Maintaining and Troubleshooting Avaya Session Border Controller

Release 10.2.x
Issue 1
February 2024

© 2014-2024, Avaya LLC
All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

Licenses

License types

Copyright

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

Virtualization

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

Third Party Components

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

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.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 to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

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

Avaya is a registered trademark of Avaya LLC.

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

Contents

Chapter 1: Introduction

Purpose

This document describes how to maintain and troubleshooting your Avaya Session Border Controller (Avaya SBC) system. The document contains routine maintenance procedures, monitoring tools and utilities, and troubleshooting procedures. This document is intended for people who do maintenance and troubleshooting tasks.

Chapter 2: Maintenance procedures

Backup and restore

Creating a backup

Procedure

1. Log in to the CLI interface as a root user.
2. Run the following command: `/usr/local/ipcs/icu3/scripts/sbc-take-backup`

   Note:

   If you do not provide a backup file, Avaya SBC generates a file in the working directory.

Restoring the data

Procedure

1. Log in to the CLI interface as a root user.
2. Run the following command: `/usr/local/ipcs/icu3/scripts/sbc-restorebackup <backupfile>`
3. If you perform a backup and restore on different hardware, run the following commands:
   a. `rm /etc/udev/rules.d/99_ifrename.rules`
   b. `/usr/local/ipcs/icu3/scripts/ifnamer.py`
4. Reboot Avaya SBC.

Changing the ipcs password and unlocking the ipcs user account

About this task

If you know your root password, you can log on to Linux and use this procedure to either change or unlock the password for the ipcs user. If you do not know the root password, you must reset your passwords using the procedure Resetting the root or ipcs password on page 10.

Procedure

1. To change the password for the ipcs user:
   a. Log on to Linux as the root user.
   b. Use the following command to change the password:

      passwd ipcs

   c. Follow the prompts to create a new password.
2. To reset a locked password after too many failed attempts for the ipcs user:
   a. Log on to Linux as the root user.
   b. Use the following command to display the authentication failure records, that is, how many times the ipcs user got the password wrong:

      faillock --user ipcs

   c. Use the following command to reset the authentication failures so that the ipcs user can try to log on again:

      faillock --user ipcs --reset

Resetting the root or ipcs password

About this task

If you do not know your root or ipcs password, you can use this procedure to reset the password for the root or ipcs user. If you know the root password, you can simply change or unlock the ipcs password using the procedure Changing the ipcs password and unlocking the ipcs user account on page 9.

Procedure

1. At the boot menu, press `e` to edit the first boot entry.
2. **(Optional)** If the server prompts you to enter the user name and password for the grub menu, enter the user name as `root` and password as `@V@Y@_123`.
3. From the grub options, navigate to the end of the line that starts with **linux16** and enter:

   `rd.break`

4. Press `Ctrl+x`.

   This option will boot to the `initramfs` prompt with a root shell.

   The root file system is mounted in read-only mode to `/sysroot` and must be remounted with read/write permissions to make changes.
5. To remount the root file system with read/write permissions, run the following command:

   `mount -o remount,rw /sysroot`

6. Once the file system has been remounted, run the command:

   ```
   chroot /sysroot
   ```

7. To reset the password, do one of the following:

   - To reset the root password, run the following command:

     ```
     echo "root:SIPera_123" | chpasswd
     ```

   - To reset the root password, run the following command:

     ```
     echo "ipcs:SIPera_123" | chpasswd
     ```

   You can enter any password in place of `SIPera_123`.

8. Enter the `exit` command twice.

   Once the reboot has completed, you can use the root or ipcs account with the newly set password.

Restarting the IPCS services

About this task

When updating the Data access objects (DAOs) of the OAMP server on a standalone Avaya SBC installation, you must restart the IPCS services. The DAOs that require a restart include the Radius server, license manager, and SNMP profile configurations.

Procedure

1. Log in to the EMS CLI interface as an administrator.
2. Run the following command: `/etc/init.d/ipcs-init restart`

   Avaya SBC restarts the IPCS services.

Acquiring WebLM license on Avaya SBC

About this task

If Avaya SBC fails to acquire license from System Manager, you must enable license acquisition from WebLM on System Manager.

Before you begin

Download the System Manager pem file from the System Manager security page.

Procedure

1. Log in to the EMS CLI interface.

2. Copy the pem file to the `/home/ipcs` directory.
3. Type `keytool -import -trustcacerts -alias tomcat -file /home/ipcs/<your_CA_file> -keystore /usr/local/weblm/etc/trusted_weblm_certs.jks`
4. Type the keystore password.

   Note:

   You can get the current password by running the following command: `grep trustStorePassword /usr/local/weblm/etc/trustedcert.properties`
5. Type `/etc/init.d/ipcs-ems stop`
6. Type `/etc/init.d/ipcs-ems start`
7. Refresh the license.

Connecting Avaya SBC with an external WebLM server

About this task

Use the following procedure to connect Avaya SBC with an external WebLM server when external WebLM server's Root CA certificate is not included in the Avaya SBC `trusted_WebLM_certs.jks` keystore.

Procedure

1. Export the external WebLM server Root CA certificate.
2. Import the external WebLM server Root CA certificate into the Avaya SBC trusted_WebLM_certs.jks keystore.

Swapping a separate Avaya SBC server deployed under EMS

Before you begin

Confirm that you have created and saved the backup file of a functional Avaya SBC device.

Confirm that both Avaya SBC devices have the same software version before you start the swap procedure.

Confirm that all Avaya SBC devices involved in the swap procedures are in the commissioned state after the swap is complete.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. Install a new Avaya SBC with a different IP address. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.
5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
6. When the state of the newly added Avaya SBC device becomes Registered, click **Swap Device**.
7. Select the backup file of old Avaya SBC system (down system).

   Important:

   The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.
8. Click **Finish.**

   The EMS server does not display the old Avaya SBC device in the **Devices** tab.

Swapping Avaya SBC devices in an HA pair deployment

Before you begin

Confirm that one of the Avaya SBC devices in the HA pair is non-functional.

Confirm that both Avaya SBC devices have the same software version before you start the swap procedure.

Confirm that all Avaya SBC devices involved in the swap procedures are in the commissioned state after the swap is complete.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. Install a new Avaya SBC with different IP address.

For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

5. In the **Devices** section, do the following:
   a. Click **Add**.
   b. In the **Hostname** and **Management IP** fields, provide the relevant information.
6. When the state of the newly added Avaya SBC device becomes Registered, click **Swap Device**.
7. Select the IP address of the down Avaya SBC system in the HA pair.
8. Click **Finish.**

   The EMS server does not display the old Avaya SBC device in the **Devices** tab.

Swapping an EMS server in a single server deployment

Before you begin

Confirm that you have created and saved the backup file of a functional EMS server.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. When the state of the EMS becomes Commissioned, click **Swap Device**.

   Note:

   The EMS server displays the **Swap Device** option only when there is no SBC device installed on the system.
5. Select the backup file of old EMS device.

   Important:

   The backup file is a master .tar file. Avaya recommends not to unzip the .tar file.
6. Click **Finish** to complete the EMS swap.

Swapping a primary EMS server in an HA pair deployment

Before you begin

Confirm that the primary EMS server is non functional.

Confirm that both EMS devices have the same software version before you start the swap procedure.

The IP addresses of the old and the new EMS must be different.

Procedure

1. Log in to the newly installed EMS web interface with the administrator credentials.
2. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
3. On the Device Management page, click **Devices** tab.
4. When the state of the newly installed primary EMS becomes commissioned, click **Swap Device**.

   Note:

   The newly installed EMS server displays the **Swap Device** option only when there is no SBC device installed on the system.
5. Provide the IP address for the secondary EMS server.
6. Click **Finish** to complete the EMS swap.

Swapping a secondary EMS server in an HA pair deployment

Before you begin

Confirm that both EMS devices have the same software version before you start the swap procedure.

Procedure

1. Log in to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click **Devices** tab.
5. Click **Uninstall** corresponding to the secondary EMS from the primary EMS web interface.

The EMS server displays a confirmation pop-up to confirm your selection.

6. Click **OK**.
7. Deploy and configure a new EMS as secondary EMS. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*.

   Secondary EMS is automatically added until Release 10.1. From Release 10.1.2 onwards, users must add the secondary EMS from primary EMS Device Management on GUI.
8. On the Device Management page, click **Devices** tab.
9. Click **Restart Application** corresponding to all the EMS connected servers.

   The EMS server displays a confirmation pop-up.
10. Click **OK** to confirm.

Result

Secondary EMS will be added in the Devices section.

Deleting a device configuration

About this task

Caution:

Deleting a device configuration permanently deletes all configuration data for the device. Ensure that you have a snapshot of the configuration data if you need to reinstall the device.

Procedure

1. Log on to the EMS web interface with the administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Device Management**.

   The EMS server displays the Device Management screen in the content area.
4. On the Device Management page, click the **Devices** tab.
5. Click **Uninstall**, corresponding to the Avaya SBC security device to uninstall.

   The EMS server displays a confirmation pop-up to confirm your selection.
6. Click **OK**.

   The EMS server removes the Avaya SBC device from the list.

Reconfiguration command options

The **sbceconfigurator.py** command is used for many system-level reconfiguration tasks. This table summarizes the options available when reconfiguring your system.

Caution:

When using the **sbceconfigurator.py** command, you must use only the command options shown in this table. Do not use any other command options.

Description	Usage examples
The `change-dns-ip-fqdn` option changes the DNS configuration. When using this command, you must enter the DNS IP address, and you can optionally include the DNS FQDN (shown as *[FQDN]* in the examples). Depending on whether you have just a single server or both primary and secondary servers, you can use the command to make the following changes: • Change primary only – first two methods shown in the examples • Change primary and secondary • Change secondary only • Remove secondary – used when you have both a primary and secondary and you only want to retain the primary system	**sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN],Current Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *New Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *Current Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]* **sbceconfigurator.py change-dns-ip-fqdn** *Current Primary DNS IP Address [FQDN]*
The `change-ems-ip` option does the following: • Changes the primary or active EMS IP address on the secondary or standby EMS. • Changes the secondary or standby EMS IP address on the primary or active EMS and all the SBC servers connected to EMS. • Changes the primary or active EMS IP address on the connected SBC servers, which were not reachable while changing the primary or active EMS IP address.	**sbceconfigurator.py change-ems-ip** *Old EMS IP Address New EMS IP Address*
The `change-hostname` option changes the host name.	**sbceconfigurator.py change-hostname** *HOSTNAME*
The `change-ip-gw-mask` option changes the management IP address, gateway, and subnet mask.	**sbceconfigurator.py change-ip-gw-mask** *Management IP Address Gateway IP Address Subnet Mask*
The `change-ntp-ip` option changes the NTP IP address.	**sbceconfigurator.py change-ntp-ip** *New NTP IP Address <yes/no> <<if yes provide PASSWORD>*

Table continues…

Description	Usage examples
The `change-nw-passphrase` option changes the network passphrase.	**`sbceconfigurator.py change-nw-passphrase`** *Passphrase*
The `change-sbce-ip` option changes the SBC IP address on the EMS database. Use the following steps to use this command: 1. Change the management IP address, gateway, mask on the SBC server by using the **`change-ip-gw-mask`** option 2. Run the **`change-sbce-ip`** option on the EMS CLI to notify the EMS about the SBC IP change.	**`sbceconfigurator.py change-sbce-ip`** *Old SBC IP Address New SBC IP Address*
The `change-ssl-certs yes` option changes the self-signed certificate for EMS and single SBC servers. This is an interactive command that steps you through changing the self-signed certificate. The command prompts you for the following information: • First and Last Name: [Default=] • Organizational Unit: [Default=] • Organization: [Default=] • City or Locality: [Default=] • State or Province: [Default=] • Country Code (2 letter code): [Default=]	**`sbceconfigurator.py change-ssl-certs yes`**
The `view-timezone` option displays the administered time zones. This is an interactive command that steps you through viewing a time zone.	**`sbceconfigurator.py view-timezone`**
The `change-timezone` option assigns a new time zone. This is an interactive command that steps you through selecting a time zone. The command prompts you for the following information: • Location • Country • Time Zone	**`sbceconfigurator.py change-timezone`**
The `gen-system-ssh-keys` option generates system SSH keys.	**`sbceconfigurator.py gen-system-ssh-keys`**

Table continues…

Description	Usage examples
The `exchange-ems-keys` option exchanges the SSH keys. Use this command to copy SSH keys from the primary (or secondary, if present) EMS to SBC. Do this to ensure proper function of passwordless SSH between servers.	**`sbceconfigurator.py exchange-ems-keys`**
The `factory-reset` option resets the system to the factory default state. Use the following procedure: 1. To uninstall the SBC device in a multiple server deployment from GUI, click **Device Management** > **Devices** and click **Uninstall**. This operation clears the device-specific configuration and is not required on EMS and a single server deployment. 2. Run `sbceconfigurator.py factory-reset`. This operation clears the device-specific configuration on EMS or a single server deployment. **Important:** Run this command from either a serial console or VGA session. Do not run this command from an SSH putty session since network connectivity will be lost during this operation.	**`sbceconfigurator.py factory-reset`**

Table continues…

Description	Usage examples
The `re-configure` option moves Avaya SBC from one EMS to other EMS. The option does the following: 1. Convert SingleBox deployment to Seperate Box deployment and added to EMS. Usage example: **`sbceconfigurator.py re-configure`** 2. Move Separate Box deployment from one EMS to other EMS. Usage example: **`sbceconfigurator.py re-configure`** 3. Move HA Pair deployment from one EMS to other EMS. Usage example: **`sbceconfigurator.py re-configure`** **Note:** Ensure to run **`sbceconfigurator.py re-configure`** command on the PEER Avaya SBC once the first Avaya SBC comes back up after re-configure.	**`sbceconfigurator.py re-configure`**
The **`join-ha`** option converts Separate Avaya SBC to HA by adding another Avaya SBC device. Use the following procedure: 1. Deploy new Avaya SBC and add to the EMS. 2. Make the new Avaya SBC into Registered state. 3. Run the **`sbceconfigurator.py join-ha`** command from new Avaya SBC cli. Command usage: **`sbceconfigurator.py join-ha`**	**`sbceconfigurator.py join-ha`**

Table continues…

Description	Usage examples
`generate-rest-credentials` option is used to create the rest credentials. This command is supported from Release 10.1.2. • If you run the command in EMS, it will generate the rest credentials for all Avaya SBC associated with it and other EMS incase of active active EMS. • If you run the command in HA setup, it will generate the rest credentials for other box in Pair: EMS and secondary EMS if configured. • If you run the command in separate box, it will generate the rest credentials for EMS and Secondary EMS. • Single Box (EMS+SBC) is not supported.	**`sbceconfigurator.py generate-rest-credentials`**

Changing the management IP from the EMS web interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Device Management**.
3. Find the device whose IP address you want to change, and click **Edit**.
4. In the **Management IP** field, type the new management IP, and click **Finish**.
5. **(Optional)** Find the Avaya SBC device on the Device Management page, and click **Restart Application**.
6. **(Optional)** If you change the management IP address of the EMS, restart each Avaya SBC connected to the EMS.

Changing management IP, gateway and network mask details for a single server deployment

Procedure

1. Log in to the server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The server restarts indicating that the management IP has been changed successfully.

Changing the management IP for an HA deployment

Changing management IP, gateway IP, and network mask details on primary EMS

Use the following command to change management IP, gateway, and network mask details on the primary EMS server.

```
sbceconfigurator.py change-ip-gw-mask <MGMT_IP> <GW_IP> <NW_MASK>
```

The script does the following:

1. Checks if the database is functional.
2. If the database is functional, proceeds with stopping application processes.
3. Checks if all the Avaya SBC servers connected to EMS are reachable. If any Avaya SBC server is unreachable, exits or proceeds with changing the EMS IP address on the reachable Avaya SBC servers. Later, when the devices are reachable from EMS, users can regenerate or change the EMS IP addresses on the devices.
4. Prints out the log messages, which shows the current status on screen.
5. The EMS server then reboots. The user needs to ssh using the new EMS IP address.
6. EMS generates certificates automatically and sends it to all Avaya SBCs.

Change in management IP requires a change in the NTP address configuration on all Avaya SBC servers connected to EMS.

Note:

All Avaya SBC servers must have the changed EMS IP address.

Related links

Changing primary EMS IP on unreachable Avaya SBC on page 22
Changing the NTP IP address on Avaya SBC on page 23
Changing IP address of the primary EMS server on the secondary EMS server on page 23

Changing primary EMS IP on unreachable Avaya SBC

About this task

Use this procedure only when Avaya SBC is unreachable while changing the primary EMS IP address.

Procedure

1. Log in the EMS web interface as a super user.
2. Type **sbceconfigurator.py change-ems-ip** <*EMS_OLD_IP*> <*EMS_NEW_IP*> and press `Enter`.

Changing the NTP IP address on Avaya SBC

About this task

Changing the management IP address of EMS requires a change in the NTP IP address configuration on the Avaya SBC devices connected to EMS. For proper functioning of OpenVPN, ensure that the date and time on the Avaya SBC devices match those on the EMS device. Avaya recommends configuring the EMS IP address as the NTP IP address of the Avaya SBC devices.

Before you begin

If you plan to use the system password while running the command, ensure to have it ready.

Procedure

1. Log in to the Avaya SBC device as a super user.
2. Enter the following command:

   `sbceconfigurator.py change-ntp-ip` *NewNTPIPAddress <yes/no> <if yes provide PASSWORD>*

   Where:

   - *NewNTPIPAddress* is the new NTP IP address.
   - *<yes/no> <if yes provide PASSWORD>* is either **`yes`** or **`no`**. If you type **`yes`**, you must enter the system password after running the command.

Example

```
INFO : Changing NTP Server IP..
INFO : Make sure your Date and Time matches EMS...
INFO : Updating NTP IP address IPV4 in sysinfo file...
INFO : Updating NTP Config File..
sh /usr/local/ipcs/icu3/scripts/setNTPAuth.sh 10.81.21.18 no
INFO : Restarting NTP Server..
Restarting ntp server
INFO : Syncing NTP time..
Connecting to NTP Server 10.81.21.18 to synchronize time
NTP Server Sync is successful
INFO : Sync Time To HWClock.
```

Changing IP address of the primary EMS server on the secondary EMS server

Procedure

1. Log on to the EMS device as a super user.
2. Type `sbceconfigurator.py change-ems-ip` *EMS_old_IP EMS_new_IP* and press `Enter`.

Changing management IP, gateway IP, and network mask details on secondary EMS

Procedure

1. Log on to the Avaya SBC server as a super user.

2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBC restarts indicating a successful completion of the management IP change. After changing the management IP, the primary EMS and Avaya SBC devices must be notified about the new Avaya SBC IP address of the secondary EMS.
3. Log on to the primary EMS and Avaya SBC devices as a super user.
4. Type `sbceconfigurator.py change—ems-ip` *Old_EMS_IP New_EMS_IP*.

   The system changes the IP address of the secondary EMS.

   Note:

   Ensure that you change the IP address of the secondary EMS in the primary EMS and each Avaya SBC device.

Changing management IP, gateway IP, and network mask details on Avaya SBC

Procedure

1. Log on to the Avaya SBC server as a super user.
2. Type `sbceconfigurator.py change-ip-gw-mask <Management IP> <Gateway IP> <Network Mask>`.

   The Avaya SBC restarts indicating successful completion of the management IP change. After changing the management IP, the EMS must be notified about the new Avaya SBC IP address.
3. Log on to the EMS server as a super user.
4. Type `sbceconfigurator.py change—sbce-ip` *Old_SBCE_IP New_SBCE_IP*.

   The system changes the IP address of the Avaya SBC in the EMS database.

Changing hostname

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Type `sbceconfigurator.py change-hostname Hostname`.
3. Restart the system.

   For the hostname change to take effect, you must perform a soft reboot of the Avaya SBC.

Changing network passphrase

About this task

Network passphrase is important for EMS-Avaya SBC authentication. If you change the network password for an Avaya SBC, ensure that you change the passphrase on all systems connected to the Avaya SBC.

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Type `sbceconfigurator.py change-nw—passphrase` *`New Passphrase`*.

   The server restarts for enabling the new passphrase. The server is either the EMS or its connected SBC's where the command is executed.

Regenerating self-signed certificates

Procedure

1. Log in to the CLI with administrator credentials.
2. Run the following command:

   `sbceconfigurator.py change-ssl-certs yes`

Regenerating the rest credentials

About this task

External cases like certificate sync and upgrade package copy, and system tasks like application restart and reboot the system, might not work from GUI due to the rest credentials issues. In such cases, run the `generate-rest-credentials` command.

Procedure

1. Log in to the Avaya SBC or EMS CLI using administrative privileges.
2. Run the command: `sbceconfigurator.py generate-rest-credentials`
   - If you run the command in EMS, it will generate the rest credentials for all Avaya SBC associated with it and other EMS incase of active active EMS.
   - If you run the command in HA setup, it will generate the rest credentials for other box in Pair: EMS and secondary EMS if configured.
   - If you run the command on separate box, it will generate the rest credentials for EMS and Secondary EMS.

- Single Box (EMS+SBC) is not supported.

Note:

The `sbceconfigurator.py generate-rest-credentials` command is supported from Release 10.1.2.

Changing DNS IP and FQDN

About this task

The `change-dns-ip-fqdn` option changes the DNS configuration. When using this command, you must enter the DNS IP address, and you can optionally include the DNS FQDN (shown as *[FQDN]* in the examples). Depending on whether you have just a single server or both primary and secondary servers, you can use the command to make the following changes:

- Change primary only – first two methods shown in the examples
- Change primary and secondary
- Change secondary only
- Remove secondary – used when you have both a primary and secondary and you only want to retain the primary system

Procedure

1. Log in to the Avaya SBC CLI using administrative privileges.
2. Enter any of the following command options depending on which IP address or FQDN you want to change:.
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN],Current Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *New Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *Current Primary DNS IP Address [FQDN],New Secondary DNS IP Address [FQDN]*
   - **`sbceconfigurator.py change-dns-ip-fqdn`** *Current Primary DNS IP Address [FQDN]*

   The EMS server changes the DNS IP address and optionally, the FQDN.

Determining whether Avaya SBC is installed on KVM

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, enter the following command:

   `virt-manager`

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. To view all the KVM guests installed on the KVM host server use the **`virsh list- —all`** command.

   This command displays the Id, Name and State of all the KVM guests running on the KVM server.

Determining whether Avaya SBC is installed on VMware

Procedure

1. Log in as a root user to get root privileges.
2. Type `dmidecode | grep 'VMware'.`

   If Avaya SBC is installed on VMware, the system displays `Product Name: VMware`.

   If Avaya SBC is installed on any other server, the system does not display any data.

Viewing the job history of Avaya Aura® Appliance Virtualization Platform virtual machine operations

Procedure

1. Do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. In the lower pane, click **Job History**.
3. On the Job History page, in **Operation**, select one or more operations.
4. Click **Submit**.

   The page displays the details of jobs that you selected.

Related links

Job History field descriptions on page 28

Job History field descriptions

Name/Button	Description
Operation	The operation that is performed on a virtual machine. You can select one or more operations that are performed on a virtual machine, such as host restart, virtual machine deployment, and patch installation.
Submit	Provides details of jobs that you selected.

History

Name	Description
Job ID	The unique name of the virtual machine management job.
IP/FQDN	The IP address or host name of the virtual machine or the host where the operation is performed.
Operation	The operation performed on the virtual machine or host. For example, host refresh, virtual machine deployment, and patch installation.
Status	The status of the job.
Start Time	The start time of the job.
End Time	The end time of the job.

Related links

Viewing the job history of Avaya Aura Appliance Virtualization Platform virtual machine operations on page 27

Monitoring an Avaya Aura® Appliance Virtualization Platform system

Procedure

1. Do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Platforms**.
3. On the Monitor Hosts page, do the following:
   a. In **Hosts**, click a host.
   b. Click **Generate Graph**.

The system displays the graph regarding the CPU/memory usage of the host that you selected.

Monitoring an Avaya Aura® Appliance Virtualization Platform application

Procedure

1. Do one of the following:
   - On the System Manager web console, click **Services** > **Solution Deployment Manager** > **Application Management**.
2. Click **Monitor Applications**.
3. In the Monitor VMs page, do the following:
   a. In **Hosts**, click a host.
   b. In **Virtual machines**, click a virtual machine on the host that you selected.
4. Click **Generate Graph**.

   The system displays the graph regarding the CPU/memory usage of the virtual machine that you selected.

Deleting the virtual machine snapshot from the Avaya Aura® Appliance Virtualization Platform host

Procedure

1. In the Web browser, type the following URL: `https://<AVP IP Address or FQDN>/ui`
2. To log in to the Appliance Virtualization Platform host, provide the credentials.
3. In the left navigation pane, click **Virtual Machines**.
4. Select the virtual machine, click **Actions** > **Snapshots** > **Manage snapshots**.

   The system displays the Manage snapshots - <Virtual machine name> dialog box.
5. Select the snapshot and click **Delete snapshot**.

   The system deletes the selected snapshot.

Hardware FRUs

The following table lists the hardware field replaceable units (FRUs) for the following Avaya-provided servers:

- Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3
- Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5

	Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 3	**Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server - Profile 5**
Server	700514161	700514163
Power supply	700514176	700514176
Fan	700514177	700514177
Disk drive	700514178	700514178
1 GB 4-port NIC	700514180	700514180
1 GB 2-port NIC	700514181	NA
10 GB 2-port NIC	NA	700514182
DVD drive	700514183	700514183
RAID card	700514184	700514184
RAID battery	700514186	700514186
8 GB Memory module	700514187	NA
16 GB Memory module	NA	700514188

Chapter 3: Configuration change procedures

About making configuration changes

This chapter describes how you can make changes to the current EMS and SBC configuration of a deployment. For example, one of the procedures shows you how you can convert a standalone server that has the EMS and SBC functionality into a dedicated SBC server that you will then associate with a dedicated EMS server.

Caution:

Configuration changes are service affecting. Do these procedures during a planned maintenance window when there is no traffic on the system. Inform all users that calls cannot be placed during this time frame, and that any active calls will be dropped.

Converting a standalone EMS and SBC to a dedicated SBC

About this task

Caution:

Configuration changes are service affecting. Do these procedures during a planned maintenance window when there is no traffic on the system. Inform all users that calls cannot be placed during this time frame, and that any active calls will be dropped.

Before you begin

Collect the following information:

- IPv4 IP address of the EMS server
- Network Passphrase

  This was the passphrase used when the system was first deployed. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*, *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*, or *Deploying Avaya Session Border Controller on an Avaya Aura® Appliance Virtualization Platform*.
- (Optional) - IPv4 IP address of the system NTP server
- (Optional) - IPv6 address of the EMS server

Take a backup of your system.

Procedure

1. Log in to the CLI with administrator credentials.
2. Enter the following command:

   `sbceconfigurator.py re-configure` *<EMS_IP> <Network_Passphrase> [<NTP_IP> <V6_EMS_IP>]*

   Where:

   - *<EMS_IP>* is the IPv4 IP address of the EMS server
   - *<Network_Passphrase>*
   - *<NTP_IP>* is optional, the IPv4 IP address of the deployment NTP server
   - *<V6_EMS_IP>* is optional, the IPv6 IP address of the EMS server

   If the conversion is successful, you will see a message similar to the following example and the system reboots:

   ```
   Rebooting the system for changes to take effect
   SBCE Re-configure Successful. Check the IPCS CM log for more information..
   ```

   If the system does not reboot and you see error messages on the screen, contact Avaya support.

   Important:

   If the EMS is unreachable, or if the EMS version does not match the SBC version, the command stops and no changes are made.

Next steps

After the SBC reboots and processes restart, if the SBC is not shown as **Commissioned** under **Device Management** > **Devices**, restart the processes on the SBC using the following command:

`/etc/init.d/ipcs-init restart`

For EMS to manage the license on the new SBC, navigate to **Device Management** > **Licensing** and update the license.

Moving an SBC from one EMS to another EMS

About this task

Caution:

Configuration changes are service affecting. Do these procedures during a planned maintenance window when there is no traffic on the system. Inform all users that calls cannot be placed during this time frame, and that any active calls will be dropped.

Before you begin

Collect the following information:

- IPv4 IP address of the EMS server
- (Optional) Network Passphrase

  This was the passphrase used when the system was first deployed. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*, *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*, or *Deploying Avaya Session Border Controller on an Avaya Aura® Appliance Virtualization Platform*.
- (Optional) - IPv4 IP address of the system NTP server
- (Optional) - IPv6 address of the EMS server

Confirm that the EMS IP address can be pinged from the SBC network.

Take a backup of your system.

Procedure

1. Log in to the CLI with administrator credentials.
2. Enter the following command:

   `sbceconfigurator.py re-configure` *<EMS_IP> [<Network_Passphrase> <NTP_IP> <V6_EMS_IP>]*

   Where:

   - *<EMS_IP>* is the IPv4 IP address of the EMS server
   - (Optional) *<Network_Passphrase>* is optional, the network passphrase
   - (Optional) *<NTP_IP>* is optional, the IPv4 IP address of the deployment NTP server
   - (Optional) *<V6_EMS_IP>* is optional, the IPv6 IP address of the EMS server

   If the conversion is successful, you will see a message similar to the following example and the system reboots:

   ```
   Rebooting the system for changes to take effect
   SBCE Re-configure Successful. Check the IPCS CM log for more information..
   ```

   If the system does not reboot and you see error messages on the screen, contact Avaya support.

   Important:

   If the EMS is unreachable, or if the EMS version does not match the SBC version, the command stops and no changes are made.

Next steps

After the SBC reboots and processes restart, if the SBC is not shown as **Commissioned** under **Device Management** > **Devices**, restart the processes on the SBC using the following command:

`/etc/init.d/ipcs-init restart`

For EMS to manage the license on the new SBC, navigate to **Device Management** > **Licensing** and update the license.

Moving an HA SBC from one EMS to another EMS

About this task

Caution:

Configuration changes are service affecting. Do these procedures during a planned maintenance window when there is no traffic on the system. Inform all users that calls cannot be placed during this time frame, and that any active calls will be dropped.

Before you begin

Collect the following information:

- IPv4 IP address of the EMS server
- (Optional) Network Passphrase

  This was the passphrase used when the system was first deployed. For more information, see *Deploying Avaya Session Border Controller on a Hardware Platform*, *Deploying Avaya Session Border Controller on a Virtualized Environment Platform*, or *Deploying Avaya Session Border Controller on an Avaya Aura® Appliance Virtualization Platform*.
- (Optional) - IPv4 IP address of the system NTP server
- (Optional) - IPv6 address of the EMS server

Confirm that the EMS IP address can be pinged from the SBC network.

Take a backup of your system.

Procedure

1. Log in to the CLI with administrator credentials.
2. Enter the following command:

   `sbceconfigurator.py re-configure` *<EMS_IP> [<Network_Passphrase> <NTP_IP> <V6_EMS_IP>]*

   Where:

   - *<EMS_IP>* is the IPv4 IP address of the EMS server
   - (Optional) *<Network_Passphrase>* is optional, the network passphrase
   - (Optional) *<NTP_IP>* is optional, the IPv4 IP address of the deployment NTP server
   - (Optional) *<V6_EMS_IP>* is optional, the IPv6 IP address of the EMS server

   If the conversion is successful, you will see a message similar to the following example and the system reboots:

   ```
   Rebooting the system for changes to take effect
   SBCE Re-configure Successful. Check the IPCS CM log for more information..
   ```

   If the system does not reboot and you see error messages on the screen, contact Avaya support.

Important:

If the EMS is unreachable, or if the EMS version does not match the SBC version, the command stops and no changes are made.

3. After the system reboots and processes successfully restart on current SBC , repeat these steps on the other SBC in the HA pair.

Note:

After the second SBC reboots and processes restart, if the HA pair are not shown as **Primary / Secondary** under **Device Management** > **Devices**, restart the processes on both servers using the following command:

```
/etc/init.d/ipcs-init restart
```

Next steps

For EMS to manage the license on the new SBC pair, navigate to **Device Management** > **Licensing** and update the license.

Converting a single commissioned SBC into an HA deployment

About this task

Use this procedure to convert a dedicated SBC in the Commissioned state to an HA deployment by joining the Commissioned SBC with another SBC that is in the Registered state. Both SBCs will be within the same EMS.

Caution:

Configuration changes are service affecting. Do these procedures during a planned maintenance window when there is no traffic on the system. Inform all users that calls cannot be placed during this time frame, and that any active calls will be dropped.

Before you begin

Collect the IPv4 IP address of the Commissioned SBC server to which you want to join as an HA deployment.

Confirm that the SBC you want to join in an HA deployment is in the Commissioned state and that the existing SBC is in the Registered state.

Take a backup of your system.

Procedure

1. Log on to the CLI of the SBC that is in the Registered state with administrator credentials.
2. Enter the following command:

   `sbceconfigurator.py join-ha` <*PEER_HA_IP*>

Where <*PEER_HA_IP*> is the IPv4 IP address of the SBC server that is in the Commissioned state.

You will see the message `Successfully joined HA Pair` and processes are restarted on the current SBC.

If you see error messages on the screen, contact Avaya support.

3. Once processes come up on the current SBC, restart the processes on the peer Commissioned SBC so that the HA state comes up properly. Use the following command:

   `/etc/init.d/ipcs-init restart`

Removing an SBC or EMS from VMware

Procedure

1. Locate the SBC or EMS.
2. Right-click the SBC or EMS.
3. Click **Power** > **Power Off**.
4. When the system displays a dialog box for confirmation, click **Yes**.
5. Right-click the SBC or EMS, and click **Delete from Disk**.
6. When the system displays a dialog box for confirmation, click **Yes**.

Removing an SBC or EMS from KVM

Procedure

1. Log in to the KVM host with root permissions.
2. At the console, enter the following command:

   `virt-manager`

   The system displays the Virtual Machine Manager GUI.
3. Type `2` for CLI mode.
4. Stop the virtual machine using the **`virsh destroy VM_NAME`** command.
5. To delete the virtual machine from KVM use the **`virsh undefine VM_NAME`** command:

   #virsh undefine <Name of the KVM Guest Machine>

Migrating to VMware

Cloned and copied OVAs are not supported

To redeploy a virtual machine, do *not* create a copy of the virtual machine or clone the virtual machine. These processes have subtle technical details that require a thorough understanding of the effects of these approaches. To avoid any complexities and unexpected behavior, deploy a new OVA. At this time, Avaya only supports the deployment of new OVAs.

Migrating from a hardware platform to a VMware platform

About this task

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the **Device** menu, click **EMS** for creating a snapshot for the EMS device or **SBC** for a device-specific snapshot configuration.
3. Navigate to **Backup/Restore**.
4. Click the **Snapshots** tab.
5. Select the designated shapshot server.
6. Click **Create Snapshot**.

   The EMS device displays the Create Snapshot window.
7. Enter a name for the snapshot.
8. Click **Create**.
9. Select the snapshot file that you created, and click **Download**.

   Save the snapshot file for Avaya SBC deployed on the physical server. You can then use this snapshot to restore the same configurations to VMware.
10. Turn off the power to the server on which EMS is deployed.
11. Deploy the EMS or the SBC OVA file on VMware with the same build number and management IP as on the physical server.

    After the EMS or SBC deployed on VMware is up, you can restore the snapshot you saved from the physical server.

Chapter 4: Troubleshooting procedures

Installation problems

Avaya SBC takes a long time to install on AWS

Condition

After you click **Launch instances**, Avaya SBC takes a long time to install.

During installation, the instance is unreachable through RDP for Windows and SSH for Linux. Therefore, investigating the issue might be difficult. To counter this, Amazon Web Services provides instance screenshots and system logs for visibility of the current state of the instance during installation.

Solution

1. Select the instance and right-click.
2. To view the instance screenshot, click **Instance Settings** > **Get Instance Screenshot**.
3. To view the system logs, click **Instance Settings** > **Get System Log**.

System reachability checks do not pass

Condition

System reachability checks do not pass. Therefore, screenshots do not provide sufficient information to investigate and correct the issue.

Solution

Do one of the following:

- Detach the volume and attach it to another virtual machine. Then, go through the logs to troubleshoot.
- Remove interfaces from all the instances. Reboot and log in by using new root password and port number 222 to investigate and troubleshoot.

Related links

Detaching the volume from AWS on page 39
Attaching the volume to a virtual machine for AWS on page 39

Detaching the volume from AWS

Before you begin

Unmount the device by using the following command:

```
[ec2-user~] umount -d /dev/sda1
```

Procedure

1. Sign in to the Amazon Web Services Management console at:

   https://console.aws.amazon.com/ec2/

2. Navigate to **Services** > **Compute** > **EC2**.

   The system displays the EC2 Management Console page.

3. Select a volume, click **Actions** > **Detach Volume**.

4. In the confirmation dialogue box, click **Yes, Detanch**.

   AWS detaches the specified volume.

Next steps

Attach the volume to another virtual machine.

Attaching the volume to a virtual machine for AWS

About this task

Use the following procedure to attach the volume to another virtual machine for troubleshooting after detaching it from AWS.

Before you begin

Attach the volume to the instance which is available in the same zone.

Procedure

1. Sign in to the Amazon Web Services Management console at:

   https://console.aws.amazon.com/ec2/

2. Navigate to **Services** > **Compute** > **EC2**.

   The system displays the EC2 Management Console page.

3. Select a volume, click **Actions** > **Attach Volume**.

4. In the **Attach Volume** dialog box, type the name of the instance to attach the instance to the volume.

5. Click **Attach**.

Next steps

Troubleshoot the machine.

Networking problems

Network configuration checklist

Use this checklist while troubleshooting network configurations.

Task	Description	✔
Create a site network map.	Identifies where each device is physically located on your site. Use the map to systematically search each part of your network for problems.	
Identify logical connections.		
Document device configurations.	Maintain online and paper copies of device configuration information.	
Store passwords in a safe place.	Keep records of your previous passwords if you must restore a device to a previous software version and need to use the old password that was valid for that version.	
Create a device inventory checklist.	List all devices and relevant information for the network including device type, MAC addresses, ports, and attached devices.	
Create an IP address and port number list.	List the IP addresses and port numbers of all devices.	
Maintain a change control system.		
Create a support contact list.	Store details for support contracts, support numbers, engineering details, telephone and fax numbers.	

Verifying integration configuration

You can verify the operational status of the EMS by either attempting to access the EMS server using the web interface or by establishing a CLI session via a secure shell session (SSH) and manually checking the status of various internal processes.

Logging on to the EMS web interface

Procedure

1. Open a new browser tab or window.
2. Type the following URL:

   ```
   https://<Avaya EMS IP address>
   ```

3. Press **Enter**.

   The system displays a message indicating that the security certificate is not trusted.

4. Accept the system message and continue to the next screen.

If the Welcome screen is displayed, the EMS is operating normally and available for use. You can log in to EMS and perform normal administrative and operational tasks. See *Administering Avaya Session Border Controller for Enterprise*.

5. Type the username and password as `ucsec`.

   On first login, system prompts you to change the password.

6. Enter a new password and login with the new password.

Logging in to EMS through console

To log in to EMS through a console, use the VGA connection.

Accessing Avaya SBC or EMS device using VGA connection

Before you begin

- Ensure that you connect the monitor to EMS through a VGA cable.
- Ensure that you connect a keyboard to EMS.

Procedure

1. Press `Enter` to establish a communication connection.
2. Enter your username and password, and press `Enter`.

Logging in to the EMS using SSH

Procedure

1. Log in to SSH client using PuTTy.
2. Type the IP address for Avaya SBC.
3. Specify the port as **22** or **222**.
4. Select the connection type as SSH and press `Enter`.
5. Enter the user name and password to log in.

   Note:

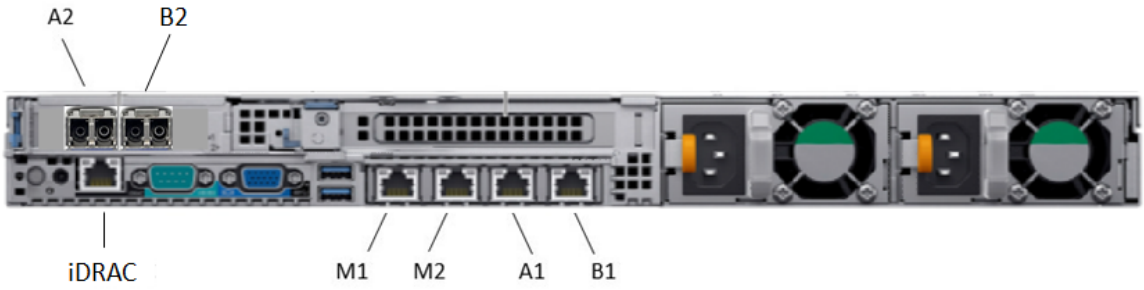
   You cannot gain access to shell with user account `ucsec`.

   User account `ipcs` or user accounts that have shell access can be used for logging in to Avaya SBC.

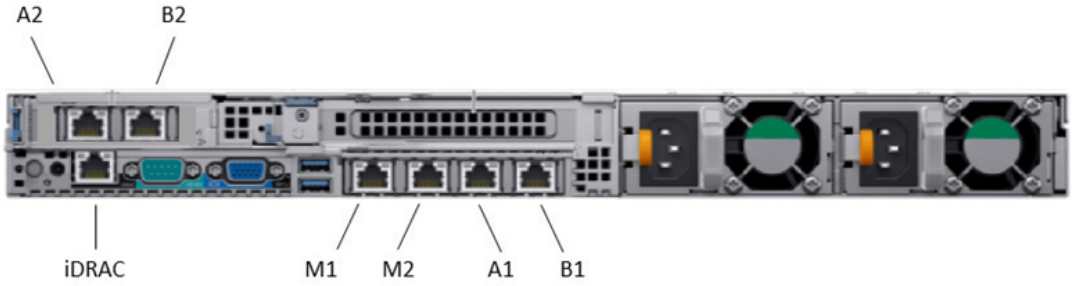
Back panel Ethernet port labeling

Dell PowerEdge R640 Avaya Solutions Platform 110 Appliance Ethernet port labeling

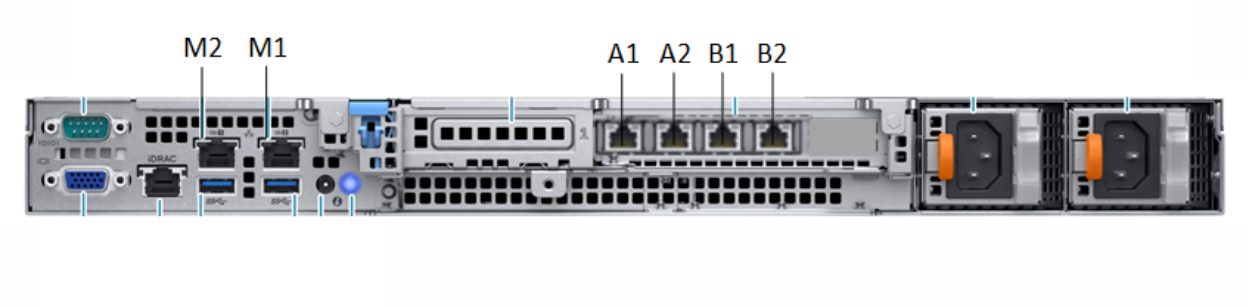
Profile 5 port labeling



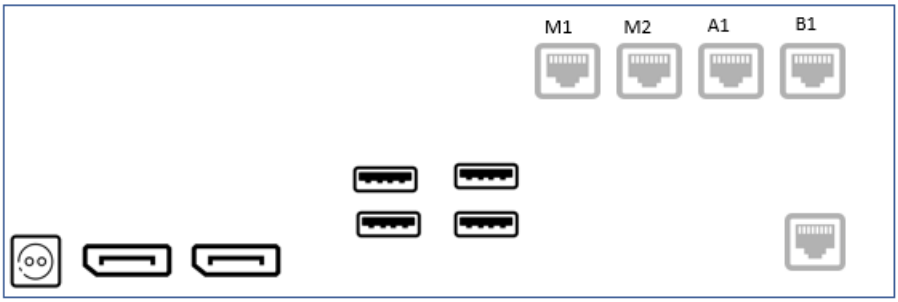
Profile 3 port labeling



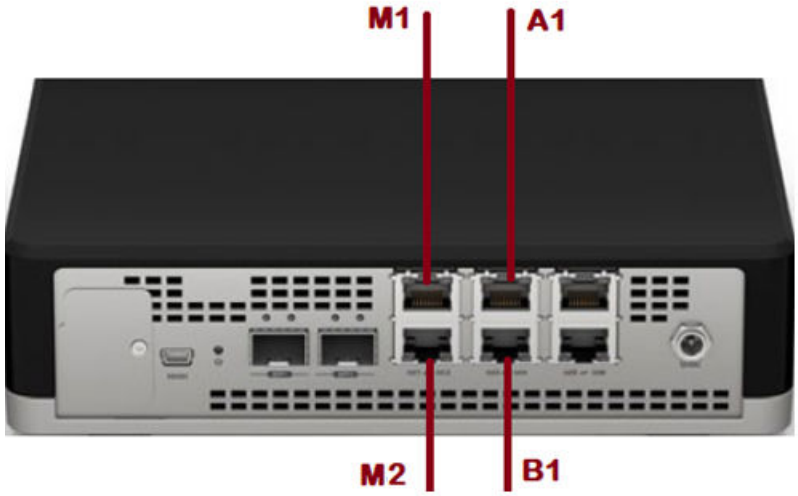
Dell R340 Avaya Solutions Platform 110 Appliance Ethernet port labeling



Dell 3240 Ethernet port labeling



Dell VEP1425N Ethernet port labeling



Loss of audio and active call drops during HA failover

During high availability failover, you might notice loss of audio or active call drops. This issue can occur if the internal IP of Avaya SBC and the internal Avaya Aura® core are on the same subnet. To resolve this issue, move the internal IP of Avaya SBC to a different subnet. For more information, see the Configuring High Availability section in *Administering Avaya Session Border Controller*.

Unable to PING gateways during high call traffic conditions

Condition

The Avaya SBC network interface gateways are not responding to PING commands issued during high call traffic. PING commands from the command line nor the administration GUI return any results. This occurs when doing Internet Control Message Protocol (ICMP) monitoring from the customer Network Management System (NMS).

Cause

ICMP traffic receives low priority based on other traffic on Avaya SBC. The Avaya SBC firewall limits the traffic based on priority. Because of this designed set of priorities, ICMP responses are rate limited. On data interfaces, where ICMP traffic should be minimal, a threshold of 1% of the available bandwidth is allowed for ICMP traffic. ICMP traffic is treated as a lower priority to more important traffic, such as active calls, and ICMP requests will be dropped during high call traffic periods.

Solution

Run ICMP requests during low traffic periods.

Upgrade and rollback problems

Roll back to an earlier release

For information about upgrading to the latest Avaya SBC Release or rolling back to an earlier release, see *Upgrading Avaya Session Border Controller*.

Mount failure during rollback

Condition

During rollback, the system displays messages similar to the following example:

```
         Mounting /tmp
         Mounting /home
. . .
. . .
[FAILED] Failed to mount /home.
See 'systemctl status home.mount' for details
. . .
. . .
Welcome to emergency mode! After logging in, type "journalctl -xb" to view
system logs, "systemctl reboot" ro reboot, "systemctl default" or ^D to
try again to boot into default mode.
Give root password for maintenance
(or type Control-D to continue):
```

Cause

During rollback, the `/etc/fstab` file was not properly updated and the `/home` partition was not able to mount.

Solution

1. At the error message prompt, enter the root password.
2. At the OS prompt, run the following command:

   `cat /archive/backup/upgrade/upgrade.conf | grep home`

3. Record the partition number of the `/home` partition.

4. Run the following command and check to see if the `/home` partition number matches what you found in the `upgrade.conf` file.

   `more /etc/fstab`

5. If the partition numbers do not match, edit the `/etc/fstab` file so that the partition number matches what you found in the `upgrade.conf` file.
6. Save and close the file.
7. Reboot the SBC server.
8. If this does not fix the problem, contact Avaya support.

Performance problems

Disk full alarms causing performance problems

Condition

The system is suffering from poor performance. Disk full alarms might accompany the condition.

Cause

The disk is full of old upgrade and repository files that can be deleted.

Solution

1. Log on as root to the operating system.
2. Inspect the following directories for large files that are taking up space:
   - `/archive/urpackages`
   - `/archive/SBC-RPM-Repository`
3. In the `/archive/urpackages` directory, you can delete any old upgrade files that were uploaded to the system.
4. In the `/archive/SBC-RPM-Repository` directory, you can delete any old repository files that start with `sbce-*`.

TG3 custom driver does not load correctly

Condition

When the TG3 custom driver does not load correctly on the Dell™ PowerEdge™ R640 Avaya Solutions Platform 110 Appliance server with Profile 3, it affects the system performance. The CPU0 software interrupt (SI) value reports 90% occupancy when using the A2 or the B2 interfaces.

Cause

During a new installation or an upgrade, the OS dracut tool functionality fails to update the custom module. Run the following commands to check the A2 and B2 interfaces:

ethtool –i A2

ethtool –i B2

In the output, **driver: tg3** implies that the correct driver is not loaded.

For example,

```
driver: tg3-udp4t
version: 3.137
firmware-version: FFV20.8.4 bc 5720-v1.39
expansion-rom-version:
bus-info: 0000:3b:00.0
supports-statistics: yes
supports-test: yes
supports-eeprom-access: yes
supports-register-dump: yes
supports-priv-flags: no
```

Solution

1. Log in to the operating system as a root user.
2. Run the following command:

   `/usr/local/ipcs/icu3/scripts/tg3_update.sh`
3. Reboot the server.
4. Run the following commands to confirm that the correct TG3 driver is installed:

   `ethtool –i A2`

   `ethtool –i B2`

Database tables filling up /var disk space

Condition

Incident tables in the postgres database are not being cleaned up, causing the `/var` directory to run out of space.

Cause

An archival script should normally clean up this file space, but other issues may cause unneeded tables to be left in the `/var` directory and might require manual cleanup.

Caution:

Cleaning up postgres database tables might cause service interruptions and performance issues. Do this procedure during low or no traffic times, or during a normal maintenance window.

Solution

1. Log on as root to the operating system.
2. Enter the following command:

   df -h

Look for output similar to the following example for the `/var` directory:

```
Filesystem   Size   Used   Avail   Use%   Mounted on
/dev/sda8             4.7G   4.5G    248M    95%      /var
```

3. If the amount of space being used is 95% or more, enter the following command to see if any postgres tables are using up 1 GB or more storage in the `/var` directory:

   `ls -hltr XXXX*`

   For example, there are three postgres tables that are taking up 1 GB of disk space, and another that is taking up almost 1 GB of disk space in this example.

```
------ 1 postgres postgres 1.0G Dec 13 2019 XXXX
------ 1 postgres postgres 1.0G Mar 11 22:47 XXXX.1
------ 1 postgres postgres 1.0G Jun 2 19:45 XXXX.2
------ 1 postgres postgres 1016K Aug 11 09:38 XXXX_fsm
------ 1 postgres postgres 882M Aug 11 09:40 XXXX.3
```

4. Before cleaning up any files, do a backup of the current database using the following command:

   `/usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup`

   A backup of the database is saved in the `/archive/backup/db/` directory.

5. Enter the following command:

   `vacuumdb -U postgres --all --freeze --echo --analyze`

   This command cleans up any large postgres database table files and frees up space in the `/var` directory.

Licensing problems

License status showing grace period active on secondary EMS

Cause

A license file has been installed on the secondary EMS in an active-active deployment. You must not install an Avaya SBC license file on a secondary EMS if used in an active-active deployment. If you install a license file on a secondary EMS in an active-active deployment, the licensing system will always show that the secondary EMS is in Grace Period State.

Solution

Uninstall the license file for the secondary EMS in an active-active deployment.

Enhanced Access Security Gateway

The Enhanced Access Security Gateway (EASG) system is a key element in protecting passwords and preventing unauthorized use of maintenance and administration login. EASG

provides a secure method for Avaya support personnel to access Avaya SBC remotely. Access is under the control of the customer. EASG is a 128–bit AES encrypted challenge-response mechanism for authentication. With this mechanism, Avaya SBC can maintain secure access for services, administration, and maintenance. On Avaya Enterprise Communications System (ECS) products, Avaya services personnel use the EASG challenge and corresponding response for a single access attempt only. After each login, EASG uses a new challenge and response .

Checking EASG status

Before you begin

Log in to the application with the customer account.

Procedure

1. On the command line interface, type `EASGStatus`.
2. Press `Enter`.

   The system displays one of the following:

   - **`EASG is enabled`** — if EASG is enabled.
   - **`EASG is disabled`** — if EASG is disabled.

Enabling and disabling EASG using web interface

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **System Administration** > **AAA**.
4. Click the **EASG** tab.
5. In the EASG Authentication Status section, do one of the following:
   - To enable EASG, click **Enable**.
   - To disable EASG, click **Disable**.

Enabling and disabling EASG using CLI

About this task

Avaya recommends enabling EASG. By enabling Avaya Logins you are granting Avaya access to your system. This is necessary to maximize the performance and value of your Avaya support entitlements and allowing Avaya to resolve product issues in a timely manner. See the Avaya support site for additional information for registering products and establishing remote access and alarming.

By disabling Avaya Logins, you are preventing Avaya access to your system. This is not recommended, as it impacts Avaya’s ability to provide support for the product. Unless the customer is well versed in managing the product themselves, Avaya Logins should not be disabled.

Before you begin

Log in to the application with the customer account.

Procedure

1. On the command line interface, do one of the following:
   - To enable EASG, type `EASGManage --enableEASG`.
   - To disable EASG, type `EASGManage --disableEASG`.

   The system displays the message **`Do you want to continue [yes/no] ?`**
2. Type `yes` or `no`.
3. Press `Enter`.

EASGManage

Use **`EASGManage`** to enable or disable the EASG authentication, check the status of EASG feature for the specified users, and display information about the available EASG users.

Syntax

```
EASGManage [--enableEASG] [--disableEASG] [--enable user] [--disable user] [--
userStatus user] [--listUsers] [--printDisableWarning] [--printEnableWarning]
```

--enableEASG	Enables Enhanced Access Security Gateway (EASG) authentication.
--disableEASG	Disables EASG authentication.
--enable	Enables EASG authentication only for the Avaya Services logins specified in the *user* variable. If the main EASG enable/disable switch is disabled, no Avaya Services logins will have access, no matter what this setting reflects for an individual Avaya Services Login. EASG supports only Avaya services logins, such as init, inads, and craft.
--disable	Disables EASG authentication only for the Avaya Services logins specified in the *user* variable.
--userStatus	Displays the EASG status of the user specified in the *user* variable.
--listUsers	Lists the available EASG users.
--f	Forces the enable or disable action to run without prompts.
--printDisableWarning	Displays the warning message for disabling EASG on the system.
--printEnableWarning	Displays the warning message for enabling EASG on the system.

Loading and managing site certificate

About this task

You can load a site certificate using `EASGSiteCertManage --add <pkcs7_file_path>`. You will need to specify a Site Authentication Factor (SAF). The SAF must be provided to the technician and is also used by EASG Site Manager to generate a response to the EASG challenge.

Before you begin

Procedure

1. Log in to a Linux® shell by using the customer account.

   The customer account is created during the deployment procedure.

2. To manage site certificates, type the following command:

```
[cust@host ~]$  EASGSiteCertManage --add johndoe.p7b
You are about to install this site certificate into your trusted repository:
Technician Name: johndoe
Expiration Date: Nov 10 17:02:15 2016 GMT
Do you want to continue [yes/no]? yes
Please enter a site authentication factor (SAF) for the technician to use
when getting access to your machine. The SAF is alphanumeric with at least 10
characters and no more than 20 characters.
  Please enter your SAF:  Site Authentication Factor
  Please confirm your SAF: Site Authentication Factor
Site Certificate installed successfully.
```

   Save the Site Authentication Factor to share with the technician once on site.

3. To display information about a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --show johndoe.p7b
Subject:        CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
User Name:      johndoe
Expiration:     Nov 10 17:02:15 2016 GMT
Trust Chain:
    1. O=Avaya, OU=IT, CN=AvayaITrootCA2
    2. DC=com, DC=avaya, DC=global, CN=AvayaITserverCA2
    3. O=Avaya LLC, OU=EASG, CN=EASG Intermediate CA
    4. CN=Site EASG Intermediate CA, OU=EASG, O=Avaya LLC
    5. CN=Avaya Technician johndoe, OU=EASG, O=Avaya LLC
```

4. To remove a site certificate, type the following command with the name of a valid site certificate:

```
[cust@host ~]$ EASGSiteCertManage --delete johndoe.p7b
Successfully removed Site Cert: johndoe.p7b
```

Statistics viewer displays non-numeric values

Solution

1. Log in to the CLI with administrator credentials.

2. Run the following command:

   /usr/local/ipcs/icu3/scripts/ResetSnmpConfig.sh

3. When the system prompts for confirming, press `Y`.

SNMP traps are not send outside

Solution

1. Log in to the CLI with administrator credentials.
2. Run the following command to restart spiritAgent:

   systemctl restart spiritAgent

3. Run the following command to ensure that spiritAgent is up and running:

   systemctl status spiritAgent

Support contact checklist

Use this checklist to collect the critical information that you must gather before you contact Avaya Technical Support.

Try to resolve the issue by using this document before you contact Avaya. Contacting Avaya is the final step only after you are unable to resolve the issue.

Task	Description	Notes	✔
Your full name, organization, and telephone number where an Avaya representative can contact you about the problem.			
The Sold To number.	Also known as the Functional Location (FL) number.		
Detailed description of the problem.			
The type of service contract your organization has with Avaya.			

Table continues…

Task	Description	Notes	✔
Your product release information.	Include the software versions, hardware deployment type, operating system, third-party software and database versions.		
Description of any Avaya Professional Services contracts.			
Description of remote access availability.			
Date and time when the problem started.	Refer to log files if applicable.	If the problem is intermittent, determine when the problem started and stopped.	
Frequency of the problem.			
What InSite Knowledge Base solutions have you tried?	Use the Advanced Search option to narrow your search to specific categories and document types.		
Detailed information about recent system upgrades, network changes, or custom applications.	Include the date and the time when the changes were made. Also include information about who made the changes.		
Appropriate logs and packet captures of the issue.	Take packet captures when the issue occurs and save appropriate logs to facilitate investigation.		

Chapter 5: System monitoring

About system monitoring

There are many tools available to help you monitor the health and status of your Avaya SBC. This section describes the following tools:

- Dashboard – The first screen you see when you log on to the system. It summarizes connectivity, alarms, and incidents, giving you quick access to troubleshoot any problems.
- System alarms – The **Alarms** menu provides access to any open alarms and allows you to resolve and close alarms.
- Incidents – The **Incidents** menu item provides quick access to the list of the most recent incidents so you can troubleshoot problems.
- System status - The **Status** menu gives you access to SIP, user, server, and performance status.
- Logs – The **Logs** menu gives you access to system logs and audit logs.
- Diagnostics – The **Diagnostics** menu item allows you to run a quick diagnostics on links between servers within your deployment and ping specific servers.
- Administrative users – The **Users** menu item gives you a quick listing of which administrative users are logged on to the system.

In addition, there are other tools described in this section to help diagnose and fix problems within your system.

Dashboard

The Dashboard screen displays system information, installed devices, alarms, and incidents. The screen displays additional separate summary windows, such as Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The summary windows contain active, up-to-the-minute alarms, incident, statistical, log, diagnostic, and user information, and review and exchange textual messages with other administrative user accounts.

The Content area of the Dashboard screen contains various summary areas that display top-level, systemwide information, such as:

- Which alarms and incidents are currently active.

- Links to available Quick Links.
- List of installed Avaya SBC security devices.
- Avaya SBC deployment information.
- Area for viewing and exchanging text messages with other administrators.

Dashboard content descriptions

Name	Description
System Time	The current system time.
Version	The system software version.
GUI Version	The system GUI version.
Build Date	The system software build date.
License State	The license state.
Aggregate Licensing Overages	The aggregate license information.
Peak Licensing Overage Count	The peak licensing count.
Last Logged in at	The date and time when the user last logged in.
Failed Login Attempts	The number of failed login attempts.
Installed Devices	A list of all Avaya SBC security devices currently deployed throughout the network.
Incidents (past 24 hours)	A list of current incidents reported by Avaya SBC security devices to the EMS web interface.
Active Alarms (past 24 hours)	A list of current alarms reported by Avaya SBC security devices to the EMS web interface.
Add	A user-editable text message exchange area.
Notes	The text message created by using the **Add** function.

Alarms

Current system alarms are reported to the EMS web interface. The alarms are displayed as a red indicator on the Alarm viewer page and on the dashboard for the respective device.

The notifications provide the information necessary to clear the condition causing the alarm notification.

Viewing current system alarms

About this task

The Alarms screen displays a summary of all currently active system alarms. If no alarms are active, the system displays a blank screen. The Alarms screen is accessed only if the **Alarm Status Indicator** on the toolbar indicates an alarm status, flashed red. Use the following procedure to view current system alarms.

Procedure

1. Log in to the EMS web interface web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. On the toolbar, click **Active Alarms** or click on the specific alarm you want to view from the **Alarms (past 24 hours)** section of the Dashboard screen.

   The EMS server displays the Alarms Viewer screen.
4. Select the Avaya SBC device for which you want to view the alarms.

   The Alarms section displays all the currently active alarms for the selected Avaya SBC security device.

   For the field description of each security reporting component of the Alarms screen, see Alarm Viewer field descriptions.

Alarm Viewer field descriptions

Name	Description
ID	Sequential, numerical identifier of the alarm being reported.
Details	The specific or descriptive name of the active alarm.
State	Current state of the alarm: ON The **State** field for any displayed alarm is always: ON
Time	Date and time when the alarm was generated.
Device	The Avaya SBC device that generated the alarm.

Clearing system alarms

About this task

You can either delete a selected alarm or all alarms. Most of the alarms are cleared automatically when the condition to create these alarms no longer exist. However, there are some alarms that need to be cleared manually.

Procedure

1. Log in to the EMS web interface web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. To clear the selected alarm or all alarms, on the Alarms screen, click **Clear Selected** or **Clear All**.

   The EMS server displays a confirmation pop-up window.
4. Click **OK**.

System alarms list

This section covers the description of system alarms. Some system alarms require manual intervention, while some get cleared automatically. For information about clearing these alarms, see the Clearing event and Manual intervention columns. System alarms are reported on both the primary and secondary servers in High Availability (HA) deployments.

CPU alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
CPU	CPU utilization is over 80%	CPU utilization is between 80%-89%.	No	Alarm	Minor	CPU utilization is between 80%-89%.	CPU utilization goes below 80% or above 89%.	No
CPU	CPU utilization is over 90%	CPU utilization is between 90%-99%.	No	Alarm	Major	CPU utilization is between 90%-99%.	CPU utilization goes below 90% or becomes 100%.	No
CPU	CPU utilization is 100%	CPU utilization is 100%.	Yes	Alarm	Critical	CPU utilization is 100%.	CPU utilization becomes 100%.	No

Memory alarms (including Swap Space)

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Memory	Memory utilization is over 80%	Memory utilization is between 80%-89%.	No	Alarm	Minor	Memory utilization is between 80%-89%.	Memory utilization goes below 80% or above 89%.	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Memory	Memory utilization is over 90%	Memory utilization is between 90%-99%.	Yes	Alarm	Major	Memory utilization is between 90%-99%.	Memory utilization goes below 90% or becomes 100%.	No
Memory	Memory utilization is 100%	Memory utilization is 100%.	Yes	Alarm	Critical	Memory utilization is 100%.	Memory utilization becomes 100%.	No

Disk partition space alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Disk partition <partition_name> utilization is over 80%	Disk partition utilization is between 80%-89%.	No	Alarm	Minor	Disk partition utilization is between 80%-89%.	Disk partition utilization goes below 80% or above 89%.	No
Disk partition space	Disk partition <partition_name> utilization is over 90%	Disk partition utilization is between 90%-99%.	Yes	Alarm	Major	Disk partition utilization is between 90%-99%.	Disk partition utilization goes below 90% or becomes 100%.	No
Disk partition space	Disk partition <partition_name> utilization is 100%	Disk partition utilization is 100%.	Yes	Alarm	Critical	Disk partition utilization is 100%.	Disk partition utilization becomes 100%.	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Database pg_committs usage more than 1GB	If disk usage of '/var/lib/pgsql/9.4-bdr/data/pg_xlog/' gets more than 1 GB, this alarm is raised.	No	Alarm	Critical	pg_committs directory size is more than 1 GB.	Yes	No
Disk partition space	Database replication pg_xlog usage more than 1GB	If disk usage of '/var/lib/pgsql/9.4-bdr/data/pg_committs/' gets more than 1 GB, this alarm is raised.	Yes	Alarm	Critical	Pg_xlog directory size is more than 1 GB.	No	Yes
Disk partition space	Database replication pg_logical snapshots usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/snapshots' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / snapshots directory.	Yes	No

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Disk partition space	Database replication pg_logical mappings usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/mappings' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / mappings directory.	Yes	No
Disk partition space	Database replication pg_logical checkpoints usage more than 1000 Files	If the number of files in '/var/lib/pgsql/9.4-bdr/data/pg_logical/checkpoints' Is more than 1000 this alarm is raised	No	Alarm	Critical	There are more than 1000 files in pg_logical / checkpoints directory.	Yes	No

Hard disk failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Hard disk failure	Hard disk <disk_id> failure	Hard disk failure	Yes	Alarm	Critical	The hard disk drive has failed and cannot be used.	The alarm is cleared only when the kernel detects no failures when testing the hard disk drive. This will only happen when the hard disk drive is replaced.	Yes. Hard disk drive must be replaced.[1]

Link failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Link failure	Network link failure <interface>	Network link goes down on the given interface.	Yes. No traffic can be sent or received on the failed link.	Alarm	Critical	A link on a particular interface in down and cannot be used.	Network connection is restored and alarm manually cleared by user.	Yes. User needs to manually restore the link.

[1] See Swapping a separate Avaya SBC server deployed under EMS on page 12, Swapping Avaya SBC devices in an HA pair deployment on page 13, Swapping an EMS server in a single server deployment on page 14, Swapping a primary EMS server in an HA pair deployment on page 15, and Swapping a secondary EMS server in an HA pair deployment on page 15.

Process failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Process failure	Application failure	One or more system processes failed to send a heartbeat ping.	Yes. Port By-pass is automatically enabled.	Alarm	Critical	One or more system processes is malfunctioning	Malfunctioning process is restarted either automatically by the system or manually by the Security Administrator and the alarm cleared.	Yes. Required if automatic self-start is not successful.

Database failure alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database failure	Database failure	Connectivity to the database has been lost.	Yes. Port By-pass is automatically enabled after multiple failed restarts.	Alarm	Critical	Either the database is down or connectivity to the database has been lost.	The database failure being cleared either automatically by the system or manually by the Security Administrator.	Yes. Required if automatic self-start is not successful.

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database Failure	Data Replication is broken	Database replication is broken between the HA SBC systems or the active-active EMS systems	No. But if the alarm does not get user attention and if ignored in the long run could lead to disk space issues and could cause the SBC to go down. Also, in case if the SBC displays the alarm 'Database replication pg_xlog usage more than 1 GB then it needs immediate attention.	Alarm	Critical	Database Replication has stopped working between HA SBC's or the active-active EMS and needs attention.	1. If this alarm pops up in the middle of upgrade / rollback, it is safe to ignore the alarm. 2. If this alarm pops up in a working system on 8.1 where both SBC's or EMS's are at the same version, the alarm is cleared after manual intervention is successful.	1. No 2. Yes

Table continues…

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Database Failure	Peer SBC is Unreachable	The Peer HA SBC or EMS is down.	No. But in case if the SBC displays the alarm 'Database replication pg_xlog usage more than 1GB' then it needs immediate attention.	Alarm	Critical	If this alarm is seen on HA SBC, it means the peer SBC is not reachable. If this alarm shows up for EMS, it means the peer EMS is down.	Alarm gets cleared automatically once the peer SBC comes back online.	If the peer SBC was kept down intentionally, power on the SBC and make sure it comes back up again. Manual intervention is also needed in case if the SBC has hard disk failure and is never going to come back again.

Component failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Component failure	Component failure	One or more elements (signaling, media, intelligence, or EMS) in a multi-component configuration has failed to send a heartbeat ping.	Yes	Alarm	Critical	One or more SBC server elements (signaling, media, intelligence, or EMS) is malfunctioning.	The malfunctioning elements could be restarted manually and the alarm cleared manually.	Required if self restart in not successful.

Clearing a “Data Replication is broken” alarm

Use this procedure to clear a “Data Replication is broken” alarm on either an SBC HA pair or on an active-active EMS pair.

Caution:

This procedure is service interrupting and will cause down time on the deployment. Try to do this during low or no traffic periods.

Condition

Alarm message text	Data Replication is broken
Alarm level	Critical

Solution

1. On SBC A in an HA pair or the Primary EMS in an active-active EMS pair, do the following:
   a. Do a database backup using the following command:

      `/usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup`

   b. Stop replication using the following command:

      `/usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication`

2. On SBC B in an HA pair or the Secondary EMS in an active-active EMS pair, do the following:
   a. Do a database backup using the following command:

      /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup

   b. Stop replication using the following command:

      /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication
3. Reboot SBC A or the Primary EMS using the following command:

   /sbin/reboot
4. Once SBC A or the Primary EMS is online and processes are up, reboot SBC B or the Secondary EMS using the following command:

   /sbin/reboot

Clearing a “Data replication pg_xlog usage more than 1 GB” alarm

Use this procedure to clear a “Data replication pg_xlog usage more than 1 GB” alarm.

Caution:

This procedure is service interrupting and will cause down time on the deployment. Try to do this during low or no traffic periods.

Condition

Alarm message text	Data replication pg_xlog usage more than 1 GB
Alarm level	Critical

Solution

Scenario 1 — Check the replication status between the SBC systems to see if the “Data Replication is broken” alarm is active.

1. Do one of the following depending on the type of system you are troubleshooting:
   - On an SBC system, run the following commands:

     psql -U postgres -d sbcedb

     sbcedb=# select * from alarms;
   - On an EMS system, run the following commands:

     psql -U postgres -d commondb

     commondb=# select * from alarms;

   If the alarm is seen, then follow the steps in Clearing a Data Replication is broken alarm on page 64 to clear the alarm. This should also fix the “Data replication pg_xlog usage more than 1 GB” issue.

Scenario 2 — The number of pg_xlogs will grow if the peer SBC or EMS system is down for a long time. To prevent the disk space from getting full, you must act immediately when this alarm is seen.

2. Check the database alarms table. If the table has the alarm “Peer SBC is unreachable”, confirm that the peer SBC or EMS system is powered up and in operation. It must be in operation so that database replication can occur.
   - On an SBC system, run the following commands:

     psql -U postgres -d sbcedb

     sbcedb=# select * from alarms;
   - On an EMS system, run the following commands:

     psql -U postgres -d commondb

     commondb=# select * from alarms;

   If the peer SBC or EMS has a true hardware failure, break the replication on the SBC or EMS system that is in operation so that pg_xlogs will no longer grow on that system. To break the replication, downtime is required.
3. On the operational SBC or EMS system, do the following:
   a. Do a database backup using the following command:

      /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup
   b. Stop replication using the following command:

      /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication
   c. Reboot the system using the following command:

      /sbin/reboot

Scenario 3 — Disk space of `/var` becomes 100% full and the SBC or EMS system goes down. This happens when the alarms “Data Replication is broken”, “Data replication pg_xlog usage more than 1 GB”, and “Peer SBC is unreachable” have occurred and were not attended to.

4. Run the following command to check the `/var` partition files to see which files are causing the disk space issue:

   cd /var

   du –sh

   This command lists the file size of each file in the `/` root directory. Confirm whether any pg_xlog files are more than 1 GB verify that the cause of the issue is really due to log size or replication being down.
5. Do a backup of the entire database. In a HA system or active-active EMS system, do a backup of the database on both systems, if possible. In the SBC or EMS that is operational, run the following command:

   /usr/local/ipcs/db/scripts/dbmanage.py --takedb-backup
6. For any systems that are down because `/var` is 100% full, you cannot use the standard backup command. You must use the following commands:

Important:

Confirm that the archive directory you select has enough space for the complete database backup.

```
mkdir /archive/tst
tar -zcvf /archive/tst/db-bkp.tar.gz /var/lib/pgsql/9.4-bdr/data/
```

When using Steps 7–9, the down SBC will get all of the SBC configurations from the SBC that is up and running.

7. On the SBC or EMS system that is operational, break the database replication and reboot the system using the following commands:

   ```
   /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication
   /sbin/reboot
   ```

8. Confirm that the operational SBC or EMS system comes back online and starts all processes.
9. On the SBC or EMS system that is down or has database issues, confirm that both application processes and the database are down. Run the following commands to delete the database directory, recreate the database directory, recreate the database, break replication, and reboot the server:

   ```
   rm -rf /var/lib/pgsql/9.4-bdr/data/
   /usr/local/ipcs/db/scripts/db_post_tasks.sh 1
   /usr/local/ipcs/db/scripts/dbmanage.py --dbcreate --dbname sbcedb
   --dbtype sbcedb --no-schema True
   /usr/local/ipcs/icu3/scripts/bdrmon.py --breakreplication
   /sbin/reboot
   ```

GUI and console alarm list

New user-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New User Added	New User Added: <username>	A new GUI/ System user was added.	No	Alarm	Informational	A new user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

New Administrator-added alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
New Admin-added	Admin User Added: <username>	A new GUI/ System admin user was added.	No	Alarm	Informational	A new admin user was added to the system.	Alarm either cleared by the administrator or it times-out.	No

User privilege change alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Privilege Change	User Privilege Changed: <username>	A user's access privilege was changed (either from admin to normal or from normal to admin).	No	Alarm	Informational	A user's access privilege was changed (either from admin to normal or from normal to admin).	Alarm either cleared by the administrator or it times-out.	No

User deleted alarms

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
User Deleted	User deleted: <username>	A new GUI/ System admin user was deleted.	No	Alarm	Informational	A user was deleted from the system.	Alarm either cleared by the administrator or it times-out.	No

Login failure alarm

Alarm	Message	Condition	Service affecting	Type	Severity	Description	Clearing event	Manual intervention
Login failure	User login failure: <username>	A user had multiple consecutive login failures.	No	Alarm	Warning	A user had more than a certain number of consecutive login failures.	Alarm either cleared by the administrator or it times-out.	No

Incidents

The following sections describe the incidents that can occur in Avaya SBC.

Denial of Service (DoS) incidents

Incident Name	Component generating the trap	Cause and solution
ipcsSingleSourceDoS	SBC	Avaya SBC detects a single source DoS
ipcsSingleSourceCallWalkDoS	SBC	Avaya SBC detects a call walk DoS
ipcsPhoneDoS	SBC	Avaya SBC detects a phone DoS
ipcsPhoneStealthDoS	SBC	Avaya SBC detects a phone stealth DoS

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsServerDoS	SBC	Avaya SBC detects a server DoS or blocks a server DoS The incident occurs due to any of the following reasons: • Initiated Threshold Crossed - Action Whitelist • Pending Threshold Crossed- Action Whitelist • Failed Threshold Crossed- Action Whitelist • attack from Server side - Initiated Threshold Crossed- Action SIV • attack from Server side - Pending Threshold Crossed- Action SIV • attack from Server side - Failed Threshold Crossed- Action SIV • Initiated Threshold Crossed- Action Limit • Pending Threshold Crossed- Action Limit • Failed Threshold Crossed- Action Limit
ipcsPhoneStealthDDoS	SBC	Avaya SBC detects a phone stealth DDoS
ipcsDomainDoS	SBC	Avaya SBC detects a domain DoS

Blacklist/Whitelist incidents

Incident Name	Component generating the trap	Cause and solution
ipcsBlackipcsListCallBlocked	SBC	Avaya SBC comes across a blacklisted caller

Scrubbing related incidents

Incident Name	Component generating the trap	Cause and solution
ipcsDroppedScrubMsg	SBC	Avaya SBC comes across a SDP parser error or scrubber anomaly
ipcsRejectedScrubMsg	SBC	Avaya SBC comes across a scrubber anomaly
ipcsDetectedScrubMsg	SBC	Avaya SBC comes across a scrubber anomaly

Protocol discrepancy incidents

Incident Name	Component generating the trap	Cause and solution
ipcsACKMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue ACK message
ipcsBYEMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue BYE message
ipcsCANCELMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue CANCEL message
ipcsNOTIFYMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue NOTIFY message
ipcsPRACKMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue PRACK message
ipcsREINVITEMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue REINVITE message
ipcsREFERMsgOutofDialogue	SBC	Avaya SBC gets an out of dialogue REFER message
ipcs1XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 1xx class response
ipcs2XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 2xx class response
ipcs3XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 3xx class response
ipcs4XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 4xx class response
ipcs5XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 5xx class response
ipcs6XXMsgOutofTransaction	SBC	Avaya SBC gets an out of dialogue 6xx class response
ipcsAuthRealmMismatch	SBC	Avaya SBC comes across a realm mismatch

Policy related incidents

Incident Name	Component generating the trap	Cause and solution
ipcsCallDenied	SBC	Calls to the Avaya SBC are denied due to any of the following reasons: • Video is disabled or disallowed • Audio is disabled or disallowed • Maximum number of video sessions is exceeded • Maximum number of audio sessions is exceeded • Maximum number of audio sessions per endpoint is exceeded • Maximum number of video sessions per endpoint is exceeded • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed out of dialog message • Standard method disallowed out of dialog message • No Routing Rule is matched • Codec is disallowed • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsRegistrationDenied	SBC	Avaya SBC denies registration because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed out of dialog message • Standard method disallowed out of dialog message • No Routing Rule is matched • Method is disallowed
ipcsSubscriptionDenied	SBC	Avaya SBC denies subscription because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed in dialog message • Standard method disallowed in out of dialog message • No Routing Rule is matched • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsRedirectionDenied	SBC	Avaya SBC denies redirection because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Prop method disallowed in dialog message • Standard method disallowed in dialog message • Prop method disallowed in out of dialog message • Standard method disallowed in out of dialog message • No Routing Rule is matched • Method is disallowed

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsMessageDropped	SBC	Avaya SBC drops a message because of any of the following reasons: • No Server Flow is matched for incoming message • No Server Flow is matched for outgoing message • No Subscriber Flow is matched • Response prop header is disallowed • Response standard header is disallowed • Response prop header is mandatory • Response standard header is mandatory • Response prop header is disallowed • Response standard header is disallowed • Request prop header is mandatory • Request standard header is mandatory • Prop method disallowed in dialog message • Standard method disallowed in dialog message • Method is disallowed • Prop method disallowed in out of dialog message • Standard method disallowed in out of dialog message

Route incidents

Incident Name	Component generating the trap	Cause and solution
ipcsPrimaryRadiusServerUnreachable	EMS	Primary Radius server is unreachable
ipcsSecondaryRadiusServerUnreachable	EMS	Secondary Radius server is unreachable

TLS certificate failure incidents

Incident Name	Component generating the trap	Cause and solution
ipcsTlsCertificate	SBC	Avaya SBC comes across a TLS certificate error because of any of the following causes: • Could not create TLS context - for default client mode • No cipher list is provided • Could not create TLS context for either server or client mode • Could not read Certificate • Could not read private key • Private key does not correspond to the loaded certificate • Unable to load Root Certificate or CA list • Unable to load CRL list • Unable to cipher list provided • No cipher list provided

Media anomaly detection incidents

Incident Name	Component generating the trap	Cause and solution
ipcsPacketSizeViolation	SBC	Avaya SBC comes across a packet size violation
ipcsSSRCViolation	SBC	Avaya SBC comes across a synchronization source
ipcsSeqNoViolation	SBC	Avaya SBC comes across a sequence number violation
ipcsTimestampViolation	SBC	Avaya SBC comes across a timestamp violation
ipcsMediaInActivityFromBothSides	SBC	Avaya SBC comes across a media inactivity from both sides of the call There is call audit that runs on the SBC. If there is no media activity or signaling activity for some specified period, that call will be cleared by the audit. You can track the call ID in the incident and then check that in using traceSBC to see the call flow for the specified call.

Table continues…

Incident Name	Component generating the trap	Cause and solution
ipcsUnsupportedMedia	SBC	Avaya SBC comes across unsupported media
ipcsRTPDoSAttack	SBC	Avaya SBC comes across an RTP denial of service attack
ipcsMediaPortUnavailable	SBC	No free media ports are available
ipcsRTPInjectionAttack	SBC	Avaya SBC comes across an RTP injection attack

HA link failover incident

Incident Name	Component generating the trap	Cause and solution
ipcsHAGracefulFailover	SBC	The primary server has gone down voluntarily
ipcsHAKaFail	SBC	High Availability keep alive messages fail
ipcsHATakeoverDone	SBC	HA takeover is completed
ipcsHASecondaryDown	SBC	HA secondary server is down and HA will not be available until the secondary server is up

License incidents

Incident Name	Component generating the trap	Cause and solution
sbcLicenseExceeded	SBC	Avaya SBC gets requests after the maximum number of licensed sessions is exceeded

TURN/STUN incidents

Incident Name	Component generating the trap	Cause and solution
sbcTurnStunMediaRelayCreationFailed	SBC	Media relay flow creation failed
sbcTurnStunMediaRelayDeletionFailed	SBC	Media relay flow deletion failed

Table continues…

Incident Name	Component generating the trap	Cause and solution
sbcTurnStunServerError	SBC	Avaya SBC detects a TURN/STUN error because of any of the following reasons: • Invalid User Name is configured • Invalid Realm is configured • Invalid Password is configured • Invalid Realm is configured • Relay Port is unavailable • TCP/TLS Listener has failed • Invalid User Account is configured • Invalid User Name is configured

CES Proxy incidents

Incident Name	Component generating the trap	Cause and solution
sbcCesProxy1xMUserLoginFailed	SBC	Login attempts from an Avaya one-X® Mobile user to the CES proxy fails because of any of the following reasons: • Protocol Type validation failed • CesProxy data is not present • Avaya SBC received an invalid response other than login response • Object Type validation failed • Login request data type validation failed • Login request key id validation failed • API object type validation failed • API data type and key Id validation failed • API data type validation failed • API key id validation failed • Object type validation failed • Avaya one-X® Mobile user login failed

Viewing system incidents

About this task

You can view a complete descriptive list of all system incidents that have occurred since the last viewing period by using the Incident screen. The screen displays the last five incidents at any point of time. With this feature, you can view system-wide incidents according to category, such

as DoS, Policy, and Scrubbing. When the Incident screen is open, the latest incident information is available, and the operator can scroll through the incidents list. The screen can display up to 15 incidents at one time. Use the following procedure to view current system incidents.

Note:

You can only view the incidents. They cannot be edited or deleted.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS Dashboard**.
3. On the toolbar, click **Incidents**.

   The EMS server displays the Incidents Viewer page.

   You can view the incidents by clicking the specific incident on the **Incidents (past 24 hours)** section of the Dashboard screen.
4. Using the **Device** and **Category** fields, choose a search filter to find and display the particular incidents that you want to view.

   The Incident screen display changes to reflect the search criteria when a selection is made.
5. To ensure that the EMS server displays all required incidents, periodically click **Refresh** to refresh the display.
6. Click **Clear Filters**.

   The EMS server clears the filtering criteria of the **Device** and **Category** fields and sets the value of the fields to All.
7. Click **Generate Report** and select the start and end date to generate the report.

Incident Viewer field descriptions

Search Criteria

Name	Description
Device	The device for which you want to view incidents.

Table continues…

Name	Description
Category	The category of the incident. The options are: • Authentication • Black White List • DoS • High Availability • Media Anomaly Detection • Policy • Protocol Discrepancy • RSA Authentication • Scrubbing • Spam • TLS Certificate • DNS • Licensing • TURN/STUN • CES Proxy • Accounting • WebUA

Search Results

Name	Description
Type	The type of incident.
ID	A number that identifies the incident.
Date	The date on which the incident occurred.
Time	The time at which the incident occurred.

Table continues…

Name	Description
Category	The category of the incident. The options are: • **All** • **Authentication** • **Black White List** • **CES Proxy** • **DNS** • **DoS** • **High Availability** • **Licensing** • **Media Anomaly Detection** • **Policy** • **Protocol Discrepancy** • **RSA Authentication** • **Scrubbing** • **Spam** • **TLS Certificate** • **TURN/STUN**
Device	The device associated with the incident.
Cause	The cause of the incident.

Button	Description
Clear Filters	Clears filters applied to the search results and displays all incidents.
Refresh	Refreshes the list of incidents.
Generate Report	Opens the Generate Report page.

Generate Report

Name	Description
Start Date	The date from which incidents must be included in the incidents report.
End Date	The date to which incidents must be included in the incidents report.

System status

Using the **Status** menu on the administration user interface. You can view several statistics that give you an indication of how your deployment is operating.

Related links

Viewing SIP statistics on page 82
Viewing periodic statistics on page 86
User registration on page 88
Server status on page 90
Viewing IP/URI Blocklist on page 92

Viewing SIP statistics

About this task

The Statistics screen provides a snapshot display of certain cumulative, system-wide generic and SIP-specific operational information.

Note:

You can only view the statistics information. You cannot edit or delete the statistics information. However, you can reset the counters for the SIP statistics.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **SIP Statistics**.

   Important:

   Do not click **SIP Statistics** repeatedly. If you repeatedly click and trigger frequent loading of the Statistics page, the Statistics Viewer page shows a communication error.

   The EMS server displays the Statistics Viewer screen.
3. To view the statistics, click one of the following tabs:
   - **SIP Summary**
   - **CES Summary**
   - **Subscriber Flow**
   - **Server Flow**
   - **Policy**
   - **From URI**
   - **To URI**
   - **Transcoding Summary**
   - **Dynamic License Summary**

   Information for each of these tabs are shown in SIP statistics field descriptions on page 83.

SIP statistics field descriptions

SIP Summary tab

Name	Description
Active Registrations	The total number of active SIP registrations.
Active TCP Registrations	The number of active SIP registrations with TCP transport.
Active UDP Registrations	The number of active SIP registrations with UDP transport.
Active TLS Registrations	The number of active SIP registrations with TLS transport.
Total Active Calls	The total number of active calls. **Total Active Calls** is the sum of SRTP (anchored), SRTP (unanchored), RTP (anchored), and RTP (unanchored) calls.
Total Direct Media Calls	The total number of active calls in which media is unanchored. **Total Direct Media Calls** is the sum of SRTP (unanchored) and RTP (unanchored) calls. This value is a subset of **Total Active Calls**.
Active SRTP Calls	The number of active SRTP calls. **Active SRTP Calls** is the sum of SRTP (anchored) and SRTP (unanchored) calls. This value is a subset of **Total Active Calls**.
Active Direct Media SRTP Calls	The number of active SRTP calls in which media is unanchored. **Active Direct Media SRTP Calls** is the number of SRTP (unanchored) calls. This value is a subset of **Total Active Calls**, **Total Direct Media Calls**, and **Active SRTP Calls**.
Active Subscriptions	The number of active subscriptions.
Active Video calls	The number of active video calls.
Active Transfer sessions	The number of active transfer sessions.
Active Shared Control sessions	The number of shared control sessions.
ipcssipcActiveTurnSession	The number of IPCS SIP active TURN sessions. **Note:** This statistic is only shown on the **Subscriber Flow**, **Server Flow**, and **Policy** tabs.

CES Summary tab

Name	Description
1XM User Logins Failed	The number of failed Avaya one-X® Mobile user logins.
1XM User Logins Succeeded	The number of successful Avaya one-X® Mobile user logins.
Reset	All values are reset.

Subscriber Flow tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Subscriber Flow	Selects the subscriber flow for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Server Flow tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Server Flow	Selects the server flow for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Policy tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the policy group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

From URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
URI Group	Selects the source URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

To URI tab

Name	Description
Streaming	Specifies whether live statistics are displayed.
Policy Group	Selects the destination URI group for which statistics are displayed.
Name	Specifies the name of the statistic. This column lists the same statistics that the system displays in the **SIP Summary** tab.
Value	Specifies the value of the statistic.

Transcoding Summary

Name	Description
Streaming	Specifies whether live statistics are displayed.
Total Active Transcoding Sessions	The number of active transcoding sessions.
Total Transcoding Sessions	The number of transcoding sessions.
Total Transcoding Sessions Failed	The number of failed transcoding sessions.
Total Transcoding Sessions Modifications	The number of transcoding sessions that resulted in a change in codecs.
Total Transcoding Sessions Modifications Failed	The number of transcoding sessions that resulted in a failure while changing codecs.
Reset	All values are reset.

Dynamic License Summary

Name	Description
Streaming	Specifies whether live statistics are displayed.
Standard Sessions Reserved	The number of standard session licenses that are reserved.
Standard Sessions In-Use	The number of standard session licenses that are currently in use.
Advanced Sessions Reserved	The number of advanced session licenses that are reserved.
Advanced Sessions In-Use	The number of advanced session licenses that are currently in use.
Scopia Video Sessions Reserved	The number of Avaya Meetings Server video session licenses that are reserved.
Scopia Video Sessions In-Use	The number of Avaya Meetings Server video session licenses that are currently in use.
CES Sessions Reserved	The number of Client Enablement Services (CES) session licenses that are reserved.
CES Sessions In-Use	The number of CES session licenses that are currently in use.

Table continues…

Name	Description
Transcoding Sessions Reserved	The number of transcoding session licenses that are reserved.
Transcoding Sessions In-Use	The number of transcoding session licenses that are currently in use.
Premium Sessions Reserved	The number of premium session licenses that are reserved.
Premium Sessions In-Use	The number of premium session licenses that are currently in use.

Viewing periodic statistics

Before you begin

Enable periodic statistics in **Network & Flows** > **Advanced Options**, and specify a collection interval.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Periodic Statistics**.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. Enter the date and time periods for which you want to search for statistics.
5. Click **Search**.
6. To view the statistics, click any of the following tabs:
   - **Summary**
   - **Subscriber Flow**
   - **Server Flow**
   - **Policy Group**
   - **To URI**
   - **From URI**

   Information for each of these tabs are shown in Periodic statistics field descriptions on page 86.

Periodic statistics field descriptions

Name	Description
Total Registrations	The number of active SIP registration requests received.
Total Subscriptions	The number of active subscription requests received.
Registrations Rejected	The number of rejected registrations.

Table continues…

Name	Description
Subscriptions Rejected	The number of rejected subscriptions.
Deregistrations	The number of de-registered requests.
Unsubscriptions	The number of unsubscribed requests.
Total Calls	The number of SIP calls received.
Calls Terminated	The number of terminated SIP calls.
Calls Rejected	The number of SIP calls rejected by Avaya SBC because of policy violation.
Calls Rejected by SBC	The number of SIP calls rejected by Avaya SBC.
Total Transferred Calls	The number of transferred SIP calls.
Calls Failed in Transfer	The number of SIP calls failed in transfer.
Total Redirected Calls	The number of redirected call.
Calls Failed in Redirection	The number calls failed in redirection.
Total SRTP Calls	The number of SRTP calls.
SRTP Calls Terminated	The number of terminated SRTP calls.
SRTP Calls Rejected	The number of rejected SRTP calls.
SRTP Calls Rejected by SBC	The number of SRTP calls rejected by Avaya SBC.
Total Video Calls	The number of video calls.
Video Calls Terminated	The number of terminated video calls.
Total Video Calls Rejected	The number of rejected video calls.
Video Calls Rejected by SBC	The number of video calls rejected by Avaya SBC.
Transcoded Sessions	The number of transcoded sessions.
Transcoded Sessions Terminated	The number of terminated transcoded sessions.
Failed Transcoded Session	The number of failed transcoded sessions.
Early Media Calls	The number of early media calls.
Audit/Media Inactivity Detected	The number of calls in which Avaya SBC detected any inactivity.
Media Relinquished Calls	The number of media relinquished calls.
Shared Control Calls	The number of shared control calls.
Shared Control Calls Terminated	The number of terminated shared control calls.
Info Sessions	The number of info sessions.
Info Sessions Rejected	The number of rejected info sessions.

User registration

You can view the list of users that are registered through Avaya SBC in the **Registrations State** column on the User Registrations page. You can also enter custom search criteria for the fields that are displayed on the system.

Viewing the list of registered users

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **User Registrations**.

   The EMS server displays the list of registered users, displaying information as shown in Registered user field descriptions on page 89.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. For complete details of a registered user, click the user details.

   The EMS server displays the following information:

   - User information:
     - Address of record of the user.
     - User Agent information related to the type of endpoint and SIP instance information.
     - Firmware type and the controller mode.
   - Servers:
     - The Avaya SBC device through which the user is registered to Avaya Aura®.
     - The subscriber flow and server flow that were used for registration.
     - Session Manager address, port, and transport used for registration.
     - Endpoint private IP, natted IP, and transport.
     - Endpoint registration state and last reported time.

Filtering registered users

About this task

Use this procedure to search for the required registered users.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **User Registrations**.

   The EMS server displays the list of registered users.
3. Click **Add Criteria**.

4. Select one of the following criteria from the drop-down list:
   - **AOR**
   - **SIP Instance**
   - **User Agent**
   - **Controller Mode**
   - **Firmware**
   - **SBC Device**
   - **Subscriber Flow**
   - **Server Flow**
   - **SM Address**
   - **SM Port**
   - **SM Transport**
   - **Endpoint Private IP**
   - **Endpoint Natted IP**
   - **Endpoint Transport**
   - **Registration State**
5. Select one of the following options and enter the required value in the text box:
   - **Contains**
   - **Starts with**
   - **Ends with**
   - **Exact Match**
6. To add more filter criteria, repeat Steps 3 to 5.
7. To remove a filter criteria, click **Remove**.
8. Click **Filter**.

   The EMS server displays the results based on the ANDing of the criteria.

Registered user field descriptions

The User Registrations screen displays the list of endpoints registered through Avaya SBC with the following details for each registration.

Name	Description
AOR	The SIP URI used by the endpoint to register to Session Manager.
SIP Instance	The MAC address of the endpoint.
Last Reported Time	The time when the user registration status was last updated.

When the endpoint tries to register to Avaya SBC, each call server uses the following information:

Name	Description
SBC Device	The Avaya SBC device that receives the REGISTER message.
SM Address	The Session Manager address of the call server with the primary or secondary status.
Registration State	The registration status of the endpoint.

Server status

You can view the current status of the configured SIP servers. The EMS server displays the connectivity status for trunk servers and enterprise call servers. The Server Status screen displays the list of servers based on the settings on the Server Configuration screen.

Note:

For the servers to appear in the Status window, you must configure the server heartbeat in Server Configuration.

Configuring Avaya SBC real-time trunk status

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Services** > **SIP Servers**.
4. Click the **Heartbeat** tab.
5. To enable the heartbeat, select the **Enable Heartbeat** check box.
6. Navigate to **Network & Flows** > **Endpoint flows** > **Server flows**.

   For more information about creating server flows, see “Creating Flow toward Call Server” in *Administering Avaya Session Border Controller*.

   Note:

   In a high availability failover scenario, the EMS server displays the actual status of the server after 5-10 seconds.

   To display the server status, the Avaya SBC must successfully resolve the FQDN used as the server address.

Viewing server status

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Server Status**.

The EMS server displays the Status screen, as shown in Server Status field descriptions on page 91.

Server Status field descriptions

Name	Description
Server Profile	The name of the server profile.
Server FQDN	The Fully Qualified Domain Name (FQDN) of the server.
Server IP	The IP address of the server.
Server Port	The port number of the server.
Server Transport	The transport protocol that the server uses.
Heartbeat Status	The heartbeat status of the server. **Note:** When the Heartbeat feature is disabled and the Registration feature is enabled on the Server Configuration page, the Server Status page displays the **Heartbeat Status** as UNKNOWN.
Registration Status	The registration status of the server. **Note:** When the Heartbeat feature is enabled and the Registration feature is disabled on the Server Configuration page, the Server Status page displays the **Registration Status** as UNKNOWN.
TimeStamp	The date and time when the server status was updated.

Viewing performance statistics

About this task

You can view the current performance status of several facets of the servers in your deployment. The system displays CPU usage, memory usage, total media ports, used media ports, queues, and quality of service (QoS).

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Status** menu, click **Performance Status**.
3. For deployments with multiple SBC servers, select the server for which you want to view statistics.
4. Enter the date and time periods for which you want to search for statistics.
5. Click **Search**.

The system displays statistics for the following items. Information is shown in 5 minute intervals within the period of time selected in the search criteria.

- CPU usage for processes like SSYNDI, OAMP, and TURN-server, and threads like, HA, SIPCC, Transport, and Relay
- IPCS memory usage
- Resident memory usage for SSYNDI, OAMP, and TURN activity
- Number of available A1, A2, B1, and B2 media ports
- Number of A1, A2, B1, and B2 media ports in use during that time period
- Queue size for HA, SIPCC, Transport, and Relay threads
- Mean value of Jitter on the system

Viewing IP/URI Blocklist

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the menu bar, select **Status** > **IP/URI Blocklist**.

   You can view the **IP/URI Blocklist** page with a list of blocked IPs and URIs.
3. You can view the following options:
   - **Block Permanently** to block a IP/URI permanently.
   - **Block Subnet** to block a subnet.
   - **Unblock** to unblock an IP/URI.
   - **Propagate To** to propagate information to other Avaya SBCs managed by the EMS.

     Note:

     You can view the **Propagate To** option only when the EMS manages other Avaya SBCs.

Related links

System status on page 81

Log files

Using the log collection feature you can:

- Collect log files for a 24 hour period of time.
- Download log files for investigating and troubleshooting an issue.
- Copy log files to a remote server for viewing and storage.

- Sort the collected log files by the file name, the file size, and the date the file was last modified.
- Sort the collected log files in ascending and descending order.
- Delete the log files no longer needed.

Viewing system logs

About this task

SysLog Viewer displays the syslog file according to certain user-definable filtering criteria, such as log type, time period, and severity. Use the following procedure to define and view syslog reports.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. Select the **Logs** option from the toolbar, and click the **System Logs** menu.

   The EMS server displays the Syslog Viewer screen. On this screen, you can specify criteria in the **Query Options** section to filter the results displayed.
3. In the **Start Date** and **End Date** fields, filter the results displayed in a search report to fall within starting and ending dates and times. In previous Avaya SBC Syslog Viewer windows, there were four separate fields: **Start Date**, **Start Time**, **End Date**, and **End Time**.

   Note:

   The date and time entries are combined in a single field, mm/dd/yyyy [hh:mm], with the time entry, [hh:mm], being optional. An **End Date** or **End Time** entry is not required when you enter a **Start Date** or **Start Time**.

   You can also select additional search criteria in the **Query Options** section.
4. In the **Keyword** field, type one or more words to define the limits of the log report, and click **Search**.

   The system runs the report and displays the output.

   Note:

   Keyword searches are case-insensitive and tokenized. Each keyword term entered in the **Keyword** field is searched. However, for a log line to be included in a report, all keyword terms that are entered in the **Keyword** field must be found in that log line.

Syslog Viewer field descriptions

Query Options section

The Query Options section on the Syslog Viewer screen contains options for filtering the Syslog logs.

Name	Description
Keyword	Search keywords for viewing logs.
Start Date	Date and time from which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
End Date	Date and time up to which you want to view logs You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
Show	Number of entries to be displayed on a page.
Class	Class of the logs to be displayed. The options are: • **All** • **Platform** • **Trace** • **Security** • **Protocol** • **Incidents** • **Registration** • **Audit** • **GUI** • **Unknown**
Severity	Severity of the logs to be displayed. The options are : • **Unknown** • **Info** • **Notice** • **Warning** • **Error** • **Critical** • **Alert** • **Emergency**

Results section

Name	Description
Timestamp	Timestamp of the log message.

Table continues…

Name	Description
Host	Device for which the log is generated.
Severity	Severity of the message.
Class	Class of the message.
Summary	Summary of the message.

Viewing audit logs

About this task

Audit Log Viewer displays the contents of the audit log. The audit log contains a record of security related events, such as logins, session starts, session ends, new user additions, and password attempts/retries/changes. Use the following procedure to view the Audit Log Viewer information.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Logs** > **Audit Logs**.

   The EMS server displays the Audit Log Viewer page.
3. In the **Start Date** and **End Date** fields, you can filter the results that are displayed in a search report to fall within starting and ending dates and times.
4. In the **Keyword** field, type one or more words to define the limits of the log report, and click **Search**.

   In the Results section, the EMS server displays the report output.
5. To see additional details about a particular log line in a report, select the log line.

   The EMS server displays the Audit Log Details page.
6. On the **Monitoring & Logging** > **Syslog Management** page, you can set the log level rules for the Audit Log and other logs.

   Audit Logging is enabled in the Log Level row for the Audit class and Audit Facility as LOG_LOCAL6.

   The Log Level Facility name, LOG_LOCAL6, is reserved for Audit Logging and cannot be changed. The LOG_LOCAL6 file path destination cannot be changed either. The file path is `/archive/syslog/ipcs/audit.log`.

Audit Logs field descriptions

Query Options section

The Query Options section on the Audit Log Viewer screen contains options for filtering the audit logs.

Name	Description
Keyword	Search keywords for viewing logs.
Start Date	The date and time from which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
End Date	The date and time up to which you want to view logs. You can enter values in the format mm/dd/yyyy [hh:mm]. Entering time is optional.
Show	The number of entries to be displayed on a page.

Results section

Name	Description
Timestamp	The timestamp of the log message.
Host	The device for which the log is generated.
Summary	The summary of the message.

Collecting and downloading log files

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click **EMS** or the SBC name to administer.
3. Navigate to **Monitoring & Logging** > **Log Collection**.
4. **(Optional)** Select the SBC device for which you want to collect log files. For an EMS, there cannot be multiple devices.
5. Click the **Collect Logs** tab and do the following:
   a. Select the type of log files that you want to collect. For more information, see Collect Logs field descriptions on page 97.
   b. Select a “from” and “to” time frame for the collection. You can collect up to 24 hours of logs.
   c. Click **Collect Logs** to collect the selected logs.

   The system collects the logs into an archive file. Once finished, a link to the log file is displayed on the **Collect Logs** tab.
6. Do one of the following steps to download the log file:
   - Click the log file link displayed on the **Collect Logs** tab.
   - Click the **Log Archive** tab and click the file name you want to download. For more information, see Log Archive field descriptions on page 97.
7. Using your browser controls, open or save the log file.

8. When you want to delete a log file, click **Delete** next to the log file you want to delete. Click **OK** to delete the file.

Collect Logs field descriptions

Name	Description
All Logs	Collects the database, application, GUI (EMS only), and upgrade logs that show the status of the system and configuration information. Crash dumps logs are not included in the **All logs** option because of the large size. Crash dumps logs can be collected separately. **Note:** The remaining options are clear when you select the **All Logs** check box .
Database logs	Collects the database dump logs.
Application Logs	Collects the SSYNDI logs.
GUI Logs	Collects the web interface and jsp logs. **Note:** The **GUI logs** option is available for EMS only.
Upgrade Logs	Collects the upgrade related logs.
Crash Dumps	Collects the system crash dumps.
From Date & Time	Specifies the day and time of day when you want to start collecting log files.
To Date & Time	Specifies the day and time of day when you want to stop collecting log files. You can collect a maximum of 24 hours of logs in one file.

Log Archive field descriptions

Name	Description
File Name	The file name of the collected log file.
File Size	The size of the collected log file in bytes.
Last Modified	The date and time when the collected log file was last modified.

Button	Description
Delete	Deletes the selected log file.

Debugging logs

Enabling application debug logs

About this task

The debugging logs are located at `/archive/log/ipcs/ss/logfiles/elog/`. You can collect the logs from the console.

The **Subsystem Logs** tab displays a list of processes, each of which contains subsystems. You can select the required subsystems for which you want to enable logs.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
3. Click the **Subsystem Logs** tab.
4. Select the device on which you want to toggle the log settings.

   The EMS server categorizes the subsystem logs under the following processes:

   - **LogServer**
   - **OAMPSERVER**
   - **SYSMON**
   - **SSYNDI**
   - **TURNCONTROLLER**
5. Do one of the following:
   - To turn on all debug information on the device, select the **Debug**, **Info**, and **Warning** log level check boxes at the table header.
   - To select a specific log level for all subsystems, select the **Debug**, **Info**, or **Warning** log level check box at the table header.
   - To select log levels for a specific process, select the **Debug**, **Info**, or **Warning** log level check box next to the process name.
   - To select log levels for a specific subsystem, expand the process name and select the **Debug**, **Info**, or **Warning** log level check box next to the subsystem.

   By default, the **Warning** log level check box is enabled.
6. Click **Save**.

Debugging field descriptions

Subsystem Logs

Name	Description
Process Name	Specifies the process for which you want to enable logs. This field displays processes such as: • LogServer • OAMPSERVER • SYSMON • SSYNDI • TURNCONTROLLER Each process contains subsystems. You can select the required subsystems for which you want to enable logs.
Debug	Specifies that debug logs are enabled for a subsystem. If you select the **Debug** check box in the table header, the system selects debug logs for all processes.
Info	Specifies that informational logs are enabled for a subsystem. If you select the **Info** check box in the table header, the system selects informational logs for all processes.
Warning	Specifies that warning logs are enabled for a subsystem. If you select the **Warning** check box in the table header, the system selects warning logs for all processes.

GUI logs

Name	Description
GUI	Controls master log levels for all GUI logs. The options are: • Info • Warn • Error
SOAP	Includes detailed logs generated by a GUI SOAP client. SOAP handles communication with EMS and Avaya SBC Communication Manager servers, for example, restart application, reboot device, and uninstall device. This option is deprecated.
Statistics	Includes the trace logs for Statistics when this field is enabled.
HTTP	Includes the HTTP communication logs for REST API between EMS and SBCs when this field is enabled.

Table continues…

Name	Description
Shell Commands	Include detailed logs when you start any external process.
File Uploads	Includes detailed logs for user file uploads, for example, upgrade packages, scrubber packages, and certificates.
Licensing	Includes detailed logs generated by a GUI WebLM client.
Certificates	Includes the trace logs for TLS certificate installation when this field is enabled.
Backup / Restore	Includes the trace logs for backup and restore when this field is enabled.
Third Party Components	Controls a master log level for third-party logs. This log level covers any logs from third-party libraries that the GUI uses. The options are: • Debug • Info • Warn • Error
SSH	Controls log levels for a third-party SSH library used for backup or restore and remote actions. The options are: • Inherit • Debug • Info • Warn • Error
SNMP	Includes the SNMP logs based on the log level selected.
LDAP	Includes the LDAP logs based on the log level selected.
RADIUS	Includes the RADIUS logs based on the log level selected.
Spring	Includes the Spring framework logs based on the log level selected.
Square Utilities	Includes the Square Utilities logs based on log the level selected.

Third-Party Logs

Name	Description
Nginx	Controls log levels for nginx. The options are: • Info • Notice • Warn • Error • Crit • Alert • Emerg
Ldap	Controls log levels for LDAP. The options are: • Any • Packets • Config • Stats
Transcoding	Controls log levels for transcoding. The options are: • None • All
H248	Controls log levels for H248. The options are: • None • Error • Trace

Disabling application debug logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
3. Click the **Subsystem Logs** tab.
4. Do one of the following:
   - To disable all debug information on the device, clear the **Debug**, **Info**, and **Warning** log level check boxes at the table header.

- To disable a specific log level for all subsystems, clear the **Debug**, **Info**, or **Warning** log level check box at the table header.
- To disable log levels for a specific process, clear the **Debug**, **Info**, or **Warning** log level check box next to the process name.
- To disable log levels for a specific subsystem, expand the process name and clear the **Debug**, **Info**, or **Warning** log level check box next to the subsystem.

5. Click **Save**.

Enabling GUI debug logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
4. In the content area, click **Third-Party Logs** tab.
5. Select the required log levels.
6. Click **Save**.

Disabling GUI Logs

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **EMS**.
3. In the navigation pane, click **Monitoring & Logging** > **Debugging**.
4. In the content area, click **Third-Party Logs**.
5. Clear the required log levels.
6. Click **Save**.

Location of debug log files

Debug logs can be viewed or collected from the console.

The elog files for processes running on SBC are available at:

`/archive/log/ipcs/ss/logfiles/elog/`

The elog files for processes running on EMS are available at:

`/archive/log/ipcs/sems/logfiles/elog/`

The traceSBC logs for SIP are available at:

`/archive/log/tracesbc/tracesbc_sip`

The traceSBC logs for PPM are available at:

`/archive/log/tracesbc/tracesbc_ppm`

Core dumps are generated at:

`/archive/crash`

Smdumps for each process is available at:

`/usr/local/ipcs/smdump/`

Table 1: Elog locations for processes

Process	elog Path	Purpose
EMS		
SYSMON	`/archive/log/ipcs/sems/logfiles/elog/SYSMON`	To debug connectivity issues between Avaya SBC and EMS, process restart due to ping failure, and HA issues
OAMPSERVER	`/archive/log/ipcs/sems/logfiles/elog/OAMPSERVER`	To manage SNMP configuration of EMS
LOGSERVER	`/archive/log/ipcs/sems/logfiles/elog/LogServer`	To debug issues related to logging for other processes
Avaya SBC		
SBC SYSMON	`/archive/log/ipcs/ss/logfiles/elog/SYSMON`	To debug connectivity issues between Avaya SBC and EMS, process restart due to ping failure, and HA issues
SSYNDI	`/archive/log/ipcs/ss/logfiles/elog/SSYNDI`	To debug SIP application and media issues
OAMPSERVER	`/archive/log/ipcs/ss/logfiles/elog/OAMPSERVER`	To debug SNMP and statistics
TURNCONTROLLER	`/archive/log/ipcs/ss/logfiles/elog/TURNCONTROLLER`	To debug issues with TURN/STUN

Troubleshooting

Use the **Troubleshooting** menu item to:

- View system information, installed packages, and application status.
- Run a quick diagnostics on links between servers within your deployment and ping specific servers.

Related links

Viewing system information on page 104

Viewing system information

About this task

You can view the system information, installed packages, and application status.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Troubleshooting** > **System Information**.

   The application pane displays the System Information page.

   The Overview tab displays information about the following:

   - CPU
   - Memory
   - NIC
   - BIOS/UEFI
   - OS
   - Kernel

   The Versions tab displays the list of installed packages along with the following information:

   - Name
   - Base Version
   - Patch Version

   The Process Status tab displays the list of services along with the following information:

   - Name
   - Type
   - Status: Up or Down
   - CPU Usage
   - Memory Usage
   - Uptime

Related links

Troubleshooting on page 103

Running diagnostics tests

About this task

The Diagnostic Tests screen provides a variety of tools to aid in troubleshooting Avaya SBC operation. Available tools include a full diagnostic test suite, and individual tabs to monitor certain functional aspects of Avaya SBC, such as TCP and TLS activity.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Troubleshooting** > **Diagnostic Tests**.

   The application pane displays the Diagnostic Tests page.
3. Click **Full Diagnostics**.
4. Click **Start Diagnostic**.

   The tests listed in the **Task Description** column of the display are sequentially run, with the results of the test displayed in the **Status** column. If an error is encountered while running a test, the test continues until all tests are run. The application pane displays the reason for the error in the **Status** column.
5. Click **Ping Test**.

   The ping test can be used to verify basic IP connectivity to elements beyond the gateways. For example, ASM or the trunk server.

Diagnostics field descriptions

Full Diagnostic tab

Name	Description
EMS Link Check	Checks the EMS link.
EMS to Radius	Sends a ping request from EMS to the Radius server.
Ping: SBC to EMS	Sends a ping request from Avaya SBC to EMS.
Ping: EMS to SBC	Sends a ping request from EMS to Avaya SBC.
SBC Link Check: A1	Checks the Avaya SBC A1 interface. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2
Ping SBC [A1] to Gateway	Sends a ping request from the Avaya SBC A1 interface to the Gateway. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2

Table continues…

Name	Description
Ping SBC [A1] to Primary DNS	Sends a ping request from the Avaya SBC A1 interface to the Primary DNS. The interface can be from any of the following media interfaces: • A1 • A2 • B1 • B2
EMS to Radius	Sends a ping request from Avaya SBC to the Radius server.

Ping Test

Name	Description
Source Device / IP	The IP address of the device from where the ping originates.
Destination IP	The IP address to which the ping is sent.

Users

The **Users** menu item gives you a quick listing of which administrative users are logged on to the system.

Viewing administrative users

About this task

The Active Users page provides a summary of all active system administrative accounts currently logged on to the EMS web interface.

Note:

You can only view the users account information. You cannot modify the information.

Use the following procedure to view the system administrative accounts that are currently logged on to the interface.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the toolbar, click **Users**.

   The EMS server displays the Active Users page.

Active Users field descriptions

Name	Description
User Name	The name assigned to the user.
Role	The role of the user.
Real Name	The real name of the user.
Contact Info	The contact information of the user.
Time Logged In	The time when the user last logged in to EMS.

License usage

About this task

Use this procedure to monitor license usage and compliance with your purchased license limits. This information is useful to keep track of how often you are using and acquiring a license, and also the number of times you are exceeding your license limits. If you are exceeding your license limits regularly or excessively, it may indicate that you need to expand your licensing agreement or upgrade your system.

You can display license usage based on a range of dates and license types. The license types include:

- Standard
- Advanced
- Video
- Transcoding
- Client Enablement Services (CES)
- Premium

Licensing statistics are collected hourly and are displayed on a maximum per day basis.

You can export and save the license usage information into a CSV spreadsheet.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. Navigate to **Device Management** > **License Compliance**.
4. Enter a start and end date for which you want to view license usage.
5. Click **Search**.

   The system displays a line chart that shows the license usage for the dates selected.

6. You can then do any of the following steps to view usage data:
   - Hover over a date on the chart to display the number of licenses used, the number of licenses acquired, and the number of times the license was used over the purchased limit for that date.
   - Using the **Select License** drop-down, you can select other license types to see the same values for different license types.
   - Click **Export Data** to download and save the license statistics into a CSV spreadsheet.

Command line monitoring tools

Avaya SBC provides several command line tools to help you monitor status of your system.

Related links

traceSBC on page 108
Trace on page 114
tcpdump on page 115
showflow on page 116
sbceinfo on page 118
clipcs on page 118
swversion on page 119
Hardware specifications report file on page 120

traceSBC

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the non-encrypted private key of the Avaya SBC is needed to decrypt the TLS and HTTPS traffic.

The traceSBC tool offers solutions for both issues. traceSBC is a perl script that parses Avaya SBC log files and displays SIP and PPM messages in a ladder diagram. Because the logs contain the decrypted messages, you can use the tool easily even in case of TLS and HTTPS. traceSBC can parse the log files downloaded from Avaya SBC. traceSBC can also process log files real time on Avaya SBC, so that you can check SIP and PPM traffic during live calls. The tool can also work in the noninteractive mode, which is useful for automation testing.

Note:

In Release 10.1.2, traceSBC tool can only be run as "root" user.

Log files

Avaya SBC can log SIP messages as processed by different subsystems and also log PPM messages. The traceSBC utility can process the log files in real-time by opening the most recent log files in the given directories. traceSBC also checks regularly if a new file is generated, in which case the old one is closed and processing continues with the new one. A new log file is generated

every time the relevant processes restart, or when the size of the file reaches the limit of about 10 MBytes.

Log locations:

The traceSBC logs for SIP are available at:

`/archive/log/tracesbc/tracesbc_sip`

The traceSBC logs for PPM are available at:

`/archive/log/tracesbc/tracesbc_ppm`

Active files are of the following format:

```
-rw-rw---- 1 root root 112445 Aug 21 10:12 tracesbc_sip_1408631651
```

Inactive or closed files are of the following format:

```
-rw-rw---- 1 root root 175236 Aug 21 06:33
tracesbc_sip_1408617250_1408620820_1
```
or

```
-rw-rw---- 1 root root 31706 Jul 10 13:34
tracesbc_sip_1436549674_1436553270_1.gz
```

SIP and PPM logging administration

SIP logging is always enabled by default. You can enable PPM, STUN, TLS, and AMS logging, if required.

Performance benefits

Memory

After 10000 captured messages, traceSBC stops processing the log files to prevent exhausting the memory. This check is done during the capture when the tool is parsing the log files. The tool counts the number of SIP and PPM messages in the logs. This number is not the number of messages sent or received on the interfaces. This counter is a summary of messages from all logs, not for each log. Note that this safeguard is present only for real-time mode. When the tool is used in non real-time mode, this counter does not stop processing the logs specified in the command line. The counter continues processing the logs specified in the command line to be able to process more files or messages in off-line mode.

Processor

A built-in mechanism is available to prevent high CPU usage. Throttling is not tied to CPU level. In the current implementation, throttling is done by releasing the CPU for a short period after each line of the file is processed. The result is that CPU occupancy is low on an idle system when the tool actively processes large log files. You can disable throttling by the –dt command line parameter which can be useful when processing large log files offline. However, in this case CPU occupancy might go up to 100%, and so you must not use this option on a live system.

Operational modes

Non real-time mode

The tool starts with at least one file in the command line parameters. The tool automatically detects the type of files, processes the files, and finally displays messages from the different files in one diagram ordered by the timestamp. If filters are set, only the messages that match the filters are displayed in the diagram. In this mode, enabling live capture is not an option.

Examples:

traceSBC tracesbc_sip_1408635251

traceSBC /archive/log/tracesbc/tracesbc_sip/tracesbc_sip_1408635251 archive/log/tracesbc/tracesbc_ppm/tracesbc_ppm_1408633429

Real-time mode

In this mode, traceSBC runs interactively. You must run traceSBC on the active SBC and without specifying a file in the command line parameters. When you run **traceSBC**, the tool opens, displaying a list of options at the bottom of the screen. Those options are described in User interface elements and options on page 111.

Once you start the trace, the system automatically starts processing the log files. The live capture can be started and stopped anytime without affecting service.

Automatic mode

In this mode, traceSBC must be on the SBC and the command is called with -a and -w parameters at a minimum.

Example:

traceSBC -a "sip|ppm" -w /tmp/trace.log

Use this mode for test automation. You can also use this mode to stop capture when a certain condition is met, and then save filtered messages automatically. Multiple stop triggers are present, such as number of packets, time, regular expression, and a combination of these. When a stop trigger fires, or when you press CTRL+C, the tool automatically saves the filtered messages and stops the captures.

Command line options

Use **traceSBC** to start the traceSBC tool from the command line interface. For command line help, use the “–h” parameter.

traceSBC [-h] [options *SBC_LOG_FILE*

Where options are

-u *URI|NUMBER*	Filter calls that contain URI|NUMBER in the **From** or **To** field.
-i *IP*	Filter messages from/to <IP> address.
-c *CALL-ID*	Filter based on the SIP 'Call-ID' header field.
-r *REGEXP*	Filter messages based on the regular expression.

-g *HEA=VALUE*	Filter SIP header field <HEA> for value <VALUE>.
-or	Use a logical OR operator instead of the implicit. Use AND when using multiple filter options.
-nr	Do not display REGISTER messages.
-ns	Do not display SUBSCRIBE/NOTIFY/PUBLISH messages.
-no	Do not display OPTIONS messages.
-np	Do not display PPM messages.
-uni	Use Unicode/UTF-8 characters. Display the arrows and other lines in graphic mode. Your terminal client has to support Unicode to display this correctly.
-m	Use to run multiple instances of traceSBC.
-k	Kill other traceSBC instances.
-w *FILE*	Set filename for saving filtered messages.
-a *TYPE*	Starts specific captures in non-interactive mode where <TYPE> can be `sip|ppm|callp`.
-st *SEC*	Stops capture after given seconds.
-sp *PACKET*	Stops capture after given number of captured messages.
-sr <REGEXP>	Stops capture if regular expression found a match.
-srt <SEC>	Run trace <SEC> more seconds after REGEXP match.
-srp <PACKET>	Collect <PACKET> more messages after REGEXP match.
SBC_LOG_FILE	File name of the SSYNDI file or files previously captured with traceSBC. More than one file can be specified. If no file is specified, then you can start or stop the capture using the **s** key.

User interface elements and options

Window header

The window header shows the hostname, the name of the script, the number of captured messages, and the number of displayed messages that matched the filters. The header also displays warning messages such as MAX NUM PACKETS 10000 EXCEEDED.

Status bar

The status bar on the bottom of the screen is the most important and most used part of the tool. The bottom line has two areas, and its content depends on which mode the tool is in. The left side of the status bar shows the filename in nonreal-time mode, or shows Multiple files when the tool

was called with more than one file. In real-time mode, this area shows which trace is active. Red means disabled, and green means enabled.

The rest of the status bar lists the available commands:

s=Start / s=Stop : Starts or stops live capture, which means the tool enables or disables the appropriate logging. Capture can be enabled for SIP and PPM individually. Stop disables all logging at the same time and stops processing the log files. This command shows only if the tool was started in real-time mode.

Note:

Depending on the traffic and the capture modes at the time of stopping the trace, the log files might contain more messages than the messages already captured by the tool.

q=Quit: Quit from the tool. If capture is running, the tool shows a pop-up to confirm the exit without stopping the logging.

w=Write: Export filtered messages to a file. The dialog prompts you for a filename. The system saves SIP messages in the specified file to the current directory. The system saves PPM messages in a separate file with a `.ppm` extension. The system also exports SIP messages in pcapng format to a file with a `.pcapng` extension. SIP messages can be exported if text2pcap and tshark utilities are available on the machine where you run traceSBC.

i=IP / i=Name: Toggle between IP and user name presentation of the hosts in the header of the ladder diagram.

r=RTP: Turn RTP simulation on or off. When a session is established early or confirmed, the tool inserts a line in the diagram. This line represents the RTP stream between the two hosts described by the SDP. The diagram also shows the negotiated codec type.

Note:

The RTP stream is created based on the negotiated information in SDP. However, there is no guarantee that these RTP streams come to the system.

u=Full Screen: Use the full screen for the message detail box without having the left and right side of the frame. This option is useful not only to see more about the message, but to easily copy or paste the content.

d=Calls: Shows the summary of all calls.

Ladder diagram

The ladder diagram displays the filtered messages. The arrow shows the direction of the message between the SBC and the host from where the message arrived or was sent to. The IP of the host is at the top of the column. If the host is an Avaya phone, traceSBC attempts to extract the user information from the message, and replaces the IP with the user handle. To navigate between the messages, use the UP/DOWN arrow keys. The message is highlighted. To see the details of the message, press `Enter`. The header of the message detail form shows the source and destination IP or port and the transport protocol.

Filter options

The **f=Filters** filter options set in the dialog window override the command line option settings. If no new filter is entered, the current filter will remain active. To clear all filters, type **e** or **erase** in the **New Filter** field. The following is an example of the available filters:

```
Display Filter Usage:
  -u <URI|NUMBER>  Filter calls that contain <URI|NUMBER> in
                   the 'From' or 'To' field.
  -i <IP>          Filter messages from/to <IP> address.
  -port <PORT>     Filter messages from/to <PORT>.
  -noport <PORT>   Filter messages from/to any ports except <PORT>.
  -c <CALL-ID>     Filter on the SIP 'Call-ID' header.
  -r <REGEXP>      Filter messages based on regular expression.
  -s <GSID>        Filter on the SIP 'Av-Global-Session-ID' header.
  -g <HEA>=<VALUE> Filter SIP header field <HEA> for value <VALUE>.
  -or              Use a logical OR operator instead of the implicit
                   AND when using multiple filter options.
  -nr              Do not display REGISTER messages.
  -ns              Do not display SUBSCRIBE/NOTIFY/PUBLISH messages.
  -no              Do not display OPTIONS/PING messages.
  -ni              Do not display INFO messages.
  -np              Do not display PPM messages.
  -nu              Do not display STUN/TURN/ICE messages.
  -nt              Do not display TLS Handshake messages.
  -nh              Do not display HTTP/WEBRTC messages.
  -nm              Do not display AMS WEBUA messages.
  -nl              Do not display LDAP messages.
```

Usage examples

Start a new capture

To start a new capture, run **traceSBC** without arguments and then press `s`: **traceSBC**

Filter a GSID

The “s” filter provides a way to trace the Avaya Global Session Identifier (GSID) header to filter SIP call traces. A GSID is in a form similar to 16169a40-cfe2-11ea-aeb9-00505694198d.

Note:

To use the GSID filter, the **Extensions** option in server interworking must be set to **Avaya**.

Filter SIP messages

To filter SIP messages from/to 1.1.1.1 and 2.2.2.2, enter the following command:

traceSBC -i *"1.1.1.1|2.2.2.2”*

Analyze an SSYNDI file

To analyze a previously captured SSYNDI file named `my_sbc.log`, enter the following command:

traceSBC my_sbc.log

Note:

Enable the debug log setting before performing the analysis. traceSBC does not display the logs if the debug log settings are not enabled. To enable SSYNDI debug logs, log on to the

EMS and navigate to **Monitoring & Logging** > **Debugging**. Select the SBC device and then click the **SSYNDI debug logs**checkbox.

Trace

With the Trace function, you can trace an individual packet or group of packets comprising a call through Avaya SBC. The information shows how the call traversed the Avaya SBC-secured network.

Configuring Packet Capture

About this task

Use the following procedure to set the filtering options and to capture packets or message flow.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. On the **Device** menu, click the **SBC** name to administer.
3. In the navigation pane, click **Monitoring & Logging** > **Trace**.
4. Click **Packet Capture** or the **Captures** tab for the required information.
5. Navigate to a directory for saving the Packet Capture (pcap) file and click **Save** to save the file to the new directory.
6. Use Wireshark or a similar application to open up the Packet Capture (pcap) file. If Wireshark is already installed, you can double-click the file to open it with Wireshark. Otherwise, start Wireshark first and then either open the file from within the Wireshark application or double-click the Packet Capture file.

Note:

You can view the file using Wireshark (originally named Ethereal), a free and open-source packet analyzer application used for network troubleshooting, analysis, and software protocol development. You can download and install Wireshark, or a similar network analyzer program, to view the Packet Capture (pcap) file.

Trace field descriptions

Packet Capture

Name	Description
Status	The current status of the system for capturing packets.
Interface	The interface used for packet capture.
Local Address	The local IP address and port. The default value for this field is All.

Table continues…

Name	Description
Remote Address	The remote IP address and port. The default value for this field is an asterisk (*).
Protocol	The protocol used for packet capture. The options are: • **All** • **UDP** • **TCP**
Maximum Number of Packets to Capture	The number of packets to capture data. You can enter a value between 1 and 10,000.
Capture Filename	The name of the file used to capture data. If you use the name of an existing capture file, the system overwrites the file.

Button	Description
Start Capture	Begins the packet capture.
Clear	Clears the values that you entered in the **Packet Capture** tab.

Captures tab

Name	Description
File Name	The name of the packet capture file.
File Size (bytes)	The size of the packet capture file.
Last Modified	The latest date and time at which the capture file was changed. The default value for this field is **All**.

In addition to these fields, the **Captures** tab has two additional fields for sorting the packet captures by file name, file size, or last modified date.

Button	Description
Sort	Sorts the list of packet capture files by file name, file size, or last modified date.
Reset	Clears the values that you selected for sorting the data.

tcpdump

The tcpdump tool is the main troubleshooting tool of Avaya SBC, which can capture network traffic. Using tcpdump is a reliable way to analyze the information arriving to and sent from Avaya SBC. However, tcpdump has its own limitations, which can make troubleshooting difficult and time consuming. This traditional tool is not useful in handling encrypted traffic and real-time troubleshooting.

You can use tcpdump to capture packets from the CLI if you need to capture more than 10000 packets. After the captures are taken, ensure you stop the command.

SIP and PPM traffic is encrypted especially in Remote Worker configurations. Checking encrypted traffic with a network capture is difficult and time consuming. The delay occurs because the unencrypted private key of the Avaya SBC is needed to decrypt the TLS and HTTPS traffic.

For packet capture started through GUI, the output files are stored in `/archive/pcapfiles/IPCS2`.

Running tcpdump in CLI

Procedure

1. Log on to the EMS server through SSH with ipcs user credentials.
2. At the command prompt, type `cd /archive/pcapfiles/IPCS2`.
3. Type `tcpdump -ni any -s 0 -w '`*`filename`*`.pcap'`, where *filename* is the name of the packet capture file.
4. To run packet captures on a specific interface, type `tcpdump -i any -s 0 -w '`*`filename`*`.pcap'`

   To run packet captures on a specific interface, use **`tcpdump -I`** *data_interface*. Packet capturing on Avaya SBC negatively impacts packet latency.
5. Wait for the capture to end, and press `Ctrl+C`.
6. Type `chown ipcs:ipcs `*`filename`*`.pcap`.

   The system displays the packet capture file in the **Captures** tab in the EMS web interface.

showflow

A flow is a connection between an endpoint and Avaya SBC. Types of flows are:

- Static: A static flow is configured on the Avaya SBC only one time. Static flows do not change until the administrator changes the flows. Static flows are used, for example, for connections between endpoints and an Avaya SBC signaling address.
- Dynamic: A dynamic flow is a transient connection between an endpoint and Avaya SBC. Software creates, modifies, and deletes dynamic flows to support the transfer of media packets through Avaya SBC.

Many flows can exist on Avaya SBC simultaneously. To troubleshoot issues with Avaya SBC, you can use the **`showflow`** command to display flows with varying levels of detail.

Description

`showflow` is a root-level console command to display the flows that are currently active on Avaya SBC.

Syntax

`showflow` 310 *flow-type detail-levelfilter-ip*

flow-type

The flow type can be:

- static: Shows all static flows.
- dynamic: Shows all dynamic flows.
- turn_client_side: Shows all TURN flows on the listen interface of Avaya SBC.
- turn_far_side: Shows all TURN flows on the relay interface of Avaya SBC.
- blacklist: Shows all IP addresses that are currently blacklisted. Packets from blacklisted addresses do not match any flows.
- whitelist: Shows only those static flows that require whitelisting of the endpoint IP address.

detail-level

You can specify the detail level for dynamic flows. The detail level for all other flows is fixed. When levels exceed the default detail level 0, you can see the default flow information and also additional information for the flow. The detail levels for dynamic flows can be:

- 0: Shows the default level of information. If a detail level is not specified in the command, the system uses 0 detail level.
- 1: Adds more decrypt information to every flow.
- 2: Adds more encrypt information to every flow.
- 3: Adds the physical port number for the output of the flow. Packets matching this flow are sent out of this physical port.
- 4: Adds relay information. Packets matching this flow are changed according to this relay before they are forwarded.
- 5: Adds VLAN identifiers and flow statistics.
- 6: Adds SIPREC information. This option does not change non-SIPREC flows.
- 7: Adds encrypt information for a SIPREC flow. This option does not change non-SIPREC flows.
- 8: Adds decrypt information for a SIPREC flow. This option does not change non-SIPREC flows.
- 12: Shows RTCP-MUX actors applied on "dynamic flows".

filter-ip

If you specify a filter IP address, the **`showflow`** command displays dynamic flows that use the IP address that you specified as:

- An input or a packet source
- An output or a packet destination

When you specify a filter IP address, the **`showflow`** command displays dynamic flows pertaining to an endpoint with that IP address. If you do not provide a filter IP address, the system displays all dynamic flows.

Example

The following example displays full details of all dynamic flows with 10.20.30.40 as a source or destination:

showflow 310 dynamic 8 10.20.30.40

The following example displays all static flows:

showflow 310 static

sbceinfo

Use the **sbceinfo** command options to obtain system version, application type, and hardware details.

Syntax

```
sbceinfo [options]
```

Where options are:

getversion	Displays Avaya SBC version information.
gethwtype	Displays Avaya SBC hardware information.
getemsip	Displays the EMS IP address.
getapptype	Displays the application type running on the server.

clipcs

About this task

The **clipcs** commands are used to display basic information about Avaya SBC system configuration and status. You can run the **clipcs** console commands by logging in as a root user. To run these commands, first enter **clipcs** at the root prompt.

Note:

clipcs commands are deprecated in Release 10.1.2.

The **clipcs** commands are grouped according to two modes of operation: Console and Instance. The Console mode is the top-level command structure from which basic Avaya SBC systemwide commands can be executed. The Instance mode is the next level of administrative control that provides direct access to a particular Avaya SBC functional node.

Use the following procedure to run the **clipcs** console commands.

Note:

All **clipcs** commands and arguments are case-sensitive.

Procedure

1. On the root level prompt (#), enter the following command:

clipcs

The system displays the Avaya SBC console.

```
[root@EMS ~]# clipcs
Starting SBC Console...Please wait.
SBC Version x.x.x (C) Avaya Inc.
SBC Status:
Installation    Status
--------------- ----------------------------------------
sems           Running since Jul 30 12:23:50
ss                Running since Jul 30 12:23:50
SBC#
```

2. At the `SBC#` prompt, enter the following command:

   help

   The system displays the list of available **clipcs** commands.

clipcs commands and descriptions

The following table contains a list of **clipcs** commands and descriptions of commands available at the console prompt (#):

Command	Description
clear	Clears the display screen.
clock	Displays, sets, and clears the internal system clock.
exit	Moves the command level from instance mode to console mode. Also closes the clipcs screen when the command level is in the Console mode.
quit	Closes the clipcs screen when the command level is in the Console mode.
help	Displays a list of available commands and their descriptions.
refresh	Refreshes the open session screen.
spool	Spools to file settings.
status	In the Console mode, this command displays the status of Avaya SBC nodes. In the Instance mode, this command displays the detailed operational status of the node being accessed.
select	Selects a particular Avaya SBC node for access and activates the Instance mode.

swversion

The **swversion** command displays the product name, instance name, software version, and product deployment. See the following example:

```
Product Name            : ASBCE-8.X
Product Instance Name   : IPCS ID=[2] NODE ID=[11]
Product Version         : 8.1.2.0-25-19490
Product Deployment      : VMware Virtual Platform
```

Note:

You must be logged on as superuser, such as root, to run this command.

Hardware specifications report file

When a system is deployed, Avaya SBC automatically creates the file `/usr/local/ipcs/etc/hw_specs_report.txt` that contains hardware-related information about the system. To view this file, you must be logged on as root.

The following are some examples of the information stored in this file:

```
Number of NICs: 6
Product Information: MicroSBC
HWModel: CAD0230
Number of CPUs: 2
CPU Type:               64-bit capable
Number of Disks: 1
Disk space: 476940 MB
RAM: 1819 MB
manufacturer:Portwell
Applications Supported: EMS+SBCE
Model:110
```

```
Number of NICs: 2
Product Information: VMware Virtual Platform
HWModel: UNKNOWN
CPU Type:               64-bit capable
Number of CPUs: 4
Number of Disks: 1
Disk space: 163840 MB
RAM: 7725 MB
manufacturer:VMware,Inc.
Applications Supported: EMS
Model:EMS
```

```
Number of NICs: 4
Product Information: VMware Virtual Platform
HWModel: UNKNOWN
CPU Type:               64-bit capable
Number of CPUs: 8
Number of Disks: 1
Disk space: 163840 MB
RAM: 7820 MB
manufacturer:VMware,Inc.
Applications Supported: EMS+SBCE
Model:110
```

```
Number of NICs: 6
Product Information: VMware Virtual Platform
HWModel: ESXi6.5
CPU Type:               64-bit capable
Number of CPUs: 4
Number of Disks: 1
Disk space: 163840 MB
RAM: 7821 MB
manufacturer:VMware,Inc.
Applications Supported: SBCE EMS+SBCE
Model:310
```

Instance commands

Instance commands are also referred to as **top** commands. These commands are used to display detailed information about a specific Avaya SBC node in the network and EMS node with multiple Avaya SBC nodes.

Instance commands are only available within the instance mode, which is enabled when you run the **clipcs select** command for a node or application instance. Instance commands communicate directly with the active Avaya SBC node or communicate with the selected EMS or Avaya SBC application instance that runs on a single platform. Instance commands provide output from the active node or instance only.

Screen displays for the presented instance commands are automatically refreshed at a rate determined by the **refresh** command. The default refresh rate is 5 seconds.

top command description

You can use the **top** command for troubleshooting.

Command	Description
top	Displays a detailed functional status of the selected Avaya SBC node. The display is automatically refreshed every 5 seconds.

Traps

To see Avaya SBC alarms on System Manager, you must upload the Avaya SBC common alarms definition file (cadf) to System Manager.

Trap descriptions

SNMP trap is a message sent from a network device to an SNMP management system. Trap is triggered when a specific event or condition occurs on the device, such as a link going down, an authentication or a power failure.

The SNMP trap message contains information about the event or condition, such as the device and interface where the event occurred, the time the event occurred and the information related to the event.

Clear traps or alarms are not associated with all the events.

Avaya SBC sends an alarm and a trap during a system event and clears the trap and the alarm when the event is resolved. For some events, clearing the traps and alarms is not required.

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
CPU Usage	ipcsCPUUsage	ipcsCPUUsageClearAlarm	CPU usage exceeded a set threshold.	System	Critical: CPU utilization is 100% Major: CPU utilization is over 95%	EMS SBC
Memory Usage	ipcsMemoryUsage	ipcsMemoryUsageClearAlarm	Memory usage exceeded a set threshold.	System	Critical: Memory utilization is 100%	EMS SBC
Disk Usage	ipcsDiskUsage	ipcsDiskUsageClearAlarm	Disk usage exceeded a set threshold.	System	Critical: Disk usage is over 90% Major: Disk usage is over 80% Minor: Disk usage is over 70%	EMS SBC
Network Failure	ipcsNetworkFailure	ipcsNetworkInterfaceClearAlarm	Network failed.	System	Critical	EMS SBC
Process Fail	ipcsProcessFail	ipcsProcessFailClearAlarm	Process in use failed.	System	Critical	EMS SBC
Database Fail	ipcsDatabaseFail	ipcsDatabaseFailClearAlarm	Database failed.	System	Critical	EMS SBC
HA Failure	ipcsHAFailure	-	High Availability failed.	System	Critical : Primary server is down Informational: Secondary server is coming to Primary server	SBC: For HA deployment mode

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
HA Heart Beat Failure	ipcsHAHeartBeatFailure	-	Heartbeat from secondary HA server failed.	System	Critical	SBC: For HA deployment mode
RSA Failure	ipcsRSAFailure	-	RSA algorithm failed.	System	Critical	EMS SBC
Incidence Notification	ipcsIncidenceNotification	-	Notification for incidence occurring in Avaya SBC.	System	No severity level is defined for this alarm.	EMS SBC
Certificate Expiry Alert	ipcsCertificateExpiryAlert	ipcsCertificateExpiryAlertClearAlarm	Certificate expiry alert.	System	Critical	EMS SBC
Network Interface M1 Alarm	ipcsNetworkInterfaceM1FaultAlarm	ipcsNetworkInterfaceM1ClearAlarm	Network Interface M1 alarm.	System	Critical	EMS SBC
Network Interface M1 Alarm	ipcsNetworkInterfaceM2FaultAlarm	ipcsNetworkInterfaceM2ClearAlarm	Network Interface M2 alarm.	System	Critical	EMS SBC
Ssyndi alarm	ipcsSsyndiFaultAlarm	ipcsSsyndiClearAlarm	Ssyndi alarm.	System	Critical	SBC
Log server alarm	ipcsLogServerFaultAlarm	ipcsLogServerClearAlarm	Log server alarm.	System	Critical	EMS SBC
OAMP Server alarm	ipcsOAMPServerFaultAlarm	ipcsOAMPServerClearAlarm	OAMP server alarm.	System	Critical	EMS SBC
Turn Controller Alarm	ipcsTurnControllerFaultAlarm	ipcsTurnControllerClearAlarm	Turn controller alarm.	System	Critical	EMS SBC
Kernel Core Alarm	ipcsKernelCoreFaultAlarm	ipcsKernelCoreClearAlarm	Kernel core alarm.	System	Critical	EMS SBC
Slapd alarm	ipcsSlapdFaultAlarm	ipcsSlapdClearAlarm	Slapd alarm.	System	Critical	EMS SBC
Nginx management alarm	ipcsNginxMgmtFaultAlarm	ipcsNginxMgmtClearAlarm	Nginx management alarm.	System	Critical	EMS SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Nginx data alarm	ipcsNginxDataFaultAlarm	ipcsNginxDataClearAlarm	Nginx data alarm.	System	Critical	EMS SBC
Firewall alarm	ipcsFirewallFaultAlarm	ipcsFirewallClearAlarm	Firewall alarm.	System	Critical	EMS SBC
Standard Sessions License Use Exceed	ipcsStdSesLicenseUseExceed	ipcsStdSesLicenseUseExceedClearAlarm	Standard sessions license usage exceeded the set threshold.	System	Critical	EMS SBC
Advanced Sessions License Use Exceed	ipcsAdvSesLicenseUseExceed	ipcsAdvSesLicenseUseExceedClearAlarm	Advanced sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Ces Proxy Sessions License Use Exceed	ipcsCesProxySesLicenseUseExceed	ipcsCesProxySesLicenseUseExceedClearAlarm	CES proxy sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Transcode Sessions License Use Exceed	ipcsTranscodeSesLicenseUseExceed	ipcsTranscodeSesLicenseUseExceedClearAlarm	Transcode sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC
Video Sessions License Use Exceed	ipcsVideoSesLicenseUseExceed	ipcsVideoSesLicenseUseExceedClearAlarm	Video sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Standard Concurrent Sessions Limit Exceed	ipcsStdConcurrentSesLimitExceed	ipcsStdConcurrentSesLimitExceedClearAlarm	Standard concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Advanced Concurrent Sessions Limit Exceed	ipcsadvConcurrentSesLimitExceed	ipcsadvConcurrentSesLimitExceedClearAlarm	Advanced concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
CESP Concurrent Sessions Limit Exceed	ipcsCESPConcurrentSesLimitExceed	ipcsCESPConcurrentSesLimitExceedClearAlarm	CESP concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Transcode Concurrent Sessions Limit Exceed	ipcsTrcdConcurrentSesLimitExceed	ipcsTrcdConcurrentSesLimitExceedClearAlarm	Transcode concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Video Concurrent Sessions Limit Exceed	ipcsVIDConcurrentSesLimitExceed	ipcsVIDConcurrentSesLimitExceedClearAlarm	Video concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Prem Sessions License Use Exceed	ipcsPremSesLicenseUseExceed	ipcsPremSesLicenseUseExceedClearAlarm	Prem sessions license usage exceeded the set threshold.	System	Critical Major Minor	SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Prem Concurrent Sessions Limit Exceed	ipcsPremConcurrentSesLimitExceed	ipcsPremConcurrentSesLimitExceedClearAlarm	Prem concurrent sessions limit exceeded the set threshold.	System	Critical	SBC
Standard Sessions License Acquire Failed	ipcsStdSesLicenseAcquireFailed	ipcsStdSesLicenseAcquireFailedClearAlarm	Standard sessions license acquire failed.	System	Major	SBC
Advanced Sessions License Acquire Failed	ipcsAdvSesLicenseAcquireFailed	ipcsAdvSesLicenseAcquireFailedClearAlarm	Advanced sessions license acquire failed.	System	Major	SBC
CESP Sessions License Acquire Failed	ipcsCESPSesLicenseAcquireFailed	ipcsCESPSesLicenseAcquireFailedClearAlarm	CESP sessions license acquire failed.	System	Major	SBC
Transcode Sessions License Acquire Failed	ipcsTransSesLicenseAcquireFailed	ipcsTransSesLicenseAcquireFailedClearAlarm	Transcode sessions license acquire failed.	System	Major	SBC
Video Sessions License Acquire Failed	ipcsVideoSesLicenseAcquireFailed	ipcsVideoSesLicenseAcquireFailedClearAlarm	Video sessions license acquire failed.	System	Major	SBC
Prem Sessions License Acquire Failed	ipcsPremSesLicenseAcquireFailed	ipcsPremSesLicenseAcquireFailedClearAlarm	Prem sessions license acquire failed.	System	Major	SBC
Single Source DoS	ipcsSingleSourceDoS	-	Single Source DoS.	Incidences		SBC
Single Source Call Walk DoS	ipcsSingleSourceCallWalkDoS	-	Single Source Call Walk DoS.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Phone DoS	ipcsPhoneDoS	-	Phone DoS.	Incidences		SBC
Phone Stealth DoS	ipcsPhoneStealthDoS	-	Phone Stealth DoS.	Incidences		SBC
Server DoS	ipcsServerDoS	-	Server DoS.	Incidences		SBC
Phone DDoS	ipcsPhoneDDoS	-	Phone DDoS.	Incidences		SBC
Phone Stealth DDoS	ipcsPhoneStealthDDoS	-	Phone Stealth DDoS.	Incidences		SBC
Domain DoS	ipcsDomainDoS	-	Domain DoS.	Incidences		SBC
Black List Call Blocked	ipcsBlackListCallBlocked	-	Black listed call is blocked.	Incidences		SBC
Turing Test Failed	ipcsTuringTestFailed	-	Turing test failed.	Incidences		SBC
Dropped Scrub Message	ipcsDroppedScrubMsg	-	Dropped Scrub message.	Incidences		SBC
Rejected Scrub Message	ipcsRejectedScrubMsg	-	Rejected Scrub message.	Incidences		SBC
Fingerprint Failed	ipcsFingerprintFailed	-	Fingerprint failed.	Incidences		SBC
ACK Message Out of Dialogue	ipcsACKMsgOutofDialogue	-	ACK Message out of dialogue.	Incidences		SBC
BYE Message Out of Dialogue	ipcsBYEMsgOutofDialogue	-	BYE Message is out of dialogue.	Incidences		SBC
CANCEL Message Out of Dialogue	ipcsCANCELMsgOutofDialogue	-	CANCEL Message is out of dialogue.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
NOTIFY Message Out of Dialogue	ipcsNOTIFYMsgOutofDialogue	-	NOTIFY Message is out of dialogue.	Incidences		SBC
PRACK Message Out of Dialogue	ipcsPRACKMsgOutofDialogue	-	PRACK Message is out of dialogue.	Incidences		SBC
REINVITE Message Out of Dialogue	ipcsREINVITEMsgOutofDialogue	-	REINVITE Message is out of dialogue.	Incidences		SBC
REFER Message Out of Dialogue	ipcsREFERMsgOutofDialogue	-	REFER Message is out of dialogue.	Incidences		SBC
1XX Message Out of Transaction	ipcs1XXMsgOutofTransaction	-	1XX Message out of transaction.	Incidences		SBC
2XX Message Out of Transaction	ipcs2XXMsgOutofTransaction	-	2XX Message out of transaction.	Incidences		SBC
3XX Message Out of Transaction	ipcs3XXMsgOutofTransaction	-	3XX Message out of transaction.	Incidences		SBC
4XX Message Out of Transaction	ipcs4XXMsgOutofTransaction	-	4XX Message out of transaction.	Incidences		SBC
5XX Message Out of Transaction	ipcs5XXMsgOutofTransaction	-	5XX Message out of transaction.	Incidences		SBC
6XX Message Out of Transaction	ipcs6XXMsgOutofTransaction	-	6XX Message out of transaction.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
Auth Realm Mismatch	ipcsAuthRealmMismatch	-	Authorization Realm is mismatched.	Incidences		SBC
Halo Finger Print Failed	ipcsHaloFingerPrintFailed	-	Halo Finger Print has failed.	Incidences		SBC
Call Denied	ipcsCallDenied	-	Call is denied.	Incidences		SBC
Registration Denied	ipcsRegistrationDenied	-	Registration is denied.	Incidences		SBC
Subscription Denied	ipcsSubscriptionDenied	-	Subscription is denied.	Incidences		SBC
Redirection Denied	ipcsRedirectionDenied	-	Redirection is denied.	Incidences		SBC
Message Dropped	ipcsMessageDropped	-	Message dropped.	Incidences		SBC
Routing Failure	ipcsRoutingFailure	-	Routing failed.	Incidences		SBC
Server Heartbeat	ipcsServerHeartbeat	-	Server heartbeat.	Incidences		SBC
Radius Auth Failed	ipcsRadiusAuthFailed	-	Radius authorization failed.	Incidences		SBC
Primary Radius Server Unreachable	ipcsPrimaryRadiusServerUnreachable	-	Primary Radius server is not reachable.	Incidences		SBC
Secondary Radius Server Unreachable	ipcsSecondaryRadiusServerUnreachable	-	Secondary Radius server is not reachable.	Incidences		SBC
TLS No Client Cert Present	ipcsTlsNoClientCertPresent	-	TLS no client certificate is present.	Incidences		SBC
TLS Client Cert In CRL	ipcsTlsClientCertInCRL	-	TLS client certificate in CRL.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
TLS Certificate	ipcsTlsCertificate	-	TLS certificate.	Incidences		SBC
Codec Violation	ipcsCodecViolation	-	Codec is violated.	Incidences		SBC
Packet Size Violation	ipcsPacketSizeViolation	-	Packet size is violated.	Incidences		SBC
SSRC Violation	ipcsSSRCViolation	-	SSRC is violated.	Incidences		SBC
Sequence Number Violation	ipcsSeqNoViolation	-	Sequence number is violated.	Incidences		SBC
Timestamp Violation	ipcsTimestampViolation	-	Timestamp is violated.	Incidences		SBC
Media In Activity From Both Sides	ipcsMediaInActivityFromBothSides	-	Media is in activity from both sides.	Incidences		SBC
Unsupported Media	ipcsUnsupportedMedia	-	Media is not supported.	Incidences		SBC
RTP DoS Attack	ipcsRTPDoSAttack	-	RTP DoS attack.	Incidences		SBC
RTP DDoS Attack	ipcsRTPDDoSAttack	-	RTP DDoS attack.	Incidences		SBC
RTP Injection Attack	ipcsRTPInjectionAttack	-	RTP Injection attack.	Incidences		SBC
Media Port Unavailable	ipcsMediaPortUnavailable	-	Media Port is unavailable.	Incidences		SBC
HA Graceful Failover	ipcsHAGracefulFailover	-	HA Graceful failover.	Incidences		SBC
HA Ka Fail	ipcsHAKaFail	-	HA Ka failed.	Incidences		SBC
HA Takeover Done	ipcsHATakeoverDone	-	HA Takeover is done.	Incidences		SBC
HA Oct Core Crashed	ipcsHAOctCoreCrashed	-	HA Oct Core crashed.	Incidences		SBC

Table continues…

Alarm name	Trap name	Clear trap/ alarm name	Description	Category	Level	Component generating the trap
HA Secondary Down	ipcsHASecondaryDown	-	HA Secondary server is down.	Incidences		SBC
HA Octeon Communication Failed	ipcsHAOcteonCommunicationFailed	-	HA Octeon Communication failed.	Incidences		SBC
SBC License Exceeded	sbcLicenseExceeded	-	SBC license exceeded a set threshold.	Incidences		SBC
SBC Turn Stun Media Relay Creation Failed	sbcTurnStunMediaRelayCreationFailed	-	SBC Turn Stun Media Relay creation failed.	Incidences		SBC
SBC Turn Stun Media Relay Deletion Failed	sbcTurnStunMediaRelayDeletionFailed	-	SBC Turn Stun Media Relay deletion failed.	Incidences		SBC
SBC Turn Stun Server Error	sbcTurnStunServerError	-	SBC Turn Stun Server error.	Incidences		SBC
SBC Ces Proxy 1xM User Login Failed	sbcCesProxy1xMUserLoginFailed	-	SBC Ces Proxy 1xM User Login Failed	Incidences		SBC
Detected Scrub Mssage	ipcsDetectedScrubMsg	-	Detected Scrub Message	Incidences		SBC

SNMP MIBs

Avaya SBC supports the Management Information Base (MIB) for data interfaces as defined in RFC-1213, rfc1213.mib. This section describes the MIBs you can download and view using SNMP.

Downloading the Avaya SBC MIB

The latest Avaya SBC MIB file is available in the downloads section on the support website at: http://support.avaya.com/downloads/.

Avaya SBC OID Descriptions

This section describes the key Object Identifiers (OIDs).

Private Enterprise OIDs

OID	Description
ipcs stats sip calls: .1.3.6.1.4.1.6889.2.77.1.3.1	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipcalls
ipcs stats sip protocol: .1.3.6.1.4.1.6889.2.77.1.3.3	.iso.org.dod.internet.private.enterprises.Avaya.ipcsstatisticsinfo.ipcsstatssip.ipcsstatssipprotocol
Ipcsincidencesinfo: .1.3.6.1.4.1.6889.2.77.4	.iso.org.dod.internet.private.enterprises.Avaya.ipcsincidencesinfo
Ipcsalarmsinfo: .1.3.6.1.4.1.6889.2.77.2	.iso.org.dod.internet.private.enterprises.Avaya.ipcsalarmsinfo

Key OIDs

Classification of Requests/Responses matching a particular Domain Policy Group at the node

OID	Description
ipcsTotalINVITES	Number of SIP INVITE messages
ipcsTotalINVITERetransmits	Number of SIP INVITE Retransmits
ipcsTotalINVITE100Responses	Number of SIP INVITE 100 Responses
ipcsTotalINVITE1XXResponses	Number of SIP INVITE 1XX class Responses excluding SIP 100 Response.
ipcsTotalINVITE200Responses	Number of SIP INVITE 200 Responses
ipcsTotalINVITE200ResponseRetransmits	Number of SIP INVITE 200 Response Retransmits
ipcsTotalINVITE4XX6XXResponses	Number of SIP INVITE 4XX 6XX Responses
ipcsTotalINVITE4XX6XXResponseRetransmits	Number of SIP INVITE 4XX 6XX Response Retransmits
ipcsTotalBYESent	Number of SIP BYE requests
ipcsTotalBYERetransmits	Number of SIP BYE Retransmits
ipcsTotalBYE200Responses	Number of SIP BYE 200 Responses
ipcsTotalCANCELSent	Number of SIP CANCEL requests

Table continues…

OID	Description
ipcsTotalCANCEL200Responses	Number of SIP CANCEL 200 Responses
ipcsTotalACK200Responses	Number of SIP ACK requests for INVITE 200 OK Response
ipcsTotalACK4XX6XXResponses	Number of SIP ACK requests for INVITE 4xx-6xx class Responses
ipcsTotalACKTimeOuts	Number of SIP ACK timeouts ie. Number of ACK requests missing for the INVITE 200 OK/4xx-6xx class responses
ipcsTotalNonInviteRequests	Number of NonInvite Requests
ipcsTotalNonInvite1xxResponses	Number of NonInvite 1xx Responses
ipcsTotalNonInvite2xxResponses	Number of NonInvite 2xx Responses. Also includes the 200 OK responses for BYE and CANCEL requests

Get system configuration

OID	Name	Examples of displayed output
1.3.6.1.4.1.6889.2.77.12.1	sbcVersionNumber	8.1.2.0-31-19756
1.3.6.1.4.1.6889.2.77.12.2	sbcApplianceType	SingleBox
1.3.6.1.4.1.6889.2.77.12.3	sbcDeploymentMode	DMZ_ONLY
1.3.6.1.4.1.6889.2.77.12.4	processorVendor	GenuineIntel
1.3.6.1.4.1.6889.2.77.12.5	processorVersion	Intel(R) Xeon(R) Gold 6154 CPU @ 3.00GHz
1.3.6.1.4.1.6889.2.77.12.6	baseboardProductName	440BX Desktop Reference Platform
1.3.6.1.4.1.6889.2.77.12.7	baseboardManufacturer	Intel Corporation
1.3.6.1.4.1.6889.2.77.12.8	sbcPlatformMemory	8009024kB
1.3.6.1.4.1.6889.2.77.12.9	sbcPlatformDisc	160G
1.3.6.1.4.1.6889.2.77.12.10	sbcKernelVersion	3.10.0-1062.37.1.el7.AV1.x86_64
1.3.6.1.4.1.6889.2.77.12.11	sbcOperatingSystem	Red Hat Enterprise Linux Server release 7.7 (Maipo)
1.3.6.1.4.1.6889.2.77.12.12	sbcNetworkDriver	vmxnet3
1.3.6.1.4.1.6889.2.77.12.13	sbcThirdPartySoftware	'C-Ares': 'c-ares-1.10.0-3.el7.x86_64'

Out of Dialog Requests dropped

OID	Description
ipcsTotalOutOfDialogReferMesFromNW	Number of Out of Dialog REFER requests dropped at the node

Table continues…

OID	Description
IpcsTotalAckMessageOutOfDialogue	Number of Out of Dialog ACK requests dropped at the node
IpcsTotalByeMessageOutOfDialogue	Number of Out of Dialog BYE requests dropped at the node
IpcsTotalCancelMessageOutOfDialogue	Number of Out of Dialog CANCEL requests dropped at the node
IpcsTotalNotifyMessageOutOfDialogue	Number of Out of Dialog NOTIFY requests dropped at the node
ipcsTotalReinviteMessageOutOfDialogue	Number of Out of Dialog RE-INVITE requests dropped at the node

Out of Dialog Responses dropped

OID	Description
ipcsTotal1XXMessageOutOfDialogue	Number of Out of Dialog 1XX class responses dropped by the node
ipcsTotal2XXMessageOutOfDialogue	Number of Out of Dialog 2XX class responses dropped by the node
ipcsTotal3XXMessageOutOfDialogue	Number of Out of Dialog 3XX class responses dropped by the node
ipcsTotal4XXMessageOutOfDialogue	Number of Out of Dialog 4XX class responses dropped by the node
ipcsTotal5XXMessageOutOfDialogue	Number of Out of Dialog 5XX class responses dropped by the node
ipcsTotal6XXMessageOutOfDialogue	Number of Out of Dialog 6XX class responses dropped by the node

Out of Transaction Responses dropped

OID	Description
ipcsTotal1XXMessageOutOfTransaction	Number of 1XX Messages received out of transaction dropped by the node
ipcsTotal2XXMessageOutOfTransaction	Number of 2XX Messages received out of transaction dropped by the node
ipcsTotal3XXMessageOutOfTransaction	Number of 3XX Messages received out of transaction dropped by the node
ipcsTotal4XXMessageOutOfTransaction	Number of 4XX Messages received out of transaction dropped by the node
ipcsTotal5XXMessageOutOfTransaction	Number of 5XX Messages received out of transaction dropped by the node
ipcsTotal6XXMessageOutOfTransaction	Number of 6XX Messages received out of transaction dropped by the node

Table continues…

OID	Description
ipcsTotalCancelMessageOutOfTransaction	Number of CANCEL requests received out of transaction dropped by the node

Status of SIP calls

ipcssipcTotalRegistrationRequests	Number of Registration Requests received at node. This number does not include the registration triggered by node for keeping the pinhole open.
ipcssipcTotalRegistrationsChallenged	Number of Registrations Challenged by node and also includes the number of challenges from the Call Server. The number of registrations challenged by IPCS node includes the SIP 401/407 based Radius Authentication Responses (AAA feature) and SIP 407 based SIV Authentication Responses (DOS feature).
ipcssipcTotalRegistrationsRejected	Number of Registrations Rejected by the node and also includes the failed registration responses observed from the call server at the node. Failed registration responses include the SIP 4xx-6xx class responses excluding SIP 400, SIP 401/407 Responses. The registrations are rejected by the node due to failed registration challenges, failed registration processing, and registrations blocked due to security features.
ipcssipcTotalCallsReceived	Total Number of SIP Calls received at the node. This number equals Calls Blocked + Calls Allowed.
ipcssipcTotalCallsBlocked	Number of SIP calls Blocked by the node due to SIP Parse errors, failed AAA challenges, and calls blocked due to security features.
ipcssipcTotalCallsAllowed	Number of SIP calls classified by the node as Legitimate.

WebRTC statistics

OID	Description
ipcswebrtcStunBindingSuccess	Number of successful STUN bindings
ipcswebrtcStunBindingFailure	Number of failed STUN bindings
ipcswebrtcAllocateSuccess	Number of successful TURN allocations
ipcswebrtcAllocateFailure	Number of failed TURN allocations
ipcswebrtcRefreshSuccess	Number of successful TURN allocation refreshes
ipcswebrtcRefreshFailure	Number of failed TURN allocation refreshes
ipcswebrtcChannelBindSuccess	Number of successful channel bindings
ipcswebrtcChannelBindFailure	Number of failed channel bindings

Other OIDs

OID	Description
ipcssipcTotalActiveRegistrations	The number of active SIP registrations.
ipcssipcTotalActiveCalls	The number of active SIP calls.
ipcssipcTotalActiveTCPRegistrations	The number of active SIP registrations with TCP transport.
ipcssipcTotalActiveUDPRegistrations	The number of active SIP registrations with UDP transport.
ipcssipcTotalActiveTLSRegistrations	The number of active SIP registrations with TLS transport.
ipcssipcTotalActiveSRTPCalls	The number of active calls using media as SRTP.
ipcssipcTotalRegistrations	The number of active SIP registration requests received.
ipcssipcTotalTCPRegistrations	The number of SIP registrations received with TCP transport.
ipcssipcTotalUDPRegistrations	The number of SIP registrations received with UDP transport.
ipcssipcTotalTLSRegistrations	The number of SIP registrations received with TLS transport.
ipcssipcTotalCalls	The number of SIP calls received.
ipcssipcTotalCallsFailed	The number of failed SIP calls.
ipcssipTtlCallsDeniedDueToPolicy	The number of SIP calls rejected by Avaya SBC because of policy violation.
ipcssipcTotalRegistrationsDroppedByMissingPolicy	The number of SIP registrations dropped by Avaya SBC because of missing policy.
ipcssipcTotalInvitesDroppedByMissingPolicy	The number of SIP invites dropped because of missing policy.
ipcssipTtlSessDroppedDueToMaxNumofConcSessExc	The number of SIP sessions dropped by Avaya SBC because the maximum number of concurrent sessions was exceeded.
ipcsTotalCANCELSent	The number of SIP CANCEL requests.
ipcsTotalCANCEL200Responses	The number of SIP CANCEL 200 responses.
ipcsTotalCANCELRetransmits	The number of SIP CANCEL retransmits.
ipcsTotalFromAndToHeaderMatchFailure	The number of From and To header match failures.
ipcsTotalRegMesWithMoreContacts	The number of registration messages with more contacts.
ipcsTotalMesWithAddrIncomplete	The number of messages with incomplete addresses.
ipcsTotalAuthHeaderMatchFailure	The number of Auth header match failures.
ipcsTotalContactSrcAddrMatchFailure	The number of Contact Source Address match failures.
ipcsTotalViaMatchFailure	The number of Via match failures.
ipcsTotal3XXMesFromNW	The number of 3XX messages from network.

Table continues…

OID	Description
ipcsTotalRegistrationMatchFailure	The number of Registration Match failures.
ipcsTotalContactSDPConnMatchFailure	The number of Contact SDP Match failures.
ipcsTotalSpoofedSipBye	The number of spoofed SIP Bye requests.
ipcsTotalSpoofedReinvite	The number of spoofed Reinvite requests.
ipcsTotalSpoofedCancel	The number of spoofed Cancel requests.
ipcsTotalSpoofedCancelToRemote	The number of spoofed Cancel To Remote requests.
ipcsTotalSpoofed200	The number of spoofed 200 responses.
ipcsTotalSpoofedErrorResp	The number of spoofed error responses.
ipcsTotalRegistrationFailed	The number of failed registrations.
sbcTotal1xMCesUserLoginFailed	The number of failed Avaya one-X® Mobile user logins.
sbcTotal1xMCesUserLoginSucceeded	The number of successful Avaya one-X® Mobile user logins.
ipcsTotalNumberofFirewallPacketsDropped .1.3.6.1.4.1.6889.2.77.1.3.5.12	The number of packets dropped by the Avaya SBC firewall.
ipcsTestAlarmNotification	The test alarm notification.
ipcsCPUUsageNotification	The notification sent when CPU usage exceeds 80%.
ipcsMemoryUsageNotification	The notification sent when memory usage exceeds 80%.
ipcsDiskUsageNotification	The notification for disk usage exceeding a set threshold.
ipcsDiskFailureNotification	The notification for disk failure.
ipcsNetworkFailureNotification	The notification for network failure.
ipcsHAFailureNotification	The notification for HA failure.
ipcsHAHeartBeatFailureNotification	The notification for failure to receive heartbeat from both HA servers.
ipcsScpFailureNotification	The notification for SCP failure.
ipcsCopyFailureNotification	The notification for copy failure.
ipcsProcessFailNotification	The notification for process failure.
ipcsDatabaseFailNotification	The notification for database failure.
ipcsRSAFailureNotification	The notification for RSA failure.
ipcsIncidenceNotification	The notification about incidents.
ipcsStdSessionLicenseUsageExceed	The notification sent when session license usage threshold is exceeded.
ipcsAdvSessionLicenseUsageExceed	The notification sent when advanced session license usage threshold is exceeded.
ipcsCesProxySessionLicenseUsageExceed	The notification sent when CES proxy session license usage threshold is exceeded.
ipcsTranscodeSessionLicenseUsageExceed	The notification sent when transcoding session license usage threshold is exceeded.

Table continues…

OID	Description
ipcsVideoSessionLicenseUsageExceed	The notification sent when video session license usage threshold is exceeded.
ipcsPremSessionLicenseUsageExceed	The notification sent when premium session license usage threshold is exceeded.
ipcsMaxStdConcurrentSessionLimitExceed	The notification sent when the maximum standard concurrent session license limit is exceeded.
ipcsMaxAdvConcurrentSessionLimitExceed	The notification sent when the maximum advanced concurrent session license limit is exceeded.
ipcsMaxCESProxyConcurrentSessionLimitExceed	The notification sent when the maximum CES proxy concurrent session license limit is exceeded.
ipcsMaxTransConcurrentSessionLimitExceed	The notification sent when the maximum transcoding concurrent session license limit is exceeded.
ipcsMaxVIDConcurrentSessionLimitExceed	The notification sent when the maximum video concurrent session license limit is exceeded.
ipcsMaxkPremConcurrentSessionLimitExceed	The notification sent when the maximum premium concurrent session license limit is exceeded.

Statistics details with examples

Call between two remote workers through Avaya SBC

In the following scenario, a call is made from A to B.

- Number of Registrations in Statistics: Counter increases by 2

  One registration per phone, so in total 2 registrations from both A and B

  In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if both phones A and B are configured for multi-Session Manager deployment, the counter increases by 4.

- Number of Invites in Statistics: Counter increases by 2

  The counter increases whenever Avaya SBC receives an INVITE
  First INVITE from phone A towards Avaya SBC, which is sent to the call server
  Second INVITE from Call Server towards Avaya SBC, which is sent to phone B

- Number of Invites 200 Responses in Statistics: Counter increases by 2

  The counter increases whenever Avaya SBC receives a 200 OK for INVITE sent
  First 200 ok response from phone B towards Avaya SBC which is sent to the call server
  Second 200 ok response from Call Server towards Avaya SBC which is sent to phone A

- Number of Bye in Statistics: Counter increases by 2

  The counter increases whenever Avaya SBC receives a Bye
  First Bye from phone A towards Avaya SBC which is sent to the call server
  Second Bye from Call Server towards Avaya SBC which is sent to phone B

Call between a remote worker and an internal phone through Avaya SBC

In the following scenario, a call is made from A to C and the call is disconnected at A.

- Number of Registrations in Statistics: Counter increases by 1

  One registration per phone, so in total 1 registration

  Phone C registration will not be seen by Avaya SBC as this phone is an internal phone

  In a multi-Session Manager deployment, if the phone is configured with the IPs for two different Session Managers as external IP1 and external IP2, the registration counter increases by 2 for one phone. Therefore, if phone A is configured for multi-Session Manager deployment, the counter increases by 2.

- Number of Invites in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives an INVITE
  INVITE from phone A towards Avaya SBC, which is sent to the call server

- Number of Invites 200 Responses in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives a 200 Ok for INVITE sent
  200 ok response from phone C towards Avaya SBC, which is sent to phone A

- Number of Bye in Statistics: Counter increases by 1

  The counter increases whenever Avaya SBC receives a Bye
  Bye from phone A towards Avaya SBC, which is sent to the call server

Chapter 6: Resources

Documentation

The following table lists the documents related to this product. Download the documents from the Avaya Support website at http://support.avaya.com

Title	Description	Audience
Design		
Avaya Session Border Controller Overview and Specification	High-level functional and technical description of characteristics and capabilities of the Avaya SBC.	Sales engineers, solution architects, and implementation engineers
Avaya Session Border Controller Release Notes	Describes any last minute changes to the product, including patches, installation instructions, and upgrade instructions.	Sales and deployment engineers, solution architects, and support personnel
Avaya Solutions Platform Overview and Specification	Describes the key features of Avaya Solutions Platform servers.	IT Management, sales and deployment engineers, solution architects, and support personnel
Implementation		
Deploying Avaya Session Border Controller on a Hardware Platform	Describes how to plan and deploy an Avaya SBC system on the supported set of hardware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Virtualized Environment Platform	Describes how to plan and deploy an Avaya SBC system on customer-provided VMware servers.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Google Cloud Platform	Describes how to plan and deploy an Avaya SBC system on a Google Cloud Platform.	Sales and deployment engineers, solution architects, and support personnel

Table continues…

Title	Description	Audience
Deploying Avaya Session Border Controller on an Amazon Web Services Platform	Describes how to plan and deploy an Avaya SBC system on Amazon Web Services.	Sales and deployment engineers, solution architects, and support personnel
Deploying Avaya Session Border Controller on a Microsoft® Azure Platform	Describes how to plan and deploy an Avaya SBC system on a Microsoft® Azure platform.	Sales and deployment engineers, solution architects, and support personnel
Avaya Session Border Controller Port Matrix	Describes the incoming and outgoing port usage required by the product.	Sales and deployment engineers, solution architects, and support personnel
Upgrading Avaya Session Border Controller	Describes how to upgrade to the latest release of Avaya SBC.	Sales and deployment engineers, solution architects, and support personnel
Installing the Avaya Solutions Platform 110 Appliance	Describes how to install Avaya Solutions Platform 110 Appliance servers.	Sales and deployment engineers, solution architects, and support personnel
Administration		
Administering Avaya Session Border Controller	Describes configuration and administration procedures.	Implementation engineers and administrators
Maintenance and Troubleshooting		
Maintaining and Troubleshooting Avaya Session Border Controller	Describes troubleshooting and maintenance procedures for Avaya SBC.	Implementation engineers
Maintaining and Troubleshooting Avaya Solutions Platform 110 Appliance	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 110 Appliance servers.	Implementation engineers
Using		
Working with Avaya Session Border Controller and Microsoft® Teams	Describes how to set up, maintain, and use Avaya SBC with Microsoft Teams.	Implementation engineers and administrators
Working with Avaya Session Border Controller Multi-Tenancy	Describes how to set up, maintain, and use the Avaya SBC Multi-tenancy feature.	Implementation engineers and administrators
Working with Avaya Session Border Controller Geographic-Redundant Deployments	Describes how to set up, maintain, and use the Avaya SBC Geographic-redundant deployment feature.	Implementation engineers and administrators

For Dell documentation, go to https://www.dell.com/support/.

For HP documentation, go to https://www.hpe.com/support.

Finding documents on the Avaya Support website

Procedure

1. Go to https://support.avaya.com.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support** > **Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.

   This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.

   For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click to display the search results.

Accessing the port matrix document

Procedure

1. Go to https://support.avaya.com.
2. At the top of the screen, click **Sign In**.
3. Type your **EMAIL ADDRESS** and click **Next**.
4. Enter your **PASSWORD** and click **Sign On**.
5. Click **Product Documents**.
6. Click **Search Product** and type the product name.
7. Select the **Select Content Type** from the drop-down list
8. In **Choose Release**, select the required release number.
9. In the **Content Type** filter, select one or both the following categories:
   - **Application & Technical Notes**
   - **Design, Development & System Mgt**

   The list displays the product-specific Port Matrix document.
10. Press **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.

Training

The following courses are available on the Avaya Learning website at www.avaya-learning.com. After logging into the website, enter the course code or the course title in the **Search** field and click **Go** to search for the course.

Note:

Avaya training courses or Avaya learning courses do not provide training on any third-party products.

Course code	Course title
20600W	Avaya Session Border Controller 8.1 Technical Delta
21098W	Session Border Controller 8.0 Technical Delta
20660W	Administering the Avaya Session Border Controller for Enterprise - SIP Trunk
60660W	Administering Avaya SBC Release 8 for Remote Worker
20660T	Administering Avaya SBC Release 8 Test
20800C	Implementing and Supporting Avaya SBC — Platform Independent
20800T	Avaya SBC Platform Independent and Support Test
20800V	Implementing and Supporting Avaya SBC — Platform Independent
26160W	Avaya SBC Fundamentals
7008T	Avaya SBC for Midmarket Solutions Implementation and Support Test
7008W	Avaya SBC for Midmarket Solutions Implementation and Support
2035W	Avaya Unified Communications Roadmap for Avaya Equinox Clients
43000W	Selling Avaya Unified Communications Solutions
71300	Integrating Avaya Communication Applications
72300	Supporting Avaya Communication Applications

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to https://support.avaya.com/ and do one of the following:
  - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
  - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

    The **Video** content type is displayed only when videos are available for that product.

  In the right pane, the page displays a list of available videos.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
  - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at https://support.avaya.com for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Index

Special Characters

A

C

D

E

F

G

H

I

J

L

M

N

O

P

R

S

T

U

V

W