Deploying Avaya Contact Center – Extended Capacity

Release 10.0.2
Issue 2
March 2023

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Hosted Service

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

Licenses

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

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

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time as indicated in the order, Documentation, or as authorized by Avaya in writing. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

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

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Contents

Chapter 1: Introduction

Purpose

This document describes installation, initial configuration, and post-installation verification procedures that you must perform to deploy Avaya Contact Center – Extended Capacity.

This document is intended for implementation engineers and support personnel.

Required skills and knowledge

Ensure that you have the following skills and knowledge:

- Command line interface commands for Red Hat® Enterprise Linux® or Oracle Linux.
- Avaya Aura® Call Center Elite. For more information about the Call Center Elite solution, see *Avaya Aura® Call Center Elite Overview and Specification*.
- Avaya Call Management System. For more information about configuring Avaya Call Management System, see *Administering Avaya Call Management System*.
- Avaya Aura® Application Enablement Services. For more information about configuring Application Enablement Services, see *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.
- Avaya Experience Portal. For more information about configuring Avaya Experience Portal, see *Administering Avaya Experience Portal*.
- Avaya Workplace Client. For more information about administering Avaya Workplace Client, see *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows*.
- The Avaya Agent for Desktop application. For general information about Avaya Agent for Desktop, see *Using Avaya Agent for Desktop*.
- SIP endpoints, such as Avaya 9600 Series IP Deskphones and Avaya J100 Series IP Deskphones. For more information about Avaya 9600 Series IP Deskphones, see *9600 Series IP Deskphones Overview and Specifications*. For more information about Avaya J100 Series IP Deskphones, see *Avaya J100 Series SIP IP Phones Overview and Specifications*.

New in this release

Avaya Contact Center – Extended Capacity Release 10.0.2 includes the following features and enhancements:

Support for disaster recovery for geo-redundant HA deployment without Layer 2 networking

Avaya Contact Center – Extended Capacity supports disaster recovery for geo-redundant HA deployment without Layer 2 networking. The solution does not ensure call and state preservation in case of contact center failure.

Support for Avaya Workplace Client

Avaya Contact Center – Extended Capacity supports Avaya Workplace Client. Avaya Workplace Client is a soft phone application that provides access to Unified Communications (UC) and Over the Top (OTT) services.

Restricted licensing modes

Avaya Contact Center – Extended Capacity supports the License Error and License Restricted modes when it detects that the license has expired. Avaya Contact Center – Extended Capacity enters License Error mode for 60 days. The Configuration Server web portal notifies the administrator that the contact center is in License Error mode.

Avaya Contact Center – Extended Capacity enters the License Restricted mode if the administrator does not install a license after deploying the contact center or if the contact center is in License Error mode for more than 60 days.

Support for new contact center capacities

Avaya Contact Center – Extended Capacity supports new contact center capacity values, such as the number of concurrent logged in agents or registered endpoints.

Chapter 2: Avaya Contact Center – Extended Capacity overview

Avaya Contact Center – Extended Capacity is a single-server solution for large contact centers. The solution provides high availability and disaster recovery through a deployment in two geographically separate data centers. The contact center supports the active/alternate High Availability model.

Avaya Contact Center – Extended Capacity uses various routing algorithms for increasing agent productivity and maximizing resource utilization. Additionally, the solution supports Enterprise Behavioral Pairing and provides AI routing.

Component overview

In the Avaya Contact Center – Extended Capacity solution, the Routing Core Server contains all core Automatic Call Distribution (ACD) components that provide call routing, agent management functionality, and contact center connectivity.

The Routing Core Configuration Server (Configuration Server) provides the administration capabilities of Avaya Aura® System Manager. You can administer most contact center services from the Configuration Server web portal. You can also use the Configuration Server for migrating data from your previous contact center.

The contact center integrates with performance management applications, such as Avaya Call Management System. You can also connect your contact center to Computer Telephony Interface (CTI) applications using Application Enablement Services.

Additionally, you can install Session Border Controller for network security and interoperability between networks.

Most of the solution components have an HTTPS interface, through which an administrator can manage and configure your contact center.

Contact center deployment workflow

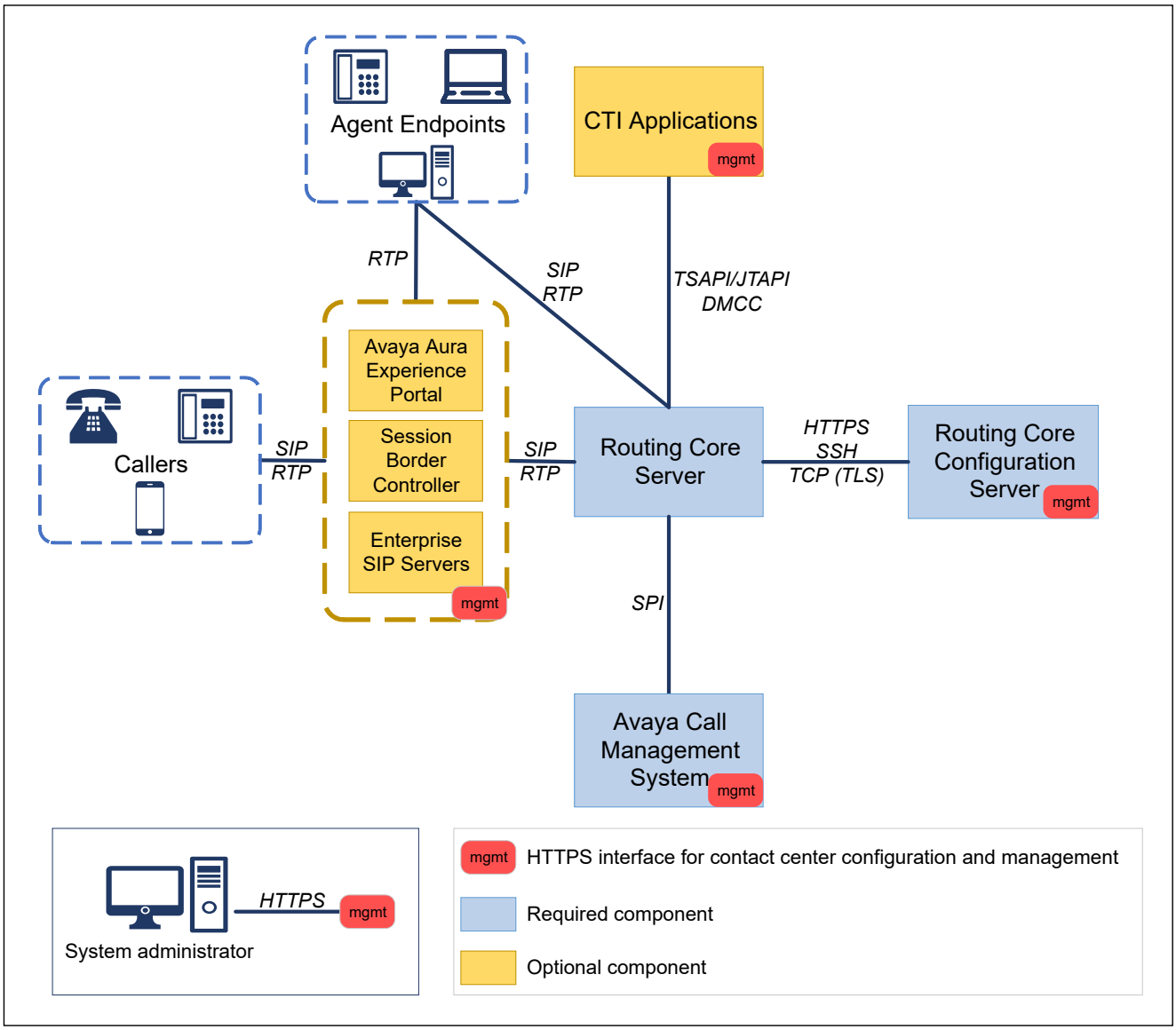
The following table provides a high-level workflow of the solution deployment:

Deployment phase	Description
Planning	Based on the contact center capacity, hardware and network specifications, and required level of component high availability, determine the contact center deployment method and environment.
Routing Core and Configuration Server installation	The Routing Core deployment includes the following: • Installing the required operating system on all Routing Core Server and Configuration Server instances • Enabling passwordless SSH • Updating deployment configuration files • Installing server certificates
Post-installation configuration	After the contact center deployment, configure contact center users and connect endpoints, CTI applications, and Call Management System to Avaya Contact Center – Extended Capacity.
Post-installation verification	Configure contact center objects, such as agents, endpoints, and skills, and verify the call functionality and contact center high availability.

Standalone Avaya Contact Center – Extended Capacity topology

In the standalone contact center deployment, the Routing Core Server and Routing Core Configuration Server are the core components that provide the telephony functionality and agent selection algorithms for voice and digital interactions. The system administrator can also connect Call Management System to the connect center for call reporting functionality.

The following diagram provides an overview of the standalone Avaya Contact Center – Extended Capacity topology:



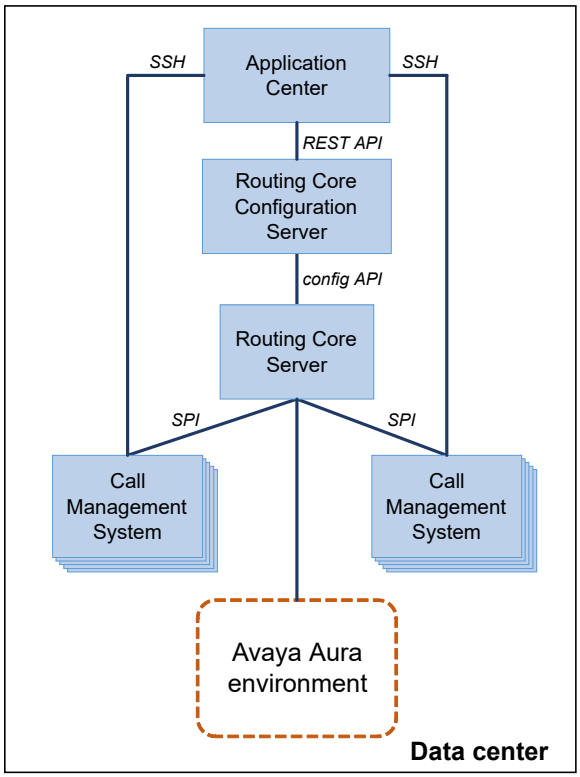
Contact center deployment environments

The system administrator can deploy Avaya Contact Center – Extended Capacity in the Simplex, local High Availability (local HA), or geo-redundant High Availability (geo-redundant HA) without Layer 2 networking environments.

Simplex deployment

In the Simplex deployment, the contact center operates in one data center that contains one Configuration Server and one Routing Core Server. The contact center does not provide server High Availability and cannot operate in case of server failure or maintenance procedures. Avaya recommends that you use Simplex deployment only in a lab environment.

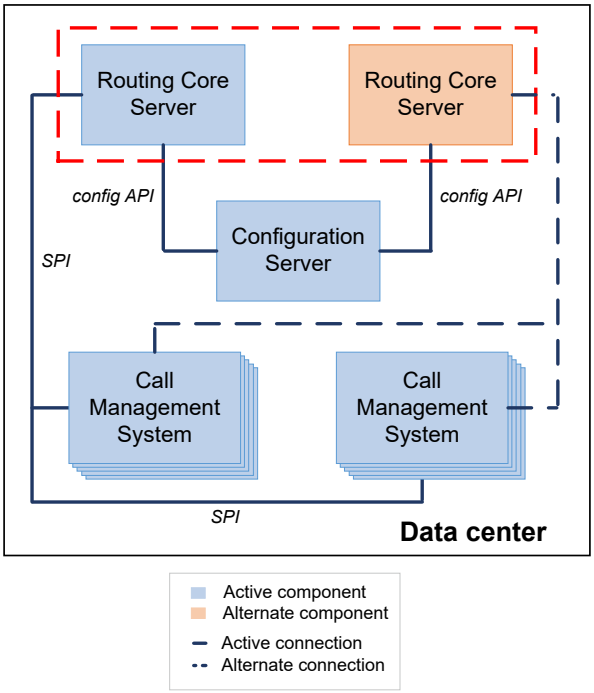
The following diagram provides an overview of the Simplex deployment architecture:



Local HA deployment

In the local HA deployment, the contact center operates in one data center that contains one Configuration Server and two Routing Core Servers.

The following diagram provides an overview of the local HA deployment architecture:

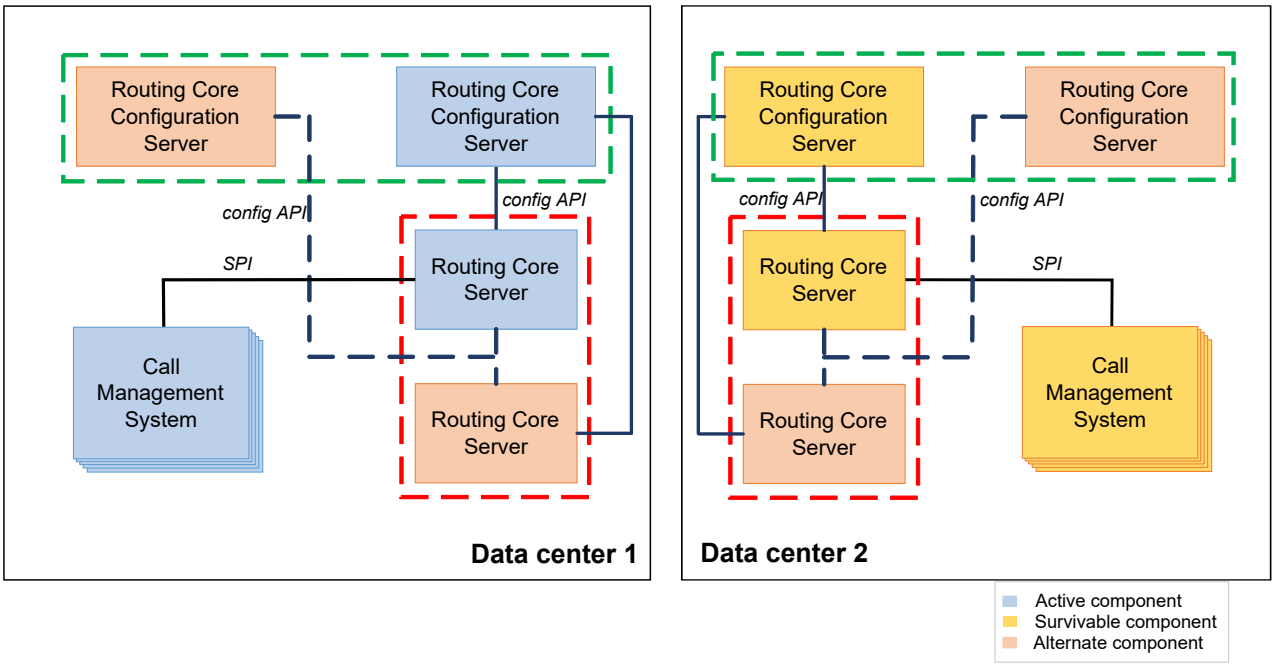


Geo-redundant HA deployment without Layer 2 networking

The contact center operates in two geographically separate data centers. Each data center contains two Configuration Server and two Routing Core Server instances.

Without Layer 2 networking, each data center contains an independent set of contact center servers and supports disaster recovery. In case of the primary data center failure, the Avaya Contact Center – Extended Capacity recovers contact center operations in the secondary data center and does not preserve active calls and agent states. The contact center supports high availability for Configuration Server and Routing Core Server instances within each data center.

The following diagrams provide an overview of the geo-redundant HA deployment architecture without layer 2 networking:


Routing Core Configuration Server
Routing Core Configuration Server
config API
config API
SPI
Routing Core Server
Call Management System
Routing Core Server
Data center 1
Routing Core Configuration Server
Routing Core Configuration Server
config API
config API
Routing Core Server
SPI
Call Management System
Routing Core Server
Data center 2
Active component
Survivable component
Alternate component

Chapter 3: Planning and pre-configuration

Hardware requirements

Routing Core Server hardware requirements

For the Routing Core Server, Avaya recommends using Dell EMC PowerEdge R940 or an equivalent server with the following specifications:

Hardware	Minimum requirements
CPU	112 hyper-threaded, 2.1 GHz cores
Memory	1 TB
Storage	8 TB
Network	10 Gbps or 100 Gbps for larger configurations

Configuration Server hardware requirements

For the Configuration Server, Avaya recommends using a virtual machine with the following specifications:

Hardware	Minimum requirements
CPU	12 vCPUs, 2.1 GHz cores
Memory	20 GB
Storage	500 GB
Network	1 Gbps

Alternatively, the system administrator can use Dell EMC PowerEdge R640 or an equivalent server with the same or greater capacities of the Configuration Server on a virtual machine.

To ensure High Availability, Avaya recommends using dual power supplies and bonded network interface cards. The administrator must also configure RAID storage.

RAID configuration	Minimum requirements
RAID 1	240 GB X 2 disks. You must install the operating system on these disks.
RAID 5+1 (1 disk as hot spare)	1.6 TB X 8 disks

You must configure VMWare and the virtual machines on the RAID 1 and RAID 5 data stores respectively.

Contact center server cabling

Routing Core Servers connect to Layer 2 switches on the traffic VLAN. Each Routing Core Server connects to both Layer 2 switches in a data center with a minimum of 10-Gbps bandwidth. To provide a higher traffic capacity, you can use 100-Gbps bandwidth. Each Configuration Server connects to the traffic VLAN using the 10-Gbps bandwidth.

In the Avaya Contact Center – Extended Capacity solution, Session Border Controller can run either inside or outside data centers.

The following diagrams provide a high-level overview of the contact center server cabling in different deployment environments:

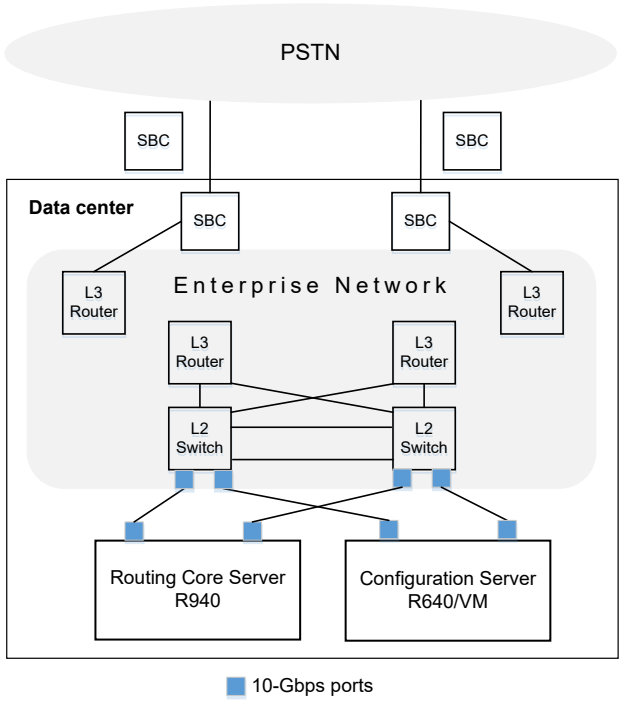


Figure 1: Cabling for the Simplex deployment

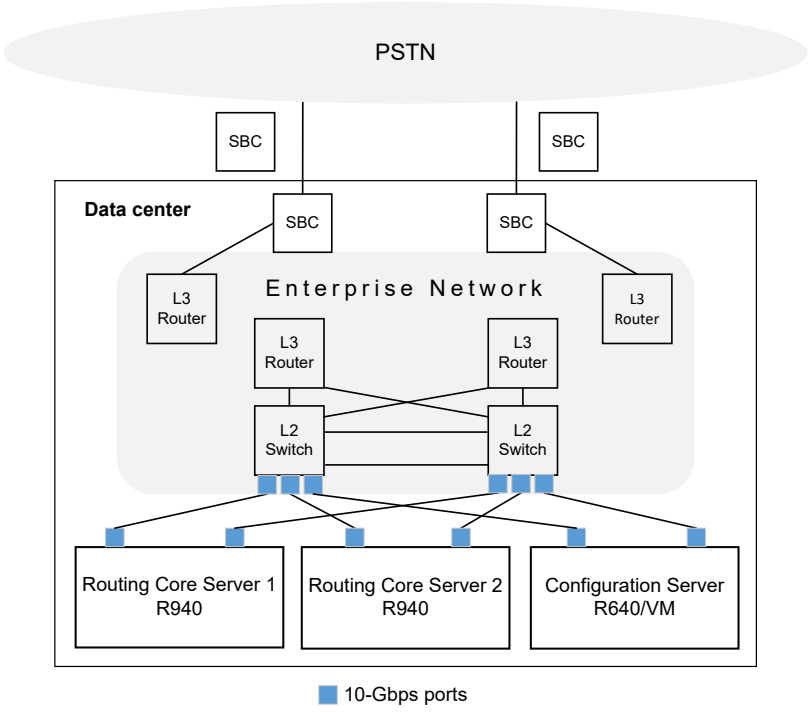


Figure 2: Cabling for the local HA deployment

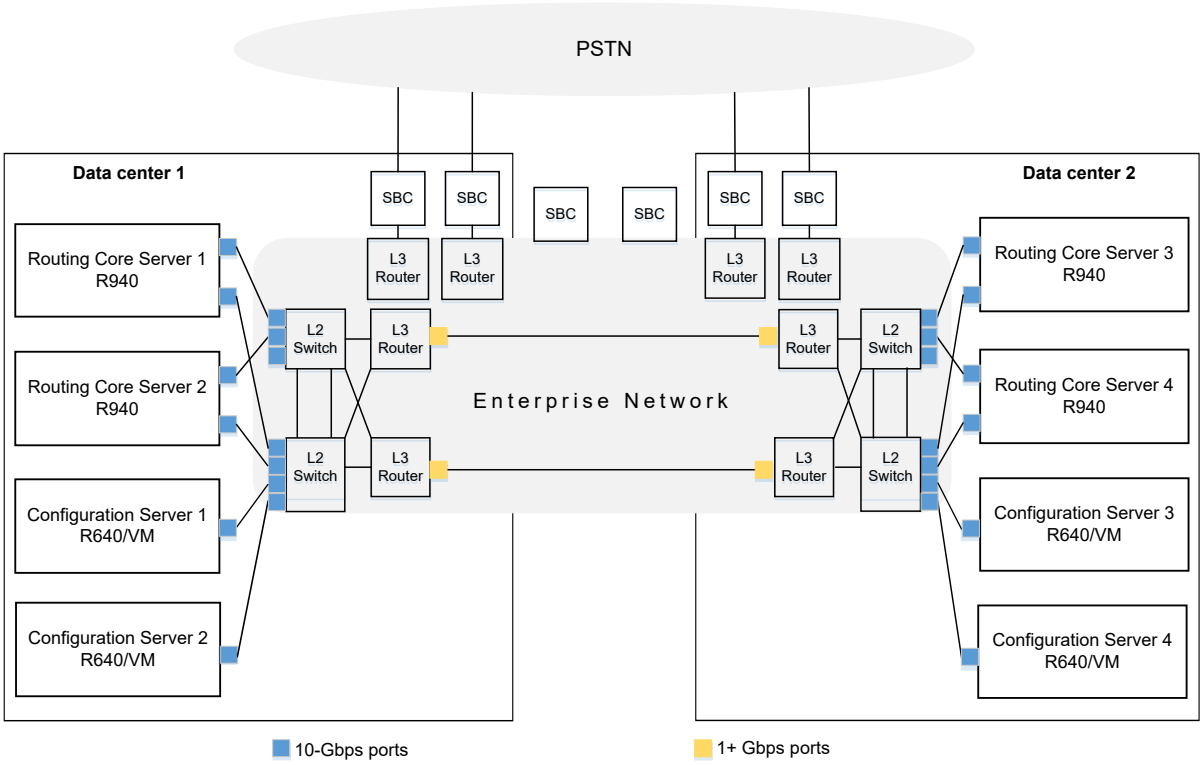


Figure 3: Cabling for the geo-redundant HA deployment without Layer 2 networking

Related links

Routing Core Server chassis on page 99
Configuration Server chassis on page 100
Setting up cabling on page 25

Software requirements

Avaya Contact Center – Extended Capacity server software requires one of the following operating systems:

- Red Hat® Enterprise Linux® (RHEL) versions 8.6
- Oracle Linux version 7.9

You must install one of the required operating systems on all Avaya Contact Center – Extended Capacity servers.

Disk partitioning requirements

When the administrator installs the operating system, Avaya recommends configuring the following disk partitioning for contact center servers:

Routing Core Server

Disk partition	Minimum storage requirements for 1 TB of disk space	Recommended increase for each extra 1 TB of disk space	Recommended storage requirements for 10 TB of disk space
`/boot`, `/boot/efi`, `swap`	Default	–	Default
`/`	100 GB	Minimal	200 GB
`/home`	150 GB	Up to 10%	800 GB
`/var`, including `/var/lib`	500 GB	Up to 50%	4.5 TB
`/var/log`	250 GB	Up to 50%	4.5 TB

Configuration Server

Disk partition	Minimum storage requirements for 500 GB of disk space	Recommended increase for each extra 500 GB of disk space	Recommended storage requirements for 5 TB of disk space
`/boot`, `/boot/efi`, `swap`	Default	–	Default

Table continues…

Disk partition	Minimum storage requirements for 500 GB of disk space	Recommended increase for each extra 500 GB of disk space	Recommended storage requirements for 5 TB of disk space
`/`	100 GB	Minimal	200 GB
`/home`	150 GB	Up to 10%	800 GB
`/var`, including `/var/lib`	150 GB	Up to 50%	2 TB
`/var/log`	100 GB	Up to 50%	2 TB

If contact center servers have more storage space available, Avaya recommends allocating most of the remaining free space to the `/var` and `/var/log` directories.

Network requirements

Before deploying your contact center, ensure the following:

- The network latency without call failures under load between the contact center servers in the same data center is not more than 50 milliseconds.
- The network latency between data centers must not exceed 250 milliseconds.
- Avaya Contact Center – Extended Capacity provides the ability to assign a virtual IP address to the server network interface.
- Layer 2 switches must be connected in a redundant manner in each data center.

IP address allocation

Before deploying your contact center, you must allocate IP addresses appropriately. The number of IP addresses required in your contact center depends on the deployment environment.

The following table provides an overview of IP address allocation for contact center deployment in the Simplex, local HA, and geo-redundant HA environments.

Component address function	Simplex deployment	Local HA deployment	Geo-redundant HA deployment with L2 networking	Geo-redundant HA deployment without L2 networking	Description
iDRAC IP address	2	3	6	8	Required for the Configuration Server and Routing Core Server configuration and management through the iDRAC port.
Configuration Server IP address	1	1	2	4	Required for managing the Configuration Server.
Configuration Server virtual IP address	-	-	1	2	Required for operation of the active Configuration Server and connection to the active Routing Core Server.
Routing Core Server IP address	1	2	4	4	Required for managing the Routing Core Server.
Routing Core Server virtual IP address	-	1	1	2	Required for operation of the active Routing Core Server and connection to the active Configuration Server.
AE Services IP address	2	4	8	4	Required for connection to the Routing Core Server and CTI applications. Each AE Services requires 2 IP addresses.
AE Services virtual IP address	-	1	2	-	Required for operation of the active AE Services server and connection to the active Routing Core Server.
MacVLAN IP address	1	2	4	4	Required for creation of a MacVLAN network on the Routing Core Server and connection to the AE Services.

Secure Access Link Gateway

Avaya Contact Center – Extended Capacity requires a Secure Access Link (SAL) Gateway for remote access and alarming. Using SAL Gateway, support personnel can troubleshoot and debug problems. With SAL Gateway, you can do the following:

- Receive alarms from the contact center
- Reformat alarms
- Forward alarms to the Avaya support center or your Network Management System

Avaya personnel is responsible for installing and configuring SAL Gateway in your network. For more information about SAL Gateway, go to the Avaya Support website at https://support.avaya.com/.

Enhanced Access Secure Gateway

Enhanced Access Secure Gateway (EASG) provides a secure method for Avaya personnel to access your contact center remotely and on-site. Avaya Contact Center – Extended Capacity requires EASG so that Avaya Services can perform tasks for ongoing support, management, and solution optimization.

For more information about installing the EASG site certificate for on-site maintenance, see the general maintenance section in *Maintaining Avaya Contact Center – Extended Capacity*.

Related links

Running the installation command on page 43
Viewing the EASG status on page 90
Managing EASG access on page 90
Installation command options on page 43

Chapter 4: Configuration Server and Routing Core installation

Configuration Server and Routing Core installation overview

You can install the Routing Core in the Simplex, local HA, or geo-redundant HA environment. Avaya Contact Center – Extended Capacity provides the Deployment Manager tool for installing and configuring your contact center servers. The Deployment Manager reduces manual configuration and simplifies the installation process. The Deployment Manager uses deployment scripts to automatically set up the installation environment and deploy Configuration Server, Routing Core Server, and internal AE Services server instances.

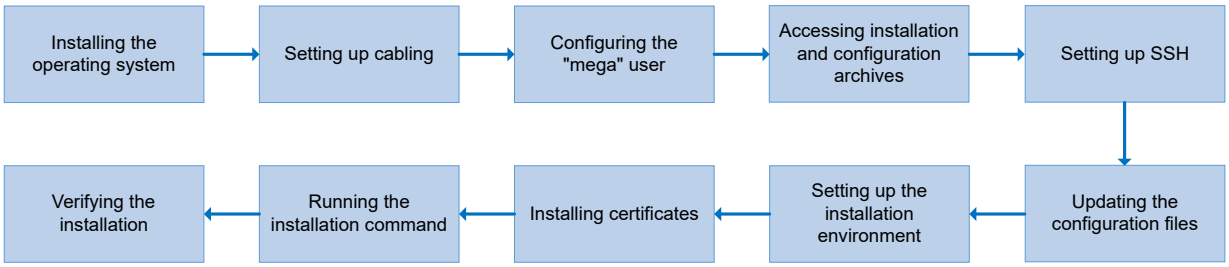
Before deploying your Routing Core, you must install the required operating system on your hardware, enable passwordless sudo on all contact center servers, enabling passwordless SSH, update the deployment configuration files, and install the server certificates. In the `mega-config.yml`, `all`, and `systemconfig` configuration files, you must provide the contact center server and deployment environment details, such as IP addresses, virtual IP addresses, hostnames, and fully qualified domain names (FQDNs).

The number of servers depends on your contact center deployment environment. The following table provides a high-level comparison of the contact center deployment environments:

	Simplex deployment	**Local HA deployment**	**Geo-redundant HA deployment without Layer 2 networking**
Data centers	1	1	2
Configuration Server	1	1	4
Routing Core Server	1	2	4
AE Services	1	2	4
Required identity certificates	• Configuration Server: 1 certificate • Routing Core Server: 1 certificate	• Configuration Server: 1 certificate • Routing Core Server: 2 certificates	• Configuration Server: 4 certificates • Routing Core Server: 4 certificates

Routing Core installation workflow

The following diagram shows a high-level sequence of procedures required to install the Routing Core:



Installing the operating system

About this task

Avaya Contact Center – Extended Capacity server software requires a Red Hat® Enterprise Linux® (RHEL) 8.6 or Oracle Linux 7.9. You must install the required operating system on all contact center servers.

You can make Avaya Contact Center – Extended Capacity Federal Information Processing Standard (FIPS) compliant by installing your operating system with the FIPS mode enabled. For more information about enabling FIPS mode while installing the operating system, see *Installing a RHEL 8 system with FIPS mode enabled* at https://access.redhat.com/.

For more information about operating system installation, see the RHEL or Oracle documentation at https://access.redhat.com/ and https://www.oracle.com/linux/.

Before you begin

- If you deploy the Configuration Server on a virtual machine, create a virtual machine using the corresponding hypervisor management application.
- For the deployment on Dell servers, configure iDRAC. For more information about the iDRAC configuration, see the iDRAC documentation at https://www.dell.com/support/.

Procedure

1. Obtain the installation file for the required operating system.
2. Connect a monitor, a keyboard, and a computer mouse to your server or virtual machine hardware.
3. Turn on or restart the server.
4. Install the operating system with minimal configuration.

   For more information about operating system installation on Dell servers, see https://www.dell.com/support/.

5. To ensure data privacy, enable disk encryption.
6. Configure disk partitioning.
7. Set a root password.
8. Configure an administrator account.

   For deployment, you must create a `mega` user account with the sudo access. You can also create a `mega` user after the operating system installation.
9. Specify the home directory for your administrator account.
10. Assign traffic VLAN IP addresses to the appropriate network interfaces.

    You can also assign traffic VLAN IP addresses after the operating system installation using CLI commands.
11. **(Optional)** Configure the connection to a remote syslog server.

    Avaya Contact Center – Extended Capacity does not currently use standard syslog facilities or store log files on the rsyslog server. The contact center generates Docker container and service log files to record contact center events. For more information about the contact center log processing, see the data privacy and security section in *Maintaining Avaya Contact Center – Extended Capacity*.

Related links

Adding a "mega" user with the sudo access on page 26
Disk partitioning requirements on page 19

Setting up cabling

About this task

For contact center management and operation, connect all contact center servers to appropriate VLANs.

Before you begin

Disable the firewall. For more information, see the RHEL or Oracle documentation at https://access.redhat.com/ and https://www.oracle.com/linux/.

Procedure

1. On the Configuration Server, connect the primary network 10-Gbps port to an L2 switch on the traffic VLAN.
2. **(Optional)** On the Configuration Server, connect the iDRAC or an equivalent port to a management VLAN.
3. **(Optional)** On the Routing Core Server, connect the iDRAC or an equivalent port to a management VLAN.

4. On the Routing Core Server, connect the primary network port to an L2 switch on the traffic VLAN.

   Based on the size of your contact center and traffic load, you can use either the 10-Gbps or 100-Gbps port to connect to the traffic VLAN.

5. On the Routing Core Server, connect the secondary network port to an L2 switch on the traffic VLAN.

   You must use a different L2 switch to connect the secondary port on the Routing Core Server to the traffic VLAN.

   Based on the size of your contact center and traffic load, you can use either the 10-Gbps or 100-Gbps port to connect to the traffic VLAN.

6. On the Routing Core Server, configure the bonding policy for primary and secondary network interface ports as `active-backup`.

   For more information about configuring bonding interface parameters, see the RHEL, CentOS, or Oracle documentation at https://access.redhat.com/ and https://www.oracle.com/linux/.

Related links

Contact center server cabling on page 17
Routing Core Server chassis on page 99
Configuration Server chassis on page 100

Adding a "mega" user with the sudo access

About this task

You can create a `mega` user account with the sudo access on every Routing Core Server and Configuration Server to deploy in your contact center. You can create a `mega` account after the operating system installation. You can access the root account using the `sudo` command.

Procedure

1. On the contact center server, open the console.
2. To log in as the root user, run the following command:

   ```
   su -
   ```

3. When prompted, enter the root password.
4. To create a `mega` user, run the following command:

   ```
   adduser mega
   ```

5. When prompted, type the root password.

The command creates a new user with the `mega` username and `home/mega/` as the home directory.

6. In New password, type the password for the `mega` user.
7. To confirm the password, retype the password.
8. **(Optional)** Provide the `mega` user details.
9. To grant the sudo access to the `mega` user, run the following command:

   ```
   usermod -aG wheel mega
   ```

   The command adds the `mega` user to the `wheel` group that grants the sudo access to users.

Enabling passwordless sudo for the "mega" user

About this task

Enable the sudo access without a password to the "mega" user in the `sudoers` file on all contact center servers. The `sudoers` file contains the information about permissions for all existing users.

Before you begin

Add a "mega" user with the sudo access.

Procedure

1. On the contact center server, open the console.
2. To log in as the root user, run the following command:

   ```
   su -
   ```

3. In the command prompt, enter the root password.
4. To open the `sudoers` file for editing, run the following command:

   ```
   vi -f /etc/sudoers
   ```

5. In the `sudoers` file, add the following line:

   ```
   mega ALL=(ALL) NOPASSWD: ALL
   ```

6. To save the file, run the following command:

   ```
   :wq!
   ```

Related links

Adding a "mega" user with the sudo access on page 26

Downloading the Avaya Contact Center – Extended Capacity installation archive from PLDS

About this task

Use the Product Licensing and Delivery System (PLDS) web portal to download the Avaya Contact Center – Extended Capacity installation archive. The PLDS web portal is available to authorized Avaya Business Partners, customers, and Avaya associates. For more information about PLDS, go to https://support.avaya.com/.

Before you begin

- Remove and clean up all installed container applications on the Configuration Server hardware.
- Ensure that you have access to PLDS.

Procedure

1. In your browser, enter http://plds.avaya.com.
2. On the PLDS website, enter your login ID and password.
3. On the Home page, click **Assets**.
4. Click **View Downloads**.

   PLDS displays the View Downloads page.
5. Click the search icon for **Company Name**.

   PLDS displays the Search Companies dialog box.
6. In **Name**, type your company name.
7. Click **Search Companies**.
8. Locate the correct entry and click **Select**.
9. To filter the available downloads, do one of the following:
   - In **Download Pub ID**, type the download publication ID.

     Publication ID is an identifier of the file to download.
   - In **Application**, click **Avaya Contact Center – Extended Capacity**.
10. Click **Search Downloads**.
11. Scroll down to the entry for the file to download and click **Download**.
12. Select a location to save the file and click **Save**.

    PLDS downloads the `aocle_routing_<tag>.tar.gz` installation archive to your computer. `<tag>` is a unique identifier of your installation archive.

Logging into a contact center server using an SSH client

About this task

Access a contact center server using an SSH client. For example, you can use PuTTY to log in to one of the Avaya Contact Center – Extended Capacity servers.

Before you begin

- Install an SSH client.
- Obtain the login and password for the "mega" account.

Procedure

1. Open your SSH client.
2. In **Host Name**, type the IP address of the server to access.
3. Click **Open**.

   The SSH client establishes an SSH session with the specified server.
4. In the SSH session window, enter `mega`.
5. When prompted, enter the "mega" account password.

Copying the installation archive onto the Configuration Server

About this task

After downloading the installation archive from PLDS, copy the archive onto the Configuration Server.

Procedure

1. On the computer where you downloaded the installation archive, open the console.
2. In the console, run the following command:

   `scp <src_path_file> <dest_path_to_copy>`, where `<src_path_file>` is the path to the installation archive and `<dest_path_to_copy>` is the path to your working directory.

   For example, the following command copies the installation archive from the `Downloads` folder on your computer to the server home directory for the "mega" user on the 10.1.2.7 IP address:

   ```
   scp C:/Users/user/Downloads/aocle_routing_<tag>.tar.gz
   mega@10.1.2.7
   ```

Unpacking the installation archive

About this task

To access the solution installation files, untar the archive. The time for unpacking the archive depends on your CPU capacity.

Note:

<tag> is a unique identifier of your installation archive.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. To access the installation archive, run the following command:

   `cd <working directory>`, where *<working directory>* is the path to the working directory that contains the installation archive.
3. To untar the installation archive, run the following command:

   `tar -xvf aocle_routing_<tag>.tar.gz`

   The command untars the contact center configuration packages into your working directory.

Installation archive contents

The installation archive contains the following packages:

- `aes_images_<tag>.tar.gz` with the internal AE Services images.
- `mbx_images_<tag>.tar.gz` with the Routing Core Server images.
- `mcs_images_<tag>.tar.gz` with the Configuration Server images.
- `mega_deployment_scripts_<tag>.tar.gz` with the solution installation scripts.
- `offline-packages-latest.tar.gz` with the Deployment Manager configuration files.
- `oversight_images_<tag>.tar.gz` with the Oversight images.
- `ui_images_<tag>.tar.gz` with the Configuration Server web portal images.

<tag> is a unique identifier of your installation archive.

Untarring the configuration archive

About this task

The `mega_deployment_scripts_<tag>.tar.gz` archive contains the contact center deployment scripts. To access the scripts, you must untar this archive.

Note:

<tag> is a unique identifier of your installation archive.

Before you begin

Download and unpack the installation archive.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   `cd <working directory>`, where *<working directory>* is the path to the directory that contains the `mega_deployment_scripts_<tag>.tar.gz` archive.
3. To untar the deployment scripts, run the following command:

   ```
   tar -xvf mega_deployment_scripts_<tag>.tar.gz
   ```

   The command creates the `mega` folder with the contact center deployment scripts.

Related links

Unpacking the installation archive on page 30

Installing the application deployment tool

About this task

Before deploying Avaya Contact Center – Extended Capacity, install the application deployment tool.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   ```
   cd mega/deployment-manager/
   ```

3. In the Deployment Manager directory, run the following command:

   ```
   ./installMega.sh -l <path to the offline packages archive>
   setup_prereqs
   ```

   For example, `./installMega.sh -l /home/mega/offline-packages-latest.tar.gz setup_prereqs`

   <tag> is a unique identifier of your installation archive.

Deployment Manager configuration

Before deploying the contact center with the Deployment Manager, you must do the following:

- Update deployment configuration files with the contact center server and deployment environment details.
- Set up the contact center installation environment.

Updating the mega-config.yml file

About this task

For the contact center deployment, specify network configuration details in the `mega-config.yml` file. The configuration file contains IP addresses of the Configuration Server, Routing Core Server, and AE Services servers. You must also specify virtual IP addresses and hostnames.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   ```
   cd mega/deployment-manager/
   ```

3. To open the `mega-config.yml` file for editing, run the following command:

   ```
   vi mega-config.yml
   ```

4. In the `mega-config.yml` file, specify the network configuration parameters for your contact center.

   To see examples of the `mega-config.yml` file configuration for different deployment environments, see the examples in *Appendix C: Configuration file examples*.

5. To save the file, run the following command:

   ```
   :wq!
   ```

Related links

mega-config.yml example on page 105

Generating SSH keys

About this task

Generate SSH keys for Configuration Server and Routing Core Server instances.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. To generate an SSH key pair, run the following command:

   ```
   ./installMega.sh sshmgr generate_keys
   ```
3. When prompted, for each Routing Core Server, enter the server user password.

   The contact center generates an SSH key pair on the Configuration Server and copies the public key to the remaining servers.

Updating the all file

About this task

After updating the `mega-config.yml` file, provide the deployment environment details in the `all` file.

Before you begin

Update the `mega-config.yml` file.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   ```
   cd mega/ansible_playbook/mega_deploy/group_vars/
   ```
3. To open the `all` file for editing, run the following command:

   ```
   vi all
   ```
4. In the `all` file, specify the deployment variables for your deployment environment.

   To see examples of the `all` file configuration for different deployment environments, see the examples in *Appendix C: Configuration file examples*.
5. To save the file, run the following command:

```
:wq!
```

Related links

all example on page 109
Updating the mega-config.yml file on page 32

Viewing the Routing Core Server interface name

About this task

In the `mega-config.yml` file, provide the interface name of the Routing Core Server. To view the interface name, you can use the `ifconfig` command.

Before you begin

Generate SSH encryption keys.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. To access Routing Core Server, run the following command:

   `ssh mega@<server_IP_address>`, where *<server_IP_address>* is the static IP address of the Routing Core Server.
3. Run the following command:

   ```
   ifconfig
   ```

   The command output displays information for all network interfaces on the Routing Core Server.
4. In the command output, locate the interface with the Routing Core Server IP address in the inet parameter.

Next steps

Specify the mbx and aes interface names in the `mega-config.yml` file.

Viewing the Configuration Server interface name

About this task

In the `mega-config.yml` file, provide the interface name of the Configuration Server. To view the interface name, you can use the `ifconfig` command.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.

2. Run the following command:

   ```
   ifconfig
   ```

   The command output displays information for all network interfaces on the Configuration Server.

3. In the command output, locate the interface with the Configuration Server IP address in the inet parameter.

Next steps

Specify the mcs interface name in the `mega-config.yml` file.

Setting up the installation environment

About this task

After updating the Deployment Manager configuration files, set up the contact center installation environment.

Before you begin

Update the `mega-config.yml` and `all` files.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   ```
   cd mega/deployment-manager/
   ```

3. In the Deployment Manager directory, run the following command:

   ```
   ./installMega.sh prepare_environment
   ```

Related links

Contact center deployment environments on page 12
Updating the mega-config.yml file on page 32
Updating the all file on page 33

Certificate installation

Avaya Contact Center – Extended Capacity requires identity and trusted security certificates for establishing secure TLS connection, client and server authentication. If you do not install certificates, you cannot use secure connections for the contact center.

Before installing certificates, you must specify the server data, such as server IP addresses, FQDNs, and hostnames specific to your deployment environment in the `systemconfig` file.

To install identity certificates, you must generate a certificate signing request (CSR), submit the request to your Certificate Authority (CA), download certificate files from your CA, and import certificates into the contact center truststore. You must ensure that signed certificates include the X509v3 Subject Alternative Names (SANs).

To install a trusted CA certificate, you must download it from your CA and import the certificate into the contact center truststore.

Updating the systemconfig file

About this task

Before installing certificates, update the `systemconfig` file with the server data specific to your contact center deployment environment. The `systemconfig` template is stored in the `mega/Helperscripts/certificates/` directory. You must copy the file template to the `/var/opt/Avaya/` directory and update it with your server data.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

   ```
   cd mega/Helperscripts/certificates/
   ```
3. To copy the file template, run the following command:

   ```
   cp systemconfig /var/opt/Avaya/
   ```

   The `systemconfig` file is copied into the `/var/opt/Avaya/` directory.
4. Run the following command:

   ```
   cd /var/opt/Avaya/
   ```
5. To open the `systemconfig` file for editing, run the following command:

   ```
   vi systemconfig
   ```
6. In the `systemconfig` file, provide the server data specific to your deployment environment.

   To see an example of the `systemconfig` file configuration, see *Appendix C: Configuration file examples*.
7. To save the file, run the following command:

   ```
   :wq!
   ```

Related links

systemconfig example on page 116

Generating a certificate signing request

About this task

Generate CSRs for each Configuration Server and Routing Core Server used in your contact center deployment.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

   ```
   cd mega/deployment_manager/
   ```

3. To generate a CSR, run the following command:

   ```
   ./installMega.sh certificate generate_signing_requests
   ```

4. When prompted, enter the CSR passphrase.
5. To confirm your CSR passphrase, re-enter the passphrase.

   After you enter the CSR passphrase, the Deployment Manager stores `.csr` files for all contact center servers used in your contact center deployment in the `/var/opt/Avaya/cert/` directory.

Next steps

Submit CSRs to your CA.

Related links

Contact center deployment environments on page 12

Creating a certificate identity

About this task

Create certificate identities for each server used in your contact center deployment to enroll server identity certificates. If you use a public CA or a separate CA server to sign the CSR, you do not need to create certificate identities.

This procedure describes how to generate certificate identities using Avaya Aura® System Manager CA.

Procedure

1. Log in to the System Manager web administration portal.
2. Go to **Security** > **Certificates** > **Authority**.
3. In the RA Functions section, click **Add End Entity**.
4. In **Username**, type a username for the new certificate identity.

5. In **Password (or Enrollment Code)**, type a password for the new certificate identity.

   You need the password to enroll your certificates.
6. In **Confirm Password**, retype the password.
7. In **CN, Common name**, type the hostname of the corresponding server interface.

   The hostname must match the server hostname specified in the `systemconfig` file.
8. In **O, Organization**, type your company name.

   The company name must match the O(Organization) value in the `systemconfig` file.
9. In **C, Country**, type the two-letter code of your country.

   The country code must match the C(Country code) value in the `systemconfig` file.
10. In **L, Locality**, type your company location.

    The company location must match the corresponding server location specified in the `systemconfig` file. For the Configuration Server and Routing Core Server instances deployed in the primary data center, you must use the L(DC1 location) value from the `systemconfig` file. For all other servers, you must use the L(DC2 location) value.
11. In **DNS Name**, type the FQDN of the corresponding server interface.

    The server FQDN must match the corresponding server FQDN specified in the `systemconfig` file.
12. In **IP Address**, type the IP address of the corresponding server.

    The IP address must match the corresponding server IP address specified in the `systemconfig` file.
13. Click **Add**.

Enrolling identity certificates

About this task

After creating identity certificate entities, enroll the certificate for each server in your contact center deployment. If you use a public CA or a separate CA server to sign the SCR, you do not need to enroll the identity certificates.

The following procedure describes how to enroll your certificates using Avaya Aura® System Manager CA. Avaya Contact Center – Extended Capacity requires identity certificate files in the `.pem` format.

Before you begin

- Log in to the System Manager web administration portal.
- On the Configuration Server, open the CSR request file for the corresponding server interface in a text editor.

Procedure

1. On the System Manager administration portal, go to **Security** > **Certificates** > **Authority**.

2. In the administration portal navigation menu, click **Public Web**.
3. Click **Create Certificate from CSR**.
4. In **Username**, provide the username of the corresponding certificate identity.

   The username must match the username that you specified when creating a certificate identity.
5. In **Enrollment code**, provide the password for the corresponding certificate identity.

   The password must match the password that you specified when creating a certificate identity.
6. In the text box, provide the contents of the corresponding CSR request file.
7. In **Result Type**, select **PEM - certificate only**.
8. Click **OK**.

   The System Manager administration portal downloads the certificate file in the `.pem` format.
9. Ensure that the certificates include the X509v3 SANs.

   You can open the certificates using a text editor.

Copying certificates to the Configuration Server

About this task

After signing identity certificates, copy them and the trusted CA certificate to the Configuration Server.

Before you begin

Download signed identity certificates and a trusted certificate from your CA.

Procedure

1. On the computer that contains the certificates, open the console.
2. In the console, run the following command:

   `scp <src_path_file> <dest_path_to_copy>`, where `<src_path_file>` is the path to the certificate and `<dest_path_to_copy>` is the path to the directory on the Configuration Server where you want to store the certificates.

   For example, the following command copies the `mcs1.pem` certificate from your local computer to the `var/opt/Avaya/certificate_manager/` directory for the "mega" user on the 10.1.2.7 IP address:

   ```
   scp C:/Users/user/Downloads/mcs1.pem mega@10.1.2.7:/var/opt/Avaya/certificate_manager/
   ```
3. Repeat step 2 until you copy all the certificates to the Configuration Server.

Importing a trusted certificate

About this task

Import a trusted CA certificate into the contact center truststore to set up a secure TLS connection, client and server authentication. You must indicate the full path to the trusted CA certificate and specify the CA alias name. After importing, the certificate is stored in the `/var/opt/Avaya/cert/` directory.

Before you begin

Copy a trusted certificate from your CA to the Configuration Server.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

   ```
   cd mega/deployment_manager/
   ```

3. In the Deployment Manager directory, run the following command:

   ```
   ./installMega.sh certificate import_trustcert -ca <path_to_ca>
   -alias <ca_alias>
   ```

   <path_to_ca> is the full path to the trusted CA certificate and *<ca_alias>* is the CA alias name.

Related links

Contact center deployment environments on page 12
Copying certificates to the Configuration Server on page 39

Importing signed identity certificates

About this task

Import your identity certificates into the contact center truststore to set up a secure TLS connection, client and server authentication. After importing, the certificates are stored in the `/var/opt/Avaya/cert/` directory.

Before you begin

Copy the signed identity certificates to the Configuration Server.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

```
cd mega/deployment_manager/
```

3. In the Deployment Manager directory, run one of the following commands depending on the deployment type:

   - For Simplex deployment:

     ```
     ./installMega.sh certificate import_identity -mcs <PATH_MCS_CERT>
     -mbx <PATH_MBX_CERT>
     ```

   - For Local HA deployment:

     ```
     ./installMega.sh certificate import_identity -mcs <PATH_MCS_CERT>
     -mbx1 <PATH_MBX1_CERT> -mbx2 <PATH_MBX2_CERT>
     ```

   - For Geo-redundant HA deployment without Layer 2 networking:

     ```
     ./installMega.sh certificate import_identity -mcs1
     <PATH_MCS1_CERT> -mcs2 <PATH_MCS2_CERT> -mbx1 <PATH_MBX1_CERT>
     -mbx2 <PATH_MBX2_CERT>
     ```

Related links

Contact center deployment environments on page 12
Copying certificates to the Configuration Server on page 39

certificate import_identity command options

When running a command to import identity certificates, you must specify full paths to certificates of the Configuration Server and Routing Core Server instances to deploy in your contact center. The following table provides an overview of the command options to specify for importing identity certificates in different deployment environments:

	Simplex deployment	Local HA deployment	Geo-redundant HA deployment
Primary data center			
The Configuration Server certificate	*<path_cs_cert>*	*<path_cs_cert>*	*<path_cs1_cert>*
Routing Core Server certificates	*<path_rcs_cert>*	• *<path_rcs1_cert>* • *<path_rcs2_cert>*	• *<path_rcs1a_cert>* • *<path_rcs1b_cert>*
Secondary data center			
The Configuration Server certificate	-	-	*<path_cs2_cert>*
Routing Core Server certificates	-	-	• *<path_rcs2a_cert>* • *<path_rcs2b_cert>*

Importing a certificate revocation list

About this task

Avaya Contact Center – Extended Capacity supports certificate revocation. CAs keep track of SSL certificates. After CA revokes an SSL certificate, CA retrieves the serial number of the invalid certificate and adds it to the certification revocation list.

By default, the certificate directory already contains a certificate revocation list. You can import your own certificate revocation list into the `/var/opt/Avaya/cert/` directory.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

   ```
   cd mega/deployment_manager/
   ```
3. In the Deployment Manager directory, run the following command:

   ```
   ./installMega.sh certificate import_crl -crl <path_to_crl>
   ```

   <path_to_crl> is the full path to the certificate revocation list file.

Related links

Contact center deployment environments on page 12

Verifying certificate installation

About this task

After importing solution certificates, verify the certificate installation.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run the following command:

   ```
   cd mega/deployment_manager/
   ```
3. In the Deployment Manager directory, run the following command:

   ```
   ./installMega.sh certificate validate
   ```

   If certificate installation fails, the command output displays an error message.

Related links

Contact center deployment environments on page 12

Running the installation command

About this task

To simplify the deployment process, you can deploy solution components on all servers simultaneously. The deployment includes the installation of the Configuration Server, Configuration Server web portal, Routing Core Server, AE Services, Oversight, EASG, and noVNC client application. Alternatively, you can install contact center components separately.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. In the command prompt, run the following command:

   ```
   cd mega/deployment_manager/
   ```
3. To install contact center components, run the following command:

   ```
   ./installMega.sh fresh-deploy all <installation archive location>
   ```
4. When prompted, accept the End User License Agreement.
5. When prompted, enable EASG.

   Avaya Contact Center – Extended Capacity requires EASG so that Avaya Services can perform tasks for the contact center support, management, and optimization.

Related links

Contact center deployment environments on page 12
Managing EASG access on page 90
Installation command options on page 43

Installation command options

You can deploy all solution components with basic configuration using the `./installMega.sh fresh-deploy all <installation archive location>` command.

You can also use the command options to install the corresponding contact center components separately. You must install contact center components in the following order:

- *easg*: To install EASG.
- *nonvc*: To install the noVNC client application.
- *mcs*: To install the Configuration Server.
- *ui*: To install the Configuration Server web portal.
- *mbx*: To install the Routing Core Server.

- *oversight*: To install Oversight.
- *aes*: To install the AE Services server.

Related links

Contact center deployment environments on page 12

Verifying the server installation

About this task

After you deploy solution components, verify that the Deployment Manager installed the Routing Core Server and Configuration Server instances correctly. The Configuration Server and one Routing Core Server in the primary data center must be active and host corresponding VIP addresses. All other servers must be in alternate mode and host only the static IP address. You can run the `hostname -I` command to check if a server hosts the VIP address.

Procedure

1. Do one of the following:
   - Open the server console.
   - Use the SSH terminal to log in to the contact center server.
2. In the command prompt, run the following command:

   ```
   hostname -I
   ```

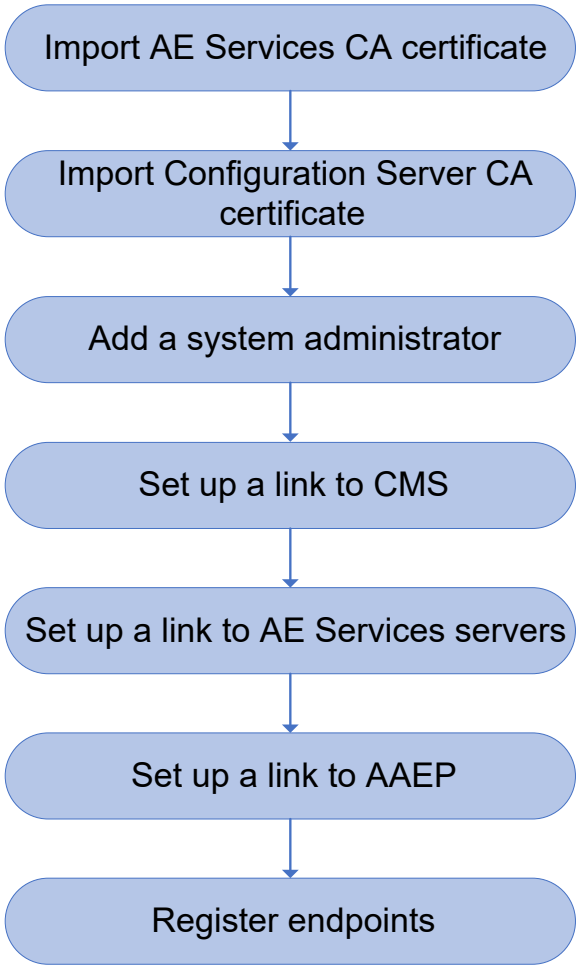
   The command output lists all IP addresses on your server network interfaces.
3. Verify the server IP addresses in the command output.

   The first IP address in the command output is the server static IP address. If the server is active, the command output displays the virtual IP address after the static IP address.

Chapter 5: Post-installation configuration

Post-installation configuration workflow

The following image shows a high-level sequence of procedures required to configure the contact center after the installation:



Logging in to the Configuration Server web portal as a super administrator

About this task

Log in to the Configuration Server web portal as a super administrator to access the Security App and add new contact center users, manage their roles and permissions.

The default login and password for a super administrator is `admin`. When you log in to the Configuration Server web portal for the first time, you must change the default credentials.

Before you begin

- Ensure you have the latest version of Google™ Chrome, Microsoft Edge, Mozilla Firefox, Opera, or Safari.
- Obtain the Configuration Server IP address. You specify the Configuration Server IP address when editing the installation file during the contact center deployment.

Procedure

1. In your browser, enter the Configuration Server IP address and port number in the following format:

   `https://<Configuration Server IP address>:8201`

   In the geo-redundant HA deployment, enter the virtual IP address and port number of the Configuration Server.
2. In **Username or email**, type the username for the super administrator account.
3. Click **CONTINUE**.
4. In **Password**, type the super administrator password.
5. **(Optional)** To view the entered password, click .
6. Click **LOGIN**.

   The Configuration Server redirects you to the App Launcher screen.
7. Click **Security**.

   The Configuration Server displays the Welcome screen of the Security App.

Adding a system administrator

About this task

After logging in to the Security App, add a system administrator. The system administrator can access the System Administration and Contact Center Administration applications. You can use this role to perform post-installation configuration and verification.

For more information about the system administrator user role, see the user management section in *Administering Avaya Contact Center – Extended Capacity*.

Before you begin

Log in to the Configuration Server Security App as a super administrator.

Procedure

1. On the Security App navigation menu, click **User Management**.
2. At the top-right corner of the User Management page, click +.
3. **(Optional)** In **First Name**, type the first name of system administrator.

   You can type a maximum of 35 Unicode characters.
4. **(Optional)** In **Last Name**, type the last name of system administrator.

   You can type a maximum of 35 Unicode characters.
5. In **Email**, type the email address of system administrator.

   The system administrator can enter the username or email address to log in to the Configuration Server web portal.
6. In **Username**, type the username of system administrator.
7. In **Password**, do one of the following:
   - Type the password of system administrator.

     You must set a unique password for each system administrator.
   - To generate the system administrator password, click **Generate Password**.
8. Under GLOBAL ROLE, select **System**.
9. At the bottom-right corner of the screen, click **Save**.

   The Configuration Server saves the system administrator configuration and redirects you to the User Management screen.

Next steps

After configuring a tenant, assign the tenant to the system administrator.

Related links

Adding a tenant on page 50
Assigning a tenant to the system administrator on page 51

Assigning the system administrator with administrative privileges

About this task

After you add a system administrator, assign them access to the System Administration and Contact Center Administration applications. The system administrator can log in to the Configuration Server and continue the contact center configuration.

Before you begin

To add a system administrator,

Procedure

1. In the Security App navigation menu, click **System Administration**.
2. On the System Administration page, in Users Permissions, select the system administrator to provide access.
3. In the Assign Role pane, select **System**.
4. At the top-right corner of the screen, click **Commit**.

   You can see the assigned role in the Role column of the Users Permissions subtab.
5. In the navigation menu, click **Contact Center Administration**.
6. On the Contact Center Administration page, in Users Permissions, select the system administrator to provide access.
7. In the Assign Role pane, select **System**.
8. At the top-right corner of the screen, click **Commit**.

   You can see the assigned role in the Role column of the Users Permissions subtab.

Related links

Adding a system administrator on page 46

Logging in to the Configuration Server as a system administrator

About this task

Log in to the Configuration Server as a system administrator to perform initial setup and verification of your contact center functionality after the installation.

Before you begin

- Obtain the Configuration Server IP address. You specify the Configuration Server IP address when editing the installation file during the contact center deployment.

- Obtain the system administrator credentials. The super administrator configures a system administrator's login and password when adding them to the contact center.

Procedure

1. In your browser, enter the Configuration Server IP address and port number in the following format:

   `https://<Configuration Server IP address>:8201`

   In the geo-redundant HA deployment, enter the virtual IP address and port number of the Configuration Server.
2. In **Username or email**, type the username or email configured for the system administrator account.
3. Click **CONTINUE**.
4. In **Password**, type the configured password.
5. **(Optional)** Click ⌀ to view the entered password.
6. Click **LOGIN**.

   The Configuration Server directs you to the App Launcher page.
7. Click **Contact Center Administration**.

   You can continue configuring the contact center using the Administration navigation menu.

Adding a Routing Core Server

About this task

On the Configuration Server web portal, you must specify the server name and static IP address for each Routing Core Server used in your contact center deployment. The IP address must match the static IP address of the corresponding Routing Core Server specified in the `systemconfig` file.

Before you begin

Log in to the Configuration Server web portal as a system administrator.

Procedure

1. On the Configuration Server web portal, click **System Administration**.
2. In the System Administration navigation menu, click **Routing Core Servers**.
3. At the top-right corner of the Routing Core Servers screen, click **Add Server**.

   The Configuration Server displays the Routing Core Server configuration fields.
4. In **Name**, type the name of the Routing Core Server instance.

   You can type a maximum of 35 Unicode characters.

5. In **IP Address**, type the static IP address of the Routing Core Server.
6. At the top-right corner of the screen, click **SAVE**.

   The Configuration Server saves the Routing Core Server configuration and redirects you to the Routing Core Servers screen.

Related links

Logging in to the Configuration Server as a system administrator on page 48

Adding a tenant

About this task

During the initial administration of the Configuration Server, configure a tenant. With tenants, you can manage contact center data per your organizational units.

Before you begin

Log in to the Configuration Server web portal as a system administrator.

Procedure

1. On the Configuration Server web portal, click **System Administration**.
2. In the System Administration navigation menu, click **Tenants**.
3. To create a new tenant, at the top-right corner of the screen, click **Add Tenant**.

   The Configuration Server displays the tenant configuration fields.
4. In **ID**, type a unique identifier for the tenant.

   You can type only letters. The tenant ID must match the TENANT value specified in the `all` file.
5. In **Tenant Name**, type the name of tenant.
6. In **Domain**, type the domain of tenant.

   For example, `avaya.com`
7. In **Primary Routing Core Server**, select the primary Routing Core Server.

   The primary Routing Core Server hosts the virtual IP address.
8. In **Secondary Routing Core Server**, select one or more alternate Routing Core Server instances.

   The number of alternate Routing Core Servers depends on the deployment environment of your contact center.
9. In **Configuration Server IP:Port**, type `192.168.1.31:4000`.
10. In **Script Executor Server IP:Port**, type `192.168.1.30:34568`.

11. In **SHM API IP:Port**, type `192.168.1.30:9085`.
12. At the top-right corner of the screen, click **SAVE**.

    The Configuration Server saves the tenant configuration and redirects you to the Tenants screen.

Related links

Contact center deployment environments on page 12
Logging in to the Configuration Server as a system administrator on page 48

Assigning a tenant to the system administrator

About this task

Assign the configured tenant to the system administrator to provide the system administrator with administrative privileges.

Before you begin

Log in to the Configuration Server as a super administrator.

Procedure

1. On the Security App navigation menu, click **User Management**.
2. On the User Management screen, select the required user.
3. At the top-right corner of the screen, click ✎.

   The Configuration Server displays the user configuration fields.
4. To assign a network tenant to the user, under TENANTS, select the required tenant.
5. At the bottom-right corner of the screen, click **Save**.

   The Configuration Server saves the user configuration and redirects you to the User Management screen.

Related links

Logging in to the Configuration Server web portal as a super administrator on page 46

Call Management System configuration overview

Call Management System (CMS) processes call traffic, generates supervisor reports, and provides an administrative interface to manage contact center features. With CMS, you can also access the CMS database, configure your contact center parameters, and monitor call activities.

To send your call center data to CMS for monitoring agent performance and generating supervisor reports, you must do a two-step configuration for each CMS that you add:

- Configure a CMS connection on the Configuration Server web portal.
- Add your contact center to CMS using the CMS CLI.

After establishing the connection from both sides successfully, you can verify the CMS link status and run a test supervisor report.

Configuring a Call Management System connection

About this task

Configure a connection to CMS on the Configuration Server web portal. The CMS port number you specify during the configuration must correspond to the TCP port number you configure when adding your contact center to CMS.

Before you begin

Obtain the CMS IP address that you defined during the CMS deployment. For more information about defining the CMS IP address, see *Deploying Avaya Call Management System*.

Procedure

1. On the Configuration Server web portal, go to **Administration** > **CMS Links**.
2. At the top-right corner of the CMS Links screen, click +.

   The Configuration Server displays the CMS connection configuration fields.
3. On the Add CMS Link screen, in **Name**, type the CMS connection name.

   You can type a maximum of 35 Unicode characters.
4. In **IP Address**, type the CMS IP address.
5. In **Port**, type the port number for connecting CMS to your contact center.

   The port number range is 5001 through 5020.
6. To enable the CMS link, select **Enabled**.
7. **(Optional)** In **Description**, type a short description of the CMS connection.

   You can type a maximum of 50 Unicode characters.
8. At the top-right corner of the screen, click **Commit**.

   The Configuration Server saves the CMS connection configuration and redirects you to the CMS Links screen.

Adding your contact center to Call Management System

About this task

After configuring the connection to CMS on the Configuration Server web portal, log in to CMS and create a connection to the contact center to send your call traffic to CMS for further processing. You must create a connection for each CMS in the contact center.

Before you begin

- Deploy a Call Management System and ensure that the Informix Database Server is turned on. For more information about deploying CMS and turning on the Informix Database Server, see *Deploying Avaya Call Management System*.
- Ensure you have user credentials for logging in to CMS.
- Obtain the Configuration Server system name and model, local and remote port numbers, and hostname.

Procedure

1. Log in to Call Management System.
2. To access CMS as a root user, run the **sudo** command.
3. In the command line, run the **cmssvc** command.

   You can see the CMS Services menu.
4. In the command prompt, enter `4` to select the **run_cms** option.
5. In the command prompt, enter `2` to turn CMS off and keep the Informix Database Server running.

   All the logged-in CMS users receive a notification about the CMS shutdown. When CMS is down, you can see `CMS is now off` in the command output.
6. To create a new contact center connection, rerun the **cmssvc** command.
7. In the command prompt, enter `5` to select the **setup** option.
8. In the command prompt, enter `y` to add a new configuration to CMS.
9. In Select the language for this server, enter the option number corresponding to your language.

   For example, you can enter `1` to select English.

   When CMS is ready for adding a new configuration, you can see `Customer CMS data successfully initialized` in the command output.
10. In Enter a name for this UNIX system, enter the name of the new system.

    You can enter a maximum of 64 alphanumeric characters.
11. To select a type of backup device, in the command prompt, enter `2`.
12. In Enter the default backup device path, enter the default path for the backup device.

    For more information about the backup device types and default paths, see the CMS configuration section in *Deploying Avaya Call Management System*.
13. In Enter the number of ACDs being administered, enter `1`.
14. In Enter switch name, enter the name of the new contact center.

    You can enter a maximum of 20 alphanumeric characters.

15. To select AECC as a switch model, in the command prompt, enter `5`.
16. In Enter the local port assigned to switch, enter the local port number.

    The port number must be in the range of 1 through 64 and match the corresponding value defined for the Routing Core Server during the contact center installation.
17. In Enter the remote port assigned to switch, enter the remote port number.

    The port number must be in the range of 1 through 64 and match the corresponding value defined for the Routing Core Server.
18. In Enter switch host name or IP Address, enter the Routing Core Server IP address.

    For the Simplex deployment, specify the static IP address of the Routing Core Server. For the local HA and geo-redundant HA deployments, specify the virtual IP address of the Routing Core Server. You define the Routing Core Server IP addresses in the `mega-config.yml` file.
19. In Enter switch TCP port number, enter the TCP port number.

    The port number range is 5001 through 5020.
20. In Number of splits/skills, enter the number of skills in your contact center.

    The value range is 1 through 15,000.
21. In Total split/skill members, summed over all splits/skills, enter the number of agents in your contact center.

    The value range is 1 through 1,000,000.
22. In Number of trunk groups, enter the number of trunk groups.

    The value range is 1 through 2000.
23. In Number of trunks, enter the number of trunks in your contact center.

    The value range is 1 through 200,000.
24. In Number of unmeasured facilities, enter the number of facilities in your contact center.

    The value range is 1 through 100,000.
25. In Number of call work codes, enter the number of call work codes in your contact center.

    The value range is 1 through 1,999.
26. In Number of vectors, enter the number of vectors in your contact center.

    The value range is 1 through 32,000.
27. In Number of VDNs, enter the number of VDNs in your contact center.

    The value range is 1 through 30,000.

    You can see `Setup completed successfully` in the command output.
28. Run the **`cmssvc`** command and select the **run_cms** option to turn CMS on.

Next steps

After you add contact center objects and test basic call functionality, generate a test supervisor report.

Related links

Generating a test supervisor report on page 88

Viewing the CMS link status

About this task

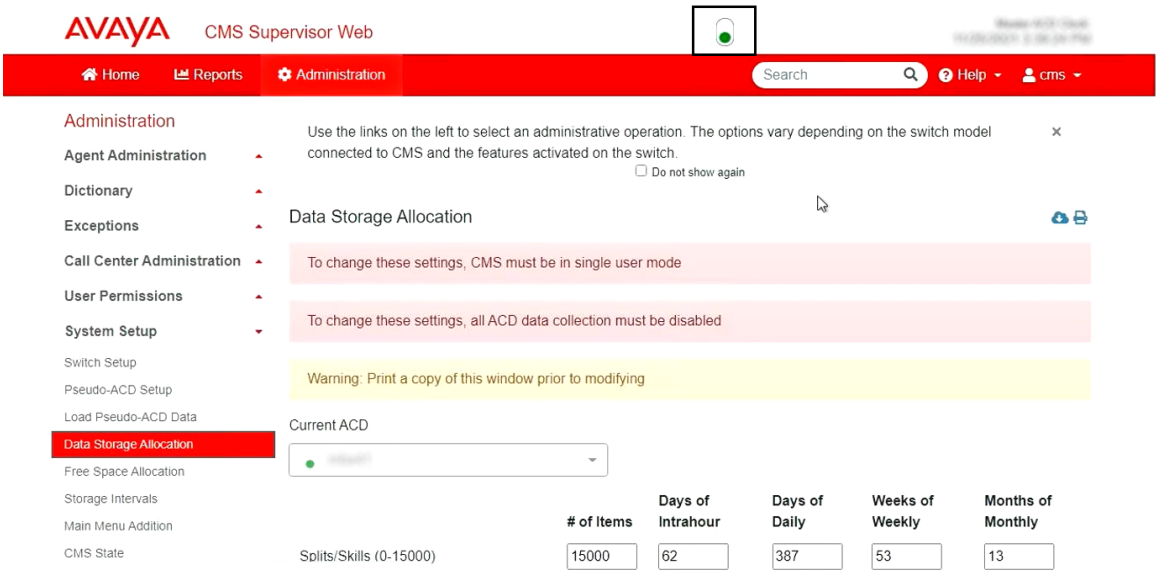
After configuring the connection to CMS on the Configuration Server web portal and add your contact center to CMS, check the CMS link status on the CMS Supervisor web portal.

Before you begin

- From the CMS CLI, run the **`cmsweb start`** command to start the web interface. For more information about using the **`cmsweb start`** command, see *Deploying Avaya Call Management System*.
- Obtain the CMS Supervisor web portal IP address and credentials from the implementation personnel or Avaya support.

Procedure

1. Log in to the CMS Supervisor web portal.
2. At the top of the page, check that the CMS link icon is green.



AE Services configuration

Internal AE Services configuration

The Deployment Manager installs internal AE Services on the Routing Core Server and automatically configures the switch connection. Add the installed AE Services server on the Configuration Server web portal and configure port and licensing settings. You can modify the port and licensing settings for all AE Services servers connected to the Routing Core Server.

You can also modify port and licensing parameters on the AE Services management console. For more information, see the network configuration and licensing sections in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*. You cannot modify the switch connection parameters on the AE Services management console.

External AE Services configuration

Avaya Contact Center – Extended Capacity uses external AE Services for migration purposes. External AE Services runs on a separate Linux server and supports the DLG service. You can migrate the external AE Services security database objects to the internal AE Services server. For more information about connecting the external AE Services server, see the AE Services migration section in *Migrating to Avaya Contact Center – Extended Capacity*.

AE Services configuration checklist

To configure AE Services in your contact center, perform the following tasks:

No.	Task	Reference	Notes	✔
1	On the Configuration Server web portal, configure the AE Services server properties.	For more information about configuring AE Services server properties, see Configuring AE Services server properties on page 58.		
2	On the Configuration Server web portal, add the AE Services server.	For more information about adding AE Services servers, see Adding an AE Services server on the Configuration Server web portal on page 59.		

Table continues…

No.	Task	Reference	Notes	✔
3	Log in to the AE Services management console.	For more information about logging in to the AE Services management console, see the AE Services overview section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.		
4	On the AE Services management console, import the trusted CA certificate.	For more information about importing certificates, see the certificate management section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.	Import the same trusted CA certificate that you imported into the contact center truststore.	

Related links

Importing a trusted certificate on page 40

Importing a trusted CA certificate to AE Services

About this task

To configure a switch connection, you must import the trusted CA certificates from Routing Core Server to AE Services. You can find the `CATrustedServers.cer` certificate file at the following location:

`/var/opt/Avaya/cert/CA/`

Procedure

1. Copy the `CATrustedServers.cer` file from `/var/opt/Avaya/cert/CA/` of the Routing Core Server host to a temporary folder. For example, `/tmp`.
2. Copy the certificate file from `/tmp` to your local computer.
3. On the AE Services management console, go to **Security > Certificate Management > CA Trusted Certificates**.
4. On the CA Trusted Certificates page, click **Import** to import the certificate.

   The AE Services management console displays a notification to restart AE Services after you import the certificate.
5. On the AE Services management console, go to **Maintenance > Service Controller**.
6. On the Service Controller page, click **Restart AE Server**.

Configuring AE Services server properties

About this task

After you deploy the internal AE Services server, AE Services generates a configuration page on the Configuration Server web portal. You can specify the port and licensing settings on the configuration page, and view the switch connection address.

Procedure

1. On the Configuration Server web portal, click **Components** > **AES** > **Configurations** > **default**.
2. **(Optional)** On the Edit Configuration page, in **Configuration Name**, type the name of the configuration template.
3. In **Switch Connection IP address**, check the IP address of the server.

   This field is automatically populated during the AE Services server deployment process.
4. In the Networking section, enable the ports that you want to use and specify the port numbers.
5. In the Licensing Servers - Admin WebLM section, in **WebLM address**, type the IP address or FQDN of the WebLM server to use for AE Services licensing.
6. In **WebLM port**, type the port number of the WebLM server.
7. **(Optional)** If you use two licensing servers, in **Secondary WebLM address**, type the IP address or FQDN of the secondary WebLM server.
8. **(Optional)** In **Secondary WebLM port**, type the port number of the secondary WebLM server.
9. To enable SSL connection for the primary WebLM server, select **SSL**.
10. **(Optional)** To enable SSL connection for the secondary WebLM server, select **Secondary SSL**.
11. To enable the hostname validation for the WebLM server, select **Hostname validation**.

    You can enable the hostname validation only if you use an FQDN as the WebLM server address.
12. In the Reserved Licenses section, in **Reserved TSAPI Basic User Licenses**, type the number of licenses that you want to reserve.
13. In **Reserved Unified Desktop Licenses**, type the number of licenses that you want to reserve.
14. In **Reserved DMCC Licenses**, type the number of licenses that you want to reserve.

Adding an AE Services server on the Configuration Server web portal

About this task

Connect each AE Services server to the Configuration Server to use the CVLAN, TSAPI, DMCC, and DLG services. With AE Services servers, you can interact with CTI applications to control endpoints and monitor calls.

When you add the internal AE Services server, you must create a new server password. For the external AE Services server, specify the switch connection password to configure on the AE Services management console. For more information about the switch connection configuration, see the AE Services migration section in *Migrating to Avaya Contact Center – Extended Capacity*.

Procedure

1. On the Configuration Server web portal, click **Administration** > **AES Servers**.
2. At the top-right corner of the AES Servers screen, click +.

   The Configuration Server displays the AE Services server configuration fields.
3. On the Add AES Server screen, in **Name**, type the AE Services server hostname.

   You can type a maximum of 15 characters. You can type alphanumeric characters and a hyphen (-).
4. In **Password**, type the AE Services server password.

   You can type a maximum of 16 alphanumeric characters.
5. To enable the AE Services server, select **Enabled**.
6. At the top-right corner of the screen, click **Commit**.

   The Configuration Server saves the AE Services server configuration and redirects you to the AES Servers screen.

CTI application connection checklist

To connect a CTI application to your contact center, perform the following tasks:

No.	Task	Reference	Notes	✔
1	On the Configuration Server web portal, configure the CTI link.	For more information about adding CTI links on the Configuration Server, see the CTI link section in *Administering Avaya Contact Center – Extended Capacity*.		

Table continues…

No.	Task	Reference	Notes	✔
2	On the AE Services management console, create a TSAPI or CVLAN link.	For more information about the CTI link configuration, see the CVLAN and TSAPI sections in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.	• For a DMCC application, configure a TSAPI link. You can administer CTI links on the AE Services management console. • Use the same link number that you configured for the CTI link on the Configuration Server.	
3	Add a new CTI user to the AE Services server.	For more information about the CTI user configuration, see the security database section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.		
4	Configure the CTI application settings.	For more information about connection requirements, see the documentation of the CTI application that you use.	Depending on your CTI application requirements, you might need to provide switch connection, CTI user, and CTI link details.	

Avaya Experience Portal connection checklist

You can configure the contact center to process Avaya Experience Portal calls through Avaya Aura® Session Manager.

No.	Task	Reference	Notes	✔
Avaya Contact Center – Extended Capacity configuration				
1	Configure number adaptations for incoming and outgoing calls.	For more information about number adaptation configuration, see the dial plan configuration section in *Administering Avaya Contact Center – Extended Capacity*.		

Table continues…

No.	Task	Reference	Notes	✔
2	Configure a SIP server.	For more information about SIP server configuration, see the network configuration section in *Administering Avaya Contact Center – Extended Capacity*.	• In **Address**, specify the Session Manager IP address. • In **Adaptation**, select the configured number adaptation.	
3	Configure a dial plan for external calls.	For more information about dial plan configuration, see the dial plan configuration section in *Administering Avaya Contact Center – Extended Capacity*.	• In **Call Type**, select **public**. • In **Destination SIP Server(s)**, select the configured SIP server.	
Session Manager configuration				
4	On the System Manager web console, configure an adaptation.	For more information about adaptation configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.		
5	On the System Manager web console, configure a SIP entity link to Avaya Contact Center – Extended Capacity.	For more information about SIP entity link configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.	• In **FQDN or IP address**, specify the IP address of the Routing Core Server. • In **Type**, select **SIP Trunk**. • In **Adaptation**, select the configured adaptation.	
6	On the System Manager web console, configure routing policy for calls to Avaya Contact Center – Extended Capacity.	For more information about routing policy configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.	On the Routing Policy Details page, in the SIP Entity as Destination section, specify the SIP entity link to Avaya Contact Center – Extended Capacity.	
7	On the System Manager web console, configure routing policy for calls to Avaya Aura® Communication Manager.	For more information about routing policy configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.		

Table continues…

No.	Task	Reference	Notes	✔
8	On the System Manager web console, configure dial patterns for incoming and outgoing calls.	For more information about dial pattern configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.	• To configure a dial pattern for calls from Avaya Contact Center – Extended Capacity, in the Originating Locations and Routing Policies section, specify the routing policy for calls to Communication Manager. • To configure a dial pattern for calls to Avaya Contact Center – Extended Capacity, in the Originating Locations and Routing Policies section, specify the routing policy for calls to Avaya Contact Center – Extended Capacity.	
Contact center configuration for connecting to Avaya Experience Portal				
9	On the System Manager web console, configure a SIP entity link to Avaya Experience Portal.	For more information about SIP entity link configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.		
10	On the System Manager web console, configure routing policy for calls to the Avaya Experience Portal.	For more information about routing policy configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.		
11	On the System Manager web console, configure a dial pattern for calls to the Avaya Experience Portal.	For more information about dial pattern configuration, see the Session Manager routing section in *Administering Avaya Aura® Session Manager*.		
12	On the Experience Portal, configure a VoIP connection for SIP signaling.	For more information about VoIP connection configuration, see the system configuration section in *Administering Avaya Experience Portal*.		

Table continues…

No.	Task	Reference	Notes	✔
13	On the Experience Portal, configure a DNIS application.	For more information about DNIS application configuration, see the speech applications in Avaya Experience Portal section in *Administering Avaya Experience Portal*.		

Endpoint configuration

Before verifying contact center functionality, you must register endpoints to Avaya Contact Center – Extended Capacity. For Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones registration, you must specify the endpoint and contact center details in the endpoint settings files and on the DHCP server. If you use Avaya Agent for Desktop, you must configure Avaya Agent for Desktop settings to process contact center calls.

The solution does not support H.323 endpoints. You must install the SIP firmware on Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones. If you use Avaya Agent for Desktop, you must configure the application to use SIP signaling.

Modifying the 46xxsettings.txt file

About this task

To register Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones to Avaya Contact Center – Extended Capacity, specify your contact center details in the `46xxsettings.txt` file.

For more information about the `46xxsettings.txt` file parameters, see *Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP* and *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Before you begin

Obtain the `46xxsettings.txt` file.

Procedure

1. Open the `46xxsettings.txt` file in a text editor.
2. For the SIP_CONTROLLER_LIST parameter, specify the IP address, port number, and port type of the SIP proxy server.

   In the Simplex deployment, the primary SIP proxy server address is the IP address of the Routing Core Server. In the local HA and geo-redundant HA deployments, the primary SIP proxy server address is the virtual IP address of the Routing Core Server. The default port number for TCP and UDP is 5060. The default port number for TLS is 5061.

For example, `SET SIP_CONTROLLER_LIST 10.1.2.6:5061;transport=tls`

3. For the SIPDOMAIN parameter, specify the SIP domain.

   You cannot register endpoints on the SIP proxy server without specifying the SIP domain.

   For example, `SET SIPDOMAIN sipdomain.example.com`

4. Set the ENABLE_PPM_SOURCED_SIPPROXYSRVR parameter to `0`.
5. Set the CONFIG_SERVER_SECURE_MODE parameter to `0`.
6. For the BRURI parameter, specify the URL address of the message storage server.

   The contact center uses the specified server to store the recorded agent greeting messages.

   For example, `SET BRURI http://10.1.2.20/greetings`

7. For the TRUSTCERTS parameter, specify the certificate file names for authentication.
8. **(Optional)** If you use TCP, set the ENABLE_OOD_MSG_TLS_ONLY parameter to `0`.
9. To use SIP for signaling, set the SIG parameter to `2`.

   Avaya Contact Center – Extended Capacity does not support H.323 endpoints.

10. Specify the required settings.
11. Save the `46xxsettings.txt` file.

Uploading settings files to the HTTP file server

About this task

To register Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones to Avaya Contact Center – Extended Capacity, upload the endpoint configuration and SIP firmware files to the HTTP file server.

For more information about the HTTP file server, see *Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP* and *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Before you begin

- Obtain SIP firmware files for Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones.
- For Avaya J100 Series IP Deskphones, obtain the `J100SUpgrade.txt` file.
- For Avaya 9600 Series IP Deskphones, obtain the `96x1Supgrade.txt` file.
- Specify contact center details in the `46xxsettings.txt` file.

Procedure

1. Access the HTTP file server.
2. Upload the SIP firmware files to your file server.

3. Upload one of the following endpoint upgrade files to your file server:
   - `J100SUpgrade.txt`: For Avaya J100 Series IP Deskphones.
   - `96x1Supgrade.txt`: For Avaya 9600 Series IP Deskphones.
4. Upload the `46xxsettings.txt` file to your file server.

Configuring the DHCP server

About this task

Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones obtain network and configuration information using the DHCP protocol. Administer endpoints to obtain endpoint settings and firmware files from the HTTP file server.

Before you begin

Set up a DHCP server. For more information about DHCP server, see *Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP* and *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Procedure

1. Access the DHCP server.
2. On the DHCP server, specify the IP address of the HTTP file server using the HTTPSRVR parameter.

   You must specify the IP address of the file server where you store `46xxsettings.txt`, `96x1Supgrade.txt`, `J100SUpgrade.txt`, and SIP firmware files.

   For example:

   ```
   option avaya-option-242 code 242 = string;
   option avaya-option-242 "HTTPSRVR=10.1.2.22";
   ```

Next steps

Start the endpoints. For more information about phone initialization, see *Installing and Administering Avaya J100 Series SIP IP Phones in Open SIP* and *Administering Avaya 9601/9608/9608G/9611G/9621G/9641G/9641GS IP Deskphones SIP*.

Configuring Avaya Agent for Desktop settings

About this task

If you use Avaya Agent for Desktop in your contact center, configure the application settings to register test endpoints to Avaya Contact Center – Extended Capacity. You must also configure Avaya Agent for Desktop to use SIP signaling.

For more information about configuring Avaya Agent for Desktop, see *Deploying and configuring Avaya Agent for Desktop*.

Before you begin

Ensure that you are using the latest version of the Avaya Agent for Desktop application.

Procedure

1. Start Avaya Agent for Desktop.
2. At the top-left corner of Avaya Agent for Desktop, click  .
3. From the menu, select **Settings**.

   Avaya Agent for Desktop displays the Avaya Agent Settings window.
4. In **AAFD Login type**, click **Use Local Configuration**.
5. In **License Server URL**, specify the URL address of the WebLM server.

   For example, `https://10.1.2.21:52233/WebLM/LicenseServer`
6. In the Local Server Settings section, in **Signaling**, select **SIP**.
7. In the Primary SIP Proxy Server section, specify the IP address, port number, and port type of the primary SIP proxy server.

   In the Simplex deployment, the primary SIP proxy server address is the IP address of the Routing Core Server. In the local HA and geo-redundant HA deployments, the primary SIP proxy server address is the virtual IP address of the Routing Core Server. The default port number for TCP and UDP is 5060. The default port number for TLS is 5061.

   For example, `10.1.2.6:5061 TLS`
8. In **SIP domain**, specify the SIP domain.

   You cannot register endpoints on the SIP proxy server without specifying the SIP domain.

   For example, `sipdomain.example.com`
9. On the navigation menu, click **Audio**.
10. On the Audio tab, in **Noise Suppression**, click **Very High**.
11. Select **Auto Gain Control**.
12. Select **Echo Cancellation**.
13. On the navigation menu, click **Security**.
14. On the Security tab, in **PPM Secure Mode**, select **HTTP**.
15. In **Certification Mode**, select **Use Local**.
16. In **Certificates**, add the required local certificates.

    If the SIP proxy uses the TLS protocol, you must also add the OpenSIPS Trusted CA certificate. You can find the certificate in the `/usr/local/etc/opensips/tls/rootCA/` directory.
17. Click **Save**.
18. Restart Avaya Agent for Desktop.

Avaya Workplace Client configuration

Installing Avaya Workplace Client on desktops

About this task

Use this procedure to install Avaya Workplace Client on desktop platforms.

Your administrator can also install Avaya Workplace Client on desktop platforms using a command line option. The administrator can deploy Avaya Workplace Client for Windows to work in a Citrix, XenApp, or VMWare environment. For more information, see *Planning for and Administering Avaya Workplace Client for Android, iOS, Mac, and Windows*.

Note:

In a Citrix environment, you must run the remote Avaya Workplace Client application using only one of the following methods:

- As a Citrix virtual application
- Through a Citrix virtual desktop

Before you begin

- Ensure that your Windows or Mac device meets the following minimum hardware requirements:
  - Dual-core processor
  - 2 GB of RAM
  - 1.5 GB free hard disk space
- Download the Avaya Workplace Client build for Windows or Mac to your computer from https://support.avaya.com/downloads/.
- For Avaya Workplace Client for Windows, ensure that:
  - You have Microsoft .NET Framework 4.8 or a later version. This is required with Windows 10 and with Windows Server 2016 and 2019.
  - Microsoft Visual C++ Redistributable for Visual Studio 2022 package is installed.
- For Avaya Workplace Client for Mac, ensure that you have Mac OS 10.11 or a later version.

Procedure

1. On the desktop for:
   - Windows: Double-click the `Avaya Workplace Setup 3.32.0.XXX.msi` file.
   - Mac: Double-click the `Avaya Workplace-XX.dmg` file.
2. Accept the terms of the license agreement, select the default values, and complete the installation.

   By default, the installer installs Outlook Plugin. Additionally, the Windows installer installs Web Extension on the Google Chrome and Microsoft Edge Chromium browsers. Outlook Plugin uses the language of the Microsoft Office suite and Web Extension uses the language of the web browser.

Note:

Avaya Workplace Client does not support the use of the Microsoft Edge Chromium browser add-in in the Internet Explorer compatibility mode.

3. **(Optional)** On Avaya Workplace Client for Windows, if you do not want to install Outlook Plugin and Web Extension by default:
   a. Select the **Custom** setup type.
   b. Disable the Outlook Plugin and Web Extension installation, and complete the installation.

Paired sign-on

Avaya Workplace Client for Windows supports paired sign-on with Avaya Workplace VDI in the Desk Phone mode. Avaya Workplace Client for Windows sends the user credentials to Avaya Workplace VDI that is running on a thin client using a virtual connection. Using these credentials and the Avaya Aura® configuration information, Avaya Workplace VDI logs in with the same extension. If Avaya Workplace VDI is already logged in and you log in to Avaya Workplace Client for Windows using a different extension, Avaya Workplace VDI is logged out and the paired sign-on process begins.

If the log in process is successful, you can use Avaya Workplace Client for Windows to control the Avaya Workplace VDI client.

Logging out from Avaya Workplace Client for Windows also logs you out from Avaya Workplace VDI.

Logging out from Avaya Workplace VDI does not log you out from Avaya Workplace Client for Windows. However, the telephony services become unavailable.

In case of a connection failure at Avaya Workplace Client for Windows, you can continue to use Avaya Workplace VDI for calls.

Avaya Paired Sign-On using the Chrome extension

Avaya Workplace Client for Windows supports paired sign-on using the Avaya Paired Sign-On extension. If you install the Avaya Paired Sign-On extension from the Chrome Web Store, you can log in to Avaya Workplace Client for Windows using the Avaya Paired Sign-On extension.

Note:

If there is a paired sign-on between the controlling and controlled client and your administrator changes the parameter value which includes the configuration URL path, you must restart the controlling client so that the controlled client receives the new URL.

Installing Avaya Workplace Client for Windows as a controlling or controlled client

About this task

Use this procedure when users need to log in to and use Avaya Workplace Client for Windows in a virtual environment. You can install Avaya Workplace Client as a controlling or controlled client.

- Controlling client means that Avaya Workplace Client is running in the Desk Phone mode on a remote virtual desktop.
- Controlled client means that Avaya Workplace Client is running in the My Computer mode on a local personal computer.

Before you begin

Install the Avaya Paired Sign-On extension from the Chrome Web Store. Also, install the native component of the Avaya Paired Sign-On extension from the Avaya Workplace Client for Windows build, which you downloaded from https://support.avaya.com/downloads/. You can then Pin the Chrome extension to your browser toolbar.

Note:

If Avaya Workplace Client on a remote computer runs as a controlling client and Avaya Workplace Client on a local computer runs as a controlled client, you do not need to install the native component with the Avaya Paired Sign-On extension in your deployment.

Procedure

1. Open Command Prompt.
2. Go to the location of the `.msi` file for Avaya Workplace Client for Windows.
3. Use the **`VDIENV`** or **`VDICONTROLLEDEP`** option in the command line to install Avaya Workplace Client.
   - As a controlling client, use the following command:

     ```
     msiexec /i "Avaya Workplace Setup.msi" VDIENV=1
     ```

   - As a controlled client, use the following command:

     ```
     msiexec /i "Avaya Workplace Setup.msi" VDICONTROLLEDEP=1
     ```

4. Start Avaya Workplace Client.

   If you install Avaya Workplace Client as a controlling client, you can view the Welcome screen with the **Join a meeting** and **Configure my account** options if the client configuration is not done.

   If you install Avaya Workplace Client as a controlled client and the client configuration is done, you can view the following message: `Waiting for paired sign-in request from controlling application....`

   If you install Avaya Workplace Client as a controlled client and if the client configuration is not done, a configuration request from the controlling client precedes the paired sign-on request.

Next steps

Open the Chrome extension from your browser toolbar and log in to Avaya Workplace Client.

Settings file template for Avaya Workplace Client as a media client in Contact Center deployments

Use this settings file template as a starting point for your deployment. Replace the email addresses and URLs in the template with the values that are specific to your organization.

```
## SIP Parameters

SET SIPENABLED 1
SET SIP_CONTROLLER_LIST "sm.abc.com:5061;transport=tls"
SET SIPDOMAIN abc.com
SET SIMULTANEOUS_REGISTRATIONS 2
SET ENFORCE_SIPS_URI 1

## PPM Parameters

SET ENABLE_PPM 1
SET ENABLE_PPM_CALL_JOURNALING 0
SET ENABLE_PPM_CONTACTS 0

## AECC Properties

SET NO_SUBSCRIBE_ON_SIP_CONNECTION_RECOVERY 15
SET ENABLE_PPM_PERSISTENT_DATA 1
SET AGTGREETINGSTAT 2
SET ENABLE_PLT_OOB_HEADSET_CALL_CONTROL 0
SET ENABLE_JABRA_OOB_HEADSET_CALL_CONTROL 0
SET AUDIO_DEVICE_CALL_CONTROL_ENABLED 0

## AUTO UPDATE SETTINGS

SET SETTINGS_CHECK_POLICY 1
SET SETTINGS_FILE_URL "https://store.abc.com/settings/Workplace_Config_Mega_CC.txt"
SET SETTINGS_CHECK_INTERVAL 1

## CLIENT UPDATE SETTINGS  (APPCAST)

SET APPCAST_ENABLED 1
SET APPCAST_CHECK_INTERVAL 1
SET APPCAST_URL "https://aads.abc.com:8442/acs/resources/webdeployment"
## UI Notifications:

SET SHOW_TEAM_BUTTON_VISUAL_ALERT 0
SET SHOW_EQUINOX_MEETING_PANEL_IN_TOM 0
SET DESKTOP_HTTP_APPLICATION_INTEGRATION 0
SET ENABLE_CALL_NOTIFICATIONS 0
SET ENABLE_AUDIBLE_CALL_NOTIFICATIONS 0

## SSO Settings

SET SSOENABLED 0
SET AUTOCONFIG_USESSO 0

## Disabling unnecessary Workplace services

SET UNIFIEDPORTALENABLED 0
SET HTTPUAENABLED 0
SET ESMENABLED 0
```

```
SET ACSENABLED 0
SET ENHDIALSTAT 0
SET ENABLE_VIDEO 0
SET ENABLE_AVAYA_CLOUD_ACCOUNTS 0
SET ENABLE_EQUINOX_MEETING_ACCOUNT_DISCOVERY 0
SET ENABLE_EWS_ACCOUNT_DISCOVERY 0
SET ENABLE_GOTO_MEETING_PORTAL 0
SET ENABLE_SPACES_MESSAGING 0

## Present Large Dial pad view for Media client

SET HOMESCREENLAYOUT 2

## Outlook Properties

SET ENABLE_OUTLOOK_ADDON 0
SET OUTLOOK_CALL_CONTACT 0
SET ENABLE_LOCAL_CONTACT 0
SET ENABLE_TOP_OF_MIND 1
SET CALENDAR_INTEGRATION_ENABLED 0
SET EWSENABLED 0

## LDAP Dir settings

SET DIRENABLED 0
SET DIRSRVR ""
SET DIRSRVRPRT 636
SET DIRUSERNAME abc
SET DIRPASSWORD ##
SET DIRTOPDN " "
SET DIRSECURE 1
SET DIRIMATTRIBUTE
SET DIRTYPE (0,1,2)
SET DIRSCOPE ' '
SET DIRMAXENTRIES

## Media parameters

SET ENCRYPT_SRTCP 0
SET ENABLE_MEDIA_HTTP_TUNNEL 0

SET SUPPORTEMAIL 'support@abc.com'
SET OTHER_PHONE_MODE_ENABLED 0
SET ENABLE_DESKPHONE_SHARE_CONTROL 0
SET ENABLE_BLIND_TRANSFER 0
SET ONLINE_HELP_ENABLED 0
SET ENABLE_TUTORIAL 0
SET CONTROLLEDEP_CONFIGURL ""
SET TRUSTCERTS "SMabc.crt","IntermediateCA.crt","OpenSSLRootCA.crt"



## Agent parameters (CC Elite Features)

SET AGENT_ENABLED 0
SET ENABLE_BUTTON_MODULE 1
SET AGENT_WORK_CODE ""
SET AUX_REASON_CODES ""
SET LOGOUT_REASON_CODES ""
SET Q_STATS_DEFAULTREFRESHTIMER 20
SET UUIDISPLAYTIME 10
SET LICENSE_SERVER_URL
SET ENABLE_CCELITE_OFF_HOOK_INVITE_SUPPORT 1

SET OBSCURE_PREFERENCES "SHOW_EQUINOX_MEETING_PANEL_IN_TOM,
```

```
DESKTOP_HTTP_APPLICATION_INTEGRATION, UNIFIEDPORTALENABLED, ESMENABLED, ACSENABLED,
ENABLE_OUTLOOK_ADDON, ENABLE_LOCAL_CONTACT, ENABLE_TOP_OF_MIND,
CALENDAR_INTEGRATION_ENABLED, DIRENABLED, ENHDIALSTAT, EWSENABLED, ENABLE_VIDEO,
ENABLE_AVAYA_CLOUD_ACCOUNTS, ENABLE_GOTO_MEETING_PORTAL, ENABLE_SPACES_MESSAGING,
OTHER_PHONE_MODE_ENABLED, ENABLE_DESKPHONE_SHARE_CONTROL,  ENABLE_TUTORIAL,
AGENT_ENABLED, SET OBSCURE_PREFERENCES
"SIP_CONTROLLER_LIST,SIPPROXYSRVR,SIPPORT,SIPSECURE,SIPENABLED,SIPDOMAIN,SIPUSERNAME,SIP
HA1,SIPPASSWORD,ESMSRVR,CONFERENCE_VIRTUAL_ROOM,DIR_CONTACT_RESOLUTION_ENABLED,CONFERENC
E_ACCESS_NUMBER,SSOENABLED,ISO_SYSTEM_LANGUAGE,UNIFIEDPORTALENABLED,WINDOWS_IMPROVIDER,C
ONTACT_MATCHING_SEARCH_LOCATION,ENABLE_OPUS,SUPPORTURL,DIRENABLED,DIRSRVR,DIRSRVRPRT,DIR
TOPDN,DIRSECURE,CONFERENCE_MODERATOR_CODE,CONFERENCE_PARTICIPANT_CODE,CONFERENCE_PARTICI
PANT_URL,RTP_PORT_RANGE,CONFERENCE_FACTORY_URI,ACSSSO,SETTINGS_CHECK_INTERVAL,RTP_PORT_L
OW,ACSSECURE,DSCPVID,DSCPAUD_FLASHOVERRIDE,SIPREGPROXYPOLICY,PHNLDLENGTH,DSCPAUD_PRIORIT
Y,ENABLE_MEDIA_HTTP_TUNNEL,SIPSSO,SP_AC,PHNOL,IOS10CALLKIT_ENABLED,PHNLD,PHNIC,PHNPBXMAI
NPREFIX,PHNREMOVEAREACODE,AUTOAPPLY_ARS_TO_SHORTNUMBERS,APPLY_DIALINGRULES_TO_PLUS_NUMBE
RS,PHNCC,DSCPAUD_FLASH,EWSSSO,EWSDOMAIN,ENABLE_DESKPHONE_SHARE_CONTROL,ESMSSO,VIDEO_MAX_
BANDWIDTH_CELLULAR_DATA,OPUS_PAYLOAD_TYPE,SUPPORTWINDOWSAUTHENTICATION,ALLOW_CREATE_LOCA
L_CONTACTS,ESMREFRESH,MEDIAENCRYPTION,EWSENABLED,DSCPAUD,SUPPORTEMAIL,ACSSRVR,DIALPLANEX
TENSIONLENGTHLIST,ENCRYPT_SRTCP,ESMSECURE,VIDEO_MAX_BANDWIDTH_ANY_NETWORK,AUTO_AWAY_TIME
,LOG_VERBOSITY,UNIFIED_PORTAL_SSO,DSCPAUD_IMMEDIATE,ANALYTICSENABLED,DSCPVID_FLASHOVERRI
DE,BFCP_TRANSPORT,DSCPVID_IMMEDIATE,ENABLE_LOCAL_CONTACT,DSCPSIG,DSCPVID_FLASH,ESMPORT,A
CSPORT,CONFERENCE_PORTAL_URI,ESMENABLED,AUTOCONFIG_USESSO,ENABLE_AVAYA_CLOUD_ACCOUNTS,ES
MHIDEONDISCONNECT,ENHDIALSTAT,EWSSERVERADDRESS,ACSENABLED,CONFERENCE_FQDN_SIP_DIAL_LIST,
APPLICATION_CLOSE_WINDOW,ADDRESS_VALIDATION,WINDOWS_IMPROVIDER_RESOLVE_CONTACT_EXTERNAL,
ENABLE_BROWSER_EXTENSION,PSTN_VM_NUM,OUTLOOK_CALL_CONTACT,ENABLE_OUTLOOK_ADDON,WINDOWS_I
MPROVIDER,ENABLE_BROWSER_EXTENSION,ADDRESS_VALIDATION,TRUST_STORE,VIDEO_MAX_BANDWIDTH_AN
Y_NETWORK,DND_SAC_LINK,PSTN_VM_NUM,ENABLE_OUTLOOK_ADDON,OUTLOOK_CALL_CONTACT,ENABLE_LOCA
L_CONTACT,HIDDEN_MODE_ENABLED"

SET LOCKED_PREFERENCES "SIP_CONTROLLER_LIST, SIPDOMAIN, SIPUSERNAME,  AGTGREETINGSTAT"
```

Chapter 6: Post-installation verification

Contact center verification overview

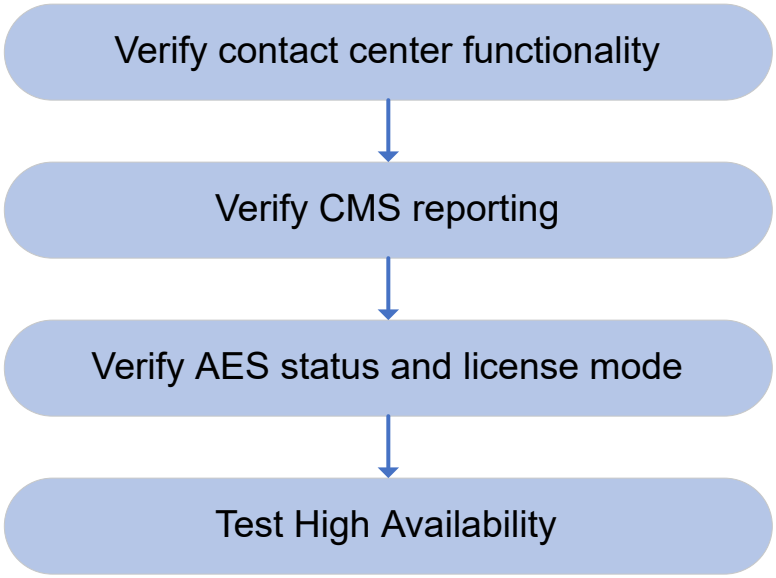
After installing the contact center, you need to test basic calling functionality, verify call reporting and connection to AE Services, and check if your contact center processes calls normally in case of a failover.

To test basic call functionality, log in to the Configuration Server as a system administrator and add test objects, such as skills, agents, endpoints, vectors, and vector directory numbers (VDNs). You can test how the contact center handles incoming and outgoing calls. For example, you can check if numbers are dialed according to the configured dial plan, check call transfers and the dial plan configuration for emergency calls, or verify speech path quality.

You need to test the functionality of your contact center in case the contact center fails over. For example, you can check call transfer and the quality of the speech path after the failover.

Contact center verification workflow

The following diagram shows a high-level sequence of procedures required to verify the contact center basic functionality after the installation:



Configuring a dial plan for testing calls

About this task

Set up a dial plan to test the basic call functionality of your contact center. When configuring a dial plan for testing calls, you can use a pre-determined call type.

Before you begin

- Log in to the Configuration Server web portal as a system administrator.
- Add a SIP server for call routing. For more information about adding destination SIP servers, see the network configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. On the Configuration Server web portal, go to **Administration** > **System** > **Dial Plan Analysis**.
2. At the top-right corner of the Dial Plan Analysis screen, click ＋.

   The Configuration Server displays the dial plan configuration fields.
3. On the top half of the screen, in **Dialed String Prefix**, type the digits that the contact center uses to identify dialed numbers or agent login IDs.
4. In **Min Length**, type a minimum length of the dialed number or agent login ID.

   For custom call types, you can type a value from 1 to the value entered in **Max Length**.

For more information about the minimum length value range for predetermined call types, see the dial plan configuration section in *Administering Avaya Contact Center – Extended Capacity*.

5. In **Max Length**, type a maximum length of the dialed number or agent login ID.

   For custom call types, you can type a value in the range from the value entered in **Min Length** to 24. For the external-prefix call type, the maximum length must match the **Min Length** value.

   For more information about the maximum length value range for predetermined call types, see the dial plan configuration section in *Administering Avaya Contact Center – Extended Capacity*.

6. In **Call Type**, select a call type to associate with the dial plan.

   You can select one of the predetermined call types or configure your call type on the Dial Plan Call Types screen.

7. Do one of the following:

   - To apply the dial plan configuration to all agent profiles, select **All Agent Profiles**.
   - To apply the dial plan configuration to certain agent profiles, in **Agent Profile(s)**, select one or several agent profiles.

   You can configure agent profiles on the Agent Profiles page.

8. **(Optional)** In **Comments**, type a short description for the dial plan.

   You can type a maximum of 50 Unicode characters.

9. In **Routing Mode**, select one of the following:

   - **Round Robin**: This is the default option. Select this option to distribute contact center calls equally between SIP servers in circular order.
   - **Priority Based**: Select this option to route contact center calls to SIP servers based on the server priority. If the first SIP server in the Destination SIP Server(s) section fails, the contact center starts routing calls to the next SIP server in the list.

10. In the Destination SIP Server(s) section, in **SIP Server**, select a SIP server that the contact center uses for call routing.

    You can configure SIP servers on the SIP Servers screen.

11. **(Optional)** To add a SIP server, click **Add**.

    When routing a call, the Routing Core Server connects to the first configured SIP server. If the server is unavailable, the contact center uses the next server that you added.

12. At the top-right corner of the screen, click **Commit**.

    Configuration Server saves the dial plan configuration and redirects you to the Dial Plan Analysis screen.

For the Public, Private, and Emergency call types, if you do not set any SIP servers, Configuration Server displays a warning. Click **OK** to continue without configuring a SIP server.

Related links

Logging in to the Configuration Server as a system administrator on page 48

Adding a test announcement

About this task

After configuring a dial plan, add an announcement to test whether the caller can hear music when the call is on hold or routed to a VDN. You can add two test announcements to distinguish between audio for held calls and VDN queues.

Before you begin

- Obtain an audio file for the test announcement. The file must be in the `.wav` format and encoded with G.729 or G.729B.
- Add a permission set on the Permission Sets (COR) screen of the System tab. For more information about adding permission sets, see the global configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. On the Configuration Server web portal, go to **Administration** > **Contact Center** > **Announcements**.
2. At the top-right corner of the Announcements screen, click +.

   The Configuration Server displays the announcement configuration fields.
3. On the top half of the screen, in **Extension**, type an extension number for the announcement.

   You can type a maximum of 16 digits.

   The contact center uses the extension number as a unique ID for announcements. When agents dial this number, they can hear an intercept tone.
4. In **Name**, type the announcement name.

   You can type a maximum of 35 Unicode characters.
5. In **Description**, type a short description for the announcement.

   You can type a maximum of 50 Unicode characters.
6. **(Optional)** To enable protected mode for the announcement, select **Protected**.

   You cannot delete or edit a protected announcement from the agent phone or file server.
7. Click **Permission Sets (COR)** and select the permission set for the announcement from the CORs pane on the right.

You can configure permission sets on the System tab.

8. In **Upload Audio File**, click **Choose File** and select the audio file.
9. At the top-right corner of the screen, click **Commit**.

   The Configuration Server saves the announcement configuration and redirects you to the Announcements screen.

Next steps

- To configure Music on Hold, assign the created announcement to an agent profile or a skill.
- To configure queue music, add **announcement** as the first vector step or assign the created announcement to a VDN.

Adding test contact center objects

About this task

After adding a test announcement, add contact center objects for testing call functionality. You must add at least one skill, three agents, three endpoints, a vector, and a VDN.

Before you begin

Add a voicemail server and a coverage path for redirecting calls. For more information about adding voicemail servers and coverage paths, see the contact center and network configuration sections in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. On the Configuration Server web portal, go to **Administration** > **Contact Center** > **Skills**.
2. At the top-right corner of the Skills screen, click +.

   The Configuration Server displays the skill configuration fields.
3. On the General, Advanced, and RONA parameters subtabs, configure the required settings.

   For more information about adding skills, see the skill configuration section in *Administering Avaya Contact Center – Extended Capacity*.
4. At the top-right corner of the Add Skill screen, click **Commit**.

   The Configuration Server saves the skill configuration and redirects you to the Skills screen.
5. On the navigation menu, go to **Contact Center** > **Agents**.
6. At the top-right corner of the Agents screen, click +.

   The Configuration Server displays the agent configuration fields.
7. Configure the required settings at the top of the Add Agent screen and on the General Options and Agent Skills subtabs.

For more information about adding agents, see the agent configuration section in *Administering Avaya Contact Center – Extended Capacity*.

8. At the top-right corner of the screen, click **Commit**.

   The Configuration Server saves the agent configuration and redirects you to the Agents screen.

9. Repeat steps 6 to 8 to add two more agents.

   One of the agents is a supervisor, as you need to test call transfer to a supervisor.

10. On the navigation menu, go to **Endpoints** > **Manage Endpoints**.
11. At the top-right corner of the Endpoints screen, click +.

    The Configuration Server displays the endpoint configuration fields.

12. Configure the required settings at the top of the Add Endpoint screen and on the General Options, Button Assignment and Profile Settings subtabs.

    For more information about adding endpoints, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

13. At the top-right corner of the screen, click **Commit**.

    The Configuration Server saves the endpoint configuration and redirects you to the Endpoints screen.

14. Repeat steps 11 to 13 to add two more endpoints.
15. On the navigation menu, go to **Contact Center** > **Vectors**.
16. At the top-right corner of the Vectors screen, click +.

    The Configuration Server displays the vector configuration fields.

17. On the Add Vector screen, configure the required settings and add vector steps.

    For more information about adding vectors and an example of vector configuration, see the vector configuration section in *Administering Avaya Contact Center – Extended Capacity*.

18. At the top-right corner of the screen, click **Commit**.

    The Configuration Server saves the vector configuration and redirects you to the Vectors screen.

19. On the navigation menu, go to **Contact Center** > **Vector Directory Numbers (VDNs)**.
20. At the top-right corner of the Vector Directory Numbers screen, click +.

    The Configuration Server displays the VDN configuration fields.

21. Configure the required settings at the top of the Add Vector Directory Number (VDN) screen and on the Basic Information and Variables Information subtabs.

    For more information about adding VDNs, see the VDN configuration section in *Administering Avaya Contact Center – Extended Capacity*.

22. At the top-right corner of the screen, click **Commit**.

    The Configuration Server saves the VDN configuration and redirects you to the Vector Directory Numbers screen.

Endpoint configuration verification

After configuring test endpoints, you must verify endpoint registration to Avaya Contact Center – Extended Capacity. You must also check that test endpoints display all the assigned buttons and test calls between endpoints.

Logging in to Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones

About this task

Before verifying the endpoint registration to Avaya Contact Center – Extended Capacity, ensure that you can log in to Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones using the endpoint extension and password associated with the test endpoint configuration.

Before you begin

Obtain the endpoint extension and password associated with the test endpoint configuration.

Procedure

1. Start your endpoint.
2. After the boot-up, on the phone screen, press **Login**.
3. On the Login screen, enter the endpoint extension.
4. Press **Enter**.
5. In **Password**, enter the password.
6. Press **Enter**.

Related links

Adding test contact center objects on page 77

Logging in to Avaya Agent for Desktop

About this task

Verify that you can log in to Avaya Agent for Desktop using the endpoint extension and password associated with the test endpoint configuration.

Before you begin

Obtain the endpoint extension and password associated with the test endpoint configuration.

Procedure

1. Start Avaya Agent for Desktop.

   Avaya Agent for Desktop displays the Avaya Agent Login window.
2. In the Station section, in **Station ID**, enter the endpoint extension.
3. In **Password**, enter the endpoint password.
4. **(Optional)** To log in automatically, in the Station section, select **Automatic Sign In**.

   When you start Avaya Agent for Desktop the next time, the application automatically logs you in with the specified endpoint credentials.
5. In the Station section, click **Sign In**.

Related links

Adding test contact center objects on page 77

Verifying endpoint registration

About this task

Use the Maintenance Shell to verify if the endpoints are registered to Avaya Contact Center – Extended Capacity. You can check the registration of multiple endpoints simultaneously.

Before you begin

- Log in to test endpoints to verify registration.
- Log in to the Configuration Server web portal as a system administrator.

Procedure

1. On the Configuration Server web portal, click **Contact Center Administration**.
2. Click **Maintenance Shell**.

   The Configuration Server displays the Maintenance Shell console.
3. Log in to the Maintenance Shell with the system administrator credentials.
4. On the Maintenance Shell console, run the following command:

   ```
   mtc list station
   ```

   The command displays a list of logged-in endpoints.
5. Verify that the command output displays the endpoints in to which you are logged.

Related links

Logging in to Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones on page 79
Logging in to Avaya Agent for Desktop on page 79

Verifying button assignment

About this task

Verify that test endpoints show all the assigned buttons. You can view a list of assigned buttons on the Configuration Server web portal.

For more information about endpoint buttons and their description, see *Using Avaya J100 Series SIP IP Phones for Call Center Agents*, *Using Avaya 9621G/9641G/9641GS IP Deskphones SIP for Call Center Agents*, and *Using Avaya Agent for Desktop*.

Before you begin

Log in to the Configuration Server web portal as a system administrator.

Procedure

1. On the Configuration Server web portal, click **Contact Center Administration**.
2. On the Configuration Server web portal, go to **Administration** > **Endpoints** > **Manage Endpoints**.
3. On the Endpoints screen, select the required endpoint.
4. At the top-right corner of the screen, click 👁.

   The Configuration Server displays the endpoint configuration fields.
5. Click the **Button Assignment** subtab.

   The Configuration Server displays a list of buttons assigned to the endpoint.
6. On the endpoints, ensure that the endpoints have the assigned buttons.

Testing calls between endpoints

About this task

After configuring test contact center objects, verify that your contact center processes calls between endpoints correctly. You also need to check the quality of the speech path between endpoints.

Procedure

1. Log in to endpoint 1 with the endpoint credentials.
2. Log in to endpoint 2 with the endpoint credentials.
3. On endpoint 1, call the extension of endpoint 2.
4. On endpoint 2, answer the incoming call.
5. On both endpoints, check the quality of the speech path.
6. Complete the call.

Logging in as an agent

About this task

Verify that you can log in to endpoints with the agent login ID and password associated with a test agent configuration. This procedure describes how to log in as an agent to Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones.

For more information about agent login in a CTI application, see your CTI application documentation.

Before you begin

Obtain the agent login ID and password associated with the test agent configuration.

Procedure

1. To access the Login screen, do one of the following:
   - On Avaya J100 Series IP Deskphones, go to **Main Menu** > **Features** > **Agent Login**.
   - On Avaya 9600 Series IP Deskphones, go to **Features** > **Agent Login**.
2. In **Agent ID**, enter the agent login ID.
3. In **Password**, enter the agent password.
4. Press **Enter**.

Related links

Adding test contact center objects on page 77

Call functionality verification

After configuring test contact center objects, ensure that the contact center processes calls correctly. Verify that you can make a conference call and complete a call transfer. Check that the contact center redirects a direct agent call to voicemail when the agent cannot answer the call. You must also ensure that your contact center routes emergency calls correctly.

Testing an internal call to a VDN

About this task

Verify that your contact center processes internal calls correctly. Make a test call to the configured VDN from an endpoint to ensure that you can hear announcements when the call is in the queue. You must check if an agent logged in to another endpoint in Auto-In mode can receive calls and hear a VOA message when they accept the call. You also need to check the quality of the speech path between the call participants.

Procedure

1. Log in to endpoint 1 with endpoint credentials.

2. Log in to endpoint 2 with agent credentials.
3. On endpoint 1, call a VDN.
4. Check if you can hear announcements.
5. On endpoint 2, change the agent work mode to Auto-In.
6. Answer the incoming call.
7. Check if you can hear the VOA message.

   The contact center plays a short message about the requested service before connecting the caller to the agent.
8. On both endpoints, check the quality of the speech path.
9. Complete the call.

Related links

Logging in to Avaya J100 Series IP Deskphones and Avaya 9600 Series IP Deskphones on page 79
Logging in to Avaya Agent for Desktop on page 79
Logging in as an agent on page 82

Testing an internal call to a supervisor

About this task

Make a test call to a supervisor to ensure that an agent can make calls to internal numbers and check the quality of the speech path. Verify that the supervisor endpoint displays the caller ID correctly.

For more information about configuring endpoint feature buttons, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. Log in to the agent endpoint with endpoint credentials.
2. Log in to the supervisor endpoint with endpoint credentials.
3. On the agent endpoint, call the supervisor extension.
4. On the supervisor endpoint, check the caller ID.

   The endpoint displays the agent endpoint extension.
5. On the supervisor endpoint, answer the incoming call.
6. On both endpoints, check the quality of the speech path.
7. On the agent endpoint, complete the call.
8. On the supervisor endpoint, verify that the call is complete.
9. Log in to the agent endpoint with agent credentials.
10. Change the agent work mode to Auto-In.

11. On the agent endpoint, call the supervisor extension.
12. On the supervisor endpoint, check the caller ID.

    The endpoint displays the agent login ID.
13. Complete the call.

Testing an external call to a VDN

About this task

After testing internal calls, verify that your contact center processes external calls correctly. Make a test call to a configured VDN from a caller's phone to ensure that callers can hear announcements in queue. Check if an agent in Auto-In mode can receive calls and hear VDN of Origin Announcement (VOA) message when they accept the call. Check the quality of the speech path between the caller and the agent.

Procedure

1. Log in to the agent endpoint with agent credentials.
2. On the caller's phone, call a VDN.
3. Check if you can hear announcements.
4. On the agent endpoint, change the agent work mode to Auto-In.
5. Answer the incoming call.
6. Check if you can hear the VOA message.

   The contact center plays a short message about the requested service before connecting the caller to an agent.
7. On the caller's phone and agent endpoint, check the quality of the speech path.
8. Complete the call.

Related links

Adding a test announcement on page 76
Adding test contact center objects on page 77

Testing a conference call

About this task

Verify that you can make a conference call. You can have up to six participants on a conference call. Enter an agent login ID, endpoint, or VDN extension to add a participant to a conference call.

For more information about configuring endpoint feature buttons, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. Log in to endpoint 1 with agent credentials.
2. Log in to endpoint 2 with agent credentials.

3. On the caller's phone, call a VDN.
4. On endpoint 1, change the agent work mode to Auto-In.
5. Answer the incoming call.
6. Check the quality of the speech path.
7. On endpoint 1, press **Conference**.
8. Enter the agent login ID.

   You must use the agent login ID you used to log in to endpoint 2.
9. Verify that all participants are on the call.
10. Check the quality of the speech path.
11. Complete the call.

Testing an attended transfer

About this task

Verify that an agent can complete a call transfer and check the quality of the speech path during the transfer call.

Procedure

1. Log in to endpoint 1 with agent credentials.
2. Log in to endpoint 2 with endpoint credentials.
3. On endpoint 1, change the agent work mode to Auto-In.
4. On the caller's phone, call a VDN.
5. On endpoint 1, answer the incoming call.
6. Initiate an attended transfer to the extension of endpoint 2.
7. On the caller's phone, check if you can hear music on hold.
8. On endpoint 2, answer the call from endpoint 1.
9. On both endpoints, check the quality of the speech path.
10. On endpoint 1, complete the transfer to endpoint 2.
11. Check the quality of the speech path.
12. Complete the call.

Related links

Adding a test announcement on page 76
Adding test contact center objects on page 77

Testing a transfer by call join

About this task

Verify that an agent can complete a transfer by call join. To transfer a call to the transfer target, an agent sets up a three-party conference call and disconnects from the call.

For more information about configuring endpoint feature buttons, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. Log in to endpoint 1 with agent credentials.
2. Log in to endpoint 2 with agent credentials.
3. On the caller's phone, call a VDN.
4. On endpoint 1, change the agent work mode to Auto-In.
5. Answer the incoming call.
6. Check the quality of the speech path.
7. On endpoint 1, press **Conference**.
8. Enter the agent login ID.

   You must use the agent login ID you used to log in to endpoint 2.
9. Verify that all participants are on the call.
10. Check the quality of the speech path.
11. On endpoint 1, complete the call.
12. On the caller's phone and endpoint 2, check the quality of the speech path.
13. Complete the call.

Testing outgoing calls

About this task

Verify that an agent can make calls to external numbers and check the quality of the speech path between the agent and the client. Verify that the client phone displays the caller ID correctly.

For more information about configuring endpoint feature buttons, see the endpoint configuration section in *Administering Avaya Contact Center – Extended Capacity*.

Procedure

1. Log in to the agent endpoint with endpoint credentials.
2. On the agent endpoint, call an external number.

   The number that you dial must comply with the configured dial plan.
3. On the client's phone, check the caller ID.
4. Answer the incoming call.

5. On the client's phone and agent endpoint, check the quality of the speech path.
6. On the client's phone, complete the call.
7. On the agent endpoint, verify that the call is complete.
8. Log in to the agent endpoint with agent credentials.
9. Change the agent work mode to Auto-In.
10. Call the same external number that you used in step 2.
11. On the client's phone, check the caller ID.

    The client phone displays a different caller ID.
12. Complete the call.

Testing call redirection to voicemail

About this task

Verify that the contact center redirects a direct agent call to voicemail when an agent cannot answer the call. Verify that an agent can access the voicemail server and listen to voice messages.

For more information about accessing voicemail, see *Using Avaya J100 Series SIP IP Phones for Call Center Agents*, *Using Avaya 9621G/9641G/9641GS IP Deskphones SIP for Call Center Agents*, and *Using Avaya Agent for Desktop*.

Before you begin

- Add a voicemail server, a coverage path, and assign the coverage path to the agent. For more information about configuring contact center objects, see *Administering Avaya Contact Center – Extended Capacity*.
- Configure a permission set for Direct Agent Calling and assign the permission set to the endpoint and agent.
- For testing purposes, on the Configuration Server web portal, on the Agent Profiles screen, set **Message Wait Lamp Indicates Status For** to **AGENT**.

Procedure

1. Log in to the agent endpoint with the endpoint credentials.
2. On the agent endpoint, call the agent login ID.

   You must make a call to the agent login ID of the logged-out agent.
3. Verify that you can hear the call redirection announcement and leave a voice message after the tone.
4. Complete the call.
5. Log in to the agent endpoint with the agent credentials.

   When you log in as an agent, the Message Waiting Indicator LED on the endpoint lights.
6. On the agent endpoint, access the voicemail server.

For example, on Avaya J100 Series IP Deskphones, you can press **Voicemail** to access the voicemail server.

7. Verify that you can access and hear the recorded message.

   After listening to the voice message, the Message Waiting Indicator LED on the agent endpoint turns off.

Testing emergency calls

About this task

Verify that the contact center routes emergency calls correctly. Verify that the emergency services receive the information about the endpoint location.

For more information about emergency calling, see the features section in *Avaya Contact Center – Extended Capacity Solution Description*.

Before you begin

- Ensure that you have an emergency service for testing calls. You can book a call time with the emergency services, use the 933 service for testing, or configure a test PSAP.
- Configure a SIP server, a network location, a dial plan, and number adaptations for emergency calls. For more information about configuring contact center objects, see *Administering Avaya Contact Center – Extended Capacity*.
- Ensure that your dial plan allows you to call an emergency service without dialing a prefix.

Procedure

1. Log in to the agent endpoint with the endpoint credentials.
2. On the agent endpoint, call the emergency services.

   If you book a call time with the emergency services, you must call the emergency number at the specified time.

3. Verify that the emergency services receive the endpoint location.

   Avaya Contact Center – Extended Capacity sends the information about the agent profile assigned to the endpoint. If the endpoint does not have an agent profile configured, the contact center uses the endpoint IP address to locate the endpoint and sends this information to the emergency services.

4. Complete the call.

Generating a test supervisor report

About this task

After adding contact center objects and testing basic call functionality, log in to the CMS Supervisor web portal and run a test report to verify that CMS is processing call data correctly. For example, you can view status details for the configured skill.

Before you begin

- Add a CMS link on the Configuration Server web portal.
- Add your contact center to CMS using the CMS CLI.
- Obtain the CMS Supervisor web portal IP address and supervisor credentials from the implementation personnel or Avaya support.

Procedure

1. Log in to the CMS Supervisor web portal as a supervisor.
2. On the navigation menu, go to **Reports** > **Realtime** > **Split/Skill**.
3. On the Realtime: Split/Skill page, click **Skill Status**.
4. In the Inputs dialogue box, in **Split/Skill**, type the skill number.
5. In **Refresh Interval**, type the time interval to refresh the report data in seconds.
6. Click **OK**.

   In the new window, you can see the names, login IDs, states, and call details of the skill agents.

Related links

Adding your contact center to Call Management System on page 52
Configuring a Call Management System connection on page 52

Verifying AE Services status and license mode

About this task

After configuring AE Services, check the connection status and the license mode of each service using the AE Services management console.

Before you begin

Log in to the AE Services management console.

Procedure

1. Click **AE Services**.
2. In the Status column, verify that the status of the required service is ONLINE.
3. In the License Mode column, verify that the license status of the required service is NORMAL MODE.

Viewing the EASG status

About this task

View the EASG status to check if EASG is enabled and Avaya personnel can access your contact center.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. To view the EASG status, run the following command:

   ```
   sudo EASGStatus
   ```

Managing EASG access

About this task

Manage Avaya personnel access to your contact center through EASG. With EASG enabled, Avaya Services can provide ongoing support and perform management and solution optimization procedures.

Procedure

1. Do one of the following:
   - Open the console on the active Configuration Server.
   - Use the SSH client to log in to the active Configuration Server.
2. Run one of the following commands:
   - `sudo EASGManage -f --enableEASG`: To enable EASG access.
   - `sudo EASGManage -f --disableEASG`: To disable EASG access.

Testing the desktop service

About this task

Verify that you can start the noVNC remote desktop session from the Configuration Server. During the noVNC session, you must verify that you can access the Configuration Server web portal and AE Services management console and use the server console. You must also check that you can access the noVNC session from different computers on your network to co-browse the noVNC remote desktop.

Procedure

1. On the active Configuration Server, start the SSH session.
2. In the command prompt, run the `remoteDesktopSession` command.

   The command output displays a web link to the noVNC remote desktop session in the following format:

   `https://<mcs-ip>:<remote session port>/?password=<remote session password>`, where `<remote session port>` and `<remote session password>` are provided automatically.
3. Copy the web link into the browser address bar and replace `<mcs-ip>` with the IP address of your Configuration Server.

   In the geo-redundant HA deployment, replace `<mcs-ip>` with the virtual IP address of the Configuration Server.
4. Verify that the browser displays the remote desktop session.
5. On the remote desktop, open a browser.
6. In the remote desktop browser, access the Configuration Server web portal.
7. Verify that you can log in to the Configuration Server as a system administrator.
8. In the remote desktop browser, access the AE Services management console.
9. Verify that you can log in to the AE Services management console.

   For more information about logging in to the AE Services management console, see the Application Enablement Services overview section in *Administering Application Enablement Services for Avaya Contact Center – Extended Capacity*.
10. On the remote desktop, open the server console.
11. Verify that you can run console commands.

    For example, you can verify that you can access contact center servers using the `ssh` command.
12. On another computer in your network, access the noVNC session using the same noVNC web link.
13. Verify that browsers on different computers display the same noVNC session screen.

Related links

Logging in to the Configuration Server as a system administrator on page 48

High Availability verification

After installing the contact center, you need to check if your contact center can fail over to alternate server without affecting call processing. You can trigger the active Routing Core Server

to fail over to an alternate server. After the failover, you can check if the contact center processes external calls and call transfers correctly. You can also check the quality of the speech path between the caller and contact center users.

Triggering a test failover

About this task

Trigger a graceful failover to verify high availability of your contact center.

Procedure

1. On Configuration Server, start the SSH session.
2. To access the active Routing Core Server, run the following command:

   `ssh mega@<server_IP_address>`, where *<server_IP_address>* is the static IP address of the active Routing Core Server.
3. In the command prompt, run the following command:

   ```
   docker exec -it main bash
   ```
4. To verify that the Routing Core Server is active, run the following commands:

   ```
   cd /app/aicore/state_tools
   ./ss_tester
   ```

   If the Routing Core Server is active, the command output displays the following before the list of actions:

   ```
   HA info: role:active sync_conn:1(out) relay_conn:0(in)
   DO_HA_SYNC: true shmsync_state:0xa
   ```
5. On the active Routing Core Server, run the following commands:

   ```
   sudo killall -2 ar_service
   docker-compose -f mega.yml down
   ```

   The contact center fails over to an alternate server.

Verifying the server status after failover

About this task

After triggering a test failover, verify that the previously active Routing Core Server is in alternate mode. You must also check that one of the previously alternate Routing Core Server instances is active and hosts the VIP address.

Before you begin

Trigger a failover.

Procedure

1. On Configuration Server, start the SSH session.
2. To access Routing Core Server, run the following command:

`ssh mega@<server_IP_address>`, where `<server_IP_address>` is the static IP address of the Routing Core Server.

3. In the command prompt, run the following command:

   `hostname -I`

4. Verify the server IP addresses in the command output.

   When you run the `hostname -I` command on the previously active server, the command output does not display the VIP address. The command output displays the VIP address for one of the previously alternate Routing Core Server instances.

Related links

Triggering a test failover on page 92

Testing calls to Avaya Contact Center – Extended Capacity after failover

About this task

After the contact center fails over, verify that your contact center processes calls normally. You can make a test call to a configured VDN from the caller's phone to verify if callers hear announcements when they are in queue and if agents in Auto-In mode can receive calls and hear VOA message when they accept the call. Check the quality of the speech path between the caller and the agent.

Procedure

1. Log in to the agent endpoint with agent credentials.

   You must enter an agent login ID and the associated password.

2. On the caller's phone, call the configured VDN.
3. Check if you can hear announcements.
4. On the agent endpoint, change the agent work mode to Auto-In.

   The system administrator can configure the endpoint feature buttons on the Configuration Server web portal.

5. Answer the incoming call.
6. Check if you can hear the VOA message.

   The contact center plays a short message about the requested service before connecting the caller to an agent.

7. On the caller's phone and agent endpoint, check the quality of the speech path.
8. Complete the call.

Related links

Adding a test announcement on page 76
Adding test contact center objects on page 77

Testing an attended transfer after failover

About this task

After the contact center fails over, verify that an agent can complete a call transfer. You can make a test call to a configured VDN from the caller's phone to verify if an agent can complete a call transfer and check the quality of the speech path.

Procedure

1. Log in to the supervisor endpoint.

   You must enter an endpoint extension and the associated password.

2. Log in to the agent endpoint with agent credentials.

   You must enter an agent login ID and the associated password.

3. On the agent endpoint, change the agent work mode to Auto-In.

   The system administrator can configure the endpoint feature buttons on the Configuration Server web portal.

4. On the caller's phone, call the configured VDN.
5. On the agent endpoint, answer the incoming call.
6. Initiate an attended transfer to the supervisor endpoint extension.
7. On the caller's phone, check if you can hear music on hold.
8. On the supervisor endpoint, answer the call from the agent.
9. On the agent and supervisor endpoints, check the quality of the speech path.
10. On the agent endpoint, complete the transfer to the supervisor.
11. On the caller's phone and supervisor endpoint, check the quality of the speech path.
12. Complete the call.

Related links

Adding a test announcement on page 76
Adding test contact center objects on page 77

Chapter 7: Resources

Documentation

Title	Use this document to	Audience
Overview		
Avaya Contact Center – Extended Capacity Solution Description	Understand high-level product functionality, performance specifications, security, and licensing.	Customers and sales, services, and support personnel
Implementing		
Deploying Avaya Contact Center – Extended Capacity	Install and configure Avaya Contact Center – Extended Capacity.	Implementation personnel
Migrating to Avaya Contact Center – Extended Capacity	Migrate from Avaya Aura® Call Center Elite to Avaya Contact Center – Extended Capacity.	Implementation personnel
Administering		
Administering Avaya Contact Center – Extended Capacity	Administer and manage Avaya Contact Center – Extended Capacity.	Implementation personnel
Administering Application Enablement Services for Avaya Contact Center – Extended Capacity	Administer and manage Application Enablement Services for integration with Avaya Contact Center – Extended Capacity.	Implementation personnel
Maintaining		
Maintaining Avaya Contact Center – Extended Capacity	Perform basic maintenance procedures and troubleshoot Avaya Contact Center – Extended Capacity services.	• System administrators • Customers and sales, services, and support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.

4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select the appropriate release number.

   The **Choose Release** field is not available if there is only one release for the product.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Avaya Documentation Center navigation

For some programs, the latest customer documentation is now available on the Avaya Documentation Center website at https://documentation.avaya.com.

Important:

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

Using the Avaya Documentation Center, you can:

- Search for keywords.

  To filter by product, click **Filters** and select a product.
- Search for documents.

  From **Products & Solutions**, select a solution category and product, and then select the appropriate document from the list.
- Sort documents on the search results page.
- Click **Languages** ( ) to change the display language and view localized documents.
- Publish a PDF of the current section in a document, the section and its subsections, or the entire document.
- Add content to your collection using **My Docs** ( ).

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

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

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

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

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

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

Note:

Some functionality is only available when you log in to the website. The available functionality depends on your role.

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 http://www.avaya.com/support.
2. Log on to the Avaya website with a valid Avaya user ID and password.

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product-specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.

5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Appendix A: Server chassis

Routing Core Server chassis

You can deploy the Routing Core Server on Dell EMC PowerEdge R940 or an alternative server. Based on the size of your contact center and traffic load, connect the Routing Core Server to the traffic VLAN using either the 10-Gbps or 100-Gbps port.

The following images show a common server chassis. Some ports can be in different chassis slots. For more information about Dell server ports, see https://www.dell.com/support/.

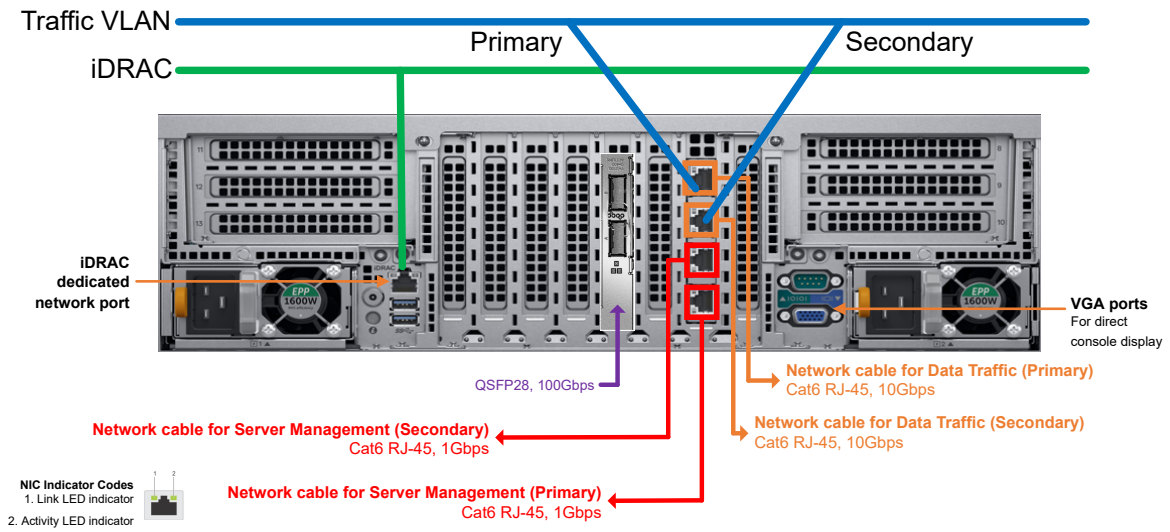


Figure 4: Dell EMC PowerEdge R940 cabling for 10-Gbps bandwidth

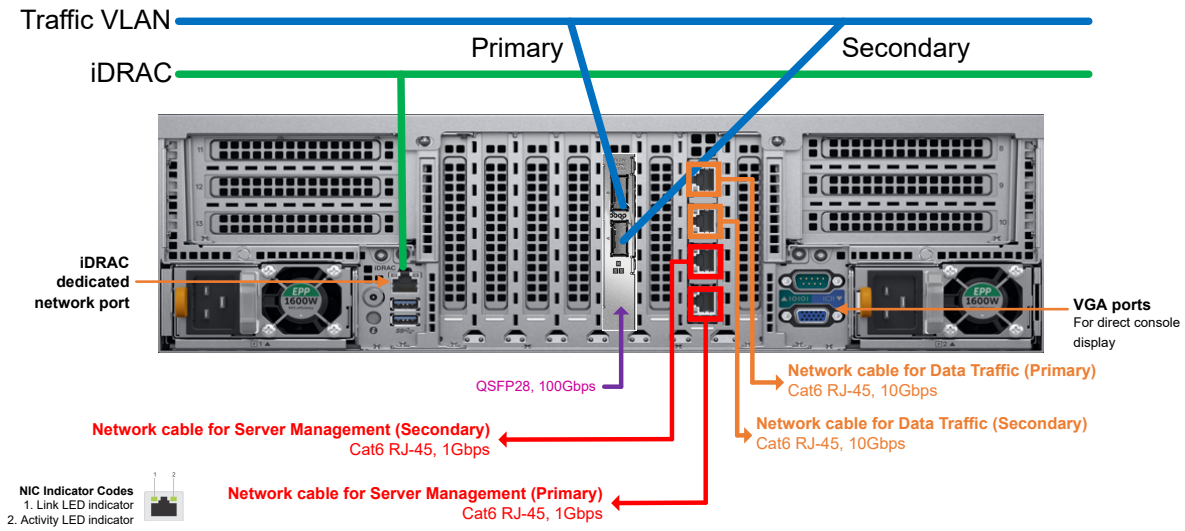


Figure 5: Dell EMC PowerEdge R940 cabling for 100-Gbps bandwidth

Configuration Server chassis

You can deploy the Configuration Server on a virtual machine, Dell EMC PowerEdge R640, or an alternative server. Connect the Configuration Server to the traffic VLAN using 10-Gbps bandwidth.

The following image shows a common server chassis. Some ports can be in different chassis slots. For more information about Dell server ports, see https://www.dell.com/support/.

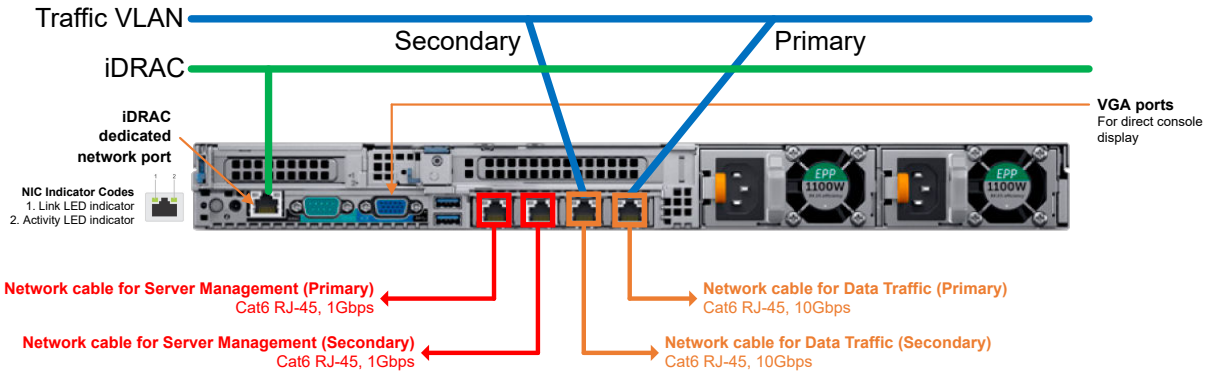


Figure 6: Dell EMC PowerEdge R640 cabling

Appendix B: Port allocation

Configuration Server port allocation

The following table lists port assignments used for communication between contact center components, such as an administrator computer and the Routing Core Server, and the Configuration Server. For more information about the Avaya Contact Center – Extended Capacity port allocation, go to the Avaya Support website at https://support.avaya.com/.

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
Administrator PC	Ephemeral	Configuration Server	22	TCP/SSH	Used for remote access through SSH
Configuration Server	Ephemeral	Configuration Server and Routing Core Server	22	TCP/SSH	Used for remote access through SSH
Configuration Server	Ephemeral	Network time server	123	UDP/NTP	Used for clock time synchronization
Administrator PC	Ephemeral	Configuration Server	443, 8443	TCP/HTTP, TLS/HTTPS/ REST/JSON	Used for administrator access to the Configuration Server web portal
Administrator PC	Ephemeral	Configuration Server	8200	TCP/HTTPS	Used for administrator access to the Contact Center Administration application on the Configuration Server web portal
Administrator PC	Ephemeral	Configuration Server	8201	TCP/HTTPS/ REST/JSON	Used for administrator access to the Configuration Server web portal authorization page and the App Launcher

Table continues…

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
Administrator PC	Ephemeral	Configuration Server	8202	TCP/HTTPS/ REST/JSON	Used for administrator access to the System Administration application on the Configuration Server web portal
Administrator PC	Ephemeral	Configuration Server	8203	TCP/HTTPS/ REST/JSON	Used for administrator access to the Online Help application on the Configuration Server web portal
Administrator PC	Ephemeral	Configuration Server	8204	TCP/HTTPS/ REST/JSON	Used for administrator access to the Security App application on the Configuration Server web portal
Administrator PC	Ephemeral	Configuration Server	5901, 6901	TCP, HTTPS	Used for administrator access to the noVNC remote desktop.

Routing Core Server port allocation

The following table lists port assignments used for communication between contact center components, such as the Configuration Server and AE Services, and the Routing Core Server. For more information about the Avaya Contact Center – Extended Capacity port allocation, go to the Avaya Support website at https://support.avaya.com/.

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
Configuration Server	Ephemeral	Routing Core Server	22	TCP/SSH, SCP, SFTP	Used for remote access through SSH
Endpoint	Ephemeral	Routing Core Server	80	TCP/HTTP	Used for access to endpoint settings file, firmware, and recorded agent greetings
Routing Core Server	Ephemeral	Network rime server	123	UDP/NTP	Used for clock time synchronization
Call Management System	Ephemeral	Routing Core Server	5001	TCP/SPI	Used for the connection to Call Management System

Table continues…

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
Endpoint, Session Border Controller	Ephemeral	Routing Core Server	5060	TCP/SIP, UDP/SIP	Used for SIP signaling
AE Services	Ephemeral	Routing Core Server	8765	TLS/AEP	Used for the connection to AE Services over ASAI protocol

AE Services port allocation

The following table lists port assignments used for communication between contact center components, such as WebLM and AESi, and the AE Services. For more information about the Avaya Contact Center – Extended Capacity port allocation, go to the Avaya Support website at https://support.avaya.com/.

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
AE Services	Ephemeral	Network time protocol	123	UDP/NTP	Used for clock time synchronization
Web browser	Ephemeral	AE Services	80, 443, 8443	TCP, HTTP/ HTTPS	Used for access to the AE Services management console, web services, and WebLM
TSAPI and JTAPI client	Ephemeral	AE Services	1050-1065	TCP	Used for unencrypted TLINK ports
TSAPI and JTAPI client	Ephemeral	AE Services	1066-1081	TCP, TLS	Used for encrypted TLINK ports
DMCC client	Ephemeral	AE Services	4721	TCP	Used for an unencrypted DMCC port
DMCC client	Ephemeral	AE Services	4722	TCP, TLS	Used for an encrypted DMCC port
TR/87	Ephemeral	AE Services	4723	TCP, TLS	Used for an encrypted TR/87 port
CVLAN client	Ephemeral	AE Services	9998	TCP, TLS	Used for an encrypted CVLAN port
CVLAN client	Ephemeral	AE Services	9999	TCP	Used for an unencrypted CVLAN port
AE Services	Ephemeral	DHCP server	67	UDP	Used for the connection to the DHCP server

Table continues…

Source		Destination		Protocol	Description
Component	**Port**	**Component**	**Port**		
AE Services	20000-24999	AESi	5060, 5061	TCP, TLS	The DMCC service uses these ports for SIP signaling
AE Services	Ephemeral	WebLM	52233	TCP/HTTP	Used for access to WebLM
AE Services	Ephemeral	AE Services	9041	TCP	Used for the connection between AE Services servers in local HA and geo-redundant HA deployments

Appendix C: Configuration file examples

mega-config.yml example

The following are examples of the `mega-config.yml` configuration in different deployment environments:

Simplex deployment

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# List of EASG login names to be enabled
# on the MCS hosts
avaya_easg_login_names: init, craft, sroot

# Virtual IP support for MBX and MCS
mcs_vip: 172.20.121.52
mbx_vip: 172.20.121.51

# Uniqe MCS setup ID
mcs_setup_id: 51

deployment_type: simplex
# Cluster network configuration (comma-separated list)

########## COLD DR #########
MCS_VIP_SECONDARY: 172.16.30.189
SECONDARY_DC_MBX_VIP: 172.16.30.190
MBX2A_IP: 172.16.30.183
MBX2B_IP: 172.16.30.184
PRIMARY_DC_MBX_VIP: 172.16.30.189
SITE: primary/secondary
FAILBACK_POLICY: automatic

data_centers:
  - name: "First data center"
    mcs:
      - mcs_ip: 172.20.121.52
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 172.20.121.51
        macvlan_ip: 172.20.121.54
        macvlan_subnet: 172.20.121.0/24
        macvlan_gateway: 172.20.121.3
        macvlan_interface: enp217s0f0
        interface: enp217s0f0
        #    aes_standalone_host: # GCP only
        #      - aeshost_ip: 100.70.2.58
        #        aes_ip: 100.70.2.78
        # hostname: "apps1dc7aes1-1"
        #interface: eth0
        #      - aeshost_ip: 100.70.2.59
```

```
        #        aes_ip: 100.70.2.158
        #hostname: "apps1dc7aes2-1"
        #interface: eth0


aes_ha:
  - primary_ip: 172.20.121.53
    # for georedundant-ha: primary aes ip for the first data center
    hostname: "internal-aes-1"
```

Local HA deployment

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# List of EASG login names to be enabled
# on the MCS hosts
avaya_easg_login_names: init, craft, sroot

# Virtual IP support for MBX and MCS
mcs_vip: 10.0.0.80
mbx_vip: 10.0.0.83

# Uniqe MCS setup ID
mcs_setup_id: 1

deployment_type: local-ha
# Cluster network configuration (comma-separated list)

########## COLD DR #########
MCS_VIP_SECONDARY: 10.1.0.90
SECONDARY_DC_MBX_VIP: 10.1.0.93
MBX2A_IP: 10.1.0.94
MBX2B_IP: 10.1.0.95
PRIMARY_DC_MBX_VIP: 10.0.0.83
SITE: primary/secondary
FAILBACK_POLICY: automatic

data_centers:
  - name: "DC1"
    mcs:
      - mcs_ip: 10.0.0.80
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 10.0.0.81
        macvlan_ip: 10.0.0.87
        macvlan_subnet: 10.0.0.0/24
        macvlan_gateway: 10.0.0.1
        macvlan_interface: ens192
        interface: ens192:1
      - mbx_ip: 10.0.0.82
        macvlan_ip: 10.0.0.88
        macvlan_subnet: 10.0.0.0/24
        macvlan_gateway: 10.0.0.1
        macvlan_interface: ens192
        interface: ens192:1

aes_ha:
  - primary_ip: 10.0.0.84
    # for georedundant-ha: primary aes ip for the first data center
    secondary_ip: 10.0.0.85
    # for georedundant-ha: secondary aes ip for the second data center
    virtual_ip:    10.0.0.86
    hostname: "mega08aes"
```

Geo-redundant HA deployment without Layer 2 Networking

To deploy Geo-redundant HA without Layer 2 Networking:

1. Fresh deploy all Routing Core Server services except AE Services on both data centers.
2. After the Routing Core Server services are up, deploy AE Services.

Fresh deploy mega-config.yml for data center 1

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# List of EASG login names to be enabled
# on the MCS hosts
avaya_easg_login_names: init, craft, sroot

# Virtual IP support for MBX and MCS
mcs_vip: 10.0.0.80
mbx_vip: 10.0.0.83

# Uniqe MCS setup ID
mcs_setup_id: 1

deployment_type: cold-dr
# Cluster network configuration (comma-separated list)

########## COLD DR #########
MCS_VIP_SECONDARY: 10.1.0.90
SECONDARY_DC_MBX_VIP: 10.1.0.93
MBX2A_IP: 10.1.0.94
MBX2B_IP: 10.1.0.95
PRIMARY_DC_MBX_VIP: 10.0.0.83
SITE: primary
FAILBACK_POLICY: automatic

data_centers:
  - name: "First data center"
    mcs:
      - mcs_ip: 10.0.0.81
        interface: ens192
      - mcs_ip: 10.0.0.82
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 10.0.0.84
        interface: ens192:1
      - mbx_ip: 10.0.0.85
        interface: ens192:1
```

Fresh deploy mega-config.yml for data center 2

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# List of EASG login names to be enabled
# on the MCS hosts
avaya_easg_login_names: init, craft, sroot

# Virtual IP support for MBX and MCS
mcs_vip: 10.1.0.90
mbx_vip: 10.1.0.93

# Uniqe MCS setup ID
mcs_setup_id: 2
```

```
deployment_type: cold-dr
# Cluster network configuration (comma-separated list)

########## COLD DR #########
MCS_VIP_SECONDARY: 10.1.0.90
SECONDARY_DC_MBX_VIP: 10.1.0.93
MBX2A_IP: 10.1.0.94
MBX2B_IP: 10.1.0.95
PRIMARY_DC_MBX_VIP: 10.0.0.83
SITE: secondary
FAILBACK_POLICY: automatic

data_centers:
  - name: "DC2"
    mcs:
      - mcs_ip: 10.1.0.91
        interface: ens192
      - mcs_ip: 10.1.0.92
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 10.1.0.94
        interface: ens192:1
      - mbx_ip: 10.1.0.95
        interface: ens192:1
```

Deploy AE Services

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# List of EASG login names to be enabled
# on the MCS hosts
avaya_easg_login_names: init, craft, sroot

# Virtual IP support for MBX and MCS
mcs_vip: 10.0.0.80
mbx_vip: 10.0.0.83

# Uniqe MCS setup ID
mcs_setup_id: 1

deployment_type: cold-dr
# Cluster network configuration (comma-separated list)

########## COLD DR #########
MCS_VIP_SECONDARY: 10.1.0.90
SECONDARY_DC_MBX_VIP: 10.1.0.93
MBX2A_IP: 10.1.0.94
MBX2B_IP: 10.1.0.95
PRIMARY_DC_MBX_VIP: 10.0.0.83
SITE: primary
FAILBACK_POLICY: automatic

data_centers:
  - name: "DC1"
    mcs:
      - mcs_ip: 10.0.0.81
        interface: ens192
      - mcs_ip: 10.0.0.82
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 10.0.0.84
        macvlan_ip: 10.0.0.87
        macvlan_subnet: 10.0.0.0/24
```

```
        macvlan_gateway: 10.0.0.1
        macvlan_interface: ens192
        interface: ens192:1
      - mbx_ip: 10.0.0.85
        macvlan_ip: 10.0.0.89
        macvlan_subnet: 10.0.0.0/24
        macvlan_gateway: 10.0.0.1
        macvlan_interface: ens192
        interface: ens192:1
  - name: "DC2"
    mcs:
      - mcs_ip: 10.1.0.91
        interface: ens192
      - mcs_ip: 10.1.0.92
        interface: ens192
    mbx: # list of mbx hosts
      - mbx_ip: 10.1.0.94
        macvlan_ip: 10.1.0.97
        macvlan_subnet: 10.1.0.0/24
        macvlan_gateway: 10.1.0.1
        macvlan_interface: ens192
        interface: ens192:1
      - mbx_ip: 10.1.0.95
        macvlan_ip: 10.1.0.99
        macvlan_subnet: 10.1.0.0/24
        macvlan_gateway: 10.1.0.1
        macvlan_interface: ens192
        interface: ens192:1


aes_ha:
  - primary_ip: 10.0.0.86
    # for georedundant-ha: primary aes ip for the first data center
    secondary_ip: 10.1.0.96
    # for georedundant-ha: secondary aes ip for the second data center
    virtual_ip:     # keep blank
    hostname: "mega08aes"
  - primary_ip: 10.1.0.98
    # for georedundant-ha: primary aes ip for the second data center
    secondary_ip: 10.0.0.88
    # for georedundant-ha: secondary aes ip for the first data center
    virtual_ip:      # keep blank
    hostname: "mega09aes"
```

all example

The `all` file has the same configuration for all deployment types. However, you must update the `ha_type` and the IP addresses for the additional data centers as required, depending on the deployment type. The following example provides the `all` configuration for the Geo-redundant HA deployment without Layer 2 Networking deployment environment:

```
---
# Variables listed here are applicable to all host groups

##### MCS ENVIRONMENT VARIABLES #####
CONFIG_SUBSCRIPTION_PORT: 4002
PGPORT: 5432

ha_type: cold-dr #Enter environment type e.g. simplex, local-ha, georedundant-ha, cold-
```

```
dr
platform:

#Note:
#define disk space in Gbs
#Suggested values for Sandbox Env: root_min_disk_space = 60 home_min_disk_space = 80
root_min_disk_space: "45"
home_min_disk_space: "25"

MCS_IPS: "10.0.0.81,10.0.0.82"

### Tenant append character
MINIO_BUCKET_CHAR: "-"

MEGA_MCS_HA: 172.16.31.190:5000/mega-mcs-ha:feature-dockerfile-mcs-ha-efc6b79
MCS_SYNC_IMG: 172.16.31.190:5000/mcs-sync:latest
CFG_BACKEND_IMG: 172.16.31.190:5000/config-backend:2.10.36
CONFIG_DB_IMG: 172.16.31.190:5000/postgres:ha_v3-latest
KONG_IMG: 172.16.31.190:5000/mega-kong:22.11.23-151-9fe0779
KEYCLOAK_IMG: 172.16.31.190:5000/mega-keycloak:22.11.23-78-21df319
REDIS_IMG: 172.16.31.190:5000/redis:6.2.7-latest
MEGA_BCK_IMG: 172.16.31.190:5000/staging-mega-acd-backend:22.11.22-2-43b1554
MEGA_SECURITY_SERVER: 172.16.31.190:5000/mega-security-server:22.11.23-0-46a6cd4
MAINTENANCE_SHELL_MCS_IMG: 172.16.31.190:5000/integration_mcs:22.11.23-0-e6ac645
MINIO_CLIENT_IMG: 172.16.31.190:5000/minio-client:latest-fips
OVERSIGHT_GRAFANA: 172.16.31.190:5000/grafana-mega:7.5.16.5
OVERSIGHT_TELEGRAF: 172.16.31.190:5000/telegraf:1.19.2-mega
OVERSIGHT_TRAP_ADAPTER: 172.16.31.190:5000/avaya-trap-adapter:1.10.0
OVERSIGHT_POSTGRES: 172.16.31.190:5000/itsm-postgress:13.7.5
OVERSIGHT_SIGNAL_INTERVAL: 1
MEGA_NOVNC_IMAGE: 172.16.31.190:5000/mega_novnc_desktop:0.0.1-19
MEGA_NGINX_IMAGE: 172.16.31.190:5000/mega-nginx:2.5
MEGA_AES_IMAGE: 172.16.31.190:5000/mega-aes:10.2.51-332
SHM_API_PORT: 9085
SHM_API_PROTOCOL: http
SHM_WS_PORT: 9002
AES_LOGIN_URL: https://172.16.30.161/aesvcs/login.xhtml
MCS_NETWORK: mcs-net

USER_MCS: "mega"
USER_SSH_PATH: "/home/mega/.ssh"
MCS_ANNOUNCEMENTS_DIR: "/data/mcs/sounds"

CONFIG_BACKEND_CONTAINER_NAME: config-backend
KONG_CONTAINER_NAME: kong
CONFIG_DB_CONTAINER_NAME: config-db
REDIS_CONTAINER_NAME: mcs-redis
BACKEND_CONTAINER_NAME: mcs-core-backend
KEYCLOAK_CONTAINER_NAME: keycloak
MINIO_SERVER_CONTAINER_NAME: mega-minio-server

LOGGING_LEVEL: info
LOGS_FOLDER: /var/log/audit-logs
SECURITY_SERVER_API_PORT: 3003
GET_LOGS_FOLDER: /var/log/mega/
GET_DBSESSIONS_FOLDER: /root/dock/
GET_LOGS_DEST_FOLDER: /home/stem/getlogs/
POSTGRES_SSLMODE: disable

# It can be TRACE | INFO | ERROR | WARN | DEBUG
AMS_LOG_LEVEL: TRACE
AMS_BINARY_STRING: "1111000000010000"

##Disable container processes from gaining new privileges.
Can be True or False
```

```
PREVENT_NEW_PRIVILEGES: true

## Limiting the Memory and CPU usage of containers
# Memory limit takes a positive integer, followed by a suffix B, K, M, G,
to indicate bytes, kilobytes, megabytes, or gigabytes.
# These parameters should be set to "0" to keep them unlimited
(containers can consume entire host's resources).
CONTAINER_MEMORY_LIMIT: "0"
# Specify how much of the available CPU resources a container can use.
# cpus:"1.5" the container is guaranteed at most one and a half of the CPUs.
# These parameters should be set to "0" to keep them unlimited
(containers can consume entire host's resources).
CONTAINER_CPUS_LIMIT: "0"

MCS_HOST_DOCKER_DIRECTORY: "/var/lib/docker"

##### NGINX ENVIRONMENT VARIABLES #####
NGINX_RATE_LIMIT: 0
NGINX_SIZE_MAX_STATIONS: 25000
NGINX_MCS_CONTAINER_NAME: mega-nginx-mcs
NGINX_MBX_CONTAINER_NAME: mega-nginx-mbx
#Note:FQDN values should be the same as FQDN fields for
the MBX/MCS certificates respectively.
MCS_CERT_FQDN: mega08mcs.avaya.com
MBX_CERT_FQDN: mega08mbx.avaya.com

##### UI ENVIRONMENT VARIABLES #####
MEGA_CM_UI: 172.16.31.190:5000/mega-cm-ui:22.11.23-1-800a542
MEGA_AUTH_UI_IMG: 172.16.31.190:5000/mega-auth-ui:22.11.24-0-34f1016
MEGA_SM_UI: 172.16.31.190:5000/mega-sm-ui:22.11.22-2-fba466a
MEGA_OLH_UI: 172.16.31.190:5000/mega-olh:22.11.22-0-08cfbd2
MEGA_SECURITY_UI: 172.16.31.190:5000/mega-security-ui:22.11.24-0-5a68a09
PROTOCOL: https
LOCAL_AUTH: 0
CMS_URL: http://cms.mega.com
OVERSIGHT_SIGNAL_INTERVAL_FOR_UI: 1

AUTH_CONTAINER_NAME: mega-auth-ui
AUTH_INTERNAL_PORT: 4000
CMUI_CONTAINER_NAME: mega-cm-ui
CMUI_INTERNAL_PORT: 4000
SMUI_CONTAINER_NAME: mega-sm-ui
SMUI_INTERNAL_PORT: 4006
SCUI_CONTAINER_NAME: mega-security-ui
SCUI_INTERNAL_PORT: 4000
OLH_CONTAINER_NAME: mega-olh-ui
OLH_INTERNAL_PORT: 80
APIDOCS_CONTAINER_NAME: mega_docs
APIDOCS_INTERNAL_PORT: 80

UI_NETWORK: ui-net
UI_SUBNET: 192.168.2.0/24
##### MBX ENVIRONMENT VARIABLES #####
RETRY_COUNT: 0
TENANT: megadr
NUMBER_OF_AGENTS: 1000
MEGA_V6_IMG: 172.16.31.190:5000/mega_v6:22.11.24-19113
OPENSIPS_IMG: 172.16.31.190:5000/opensips_3_2:22.11.22-0-fb1187f
MINIO_SERVER_IMG: 172.16.31.190:5000/minio-server:latest-fips
OVERSIGHT_AGENT: 172.16.31.190:5000/oversight-agent:1.26.4
MEGA_PPM_IMG: 172.16.31.190:5000/mega-ppm:8.1.12.0.8112090
PIPE_READER_IMG: 172.16.31.190:5000/pipe_reader:latest
DEVOPS_API_IMG: 172.16.31.190:5000/devops-api:22.11.22
MBX_NETWORK: mega-avaya
MBX_CONFIG_SUBNET: 192.168.3.0/24
```

```
MBX_CONFIG_NETWORK: mega-avaya-config

AES_NETWORK: aes-macvlan
PPM_CONTAINER_NAME: mega-ppm
PPM_DOMAIN: avaya.com
SIP_PORT: 5060

## PPM compose file variable
ENDPOINT_TRANSPORT: tcp

# Options to update SHM Size
#
# Smaller SHM AF_SHM_NUM_OF_BLOCKS=2 and AF_SHM_BLOCK_SIZE_IN_MB=512)
SHM_BLOCK_SIZE_IN_MB: 2000
SHM_HA_BUFFER_SIZE_IN_MB: 400
SHM_NUM_OF_BLOCKS: 8
DUMP_CORE: false

#### FOR CORE DUMPS ####
## Set Privileged to true to spawn containers in privileged mode
PRIVILEGED: true
## For core dumps. Set to '0' for disable and '-1' to enable.
ULIMIT_VALUE: 0

##### If external DB is used provide external db ip, if local opensips DB is used,
provide opensips IP i.e 192.168.0.25 ####
OPENSIPS_DB_IP: 192.168.0.25
#############################
##### If external DB is used provide external db port, if local opensips DB is used,
provide 5432 ####
OPENSIPS_DB_PORT: 5432

#### For Memory allocation for Opensips
#### Setting Opensips environment to Production (1) or Non-production (0)
PRODUCTION: 0
MTLS: 0

# Add IPs of MBXs here, following a space separated syntax
MINIO_IPS: "10.0.0.84 10.0.0.85"

MBX_HOST_DOCKER_DIRECTORY: "/var/lib/docker"

############################      PLEASE DONOT CHANGE BELOW VARIABLES
############################

##### MEGA LOAD PACKAGE VARIABLES #####
mega_load_path: /home/mega/S40/
mega_load_dest_path: "/home/mega/DM/"

##### CHOCOLATE SCRIPT VARIABLES #####
chocolate_src_path: "offline-packages-latest.tar.gz"
chocolate_dest_path: "{{ mega_load_dest_path }}chocolate/"

##### EASG SCRIPT VARIABLES #####
easg_rpm_src_path: "{{ chocolate_dest_path }}rpms/"
easg_enable: true

##### MEGA DEPLOYMENT SCRIPTS VARIABLES #####
mega_scripts_dest_path: "{{ mega_load_dest_path }}scripts/"
mega_self_destruct: "{{ mega_scripts_dest_path }}mega/HelperScripts/"

##### MCS FILES VARIABLES #####
mcs_files_dest_path: "{{ mega_load_dest_path }}mcs_files/"

##### MBX FILES VARIABLES #####
```

```
mbx_files_dest_path: "{{ mega_load_dest_path }}mbx_files/"

##### HELPERS SCRIPT PATH VARIABLES #####
helper_script_path: "{{ mega_scripts_dest_path }}mega/HelperScripts/"

#### REGISTRY URL ####
registry_url: "172.16.31.190:5000"

##### UI FILES VARIABLES #####
ui_files_dest_path: "{{ mega_load_dest_path }}ui_files/"

##### AES FILES VARIABLES #####
aes_files_dest_path: "{{ mega_load_dest_path }}aes_files/"

##### AES STANDALONE DEPENDENCIES FILES VARIABLES #####
aes_standalone_dependencies_files_dest_path:
"{{ mega_load_dest_path }}aes_standalone_dependencies_files/"

##### OVERSIGHT FILES VARIABLES #####
oversight_files_dest_path: "{{ mega_load_dest_path }}oversight_files/"

##### CERTIFICATE MANAGER SCRIPTS VARIABLES #####
certificate_dest_path: /var/opt/Avaya/cert/
certificate_manager_install_path: /var/opt/Avaya/certificate_manager/
certificate_manager_dest_path: /opt/avaya/sbin/
certificate_manager_src_path: "{{ mega_scripts_dest_path }}mega/HelperScripts/
certificates/"

##### NGINX ENVIRONMENT VARIABLES #####
NGINX_PATH: "{{ mega_scripts_dest_path }}mega/Installation_scripts/Nginx"

##### AES ENVIRONMENT VARIABLES #####
AES_PATH: "{{ mega_scripts_dest_path }}mega/Installation_scripts/AES"

##### MCS ENVIRONMENT VARIABLES #####
ENVIRONMENT_FILE: /.env
LOG_PATH: /var/log/mega
APP_PATH: "{{ mega_scripts_dest_path }}mega/Installation_scripts/MCS"
GF_SERVER_PROTOCOL: https
GF_AOCLE_USER: avovadministrator
GF_AOCLE_PASS: vOvgFg3ntS3c!
PG_AOCLE_USER: avovpgadmin
PG_AOCLE_PASS: avOvgFg3ntPGS3c!
PG_ADMIN_PASS: avOvgFg3ntPGaS3c!
MINIO_TLS_NO_IP_VALIDATION: 0
TLS_REJECT_UNAUTHORIZED: 1
MEDIA_STORAGE_DIRECTORY: /data/media
MINIO_CONFIG_PATH: /home/mega-acd-backend/.mc
MINIO_BUCKET_NAME: sounds
MINIO_USER: AKIAIOSFODNN7EXAMPLE
MINIO_PASSWORD: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
MCS_DOCKER_REGISTRY: mcs.dockerregistry.com
MCS_DOCKER_REGISTRY_PORT: 5000
MCS_SUBNET: 192.168.1.0/24
LISTALARM_FILTER_BASE_LEVEL: 30
ENVIRONMENT: production
GF_TIMEZONE: America/New_York
# Add IPs of Linux Host here, following a comma separated syntax
within double qoutes
AG_SNMP_MCS_HOSTS: "10.0.0.81,10.0.0.82,10.0.0.84,10.0.0.85"
# Password required for oversight
SNMP_MCS_COMMUNITY: oversight
ATA_IP: 172.16.29.223
ATA_PORT: 1160
ATA_USERNAME: admin
```

```
ATA_MODE: authPriv
ATA_PROTOCOL: sha
ATA_KEY: secret12
ATA_PRIVATE: aes
ATA_P_KEY: secret12

# Add IPs of Core MCS/MBX Host here, following a comma separated syntax
within double qoutes
AG_CORE_HOSTS: "10.0.0.81,10.0.0.82,10.0.0.84,10.0.0.85"

##### UI ENVIRONMENT VARIABLES #####
DEPLOYMENT_TYPE: MEGA
MegaUI_folder_path: "{{ mega_scripts_dest_path }}mega/Installation_scripts/MegaUI"

##### MBX ENVIRONMENT VARIABLES #####
CMSI_PORT: 5001
AESI_PORT: 8765
DCG_SMS_PORT: 8081
DCG_WEB_PORT: 9091
MEGA_REST: 9085
MEGA_WS: 9002
PG_PORT: 5435
PG_USER: postgres
PG_PASS: thisshouldbeasecret
LOG_PATH_MBX: /var/log/mega
CORE_DUMP_PATH: "{{ mega_scripts_dest_path }}mega/Installation_scripts/MBX"
APP_PATH_MBX: "{{ mega_scripts_dest_path }}mega/Installation_scripts/MBX"
WORKING_DIR: /app/
MEDIA_SERVER_IP: 192.168.0.24
OPENSIPS_IP: 192.168.0.25
MEGA_PPM_IP: 192.168.0.26
MBX_NGINX_PROXY: 192.168.0.27
MBX_REST_API: 192.168.0.28
SE_REST_IP: 192.168.0.29
MBX_WS_API: 192.168.0.30
MBX_MINIO_SERVER_IP: 192.168.0.31
OVERSIGHT_IP: 127.0.0.1
OVERSIGHT_PORT: 9089
MEGA_SUBNET: 192.168.0.0/24
MEGA_GATEWAY: 192.168.0.1
MINIO_USER_FOR_MBX: AKIAIOSFODNN7EXAMPLE
MINIO_PASSWORD_FOR_MBX: wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY

## Following are the AMS database configurations
AMS_DB_SERVER_IP_MBX: ams_db_server
AMS_DB_SERVER_PORT_MBX: 5432
AMS_DB_SERVER_USR_NAME_MBX: postgres
AMS_DB_SERVER_USR_PWD_MBX: mega123

CERT_DIR: /var/opt/Avaya/cert
tcp_keepalive_intvl: 9
tcp_keepalive_probes: 9
tcp_keepalive_time: 9

##Docker-Compose timeout value
COMPOSE_HTTP_TIMEOUT: 120

##################### Not Included in BACKUP ######################
OVERSIGHT_TESTALARM_PORT: 8089
AG_MCS_URL_PORT: 7004
MCS_VIRTUAL_IP: "{{ mcs_vip }}"
## Will be MCS VIP or FQDN
UI_URL: "{{ MCS_VIRTUAL_IP }}"
## Edit this in case of Ext-DB
PGHOST: "{{ CONFIG_DB_IP }}"
```

```
MCS_SETUP_ID: "{{ mcs_setup_id }}"
VIRTUAL_IP: "{{ mbx_vip }}"
MBX2A_IP: "{{ MBX2A_IP }}"
MBX2B_IP: "{{ MBX2B_IP }}"
MCS_VIP_SECONDARY: "{{ MCS_VIP_SECONDARY }}"
PRIMARY_DC_MBX_VIP: "{{ PRIMARY_DC_MBX_VIP }}"
SITE: "{{ SITE }}"
FAILBACK_POLICY: "{{ FAILBACK_POLICY }}"
MISC_PRUNER_PATH: "{{ mega_scripts_dest_path }}mega/Installation_scripts/Miscellaneous/"

AFUI_GATEWAY_URL: "https://{{ UI_URL }}:7004"
MEGA_AVAYA_DOMAIN: "{{ UI_URL }}"
WEBSOCKET_PROGRESSBAR_URL: "https://{{ UI_URL }}:7000"
SECURITY_SERVER_URL: "http://{{ UI_URL }}:3003"
AUTH_APP: "https://{{ UI_URL }}:8201"
CM_APP: "https://{{ UI_URL }}:8200"
SM_APP: "https://{{ UI_URL }}:8202"
OLH_APP: "https://{{ UI_URL }}:8203"
SECURITY_UI_URL: "https://{{ UI_URL }}:8204"
KONG_CONFIG_IP_PORT: "https://{{ MCS_VIRTUAL_IP }}:7004"
AF_CONFIG_SERVER: "{{ KONG_CONFIG_IP_PORT }}/config"
MEGA_VERSION: 10.0.2.0.40.22.11.25
AF_SHM_LICENSE_KEY:
GF_SECURITY_ADMIN_USER: avovadministrator
GF_SECURITY_ADMIN_PASSWORD: vOvgFg3ntS3c!
MCS_NGINX_PROXY: 192.168.1.30
INTERNAL_CONFIG_IP: 192.168.1.31
MCS_OAGENT_IP: 192.168.1.32
MCS_OAGENT_CONTAINER_NAME: mcs-oagent
MBX_OAGENT_IP: 192.168.0.32
MCS_KONG_CONTAINER_IP: 192.168.2.20
SERVER_AFUI_GATEWAY_URL: "http://{{ MCS_KONG_CONTAINER_IP }}:8000"
CONFIG_DB_IP: 192.168.1.33
SSL_VERIFY_CLIENT: "optional"
environments:
OVERSIGHT_CADDY: 172.16.31.190:5000/caddy:v1
POSTGRES_MULTIPLE_DATABASES: kong,keycloak,config,aicore,mega_acd,securityserver
MINIO_ENABLE_SECURE: 1

#Syslog Configuration
SYSLOG_SERVICE_HOST: 0.0.0.0
SYSLOG_SERVICE_PORT: 514

# Pruning utility - CronJob configurations #
# These configurations are for both MBX and MCS
cdump_retention_days: "7"
log_retention_days: "7"

upgrade_status: "false"
force_flag:
subcommand: upgrade

sysctl_config:
  net.core.rmem_max: 1342177280
  net.core.rmem_default: 1342177280
  net.core.wmem_max: 1342177280
  net.core.wmem_default: 1342177280
  net.ipv4.tcp_rmem: 33554432 67108864 1342177280
  net.ipv4.tcp_wmem: 33554432 67108864 1342177280
  net.ipv4.tcp_window_scaling: 1
  net.ipv4.tcp_keepalive_intvl: 9
  net.ipv4.tcp_keepalive_probes: 9
  net.ipv4.tcp_keepalive_time: 9
```

systemconfig example

The `systemconfig` file has the same configuration for all deployment types. However, you must update the `ha_type` and the IP addresses for the additional data centers, depending on the deployment type. For example:

- **Simplex**: Update mcsvip, mcsfqdn, mcs1ip, mcs1fqdn, mcs1hostname, mbxvip, mbx1aip, and mbx1afqdn.
- **Local-HA**: Update mcsvip, mcsfqdn, mcs1ip, mcs1fqdn, mcs1hostname, mbxvip, mbx1aip, mbx1afqdn, mbx1bip, mbx1bfqdn, and mbx1bhostname.
- **Geo-redundant HA deployment without Layer 2 Networking**: Update mcsvip, mcsfqdn, mcs1ip, mcs1fqdn, mcs1hostname, mcs2ip, mcs2fqdn, mcs2hostname, mbxvip, mbx1aip, mbx1afqdn, mbx1bip, mbx1bfqdn, and mbx1bhostname.

The following example provides the `systemconfig` configuration for the Geo-redundant HA deployment without Layer 2 Networking deployment environment:

```
# User with password less ssh and sudo access
# for the whole cluster
mega_install_user: mega
# Cluster network configuration (comma-separated list)
#
# mcsvip, mbxvip are the active virtual ip address for mcs and mbx respectively
# ONLY populate values for the servers that are in the system,
values for non-existing servers must be left blank
# E.g. for simplex system populate the values for:
#      mcsvip, mcsfqdn, mcs1ip, mcs1fqdn, mcs1hostname
#      mbxvip, mbxfqdn, mbx1aip, mbx1afqdn, mbx1ahostname
#
#      Leave the rest of the fields (for mcs2, mbx1b, mbx2a, mbx2b) blank
#mcs
mcsvip: 10.0.0.80
mcsfqdn: mega08mcs.avaya.com
#mcs1
mcs1ip: 10.0.0.81
mcs1fqdn: mega08mcs01.avaya.com
mcs1hostname: mega08mcs01
#mcs2
mcs2ip: 10.0.0.82
mcs2fqdn: mega08mcs02.avaya.com
mcs2hostname: mega08mcs02

#mbx
mbxvip: 10.0.0.83
mbxfqdn: mega08mbx.avaya.com
#mbx1a
mbx1aip: 10.0.0.84
mbx1afqdn: mega08mbx1.avaya.com
mbx1ahostname: mega08mbx1
#mbx1b
mbx1bip: 10.0.0.85
mbx1bfqdn: mega08mbx2.avaya.com
mbx1bhostname: mega08mbx2
#mbx2a
mbx2aip:
mbx2afqdn:
mbx2ahostname:
#mbx2b
mbx2bip:
mbx2bfqdn:
mbx2bhostname:
```

```
# DO NOT LEAVE THESE BLANK
# Country code must be 2 characters only
O(Organization): AVAYA
L(DC1 location): DC1
L(DC2 location): megaloc2
C(Country code): US
```

Index

Numerics

A

C

D

E

F

G

H

I

J

L

M

O

P

R

S

T

U

V

W