9. Wait approximately 30 minutes, then run `ccm smoke-test` on Cluster Control Manager and confirm that all tests pass. If `ccm smoke-test` fails, run it again in 10 minutes. If the test continuously fails for over an hour, contact your technical support representative.
10. After infra upgrade, if mstr pods are in 0/1 state then delete the pod and wait till it comes up in good state.
11. Use the following commands to stop and start the mstr pods.
    a. To stop the mstr pods, run

       ```
       k scale deployment mstr-srv --replicas=0 -n mstr
       ```

       Wait till the command completes. Then run

       ```
       k scale deployment mstr-web --replicas=0 -n mstr
       ```

       Ensure that the pods are not displaying when executing the command `k get pods -n mstr`.

    b. To start the mstr pods, run

       ```
       k scale deployment mstr-srv --replicas=1 -n mstr
       k scale deployment mstr-web --replicas=1 -n mstr
       ```

Chapter 17: Resources

Documentation

Title	Use this document to:	Audience
Overview		
Avaya Oceana® Solution Description	Use this guide to know about the tested product characteristics and capabilities, including product overview and feature descriptions, interoperability, performance specifications, security, and licensing requirements.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Implementing		
Deploying Avaya Oceana®	Use this guide to know how to deploy Avaya Oceana® Solution on the customer environment.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Avaya Oceana® and Avaya Analytics™ Disaster Recovery	Use this guide to know how to restore Avaya Oceana®, solution when there is a complete outage at the primary data center.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Migrating Avaya Oceana®	Use this guide to know how to migrate Avaya Oceana® solution from the existing version.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Deploying Avaya Analytics™	Deploy Avaya Analytics™.	• Sales engineers • Business partners • Solution architects • Implementation engineers
Administering		

Table continues…

Title	Use this document to:	Audience
Administering Avaya Oceana®	Administer Avaya Oceana®.	• System administrators • Supervisors
Using		
Using Avaya Workspaces for Avaya Oceana®	Use Avaya Workspaces for Avaya Oceana®.	• Agents • Supervisors
Using Avaya Analytics™	Use the features and capabilities of Avaya Analytics™.	• Supervisors • Administrators • Report designers
Avaya Analytics™ Data Dictionary	Use historical and real-time measures in custom reports.	• Administrators • Report designer
Maintaining and Troubleshooting		
Maintaining and Troubleshooting Avaya Oceana®	Perform maintenance and troubleshooting procedures for routine maintenance and troubleshooting of Avaya Oceana®.	• Support personnel • Implementation engineers • Administrators
Maintaining and Troubleshooting Avaya Analytics™	Perform common maintenance functions of Avaya Analytics™ and use tools and utilities for troubleshooting of Avaya Analytics™.	• Support personnel • Implementation engineers • Administrators
Avaya Oceana® Alarms	View details about Avaya Oceana® alarms.	• Support personnel • Administrators

Finding documents on the Avaya Support website

Procedure

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

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

For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.

8. Click to display the search results.

Avaya Documentation Center navigation

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

Important:

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

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

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

  You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click **<** or **>** next to the document title to navigate to the previous topic or the next topic.
- Click **Share** ( ) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** ( ). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.

- Click **Watch** ( ) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

  You can do the following:

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

Training

The following courses are available for the Avaya Oceana® program.

Table 1: Sales Credentials

Course code	Course title	Course duration in hours	Delivery type
APSS – 1202 Avaya OneCloud™ CCaaS Sales			
41511W	Selling Avaya OneCloud™ CCaaS Solutions	0.75	Web-based Training
41551T	Avaya OneCloud™ CCaaS Sales Specialized Test	1.0	Web-based Training
ALCC –2005 Avaya Multiexperience Solutions Sales (ALCC-2005)			
41710W	The Avaya OneCloud™ Contact Center Automated Story	0.50	Web-based Training
41411W	Selling Avaya Oceana®	0.75	Web-based Training
41401W	Selling Avaya Analytics™	0.50	Web-based Training
41481W	Avaya Oceana® ROI for Sales	0.50	Web-based Training
41770W	Avaya Experience Portal and Proactive Outreach Manager (POM) for Sales	0.25	Web-based Training

Table 2: Pre-Sales Design

Course code	Course title	Course duration in hours	Delivery type
ACDS – 3480 Avaya Oceana® Solution Design			
34211W	Avaya Oceana® Overview for Design	0.75	Web-based Training
34811W	Designing the Avaya Oceana Solution Part 1 of 3	1.0	Web-based Training
34821W	Designing the Avaya Oceana Solution Part 2 of 3	1.0	Web-based Training
34831W	Designing the Avaya Oceana Solution Part 3 of 3	1.0	Web-based Training
34801X	Avaya Oceana® Solution Design Exam	1.50	Exam
ALRI-7001 Avaya Oceana® Product Release Information Collection			
39001W	Avaya Oceana® R3.8 with Breeze Snap-ins Details for Pre-Sales	1.0	Portable Document Format (PDF)
39020W	Avaya Breeze® Snap-ins for Avaya Oceana Details for Pre-Sales	1.0	PDF

Table 3: Technical Services Partner Credentials

Course code	Course title	Course duration in hours	Delivery type
ACIS – 7495 Avaya Oceana® Solution Implement			
74150V	Integrating Avaya Oceana® Core and Workspaces	40.0	Virtual Instructor-Led Training
74950X	Avaya Oceana® Solution Integration Exam	1.50	Exam
ACSS-7497 Avaya Oceana®			
74550V	Supporting Avaya Oceana®	24	Virtual Instructor-Led Training
7497X	Avaya Oceana® Support Exam	1.75	Exam
74360W	Installing Avaya Analytics™ for Oceana®	1.5	Web-based Training

Table 4: Pre-requisite Courseware

Course code	Course title	Course duration in hours	Delivery type
77900W	Avaya Control Manager Training Bundle (5 courses 21900W, 77910W, 77920W, 77930W, 77940W)	5.50	Web-based Training
70160W	Avaya Breeze® Implementation and Support	30.0	Web-based Training

Table 5: End User, Programmer, Administration

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ALEU-5002 Avaya Oceana® End-User Training				
24020W	Using Avaya Workspaces for Avaya Oceana® - Agent	1.0	Web-based Training	https://www.avaya.com/oceana-agent
24040W	Using Avaya Workspaces for Avaya Oceana® - Supervisor	1.0	Web-based Training	https://www.avaya.com/oceana-supervisor
ALUC-4001 Avaya Breeze® Client SDK				
2410W	Customer Communications and Apps with Oceana® for Developers	3.0	Web-based Training	
ASDC-0010 Avaya Workspaces® Framework				
24150W	Customizing the Avaya Workspaces® Framework	3.0	Web-based Training	
24150T	Avaya Workspaces® Framework R3 Test	1.0	Online Test	
ASAC-0005 Avaya Oceana® Administration				
21160W	Avaya Oceana® Fundamentals	0.5	Web-based Training	
24300V	Administering Avaya Oceana® R3 Omnichannel	40.0	Virtual Instructor-Led Training	Attached with the sale
2430T	Administering Avaya Oceana® R3 Online Test	1.0	Online Test	
24320W	Administering Avaya Oceana® - Basic	2.5	Web-based Training	https://www.avaya.com/Oceana-admin

Table continues…

Avaya Learning Center				
Course code	**Course title**	**Course duration in hours**	**Delivery type**	**Vanity Link for Attachment**
ASAC-0031 Avaya Analytics™ R4 for Oceana® Administrator				
24380T	Administering Avaya Analytics1M R4 for Oceana8 Specialized Test	1.0	Online Test	

Table 6: Other Miscellaneous Courseware

Course code	Course title	Course duration in hours	Delivery type	Vanity Link for Attachment
ALCC-0001 Avaya Workforce Optimization Select Integration with Avaya Oceana® Workspaces				
7014W	Integrating Avaya Workforce Optimization Select with Avaya Oceana® Workspaces	3.0	Web-based Training	
7014A	Avaya Workforce Optimization Select with Avaya Oceana® Workspaces Integration Assessment	1.0	Assessment	
71610W	Integrating POM with Avaya Oceana®	1.0	Web-based Training	

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.

- 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`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

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.

Using the Avaya InSite Knowledge Base

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

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

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

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

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

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W