Upgrading Avaya Session Border Controller for Enterprise

Release 7.2.2
Issue 7
June 2018

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses

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

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

License types

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

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

Heritage Nortel Software

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

Copyright

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

Virtualization

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

Third Party Components

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

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

Service Provider

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

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

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Downloading Documentation

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

Contact Avaya Support

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

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided

Contents

Chapter 1: Introduction

Purpose

This document provides procedures for upgrading Avaya SBCE from Release 4.x or 6.x or 7.1 or 7.1.x to Release 7.2.2. The document includes upgrade checklists, and upgrade procedures.

The primary audience for this document is anyone who is involved with upgrading and maintaining Avaya SBCE. The audience includes and is not limited to implementation engineers, field technicians, business partners, solution providers, and customers.

Change history

Issue	Date	Summary of changes
1	June 2017	Release 7.2 document
2	August 2017	• Updated supported upgrade paths table • Updated upgrading EMS using a web browser topic • Updated upgrading Avaya SBCE from Release 7.1.x to Release 7.2
3	October 2017	• Updated upgrading secondary EMS procedure • Updated the note in upgrading Avaya SBCE HA pairs using web interface topic • Removed _rollback from Rolling back through CLI procedure • Added a step in upgrading Avaya SBCE from Release 7.1.x to Release 7.2 using CLI to check the upgrade status
4	November 2017	Updated the document for Release 7.2.1
5	January 2018	Updated the procedure for upgrading from Release 7.2 to Release 7.2.1.
6	April 2018	Updated the document for Release 7.2.2 for following changes: • Added the procedures for upgrading from Release 7.2 and Release 7.2.1 to Release 7.2.2

Table continues…

Issue	Date	Summary of changes
		• Updated the supported upgrade paths topic • Updated the Rolling back using web interface topic • Updated the Downloading upgrade files topic
7	June 2018	• Updated the Supported upgrade paths table for direct upgrade paths from Release 6.3.6, Release 6.3.7 and Release 7.0.2 to Release 7.2.2. • Added a note in Upgrading EMS using a web browser topic.

Chapter 2: Upgrade overview and specifications

Avaya Session Border Controller for Enterprise upgrade overview

This guide provides the procedures for upgrading Avaya Session Border Controller for Enterprise (Avaya SBCE) from Release 4.x or 6.x or 7.1 or 7.1.x to Release 7.2.2.

The upgrade procedures of Avaya SBCE depend on the current software version of Avaya SBCE. For example, Avaya SBCE Release 7.2 uses RHEL version 7.x. Depending on that, direct upgrade paths to the latest Avaya SBCE release version will vary.

Password policies

The root and ipcs passwords are determined and set during product installation. The EMS GUI has a separate password. When you log in for the first time after installation, the system prompts you to create a new password for accessing the EMS GUI. The default user ID and password is ucsec.

Password restrictions are enforced on the `ucsec` and ipcs accounts. The new password must meet the password criteria of minimum 8 characters, including:

- One uppercase letter, one lowercase letter, and one number.
- One special character from the hyphen (-), underscore(_), at sign(@), asterisk (*), and exclamation point (!).You must not use the number sign (#), dollar sign ($), and ampersand (&).

Note:

The Avaya SBCE CLI root and ipcs passwords are determined by the customer network administrator during the installation procedure. Two installation steps prompt the installer to enter a chosen password.

Supported upgrade paths

Direct upgrade support

The following table provides information related to the direct upgrade support of all previous releases:

Direct upgrade support	Release 6.2	Release 6.3	Release 7.0	Release 7.1	Release 7.2	Release 7.2.1	Release 7.2.2
4.x	Supported	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported
Release 6.2	Not applicable	Supported	Not supported	Not supported	Not supported	Not supported	Not supported
Release 6.3	Not applicable	Not applicable	Supported	Supported	Not supported	Not supported	Not supported
Release 6.3 6	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Release 6.3 7	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Release 7.0	Not applicable	Not applicable	Not applicable	Supported	Not Supported	Not supported	Not supported
Release 7.0 2	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported
Release 7.1	Not applicable	Not applicable	Not applicable	Not applicable	Supported	Not supported	Not supported
Release 7.2	Not supported	Not supported	Not supported	Not supported	Not supported	Supported	Supported
Release 7.2.1	Not supported	Not supported	Not supported	Not supported	Not supported	Not supported	Supported

Upgrading Avaya Session Border Controller for Enterprise contains the following upgrade procedures:

From		To		Procedure supported
Version	Operating system Platform	Version	Operating system Platform	
4.x	-	6.2	-	Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30
6.2.1Q18	Monta Vista / Debian	7.0	Red Hat	Upgrade from Release 6.2 to Release 7.0 on page 46

Table continues…

6.3	Red Hat	7.0 7.1	Red Hat	Installing GUI patch for upgrades from Release 7.0 or Release 6.3.6 to Release 7.1 on page 52
7.0	Red Hat	7.1	Red Hat	Installing GUI patch for upgrades from Release 7.0 or Release 6.3.6 to Release 7.1 on page 52
7.1	Red Hat	7.2	Red Hat	Upgrading Avaya SBCE from Release 7.1.x to Release 7.2 by using CLI on page 70
7.2	Red Hat	7.2.1	Red Hat	Installing pre-upgrade patch for Avaya SBCE upgrade from Release 7.2 to Release 7.2.1 using CLI on page 69
7.2.1	Red Hat	7.2.2	Red Hat	Upgrading Avaya SBCE to Release 7.2.2 using CLI on page 71

Note:

For information about the upgrade sequence and the required patches, see the latest *Avaya Session Border Controller for Enterprise Release Notes* on the Avaya Support site at http://support.avaya.com.

Supported hardware

Avaya SBCE Release 7.1 and 7.2 supports the following hardware:

- Dell R210 II
- Dell R210 II XL
- Dell R320
- Dell R330
- Dell R620
- Dell R630
- HP DL360 G8
- HP DL360 G9
- PortWell CAD 0208
- Portwell CAD 0230

For information about the Avaya port matrix, see *Avaya Port Matrix: ASBCE*.

Hardware support removal when upgrading to Release 7.0 and later

Determining whether EMS is installed on an Amax server

About this task

On Amax servers, Avaya SBCE does not support upgrades to Release 7.0 or later. Use this procedure to check whether EMS is installed on an Amax server.

Procedure

1. Log in as an ipcs user on EMS server, and type `sudo su` to get root privileges.
2. Type `dmidecode | grep 'Supermicro'`.

   For an Amax server, the system displays `Product Name: Supermicro`.

   For other servers, the system does not display any data.

Next steps

If you have Avaya SBCE Release 6.2. 1Q18 or Avaya SBCE Release 6.3, back up the existing configuration and restore on a new server.

For an HA configuration with the EMS on a Dell server and Avaya SBCE on HP DL360 G7, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

For HA configurations with the EMS on an Amax server and Avaya SBCE on HP DL360 G7, take a snapshot of the Amax server. Restore the snapshot taken on the Amax server with Avaya SBCE 6.2.1Q18 or 6.3 on new Avaya SBCE server of same version as Amax server. Ensure that the new Avaya SBCE hardware is supported for Avaya SBCE 7.0 or later. Then, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

For HA configurations with the EMS on an Amax server and Avaya SBCE on a Dell server, take a snapshot of the Amax server. Restore the snapshot taken on the Amax server with Avaya SBCE 6.2.1Q18 or 6.3 on new Avaya SBCE server of same version as Amax server. Ensure that the new Avaya SBCE hardware is supported for Avaya SBCE 7.0 or later. For information about the supported hardware on which you can restore the configuration backed up from the Amax server, see the Supported hardware for moving from HP DL360 G7 and AMAX servers section.

For more information about swapping a device, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Related links

Supported upgrade paths on page 11

Supported hardware for moving from HP DL360 G7 and AMAX servers on page 14

Supported hardware for moving from HP DL360 G7 and AMAX servers on page 14

Determining whether Avaya SBCE is installed on an HP DL360 G7 server

About this task

On HP DL360 G7 servers, Avaya SBCE does not support upgrades to Release 7.0 and later. Use this procedure to check whether Avaya SBCE is installed on an HP DL360 G7 server.

Procedure

1. Log in as an ipcs user on EMS server, and type `sudo su` to get root privileges.
2. Type `dmidecode | grep 'ProLiant DL360 G7'`.

   For an HP DL360 G7 server, the system displays `Product Name: ProLiant DL360 G7`.

   For other servers, the system does not display any data.

Next steps

If you have Avaya SBCE Release 6.2. 1Q18 or Avaya SBCE Release 6.3, back up the existing configuration and restore on a new server.

For an HA configuration with the EMS on a Dell server and Avaya SBCE on HP DL360 G7, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

For HA configurations with the EMS on an Amax server and Avaya SBCE on HP DL360 G7, take a snapshot of the Amax server. Restore the snapshot taken on the Amax server with Avaya SBCE 6.2.1Q18 or 6.3 on new Avaya SBCE server of same version as Amax server. Ensure that the new Avaya SBCE hardware is supported for Avaya SBCE 7.0 or later. Then, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

For more information about swapping a device, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Related links

Supported hardware for moving from HP DL360 G7 and AMAX servers on page 14

Supported hardware for moving from HP DL360 G7 and AMAX servers

Avaya SBCE does not support upgrades to Release 7.0 or later for AMAX and HP DL360 G7 servers. If you currently use an AMAX or HP DL360 G7 server, back up the existing configuration. You can then deploy the backed up configuration on another server.

Important:

If you have Avaya SBCE 6.2.1Q18 or 6.3 on HP DL360 G7 or AMAX servers, back up the existing configuration, restore on a new server, upgrade to Release 7.0, and later.

Snapshots taken on Avaya SBCE can be restored on another device with the same software version. If you have Amax or HP DL360 G7 servers, choose from the following options:

- AMAX customers: For an EMS only deployment on an AMAX server, take a snapshot and restore on one of the following servers:
  - Dell R210ii XL with 2 NICs

    - Dell R320
    - Dell R620
    - VMware deployed only with EMS mode
- HP DL360 G7: For a standalone SBCE+EMS deployment, take a snapshot and restore on HP DL360 G8.

  For an HA configuration with the EMS on a Dell server and Avaya SBCE on HP DL360 G7, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

  For HA configurations with the EMS on an Amax server and Avaya SBCE on HP DL360 G7, take a snapshot of the Amax server. Restore the snapshot taken on the Amax server with Avaya SBCE 6.2.1Q18 or 6.3 on new Avaya SBCE server of same version as Amax server. Ensure that the new Avaya SBCE hardware is supported for Avaya SBCE 7.0 or later. Then, add a new Avaya SBCE device installed on an HP DL360 G8 server, and swap the Avaya SBCE device on HP DL360 G7.

  For more information about swapping a device, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

You cannot move from an AMAX or HP DL360 G7 server to an HP DL360 G9, or Dell R630 server.

For information about taking and restoring snapshots, see *Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise*.

Related links

Supported upgrade paths on page 11

Changing serial number for Avaya SBCE uninstalled from an Amax server

About this task

After the EMS on the new server starts, you must uninstall the Avaya SBCE instances installed on the Amax server,and add them to the new EMS.

When you do a factory reset to remove the Avaya SBCE on the Amax server, the system generates the same serial numbers on both Avaya SBCEs. You can register the primary and secondary Avaya SBCEs with EMS only if you have unique serial numbers for every Avaya SBCE.

Therefore, to make the serial numbers unique you must:

- For restoring snapshot from Amax to Dell R210 ii XL, Dell R620 or VM: manually change the serial number on one of the Avaya SBCE instances that was on an Amax server.
- For restoring snapshot from Amax to Dell R320: download the `match-serial-from-snapshot.py` script from PLDS and run the script on an Avaya SBCE

This issue occurs only for HA configurations.

Procedure

1. Log in to the Avaya SBCE.

2. Type `vi /usr/local/ipcs/etc/sysinfo`.
3. Change the last character of the serial number for one Avaya SBCE.
4. Change the system STATE parameter to `INSTALLED`.
5. Restart both Avaya SBCE devices.

Chapter 3: Planning for upgrade

Pre-upgrade checklist

Sr. No.	Tasks	References	✔
1	Take a snapshot of Avaya SBCE. Take a backup by using the `/usr/local/ipcs/icu/scripts/BackupAndRestore.py` file to use during an upgrade failure.	Backup / Restore system information on page 19	
2	Ensure that the Avaya SBCE version is at least: • 6.2.1Q18 for upgrading to Release 7.0. • 7.0 for upgrading to Release 7.1. • 7.1 for upgrading to Release 7.2.	-	
3	Inspect the server and contents for damages and verify the power cycle. Ensure that the server passes POST tests before upgrade.	-	
4	Ensure that the system does not show any alarms related to disk space.	-	
5	Disable all debug logs.	-	
6	Ensure that Avaya SBCE servers in the deployment have unique host names. If two or more servers have the same host name, change the host name. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller*.	-	
7	Ensure that Element Management System (EMS) and Avaya SBCE are in the Commissioned state.	Do not attempt upgrading while the EMS or Avaya SBCE is in the Registered state.	
8	Ensure that the Avaya SBCE instances are not in sync state.	To verify whether Avaya SBCE instances have a problem with	

Table continues…

Sr. No.	Tasks	References	✔
		synchronization, clone a sigma profile, save the profile, and then check whether any Avaya SBCE moves to the sync state. If any Avaya SBCE instance is in the sync state, log a ticket with Avaya Support to get the issue addressed.	
9	Ensure that connectivity between EMS and Avaya SBCE instances is good.	-	
10	If you revert the VMware snapshot before upgrading, ensure that you restore the VMware snapshots in the following order: 1. EMS 2. Avaya SBCE	-	
11	For an Avaya SBCE HA pair, ensure that the HA state is showing primary and secondary, respectively.	If in the HA pair, both Avaya SBCE instances are in the same state, Avaya SBCE failover will result in an outage. Therefore, both instances must never have primary, secondary, or down state at the same time.	
12	Ensure that you place all manually installed RPMs, which came as a patch, in the `/archive/SBC-RPM-Repository/RPMs/` directory.	-	
13	Download the upgrade files from the PLDS website. If you upgrade using a USB device, ensure that the USB device has a minimum storage capacity of 4 GB.	Downloading upgrade files on page 27	

Note:

You cannot administer Avaya SBCE that are on earlier version than EMS until you upgrade Avaya SBCE to the same version as EMS.

Related links

Latest software updates and patch information on page 19

Latest software updates and patch information

Before you start the deployment or upgrade of an Avaya product or solution, download the latest software updates or patches for the product or solution. For more information, see the latest release notes, Product Support Notices (PSN), and Product Correction Notices (PCN) for the product or solution on the Avaya Support Web site at https://support.avaya.com/.

After deploying or upgrading a product or solution, use the instructions in the release notes, PSNs, or PCNs to install any required software updates or patches.

For third-party products used with an Avaya product or solution, see the latest release notes for the third-party products to determine if you need to download and install any updates or patches.

Related links

Pre-upgrade checklist on page 17

Backup / Restore system information

The Backup/Restore feature provides the ability to backup or create a snapshot of the EMS security configuration to a user-definable location or to a local EMS server. The location must be secure and physically separate from the Avaya SBCE equipment chassis for later retrieval or restoration. You can download the snapshot using the download link provided in the **Snapshot** tab.

Note:

A configuration backup can be taken manually and restored as needed, or automatic snapshots can be configured.

Designating a Snapshot Server

About this task

A snapshot contains information such as certificates and keys, which can be misused to gain unauthorized access to the Avaya SBCE server. The administrator must ensure that the storage directory on remote server is accessible only to authorized users.

The directory with the snapshot must not have read/write/execute permission for unauthorized users.

To back up to a remote server, before using the Backup/Restore feature, you can designate a server as a snapshot server to hold the backup files or save the files to the local EMS server.

Caution:

A snapshot can only be restored to the same Avaya SBCE product version on an EMS of the same hardware group. When restoring the snapshot, it is recommended that the EMS server must be configured with the same original management IP used when the snapshot was created or the system may need to be manually rebooted. If the EMS server hardware group or the Avaya SBCE product version do not match, the restore operation will fail and the system settings will revert to the earlier state.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore page.
3. Click the **Snapshot Servers** tab.

   The system displays the available snapshot server profiles in the content area.
4. On the Snapshot Servers page, click **Add**.

   The system displays the Add Snapshot Servers page.
5. Add the requested information in the fields.
6. Click **Finish**.

Next steps

Making a System Snapshot on page 20

Add Snapshot Server field descriptions

Name	Description
Profile Name	A descriptive name to refer to the snapshot server being configured.
Server Address (ip:port)	The IP address and port number of the snapshot server to which backup files or snapshots are transferred by using secure FTP (SFTP).
User Name	The user name of the administrative account that is authorized to make system backups.
Password	The password assigned to authenticate the administrative account.
Confirm Password	The password that you reenter for confirmation.
Repository Location	The path (directory) on the snapshot server where the backup files will be stored and retrieved from.
Host Key	The key used to authenticate the login of the host.

Making system snapshots

Before you begin

Designate a snapshot server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. Select **Backup/Restore** from the Task Pane.

   The system displays the Backup/Restore screen in the content area.
3. Click **Create Snapshot**.

   The system displays the Create Snapshot window.

   In a deployment with multiple Avaya SBCEs, if any of the Avaya SBCEs is out of service, you cannot create a snapshot.
4. Enter a name to designate this snapshot (backup) file, and click **Create**.

   A snapshot (backup) of the EMS security configuration is made and sent to all the configured snapshot servers. A banner is displayed on the Create Snapshot pop-up window informing you that the snapshot has been successfully created. When the process is complete, the newly created snapshot is displayed in the content area of the snapshots screen.

Configuring automatic snapshots

About this task

Use this procedure to take automatic backups on a designated server or on the local EMS server.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore page.
3. Click the **Automatic Snapshot Configuration** tab.

   The system displays the Automatic Snapshot Configuration page. The **Summary** section displays the configuration for a previously saved backup, if one existed. Otherwise, the default setting of **Never** is displayed.
4. In the **Configuration** section, do the following:
   a. Select the snapshot frequency.

      The options are Never, Daily, Weekly, and Monthly.
   b. When the Weekly or Monthly option is selected, the system displays a group of Day(s) checkboxes. For example, Su, Mo, Tu, We, Th, Fr, and Sa.
   c. When the Monthly option is selected, the system displays an additional row of checkboxes for occurrence. For example, 1st, 2nd, 3rd, 4th, and Last.
5. In the **Time** field, select the time.

   When you type in the **Time** field, the system displays a Select Time pop-up.

6. Click **Save**.

Restoration of a system snapshot

The two methods of restoring a snapshot to the EMS server are manual and automatic.

Manual

The manual method of restoring a snapshot to EMS is a two-step process. The snapshot is first retrieved from the snapshot server to the local workstation and then uploaded to EMS for reconfiguration. See the following procedures to restore EMS to a previous snapshot configuration:

- Retrieving a snapshot file
- Restoring a snapshot file

Automatic

The automatic method of restoring a snapshot to EMS is a single-step process that restores EMS to the previous configuration without further intervention. See the Restoring a snapshot file automatically section.

⚠ **Caution:**

During the manual and automatic process of restoring a snapshot file, EMS goes in the offline mode when the files are being transferred and the device is being reconfigured.

No Avaya SBCE detection or mitigation features are available for the entire duration of the restore procedure, making the system vulnerable to intrusions and attacks.

Restoration procedures must be done only during times of relative system inactivity or during scheduled periods of maintenance.

Snapshots can be restored to an EMS system of the same hardware category, manufacturer, and model of EMS. The following table lists the hardware categories:

Hardware Model	No. of NICs	Hardware Category
CAD 0208	4	110
CAD 0230	4	110
Dell 210	2	EMS
Dell 210	6	310
Dell R320	6	310
Dell R620	6	310
Dell R630	6	310
HP DL360 G8	6	311
HP DL360 G9	6	311
VMWare Small	2	EMS

Table continues…

Hardware Model	No. of NICs	Hardware Category
VMWare Medium	4	110
VMWare Large	6	310

Retrieving a snapshot file

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. From the Task Pane, click **Backup/Restore**.

   The system displays the Backup/Restore screen in the content area.
3. Click the **Snapshot** tab.
4. In the drop-down box, click the snapshot server or the local server on which you have created the snapshot.
5. Click the checkbox corresponding to the snapshot file that you want to retrieve and then click **Download**.

   The system saves the snapshot file on default download directory.

Next steps

Restoring a Snapshot File

Restoring a snapshot file manually

Before you begin

Retrieve a snapshot file.

About this task

After you retrieve the snapshot file from the snapshot server, save the file on the local workstation. You can upload the file to the EMS server where the file is uncompressed and used to reconfigure the EMS to a previous state.

Use the following procedure to upload the snapshot from your local workstation to the EMS server and reconfigure the EMS.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the Task pane, click **Backup/Restore**.

   The Content area displays the Backup/Restore screen.
3. Select the corresponding **Restore by File** option.

   The system displays the Restore by File pop-up window.
4. Click **Browse**.

   The system displays a dialog pop-up window.

5. Select the desired snapshot file, and click **Open**.

   The system enters the selected snapshot file in the **Restore Point File** field of the Restore by File window.

6. Click **Finish**.

   The system displays a warning window for confirmation to proceed with the restoration procedure.

7. Click **OK**.

   The EMS server goes offline and the snapshot file transferred to the EMS server, where the file is uncompressed and used to reconfigure the EMS software to a previous configuration.

   Note:

   After the system successfully restores a snapshot, in an HA configuration both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The system takes 2 to 3 minutes to reboot after backup configuration.

Restoring a snapshot file automatically

Before you begin

Create a system snapshot.

Procedure

1. Log on to the EMS web interface with administrator credentials.

2. In the Task pane, click **Backup/Restore**.

   The Content area displays the Backup/Restore screen.

3. Using the drop-down menu in the Content Area, select the snapshot server that contains the snapshot file that you want to retrieve.

   The system displays all snapshot files on the selected snapshot server in the content area.

4. Select the snapshot file that you want to restore to the EMS by clicking the corresponding **Restore** option.

   The system displays a warning pop-up window, asking for confirmation to proceed with the automatic restoration procedure.

5. Click **OK**.

   The EMS goes offline and reconfigures the snapshot file.

   Note:

   After the system successfully restores a snapshot, in an HA configuration both Avaya SBCE devices reboot. In a standalone configuration, the EMS+SBCE single box reboots. The system takes 2 to 3 minutes to reboot after backup configuration.

Deleting a system snapshot

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation pane, click **Backup/Restore**.

   The system displays the Backup/Restore screen.
3. Select the local server or the designated snapshot server from where you want to delete the file.
4. Select the file and click the corresponding **Delete** option.

   The system displays a warning message, asking for a confirmation to delete.
5. Click **OK**.

   The system deletes the snapshot file.

Commands for creating and restoring snapshots

The following root-level console commands are available for creating and restoring snapshots:

- #gui-snapshot-create
- #gui-snapshot-restore

Console command-gui-snapshot-create

Use the **`gui-snapshot-create`** console command to create a snapshot from the command line. The structure of the command is:

`gui-snapshot-create` options description

Description

The description can be any string value and does not need to be quoted. If not specified, the description has the default value Restore Point through CLI.

Options

The following options are available for this command:

- --version: Displays the command version that is equal to the GUI version. Usually, the GUI version matches ipcs-version.
- --help: Displays detailed information about the command, possible arguments, and a few examples.
- --debug: Sends the output of debug logs to stdout when executing the command.
- --quiet: Suppresses all output. If both the quiet option and debug option are specified, the quiet option takes precedence.

When the command is run, an exit code is returned. Any relevant details for a failure are passed to stderr. The following are examples of the returned exit codes:

- 0 – Completed successfully.
- 1 – Invalid command syntax.
- 2 – Snapshot creation partially successful. This exit code occurs when a snapshot was created successfully, but could not be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This exit code occurs if the snapshot creation fails.
- 1000 – An unknown error has occurred.

Examples

A few sample commands with descriptions are listed here:

- `gui-snapshot-create`: Creates a new snapshot with the default description Restore Point via CLI.
- `gui-snapshot-create --quiet This is a test snapshot`: Creates a new snapshot with the description This is a test snapshot. The system does not send any output to stdout or stderr.

Console Command-gui-snapshot-restore

With the **`gui-snapshot—restore`** console command, you can restore a snapshot from the command line. The general structure of the command is:

`gui-snapshot-restore` options *file*

File

Use the absolute or relative path for a valid snapshot file.

Options

Use one of the following options:

- --version: Displays the command version, which is equal to the GUI version. The GUI version usually matches the ipcs-version.
- --help: Displays detailed information about the command, possible arguments, and a few examples.
- --debug: Sends debug logs to stdout when running the command.
- --quiet: Suppresses all output. If both the quiet option and debug option are specified, the quiet option takes precedence.

After the command runs, the system returns an exit code. Any relevant details for a failure are passed to stderr. A list of possible returned exit codes follows:

- 0 – Completed successfully.
- 1 – Invalid command syntax.
- 2 – Snapshot creation partially successful. This exit code occurs when a snapshot is created successfully, but cannot be uploaded to one or more snapshot servers.
- 3 – Snapshot creation failed. This exit code occurs if the snapshot creation failed.

- 1000 – An unknown error occurred.

Examples

A few sample commands with descriptions are listed here:

- `gui-snapshot-restore /home/ipcs/snapshot folder/snapshot.zip`: Restores from a snapshot file named snapshot.zip in /home/ipcs/snapshot folder/.
- `gui-snapshot-restore ../snapshots/snapshot-1.2.3.zip`: Restores from a snapshot file named snapshot-1.2.3.zip in the sibling of the parent directory, named snapshots.

Downloading upgrade files

Procedure

Download the following files from the PLDS website at https://plds.avaya.com/:

- `sbce-7.2.2.0-xx-xxxxx-<md5sum>.tar.gz`: For upgrading from Release 7.2 and Release 7.2.1 to Release 7.2.2.
- `sbce-7.2.x.0-xx-xxxxx-<md5sum>.tar.gz`: For upgrading from Release 7.1 to Release 7.2.
- `sbce-7.2.x.0-xx-xxxxx-<md5sum>.tar.gz.asc`, `sbce-7.2.x.0-xx-xxxxx-7.tar.gz` and `sbce-7.2.x.0-xx-xxxxx-signatures.tar.gz`: For upgrading from Release 7.1.x to Release 7.2.
- `sbce-7.2.x.0-xx-xxxxx_<md5sum>.img`: For preparing a USB device on Windows or Linux for installation or upgrade. Ensure the USB device has minimum storage capacity of 4 GB.
- `sbce-7.2.x.0-xx-xxxxx.iso`: For preparing a DVD on Windows or Linux for installation or upgrade. The same file works for preparing a USB device on Linux as well.
- `ipcs_7.0.0.Qxx_<md5sum>.tar.gz`: For upgrading from Avaya SBCE Release 6.2.x to Release 7.0 using CLI. CLI is the recommended method for upgrades.
- `sbce-7.0.0-xx-xxxx.iso`: For upgrading from Avaya SBCE Release 6.2.x to Release 7.0 using DVD.
- `sbce-7.0.000-xx-xxxx_<md5sum>.img`: For upgrading from Avaya SBCE Release 6.2.x to Release 7.0 using a USB device.
- `sbce_7.0.0-xx-xxxx-<md5sum>.tar.gz`: For upgrading from Release 6.3 to Release 7.0.
- `sbce_7.1.0.0-xx-xxxx-<md5sum>.tar.gz`: For upgrading from Release 7.0 to Release 7.1.
- `sbce-7.2.x.0-xx-xxxxx-<md5sum>.tar.gz`: For upgrading from Release 7.1.x to Release 7.2

- `sbce-7.2.2.0-xx-xxxxx-<md5sum>.tar.gz`: For upgrading from Release 7.2 and Release 7.2.1 to Release 7.2.2

Preparing a USB device or DVD for installation or upgrade

Preparing a USB device on Windows

Before you begin

Ensure the USB device has minimum storage capacity of 4 GB.

Procedure

1. Download and set up a disk imaging utility like Win32 Disk Imager.
2. Copy the Avaya SBCE 7.2 USB image file (`sbce-7.2.x.0-xx-xxxxx_<md5sum>.img`) on the Windows system.
3. Ensure that the checksum matches the checksum calculated by any checksum utility.
4. Plug in the USB device on the Windows system.

   If you get an error indicating that the system is in use, format the USB device before using the Win32 Disk Imager application.
5. In the Win32 Disk Imager application, select the Avaya SBCE image that you downloaded from the PLDS website and the correct USB device and click **Write**.

   ⚠ **Warning:**

   Do not change the label of the filesystem on the USB drive. The default label is SBC_USB.
6. Wait for the image to be written to the USB device.

Preparing a USB device on Linux

Before you begin

Ensure the USB device has minimum storage capacity of 4 GB.

Procedure

1. Copy the Avaya SBCE 7.2 USB image file (`sbce-7.2.x.0-xx-xxxxx_<md5sum>.img` or `sbce-7.2.x.0-xx-xxxxx.iso`) on the Linux system.
2. Go to the location where you copied the image file, and type `md5sum` *`filename`*, where *filename* is the name of the image file.

The system displays an alphanumeric hash followed by the image filename.

3. Compare and ensure that the alphanumeric hash matches the checksum value in the file name.
4. Plug in the USB device on the linux server.

   The device can be detected as `/dev/sda` or `/dev/sdb` or `/dev/sdc`. Check with your system administrator if you are not sure.
5. Run the following command: `dd if=/path/of/the/SBCE_USB_image_file of=/dev/sdX bs=16M`

   If your USB is detected as `/dev/sdb1`, type the command `dd if=/path/of/the/SBCE_USB_image_file of=/dev/sdb bs=16M`.

   The command takes up to 10 minutes to complete.

Preparing a DVD

Before you begin

Ensure that your system has the software to burn the ISO image on the DVD.

About this task

Use this procedure to prepare a DVD for installing or upgrading Avaya SBCE, if server is unable to detect USB.

Procedure

1. Insert the DVD in a Windows or Linux system.
2. Burn the iso image (`sbce-7.2.x.0-xx-xxxxx.iso`) to the DVD.

Chapter 4: Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2

Standalone Avaya SBCE (EMS + Avaya SBCE)

The base procedure for updating an Avaya SBCE box using the internal EMS follows.

Separate EMS and Avaya SBCE(s)

When there is a separate EMS hardware box, the upgrade process is the same, but the EMS software must be updated first.

HA Pair — EMS and Primary/Secondary Avaya SBCEs

With High Availability pairs of Avaya SBCEs and separate EMS boxes, the EMS software is updated first, followed by the primary and secondary Avaya SBCE boxes as prompted by the update scripts.

Related links

Beginning software only upgrade on page 30
Upgrading EMS from a local file on page 31
Uploading via SFTP on page 32
Upgrading EMS via HTTP on a browser on page 32
Upgrading SBC boxes and HA Pairs on page 33
Upgrading HA Pairs on page 34
Upgrading SBC boxes on page 34
Performing a Rollback on page 35
Non service affecting EMS upgrade on page 35

Beginning software only upgrade

The Element Management System (EMS) or GUI interface can be upgraded when necessary using the System Management feature from the Task Pane. Use the following procedure to begin a software only upgrade on existing, supported hardware.

Procedure

1. Select the System Management feature from the Task Pane.

The System Management screen is displayed.

2. Select the Updates tab.

   The current EMS version and available upgrade options are displayed in the Content Area.
3. Verify that the current EMS version in the Version Information portion of the tab display.
4. Determine the location of the upgrade package.

   If no local upgrade packages are available, then the "Select upgrade package" field will display "No upgrades available."

   - If the upgrade package has already been uploaded to the EMS server, proceed to the procedure titled "Upgrading EMS from a local file."
   - If the upgrade package has not been uploaded to the EMS server, it can be uploaded using the procedure titled "Uploading via SFTP."
   - The upgrade can also be updated via HTTP on a browser. For more information see the procedure titled "Upgrading EMS via HTTP on a browser."

Next steps

Upgrading from a local file on page 31

Uploading via SFTP on page 63

Updating via HTTP on a browser on page 64

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Upgrading EMS from a local file

Before you begin

Copy the upgrade file to the `/archive/urpackages` directory.

Procedure

1. In the Updates tab, in the **Upgrade from local file** field, select the upgrade file.
2. Click **Upgrade**.

   The system displays the Upgrade Confirmation screen.
3. Click **Start Upgrade**.

   The system displays a series of windows to indicate that the EMS software is upgrading. When the upgrade is complete, the system displays a final window.
4. Click **Return to EMS**.

   The system displays the System Management page.

Next steps

Uploading using SFTP

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Uploading via SFTP

About this task

When upgrading an EMS from a local file (residing on the EMS box), the upgrade package must reside in the following location on the EMS: `/usr/local/ipcs/upgrades/` in order to appear in the available upgrades list in the System Upgrade section of the Updates screen.

Procedure

1. Download the upgrade package to a local or remote PC using Avaya's Product Licensing and Delivery System (PLDS)
2. SFTP into the EMS box using login credentials
3. Navigate to the /user/local/ipcs/upgrades/ folder

   If the upgrades folder does not exist, create the upgrades folder in the exact path shown above and then repeat steps 2 and 3 above
4. Copy the upgrade package to the /user/local/ipcs/upgrades/ folder
5. Login to the EMS GUI and follow the steps in the procedure titled "Upgrading from a local file."

Next steps

Upgrading from a local file on page 31

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Upgrading EMS via HTTP on a browser

About this task

Note:

It is highly recommended that you use SFTP/SCP to upload the upgrade file to the EMS box. Uploading files using a browser with larger files can sometimes be unreliable, especially when using older browser versions (i.e., IE7, IE8, or Firefox 3.x) and may result in a failed upload or checksum error. If only a slow connection is available, you should always use SFTP/SCP for the upload to the EMS box.

Procedure

1. Download the upgrade package to a local or remote PC using Avaya’s Product Licensing and Delivery System (PLDS).
2. Login to the EMS GUI.
3. Select System Management feature from the Task Pane.

   The System Management screen is displayed.
4. Select the Updates tab.
5. Select the Upgrade from uploaded file radio button from the System Upgrade portion of the tab display.
6. Select the Browse button and navigate to the folder containing the downloaded upgrade file.
7. Select the upgrade file.
8. Click Upgrade.

   The Upgrade Confirmation screen is displayed.
9. Click Start Upgrade.

   The EMS software is upgraded. A series of informational pop-up windows will be displayed as the upgrade proceeds. A final pop-up window will be displayed to let you know when the upgrade is complete.

Next steps

Upgrading SBC boxes and HA Pairs on page 33

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Upgrading SBC boxes and HA Pairs

After the EMS software has been upgraded, the following message appears on the Updates tab:

```
One or more devices are in an orphan state.  If you would like to
upgrade these devices now, please click the UPgrade button below.  You
may also choose to rollback your EMS at this point.
```

HA system pairs and all other SBC(s) will need to be upgraded before this message is resolved.

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Upgrading HA Pairs

Procedure

1. Click Upgrade on the updates tab of the System Management screen.

   The Upgrade Devices dialogue box will pop up.
2. Select the checkbox next to the Secondary HA-SBC device.

   Either primary or secondary could be upgraded first, however it is important to note that whenever you upgrade the primary, the secondary will take over as the primary and the existing primary will become secondary.
3. Click Next.

   Dialogue box will update the display as device is upgraded.
4. Click Finish

   The Upgrade Devices dialogue box will pop up.
5. Select the checkbox next to the Primary HA-SBC
6. Click Next

   Dialogue box will update the display as device is upgraded.
7. Click Finish

Next steps

Upgrading from an uploaded file on page 67

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Upgrading SBC boxes

Procedure

1. Click Upgrade on the updates tab of the System Management screen.

   The Upgrade Devices dialogue box will pop up.
2. Select the checkbox next to the device(s) to be upgraded..

   Devices can be upgraded one at a time or as a group. If more than one device is selected, they will be put in a queue and upgraded one at a time.
3. Click Next.

   Dialogue box will update the display as device is upgraded.
4. Click Finish.

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Performing a Rollback

Procedure

1. Select the System Management feature from the Task Pane.

   The System Management screen is displayed.

2. Select the Updates tab.

   The current EMS version and available upgrade and rollback options are displayed in the Content Area.

3. Click the Rollback button.

   The Rollback Status screen is displayed while rollback is happening, then the Updates tab will be redisplayed.

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Non service affecting EMS upgrade

About this task

If the system is a High Availability (EMS+Primary+Secondary) or EMS+separate SBC systems, then upgrading the EMS is non-service affecting.

If it is a single box, i.e. both EMS and SBC are on a single piece of hardware, then the service is affected during the upgrade.

Procedure

1. Log on to EMS as Administrator through the GUI from Firefox.
2. Upload new Avaya SBC software.

   From GUI, click on System Management, select Updates tab, select Upgrade from uploaded file, click Browse, choose the file and click Open

3. Click Upgrade

   You may lose connectivity to the EMS during the upgrade

4. Confirm EMS upgrade by clicking About in the top right corner of the EMS GUI
5. If EMS is unavailable or version information is inaccurate, initiate rollback

Related links

Software only upgrades to upgrade Avaya SBCE from Release 4.x to Release 6.2 on page 30

Chapter 5: Upgrading from Release 6.0 to Release 6.2

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3

Upgrading from Avaya Aura® Session Border Controller (AASBC) 6.0 to Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2 requires an evaluation of the existing hardware to determine, if any of the existing hardware will need to be replaced. In some cases a complete hardware replacement will be required and in others a migration kit can be purchased.

Introduction

The supported hardware and software platforms for Avaya SBCE 6.3 are:

- (new purchase) Dell R210–ii XL
- (existing) HP DL 360 G7
- Portwell CAD-0208
- VMWare EsXI 5.0/5.1/5.5
- VMWare ESXI 5.1

If an HA configuration is in place for AASBC, a Dell EMS server is required in the migrated configuration.

Related links

AASBC 6.0 to Avaya SBCE 6.2 on HP DL360 checklist on page 37
Preparing to upgrade on page 38
Configuring RAID on page 39
Checking BIOS settings on page 40
Installing Avaya SBCE software on page 41
Configuring Avaya SBCE on page 44
Restoring AASBC on page 44
Reference documents on page 45

AASBC 6.0 to Avaya SBCE 6.2 on HP DL360 checklist

Upgrading to Avaya Session Border Controller for Enterprise (Avaya SBCE) on the HP DL360G7 is expected to take about 2 to 4 hours. The last section is only required for recovering the Avaya Aura® Session Border Controller (AASBC) settings if the upgrade fails or the maintenance window closes. It is important to follow the steps in sequence presented as deviating may result in hard drive(s) corruption. If drives get corrupted then AASBC recovery can only be done from external backups or by re-installing AASBC from its original installation disk media.

Note:

Only certified business partners or APS personnel should be performing the upgrade/migration. The instructions are written at a high level expecting the engineer to be familiar with basic server components, usage, changing configuration, or creating backups, etc. This document shows all essential steps with detailed instructions for a complete Avaya SBCE upgrade.

#	Task	Description	Estimated time	✔
1	Discovery Call	Prior to proceeding, a discovery call needs to take place. A discovery call will cover the site survey and gather the necessary details for a successful migration/upgrade. Contact your Avaya Business Partner or APS for more information.	2 hours	
1	Technical Preparation Preparing to upgrade on page 38	Checks that need to be performed before upgrading	30 minutes	
2	RAID SettingsConfiguring RAID on page 39	Configuring RAID settings	10 minutes	
3	BIOS Settings Checking BIOS settings on page 40	Checking BIOS settings	10 minutes	
4	Avaya SBCE software installation Installing ASBCE software on page 41	Install software from the USB thumb drive	30 minutes	
5	Avaya SBCE configuration Configuring ASBCE on page 44	Configure Avaya SBCE and upgrade to latest release	2 hours	
	(Optional) AASBC restoration Restoring AASBC on page 44	Restore AASBC if Avaya SBCE installation is not successful or if the maintenance window closes	10 minutes	

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Preparing to upgrade

Procedure

1. Confirm that the migration kit is complete.

2. Locate the HP DL360G7 front panel and hard drives. See server documentation for further details.
3. Power down the server by pressing and holding the power key until server powers off.
4. Mark the three AASBC 146 Gb hard drives 1, 2, and 3.

   This can be done with a marker or tape that will remain secure on the drives.
5. Remove the three 146 Gb hard drives.
6. Insert the two 300 Gb hard drives from the migration kit into slots 1 and 2.
7. Connect a usb mouse, usb keyboard, and a vga monitor to the server.

Next steps

Configuring RAID on page 39

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Configuring RAID

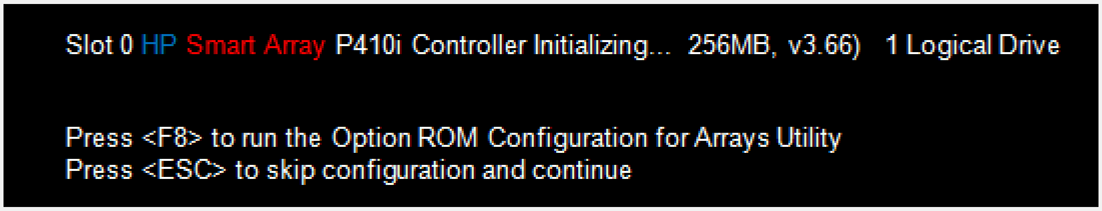
About this task

Avaya SBCE supports RAID 1 configuration with two identical 300 Gb hard drives.

Procedure

1. Boot the server.
2. Press **F2** when F9 and F11 display in the lower left hand corner of the HP Proliant splash screen.

   There is approximately a 5 second window to do this. The following Smart Array utility will appear:



```
Slot 0 HP Smart Array P410i Controller Initializing...  256MB, v3.66)   1 Logical Drive

Press <F8> to run the Option ROM Configuration for Arrays Utility
Press <ESC> to skip configuration and continue
```

3. Press **F8** to enter array controller.
4. Select **Create Logical Drive** from the main menu.

   The raid controller will recognize the drives in the server and the drive will have a blue LED indicator when recognized. If the drive is not recognized exit to the main menu and select Create Logical Drive again to see if the blue light comes on. When the drives are recognized they will be listed in the upper left hand portion of the raid controller screen.
5. Save and Exit.

The server will automatically reboot after user exits the Arrays Utility.

Next steps

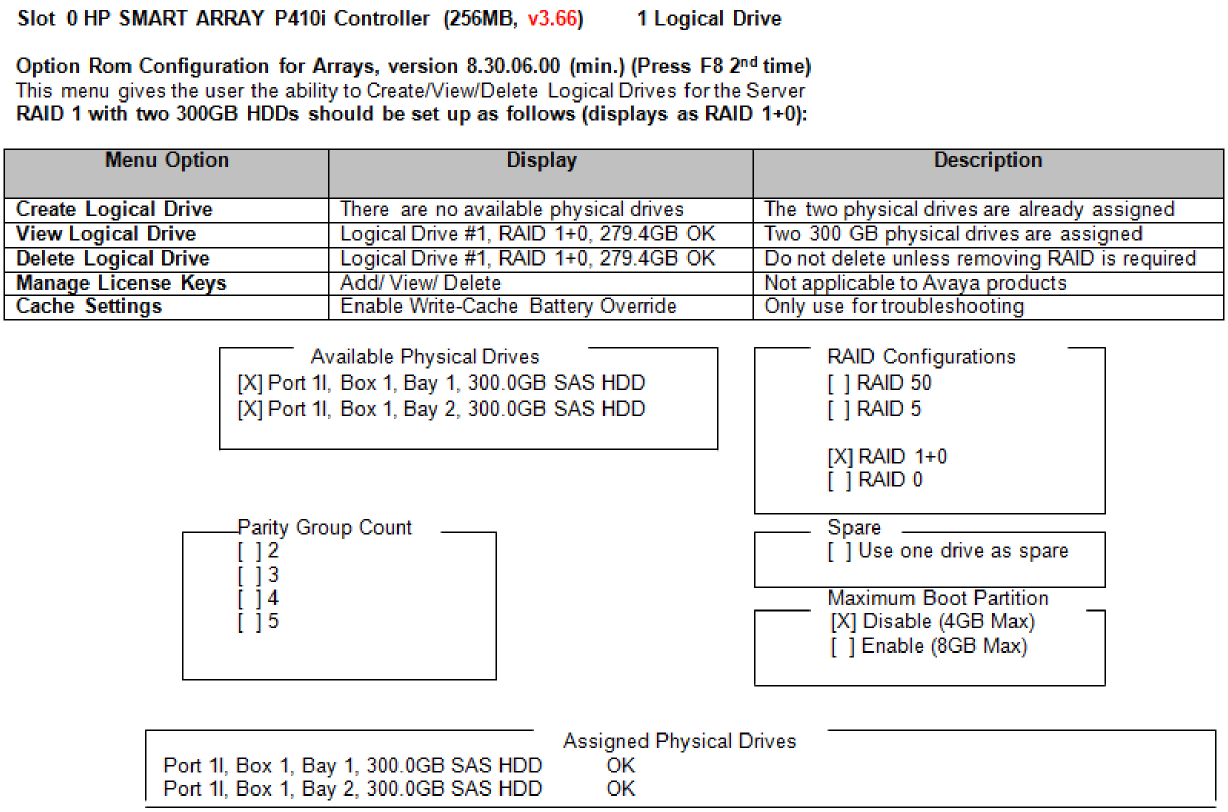
Checking BIOS settings on page 40

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

RAID 1 settings on page 40

RAID 1 settings



Slot 0 HP SMART ARRAY P410i Controller (256MB, v3.66) **1 Logical Drive**

Option Rom Configuration for Arrays, version 8.30.06.00 (min.) (Press F8 2nd time)
This menu gives the user the ability to Create/View/Delete Logical Drives for the Server
RAID 1 with two 300GB HDDs should be set up as follows (displays as RAID 1+0):

Menu Option	Display	Description
Create Logical Drive	There are no available physical drives	The two physical drives are already assigned
View Logical Drive	Logical Drive #1, RAID 1+0, 279.4GB OK	Two 300 GB physical drives are assigned
Delete Logical Drive	Logical Drive #1, RAID 1+0, 279.4GB OK	Do not delete unless removing RAID is required
Manage License Keys	Add/ View/ Delete	Not applicable to Avaya products
Cache Settings	Enable Write-Cache Battery Override	Only use for troubleshooting

Available Physical Drives
[X] Port 1I, Box 1, Bay 1, 300.0GB SAS HDD
[X] Port 1I, Box 1, Bay 2, 300.0GB SAS HDD

RAID Configurations
[ ] RAID 50
[ ] RAID 5

[X] RAID 1+0
[ ] RAID 0

Parity Group Count
[ ] 2
[ ] 3
[ ] 4
[ ] 5

Spare
[ ] Use one drive as spare

Maximum Boot Partition
[X] Disable (4GB Max)
[ ] Enable (8GB Max)

Assigned Physical Drives
Port 1I, Box 1, Bay 1, 300.0GB SAS HDD OK
Port 1I, Box 1, Bay 2, 300.0GB SAS HDD OK

Related links

Configuring RAID on page 39

Checking BIOS settings

Procedure

1. Boot the server and press **F9** from the HP Proliant splash screen to enter BIOS.
2. Set BIOS Serial Console Port to `Com 1`.
3. Set BIOS Serial Console Baud Rate to `19200`.

4. Verify that the BIOS version and other settings match the following table. If any are different, then try to correct. If unable to correct, then the server can't be upgraded because it is either defective or not compatible.

Setting	Value
BIOS version	P68 05/05/2011 P68 01/28/2011 P68 12/01/2010 P68 09/30/2010 P68 08/16/2010 P68 05/15/2010
Date and Time	Current date and time
Processor 1	Intel 2.40 GHz, 12 MB L3 Cache
Processor 2	n/a
Memory	Minimum of 4 GB required

5. Save and Exit BIOS

Next steps

Installing ASBCE software on page 41

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Installing Avaya SBCE software

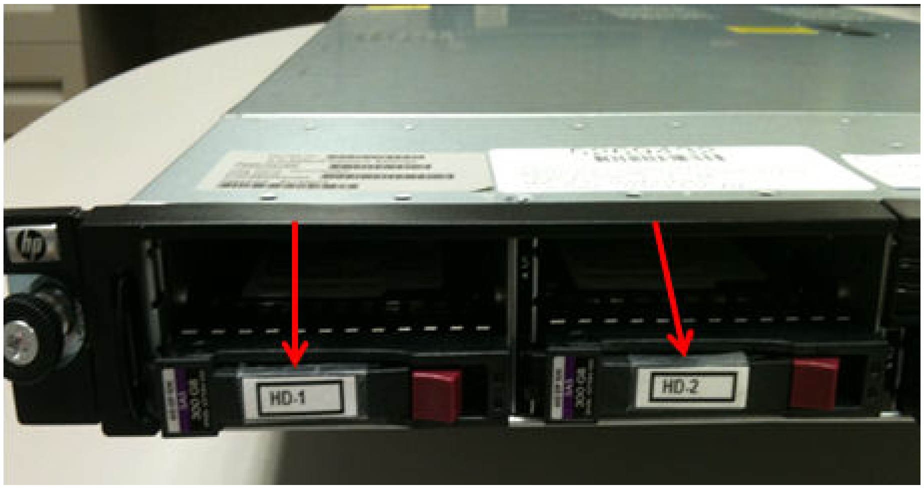
About this task

An Avaya SBCE 6.2 software image is provided on a USB thumb drive (Avaya Part # 700503875) in the migration kit. This is the procedure to install that software. This installation must be done as described and cannot be done using the mouse, keyboard, and monitor.

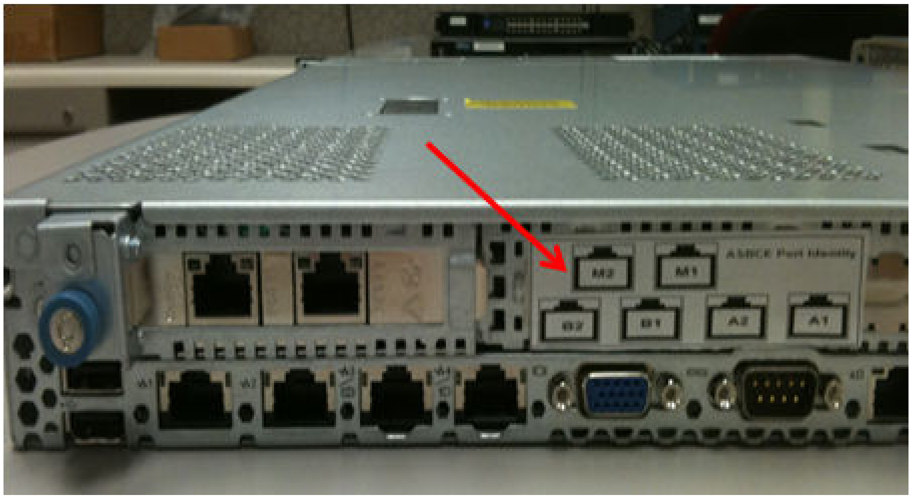
Procedure

1. Power down the server by pressing and holding Power key until server powers off.
2. Connect serial console cable to the serial port of the server and a Laptop or PC with PuTTY (use communication parameters set to 19200, 8, N, 1).

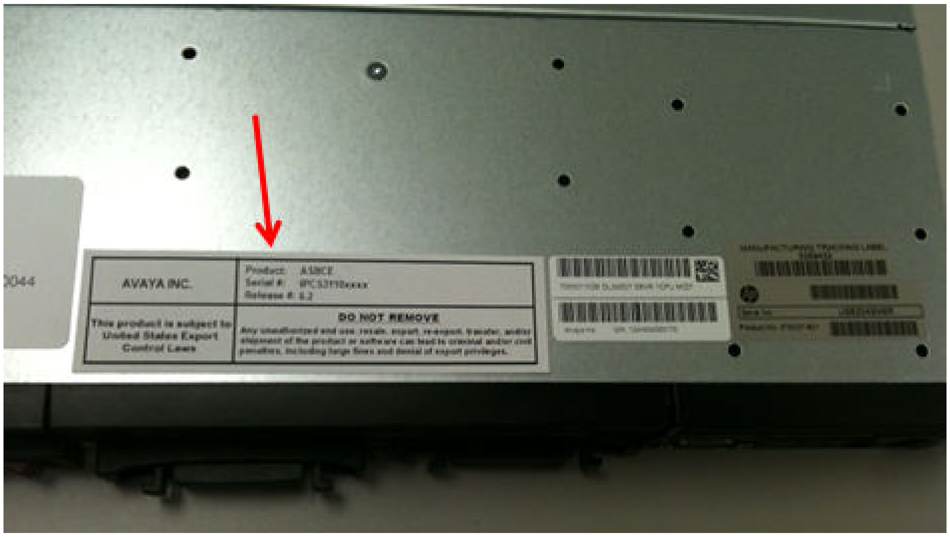
3. Apply labels to hardware
    a. Apply hard drive labels as shown in the following image.



    b. Apply NIC port identity label to the rear of the chassis cover as shown in the following image, making sure that it does not cover or block any ventilation holes.



c. Apply the serial number label to the top of the front of the chassis as shown in the following image.


AVAYA INC.
Product: ASBCE
Serial #: IPCS3110xxxx
Release #: 6.2
This product is subject to United States Export Control Laws
DO NOT REMOVE
Any unauthorized end use, resale, export, re-export, transfer, and/or shipment of the product or software can lead to criminal and/or civil penalties, including large fines and denial of export privileges.

Note:

If the server is mounted without rails, then you will have to remove the server to apply the serial number sticker.

4. Insert the Avaya SBCE thumb drive in the front USB port.
5. Turn on the server.
6. A boot prompt will appear on the PuTTY window, type `serial` in the command line and press **Enter**.

   This will take about 10 minutes.
7. When prompted, choose the image source, type `1`, and then press **Enter**.
8. This process does not have a progress bar to indicate when it is finished, so press **Enter** to reboot the system after about 10 minutes.
9. Continue, type `Y` and then press **Enter**.
10. Press any key to reboot the system.
11. Remove the USB drive and reboot the server again.
12. After reboot, the server will be identified as an `HPDL360G7`, click **Ok** and press **Enter**
13. Enter Serial Number and press **Enter** twice. Press **Enter** one more time at the confirmation – installation will continue.

    Caution:

    Failure to enter serial number correctly the first time will require the software to be reinstalled.

> ✱ **Note:**
>
> The serial number for the server is given on the serial number label with the format of "IPCS3110xxxx."

14. Software installation is complete when `Enter Y to reboot or N to shutdown the machine (Y/N)[Y]` is displayed on the terminal. Type `Y` and press **Enter**. Server will reboot shortly.

Next steps

Configuring ASBCE on page 44

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Configuring Avaya SBCE

About this task

Once the server reboots, the server is ready for Avaya SBCE configuration - refer to following documentation for details.

Procedure

Configure Avaya SBCE using the information from *Installing Avaya Session Border Controller for Enterprise* and *Administering Avaya Session Border Controller for Enterprise*.

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Restoring AASBC

About this task

Use this procedure to restore the original Avaya Aura SBC 6.0 if something goes wrong with the Avaya SBCE installation or if the maintenance window closes.

Procedure

1. Power down the server by pressing and holding the power key until server powers off.
2. Remove the two 300 Gb hard drives.
3. Install the three AASBC 146 Gb hard drives in the order that they were removed.
4. Power up the server.

   It will take about 10 minutes for AASBC to come online. Status can be monitored via the web interface. See AASBC documentation for details.

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Reference documents

All of the reference documents listed below can be obtained from https://support.avaya.com

- Upgrading Avaya Session Border Controller for Enterprise, Release 6.2
- Installing Dell R620 User Guide
- HP ProLiant DL360 G8 Server User Guide
- Installing the HP DL360 G7 Server
- Avaya Session Border Controller for Enterprise Overview and Specification
- Deploying Avaya Session Border Controller for Enterprise 6.3
- Administering Avaya Session Border Controller for Enterprise 6.3

Related links

Upgrading from Avaya SBCE 6.2 to Avaya SBCE 6.3 on page 37

Chapter 6: Upgrading Avaya SBCE from 6.2 to 7.0

Upgrade from Release 6.2 to Release 7.0

To upgrade to Avaya SBCE Release 7.1, you must first upgrade from Release 6.2 to Release 7.0 and then upgrade to Release 7.1.

After purchasing an upgrade license for Release 7.0, you can upgrade from Avaya SBCE Release 6.2 to 7.0 by using the command line interface (CLI). You can only use the CLI to upgrade from Release 6.2 to Release 7.0. However, you can use the CLI or the EMS web interface to upgrade from Release 6.3 to Release 7.0.

To upgrade from Avaya SBCE Release 6.2 to 7.0, you must have a WebLM server.

Before beginning the upgrade:

- Download the license file from PLDS.
- Assign the WebLM server as license host for the licenses on PLDS.
- Regenerate the license file.
- Ensure that Avaya SBCE servers in the deployment have unique hostnames. In case two or more servers have the same hostname, change the hostname before attempting an upgrade. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller*.

To continue using encryption for advance sessions, add a new license for encryption.

Note:

For information about Release 7.0 build, see http://support.avaya.com.

You cannot rollback from Release 7.0 to Release 6.2 directly. To rollback to Release 6.2, you must manually install the same version of Release 6.2 and restore the snapshot that you took prior to upgrade.

You can rollback from Release 7.0 to Release 6.3.

Upgrade sequence

In a multi-server deployment, the upgrade sequence is:

1. EMS server with lower node ID
2. EMS server with higher node ID

3. Avaya SBCE pair:
    1. Avaya SBCE with lower node ID
    2. Avaya SBCE with higher node ID

You can find the node IDs in `/usr/local/ipcs/etc/sysinfo`. Before upgrading, ensure that the EMS or Avaya SBCE with lower node id is secondary to avoid losing ongoing calls.

Clearing ghost devices in the database

About this task

Devices that are not present in the network can be present in the database. To avoid problems during upgrade, you must remove ghost devices in the database before upgrading the Avaya SBCE.

Before you begin

Download the fix-orphaned-devices.py script from PLDS by using the SBCE0000021 download ID.

Procedure

1. Log in as an ipcs user on EMS server, and type `sudo su` to get root privileges.
2. At the command prompt, type the following command:

    ```
    /etc/init.d/ipcs-db start
    ```

    The system starts the database. For the script to run successfully, the database must be running.

    If the database is running when you type the following command:

    ```
    /etc/init.d/ipcs-db start
    ```

    The system displays a message to indicate that the database is already running. For example,

    ```
    2015-02-18 10:18:33,031 INFO: DB is already running.
    ```

3.

    ```
    chmod +x fix-orphaned-devices.py
    ```

    The system makes the script an executable file.
4. At the command prompt, type the following command:

    ```
    ./fix-orphaned-devices.py
    ```

    After the script runs successfully, continue to upgrade Avaya SBCE.

    Important:

    If you come across ghost devices after migrating to Avaya SBCE 7.0, escalate the database migration problem to Tier 4 support.

Upgrading EMS and Avaya SBCE using CLI

Before you begin

1. Download the Avaya SBCE Release 6.2.1Q18 image file from PLDS. Set up a USB flash device with this image. This USB flash device will be useful if you have to reinstall Avaya SBCE Release 6.2.1.
2. From PLDS website at https://plds.avaya.com/, download the upgrade tar file to your desktop and then SFTP the file to `/home/ipcs` on the server. For upgrading from Avaya SBCE 6.2 to Avaya SBCE 7.0, the tar file is named `ipcs_7.0.0.Qxx_<md5sum>.tar.gz`.

About this task

Important:

During the upgrade process:

- Do not restart applications or run any web interface or CLI commands, such as reboot or shutdown.
- Ensure that EMS is reachable from Avaya SBCE.

Procedure

1. Connect a keyboard and monitor to the server (VGA mode) or a serial cable to the serial console port on the server.

   Important:

   Do not perform this procedure using SSH session.

   If the server is a primary Avaya SBCE server, ensure that the applications are stopped before starting upgrade.

2. Log in as an ipcs user and type `sudo su` to get root privileges.
3. At the command prompt, type the following command to create a temporary directory in the /archive folder. upgrade_temp is used as an example. It can be any other unique name.

   ```
   # mkdir /archive/upgrade_temp
   ```

   If this directory already exists, ensure that it is empty. To empty the directory, type the following command:

   ```
    # rm -rf /archive/upgrade_temp/*
   ```

4. Move the upgrade tar file `ipcs-7.0.0*tar.gz` from `/home/ipcs` to `/archive`.
5. Ensure that the checksum of the image matches with the checksum value in the file name by running the **md5sum** command.
6. At the command prompt, type the following commands to extract the package to the `/archive/upgrade_temp` directory:

```
# cd /archive
# tar xvzf ipcs_7.0.0.Qnn_<md5sum>.tar.gz -C /archive/upgrade_temp
```

Do not extract the migration package in the same directory in which the tar.gz file exits.

7. At the command prompt, type the following commands to start an upgrade:

   ```
   cd /archive/upgrade_temp/uber
   #./ursbce.py --migrate --console=[vga/serial]
   ```

   Note:

   For vga connection, type `--console=vga` or for serial connection, type –`console=serial`.

   The system displays `Start Migrating System`.

   The system is restarted. After restarting, the **SBC 7.0 migration** option is automatically selected. The system, then backs up data in the `/archive` partition. This procedure repartitions and reformats the system and installs the updated software packages and reboots.

8. If prompted to select option in the "error processing drive" screen, select "Re-initialize all".

Next steps

In a multi-server deployment, repeat these steps to upgrade the secondary Avaya SBCE and primary Avaya SBCE, as applicable.

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Upgrading EMS and Avaya SBCE using a USB device or DVD

Before you begin

- Ensure that you take a snapshot of the system and store the snapshot on an external storage media. During the upgrade procedure, do not restart applications or run any web interface commands, such as reboot or shutdown.
- Download the .iso or .img file from the PLDS website at https://plds.avaya.com/
- If you plan to use a DVD, burn the *.ISO image on the DVD and then insert it. If you plan to use a USB device, save the *.IMG file to the USB device.

About this task

During the upgrade process:

- Do not restart applications or run any web interface commands, such as reboot or shutdown.
- Ensure that EMS is reachable from Avaya SBCE.

Procedure

1. Connect a keyboard and monitor to the server (VGA mode) or a serial cable to the serial console port on the server.
2. Boot the system with the DVD or USB device attached.
3. Change the BIOS settings to ensure that the system boots from DVD or the USB storage device.

   You must set the BIOS boot order with USB as first priority and hard drive as second priority. If you do not change the boot order, the system boots from the hard drive.

   - For Dell servers, press `F11` to set boot options.
   - For CAD 0208, press the `Tab` or `Delete` key to set boot options.
4. Wait until the system displays the message `Found SBC version 6.2.1.Q18 installed on this system`.
5. When the system displays **Proceed with upgrade? (yes/no)**, type `Yes` to proceed with the upgrade.

   If you type `yes`, the system takes a backup of the existing Avaya SBCE specific data and creates new partitions. The system displays a message indicating the connection mode that is being used for installation. Then, the system displays a message to specify the preferred console to be used after installation.

   If you type `no` in the **Proceed with upgrade? (yes/no)** field, the system displays the prompt for a fresh installation.
6. In the **Please select default console type (vga or serial) [serial]** field, type `serial` or `vga`, depending on the connection mode, and press `Enter`.

   The console selected in this step determines the connection mode with which you can connect to the Avaya SBCE console after the upgrade.
7. If prompted to select option in the "error processing drive" screen, select **Re-initialize all**.

   This process might take up to 30 minutes. The system backs up data, repartitions and reformats remaining partitions, installs packages and bootloader, and initiates the post-installation steps. The system displays `Running OS Hardening now` and upgrades the database.
8. When the system displays `Press Enter to reboot the system`, remove the USB device, if used, and press `Enter`.

   The system is restarted. If you use a DVD, and if the DVD is not ejected automatically, then eject the DVD while the system is being restarted.
9. After the system is restarted, enable WebLM with EMS, EMS+SBCE, or an external device such as System Manager acting as WebLM server.
10. Generate the license file on PLDS and enter the number of sessions for which you have purchased a license.

For more information about generating the license file, see Configuring WebLM server IP address on EMS.

11. Log in to the EMS web interface.
12. In the left navigation pane, click **System Management**.

    The system displays the System Management page.
13. In the **Devices** tab, locate the device you upgraded, and click **Edit**.

    The system displays the Edit Device dialog box.
14. In the **Standard Sessions**, **Advanced Sessions**, and **Scopia Video Sessions** fields, type the number of licensed sessions depending on the license you purchased.
15. Click **Finish**.

Next steps

In a multi-server deployment, repeat these steps to upgrade the secondary Avaya SBCE and primary Avaya SBCE, as applicable.

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Related links

Configuring WebLM server IP address on EMS on page 76

Chapter 7: Upgrading from Release 6.3 and 7.0 to Release 7.1

Installing GUI patch for upgrades from Release 7.0 or Release 6.3.6 to Release 7.1

Before you begin

Download the GUI patch from PLDS:

- For upgrades from Avaya SBCE 7.0 to 7.1, download `7.0-upgrade_regex_patch.tar`.
- For upgrades from Avaya SBCE 6.3.6 to 7.1, download `6.3.6-upgrade_regex_patch.tar`.

About this task

Avaya SBCE Release 7.0 does not accept upgrade packages with three-digit version numbers. To overcome this issue, run the GUI patch before upgrading from Release 7.0 to Release 7.1.

You must also run the patch before upgrading from Avaya SBCE 6.3.6 to 7.1.

This patch is not required if you have already upgraded to Avaya SBCE 7.0.1.

Procedure

1. Log in to Avaya SBCE as root.
2. Untar the package to `/home/ipcs`.
3. At the command prompt, type the following command:

   ```
   cd upgrade-patch/
   ```

4. At the command prompt, type the following command:

   ```
   sh upgrade-regex.sh
   ```

Upgrade from Release 6.3 and Release 7.0

To upgrade from Release 6.3 to Release 7.1, you must first upgrade from Release 6.3 to Release 7.0 if you have a service pack earlier than 6.3.6. You must follow the same procedure to upgrade from Release 6.3 to Release 7.0 and from Release 7.0 to Release 7.1.

Note:

You can directly upgrade Avaya SBCE 6.3.6 to Release 7.1 after applying the GUI patch.

You can upgrade from Release 6.3 to Release 7.0 after purchasing an upgrade license for Release 7.0. Perform all upgrades in a maintenance window. If the system uses 6.2 or an earlier version, follow the upgrade procedures in Chapter 4. For information about the latest Release 7.1 build, see http://support.avaya.com.

Note:

Before beginning the upgrade, ensure that:

- All debug logs are disabled.
- Avaya SBCE servers in the deployment have unique hostnames.

  If two or more servers have the same hostname, change the hostname. For more information, see *Troubleshooting and Maintaining Avaya Session Border Controller*.

You can check the upgrade status at `/archive/log/icu/upgrade.log`

Supported upgrade paths from Avaya SBCE 6.3.x

If you have Avaya SBCE 6.3.5 or earlier, upgrade to Avaya SBCE 6.3.6.

From Avaya SBCE 6.3.6, you can apply the GUI patch and then upgrade to Avaya SBCE 7.1 without upgrading to release 7.0 or 7.0.1.

If you have Avaya SBCE 6.3.3, you can upgrade to release 7.0, then release 7.0.1, and finally upgrade to release 7.1.

Upgrades from Avaya SBCE 6.3.5 and 6.3.6 to release 7.0 is not supported.

Upgrade sequence in multi-server deployments

In a multi-server deployment, the upgrade sequence is:

1. EMS server with lower node ID
2. EMS server with higher node ID
3. Avaya SBCE pair:
   a. Avaya SBCE with lower node ID
   b. Avaya SBCE with higher node ID

You can find the node IDs in `/usr/local/ipcs/etc/sysinfo`. Before upgrading, ensure that the EMS or Avaya SBCE with lower node id is secondary to avoid losing ongoing calls.

Related links

Upgrading primary EMS or standalone Avaya SBCE on page 54
Upgrading secondary EMS on page 56
Upgrading HA pairs on page 57
Upgrading Avaya SBCE servers on page 58
Rolling back using web interface on page 59
Rolling back through CLI on page 60

Upgrading primary EMS or standalone Avaya SBCE

Procedure

Copy the upgrade tar file to the EMS server by using one of the following methods:

- Copy the upgrade tar file to the EMS by using the web interface.
- Copy the upgrade tar file manually to the EMS server using SFTP or SCP.

✱ **Note:**

You can use the same procedure to upgrade a standalone Avaya SBCE or EMS+Avaya SBCE deployment from Release 7.0 to Release 7.1.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52
Upgrading EMS using a web browser on page 54
Uploading using SFTP or SCP on page 55
Uploading upgrade package using SFTP or SCP on page 63
Upgrading EMS using a web browser on page 64

Upgrading EMS using a web browser

Before you begin

Download the upgrade package to a local or remote PC from Avaya Product Licensing and Delivery System (PLDS).

About this task

Uploading larger files using a browser can sometimes be unreliable, especially when using older browser versions such as Internet Explorer 7, Internet Explorer 8, or Firefox 3.x. Uploading large files through a browser might result in a failed upload or checksum error.

Transfer the file to EMS by using SFTP.

Procedure

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

   The system displays the System Management screen.
3. Click the **Updates** tab.
4. Click **Upgrade from uploaded file**.
5. Click the **Browse** button and navigate to the folder containing the downloaded upgrade file.
6. Select the upgrade file.
7. Click **Upgrade**.

The system displays the Upgrade Confirmation screen.

8. Click **Start Upgrade**.

   The system displays Upgrade Status screen with the upgrade log file in a viewable window. The upgrade process takes some time. Do not reboot when an upgrade is in progress. After the upgrade is complete, the system displays the **Return to EMS** tab.

9. Click **Return to EMS** to log back in to EMS.

Next steps

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Related links

Upgrading primary EMS or standalone Avaya SBCE on page 54

Uploading using SFTP or SCP

Before you begin

Download the tar file from the PLDS website.

Procedure

1. Log on to the EMS server as an ipcs user by using port 222.
2. Upload the upgrade tar file to the EMS server using SFTP or SCP.
3. Copy the file to `/home/ipcs`.
4. Log in with the root privileges and move the file from `/home/ipcs` to the EMS server folder:`/archive/urpackages`.

   Note:

   If the urpackages folder does not exist, create the urpackages folder in the exact path shown above and then proceed with Step 5.

5. On the command line, type `md5sum` *`filename`* to verify the integrity of the file. Ensure that results on the left match the string embedded within the file name.
6. Log on to the EMS web interface.
7. In the left navigation pane, click **System Management** > **Updates**.

   The system displays the current EMS version and the available upgrade options.

8. In the Updates tab, in the **Upgrade from local file** field, select the upgrade file.
9. Click **Upgrade**.

   The system displays the Upgrade Confirmation screen.

10. Click **Start Upgrade**.

The system displays a series of windows to indicate that the EMS software is upgrading.

When the upgrade is complete, the system displays the final window.

11. Click **Return to EMS**.

    The system displays the System Management page.

Next steps

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Related links

Upgrading primary EMS or standalone Avaya SBCE on page 54

Upgrading secondary EMS

Before you begin

Download the tar file from the PLDS website:

- For upgrading from Release 6.3 to Release 7.0, use `sbce-7.0.0-xx-xxxx-<md5sum>.tar.gz`.
- For upgrading from Release 7.0 to Release 7.1, use `sbce-7.1.0.0-xx-xxxx-<md5sum>.tar.gz`.

Procedure

1. Copy the tar file to the Secondary EMS server using ipcs user on port 222.

   You can use SFTP or SCP tools to access the Secondary EMS server.

2. Connect to the system using VGA or serial console.

3. Using root permissions, move the upgrade tar file from the ipcs user home directory to `/archive/urpackages` directory.

4. Ensure that the md5sum of the upgrade tar file matches the checksum given in the name of the file.

   You can use the **`md5sum`** command to verify whether the md5sum and the checksum match.

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

   ```
   mkdir /archive/temp_upgrade
   ```

   Where *temp_upgrade* is the name of the temporary directory.

   The system creates a temporary directory in the archive directory.

6. At the command prompt, type the following command:

   ```
   rm –rf /archive/temp_upgrade/*
   ```

   This command removes all content in the temporary directory.

7. At the command prompt, do one of the following:

   - For upgrading from Release 6.3 to Release 7.0, type the following command:

     ```
     tar xvf /archive/sbce-7.0.0-xx-xxxx-<md5sum>.tar.gz –C /archive/temp_upgrade
     ```

     Where xx-xxxx is the build number.

   - For upgrading from Release 7.0 to Release 7.1, type the following command:

     ```
     tar xvf /archive/sbce-7.1.0.0-xx-xxxx-<md5sum>.tar.gz –C /archive/temp_upgrade
     ```

   The system extracts the upgrade tar file in the temporary directory.

8. At the command prompt, type the following command:

   ```
   cd /archive/temp_upgrade
   ```

   Where *temp_upgrade* is the name of the temporary directory.

9. At the command prompt, type the following command:

   ```
   chmod +x ursbce.py
   ```

10. At the command prompt, type the following command:

    ```
    ./ursbce.py -U --daemonize
    ```

    This step reboots the system.

    ⚠ **Warning:**

    Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if the user is disconnected because of inactivity.

11. Wait for the system to reboot.

12. At the command prompt, type the following command to verify the version of the system:

    ```
    cat /etc/sbce-version
    ```

    The file `/archive/log/icu/upgrade.log` contains upgrade related logs.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52

Upgrading HA pairs

Before you begin

Ensure that EMS servers are upgraded before upgrading HA pairs.

About this task

With this procedure, you can upgrade Avaya SBCE devices that are in HA pairs. For more than one Avaya SBCE pair in HA, repeat the procedure for each HA pair.

Procedure

1. In the **Updates** tab, click **System Management** and then click **Upgrade**.

   The system displays the Upgrade Devices window.
2. Select the check box before the Device Name column.

   The system determines and selects the primary Avaya SBCE.
3. Click **Next**.

   The system displays a window that states that the Device is upgraded.
4. Click **Finish**.

   The system displays the Upgrade Devices window.
5. Select the check box before the Device Name column.

   The system now selects the other Avaya SBCE in the HA pair.
6. Click **Next**.

   The system displays a message indicating that the device is upgraded.
7. Click **Finish**.

   Note:

   After the EMS software has been upgraded, the system displays the following message for Avaya SBCE boxes and HA pairs on the **Updates** tab:

   ```
   One or more devices are in an orphan state.  If you would like
   to upgrade these devices now, please click the Upgrade button
   below. You may also choose to rollback your EMS at this point.
   ```

   HA system pairs and all other Avaya SBCE systems must be upgraded before this message is resolved.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52

Upgrading Avaya SBCE servers

Before you begin

Ensure that the EMS servers are upgraded before upgrading Avaya SBCE servers.

About this task

This procedure upgrades Avaya SBCE servers that are not in an HA pair. When more than one Avaya SBCE server is available, repeat this step for each Avaya SBCE server.

Procedure

1. In the left navigation pane, click **System Management** > **Upgrade**.

   The system displays the Upgrade Devices message box.

2. Select the check box next to the devices that you want to upgrade.

   The devices can be upgraded one at a time or as a group. If you select more than one device, the devices are put in a queue and upgraded one at a time.

3. Click **Next**.

   The system displays a message box indicating that the device is upgraded.

4. Click **Finish**.

   Note:

   After the EMS software has been upgraded, the following message is displayed for Avaya SBCE boxes and HA pairs on the Updates tab:

   ```
   One or more devices are in an orphan state.  If you would like
   to upgrade these devices now, please click the Upgrade button
   below.  You may also choose to rollback your EMS at this point.
   ```

   HA system pairs and all other Avaya SBCE servers must be upgraded before this message is resolved.

Next steps

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52

Rolling back using web interface

About this task

If you upgrade from Release 6.2 or Release 6.3, rollback option is unavailable. But, the rollback option is available if you upgrade from Release 7.0 to Release 7.1.

Procedure

1. From the left navigation pane, click **System Management**.

   The system displays the System Management screen.

2. Select the **Updates** tab.

The system displays the current EMS version and the available upgrade and rollback options.

3. Click **Rollback**.

   The system displays the Rollback Status screen during rollback, and displays the **Return to EMS** tab after the rollback is complete.

4. Click the **Return to EMS** tab to log back on to the EMS web interface.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52

Rolling back through CLI

Before you begin

Download the Avaya SBCE tar file for the release to which you want to roll back.

About this task

You can roll back to the last Avaya SBCE release from CLI.

Rolling back from Avaya SBCE 7.1 to 6.3.6 is not supported through the web interface. You must use CLI to roll back from Avaya SBCE 7.1 to 6.3.6.

Procedure

1. Log on to Avaya SBCE as a super user.
2. Delete the existing files from `/archive/temp`.
3. Untar the package to which you want to roll back, in the temp directory.
4. To begin rollback, type `./ursbce.py ——rollback —daemonize`.

   After the rollback process is complete, you can check the rollback logs stored at `/archive/log/icu`.

Related links

Upgrade from Release 6.3 and Release 7.0 on page 52

Chapter 8: Upgrading Avaya SBCE to Release 7.2 and later

Upgrade checklist

Sr. No.	Tasks/ Actions	Links/ Notes	✔
1	For multi-server deployments, ensure you follow the proper sequence.	Upgrade sequence in a multiserver deployment on page 61	
2	Upgrade primary EMS or standalone Avaya SBCE.	Upgrading the primary EMS or standalone Avaya SBCE on page 62	
3	Upgrade the secondary EMS.	Upgrading secondary EMS on page 65	
4	Upgrade the Avaya SBCE HA pairs.	Upgrading Avaya SBCE HA pairs using web interface on page 66	
5	Upgrade single Avaya SBCE servers.	Upgrading single Avaya SBCE servers on page 67	
6	Upgrade Avaya SBCE from Release 7.1.x to Release 7.2 using CLI.	Upgrading Avaya SBCE from Release 7.1.x to Release 7.2 by using CLI on page 70	
7	Upgrade Avaya SBCE from Release 7.2 to Release 7.2.1 using CLI.	Installing pre-upgrade patch for Avaya SBCE upgrade from Release 7.2 to Release 7.2.1 using CLI on page 69	
8	Check the upgrade status at `/archive/log/icu/upgrade.log`.	-	
9	In case the upgrade fails for any reason, rollback to the previous release.	Rolling back using web interface on page 72	

Upgrade sequence in a multiserver deployment

Before upgrading, ensure that the EMS or Avaya SBCE with a lower node ID is configured as the secondary server to avoid losing ongoing calls.

Find the node IDs from `/usr/local/ipcs/etc/sysinfo`.

No.	Tasks	References	Notes	✔
1	Upgrade the EMS server with a lower node ID.	See Upgrading secondary EMS on page 65	-	
2	Upgrade Avaya SBCE with a lower node ID.	See Upgrading Avaya SBCE HA pairs using web interface on page 66	-	
3	Upgrade Avaya SBCE with a higher node ID.	See Upgrading Avaya SBCE HA pairs using web interface on page 66	-	
4	Upgrade the EMS server with a higher node ID.	See Upgrading the primary EMS or standalone Avaya SBCE on page 62	-	

Upgrading the primary EMS or standalone Avaya SBCE

Follow these procedures for software-only upgrades:

No.	Task	Notes	Reference	✔
1	Copy the upgrade tar file to the EMS server.	Use one of the following methods: • The EMS web interface. • Copy to the EMS server by using SFTP or SCP. **Note:** You can use the same procedure to upgrade the following deployments from Release 7.0 to Release 7.1: • A standalone Avaya SBCE • EMS and Avaya SBCE	• For using EMS web interface, see Upgrading EMS using a web browser on page 64. • For copying using SFTP or SCP, see Uploading upgrade package using SFTP or SCP on page 63.	
2	Add the signature files.	Upload the signature file.	See Adding signatures file on page 63	
3	Add the .asc file.	Upload the .asc file.	See Adding .asc file on page 63	

Uploading upgrade package using SFTP or SCP

Procedure

1. Log on to the EMS server as an ipcs user by using port 222.
2. Upload the upgrade tar file to the EMS server using SFTP or SCP.
3. Copy the file to `/home/ipcs`.
4. Log in with the root privileges and move the file from `/home/ipcs` to the EMS server folder:`/archive/urpackages`.

   ✱ **Note:**

   If the urpackages folder does not exist, create the urpackages folder in the exact path shown above.
5. On the command line, type `md5sum` *`filename`* to verify the integrity of the file. Ensure that results on the left match the string embedded within the file name.

Adding signatures file

About this task

To upgrade from Release 7.1.x, you must add signature files in addition to running the upgrade tar file. The signatures tar file contains integrity check keys used for all packages on Avaya SBCE.

Procedure

1. In the navigation pane, click **System Management** > **Key Bundles**.
2. Click **Browse**.
3. Select the signature file from your system.
4. Click **Upload**.
5. Click **Install** when prompted by the system.

Adding .asc file

About this task

To upgrade from Release 7.1.x, you must add a .asc file in addition to running the upgrade tar file. Avaya SBCE uses the .asc file to validate the upgrade package integrity. Note that the .asc file is required only when the upgrade is done by using the web interface.

Procedure

1. In the navigation pane, click **System Management** > **Updates**.

2. Select **Upgrade from uploaded file**.
3. Click **Choose File** available next to the **Signature** field.
4. Select the .asc file from your system.
5. Click **Upgrade**.

Upgrading EMS using a web browser

Before you begin

First transfer the upgrade file to EMS by using SFTP.

About this task

Uploading larger files using a browser can be unreliable, specifically when using older browser versions, such as, Internet Explorer 7, Internet Explorer 8, or Firefox 3.x. Uploading large files through a browser might result in a failed upload or checksum error.

Note:

It is recommended to use web browser for upgrading EMS.

Procedure

1. Log in to the EMS web interface with administrator credentials.
2. In the navigation pane, click **System Management**.
3. On the System Management screen, click the **Updates** tab.
4. Select **Upgrade from uploaded file**.
5. Click **Choose File** next to **Upgrade package** and select the upgrade file.
6. Click **Choose File** next to **Signature** and select the .asc file.

   Note:

   Signature file is not required when you are upgrading Avaya SBCE from Release 6.3.6, Release 6.3.7, and Release 7.0.2 to Release 7.2.2.
7. Click **Upgrade**.
8. On the Upgrade Confirmation screen, click **Start Upgrade**.

   The system displays the Upgrade Status screen with the upgrade log file in a viewable window. The upgrade process takes some time. Do not reboot when an upgrade is in progress. After the upgrade is complete, the system displays the **Return to EMS** tab.

   Note:

   If the pre-upgrade checks fail and the system prompts to roll back, it is recommended to contact Avaya support at http://support.avaya.com instead of selecting the roll back option.

9. Click **Return to EMS** to log back in to EMS.

Next steps

To verify whether the deployment was successful or not, do one of the following:

- Log on to EMS, and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line interface, run the **ipcs-version** command to check the current version.

Upgrading secondary EMS

Procedure

1. Copy the tar file to the Secondary EMS server using ipcs user on port 222.

   You can use SFTP or SCP tools to access the Secondary EMS server.

2. Connect to the system using VGA or Serial console.

3. Using root permissions, move the upgrade tar file from the ipcs user home directory to `/archive/urpackages` directory.

4. Ensure that the md5sum of the upgrade tar file matches the checksum given in the name of the file.

   You can use the **md5sum** command to verify whether the md5sum and the checksum match.

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

   ```
   mkdir /usr/local/ipcs/temp
   ```

   Where *temp* is the name of the temporary directory.

   The system creates a temporary directory in the archive directory.

6. At the command prompt, type the following command:

   ```
   rm —rf /usr/local/ipcs/temp/*
   ```

   This command removes all content in the temporary directory.

7. At the command prompt, type the following command:

   ```
   tar -zxvf /archive/urpackages/sbce-7.2.x.0-xx-xxxxx-<md5sum>.tar.gz —C /usr/local/
   ipcs/temp
   ```

   Where xx-xxxxx is the build number.

   The system extracts the upgrade tar file in the temporary directory.

8. At the command prompt, type the following command:

   ```
   cd /usr/local/ipcs/temp
   ```

   Where *temp* is the name of the temporary directory.

9. At the command prompt, type the following command:

   ```
   chmod +x ursbce.py
   ```

10. At the command prompt, type the following command:

    ```
    ./ursbce.py -U --daemonize
    ```

    This step reboots the system.

    ⚠ **Warning:**

    Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if the user is disconnected because of inactivity.

11. Wait for the system to reboot.
12. At the command prompt, type the following command and verify the version of the system:

    ```
    cat /etc/sbce-version
    ```

    The file `/archive/log/icu/upgrade.log` contains upgrade related logs.

13. At the command prompt, type the following command to check the upgrade status:

    ```
    grep UPGRADE_STATE /usr/local/ipcs/etc/sysinfo
    ```

    The system displays `UPGRADE_STATE=UPGRADE_COMPLETED` for the successful upgrade and `UPGRADE_STATE=UPGRADE_FAILED` for a failed upgrade process.

Upgrading Avaya SBCE HA pairs using web interface

Before you begin

- Ensure that EMS servers are upgraded before upgrading HA pairs.
- Ensure that Avaya SBCE status is commissioned.

About this task

With this procedure, you can upgrade Avaya SBCE devices that are in HA pairs. For more than one Avaya SBCE pair in HA, repeat the procedure for each HA pair.

Procedure

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

   The system displays the System Management screen.

3. Click the **Updates** tab, and then select any one from the following options based on the upgrade scenario:
   - Upgrade from local file.
   - Upgrade from uploaded file.

4. Click the **Key Bundles** tab, and then upload the key bundle file.
5. Click the **Updates** tab, and then click **Upgrade**.

   The system displays the Upgrade Devices window.
6. Select the check box before the Device Name column.

   The system determines and selects the primary Avaya SBCE which needs to be upgraded first.
7. Click **Next**.

   The system displays logs and a message box indicating that the Device is upgraded.
8. Click **Finish**.

   The system displays the Upgrade Devices window.
9. Select the check box before the Device Name column.

   The system now selects the other Avaya SBCE in the HA pair.
10. Click **Next**.

    The system displays logs and a message box indicating that the Device is upgraded.
11. Click **Finish**.

    Note:

    After the EMS server has been upgraded, the system displays the following message for Avaya SBCE boxes and HA pairs on the **Updates** tab:

    ```
    One or more devices are in an upgrade required state. If you
    would like to upgrade these devices now, please click the
    Upgrade button below. You may also choose to rollback your EMS
    at this point.
    ```

    HA system pairs and all other Avaya SBCE systems must be upgraded before this message is resolved.

Upgrading single Avaya SBCE servers

Before you begin

Ensure that the EMS servers are upgraded before upgrading Avaya SBCE servers.

About this task

This procedure upgrades Avaya SBCE servers that are not in an HA pair. When more than one Avaya SBCE server is available, repeat this step for each Avaya SBCE server.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the navigation pane, click **System Management**.

   The system displays the System Management screen.

3. Click the **Updates** tab, and then select any one from the following options based on the upgrade scenario:

   - Upgrade from local file.
   - Upgrade from uploaded file.

4. Click the **Key Bundles** tab, and then upload the key bundle file.

5. Click the **Updates** tab, and then click **Upgrade**.

   The system displays the Upgrade Devices window.

6. Select the check box next to the devices that you want to upgrade.

   The devices can be upgraded one at a time or as a group. If you select more than one device, the devices are put in a queue and upgraded one at a time.

7. Click **Next**.

   The system displays logs and a message box indicating that the Device is upgraded.

8. Click **Finish**.

   Note:

   After the EMS software has been upgraded, the following message is displayed for Avaya SBCE boxes and HA pairs on the Updates tab:

   ```
   One or more devices are in an upgrade required state. If you
   would like to upgrade these devices now, please click the
   Upgrade button below.  You may also choose to rollback your EMS
   at this point.
   ```

   HA system pairs and all other Avaya SBCE servers must be upgraded before this message is resolved.

Next steps

To verify whether the deployment was successful:

- Log on to EMS and on the System Management page, verify the current Avaya SBCE and EMS versions.
- From the command line, use the **`ipcs-version`** command to check the current version.

Installing pre-upgrade patch for Avaya SBCE upgrade from Release 7.2 to Release 7.2.1 using CLI

About this task

Install the pre-upgrade patch file on all hardware devices of Avaya SBCE that are on Release 7.2 and then upgrade those devices to Release 7.2.1. Follow this procedure to install the pre-upgrade patch. This patch must be installed on both Avaya SBCE and EMS.

Before you begin

Ensure that `/home/ipcs` folder has at least 1 GB memory to copy the pre-upgrade patch file. If available memory is less than 1 GB, then clear files from `/home/ipcs` folder after logging in as root user.

Note:

- If you forget to install the pre-upgrade patch, the upgrade process from 7.2 to 7.2.1 will terminate with pre-check failure.
- For information about the upgrade sequence and the required pre-installation and post-installation patches, see the latest *Avaya Session Border Controller for Enterprise Release Notes* on the Avaya support site at http://support.avaya.com.

Procedure

1. Log in to Avaya SBCE and EMS using `ipcs` login and password.
2. Upload the pre-upgrade patch file on Avaya SBCE using **`winscp`** command and type the port number `222`.
3. At the command prompt, type **`su-root`** to switch the current user to root user.
4. At the command prompt, type **`md5sum pre7.2FP1_upgrade.tar.gz`** to verify md5sum of the patch file.
5. Create `/usr/local/ipcs/patch` directory to upgrade.
6. At the command prompt, type **`mv /home/ipcs/pre7.2FP1_upgrade.tar.gz /usr/local/ipcs/patch`** to move the patch file to `/usr/local/ipcs/patch` directory.
7. At the command prompt, type **`cd /usr/local/ipcs/patch`** to navigate to `/usr/local/ipcs/patch` directory.
8. At the command prompt, type **`tar -zxvf pre7.2FP1_upgrade.tar.gz -C /usr/local/ipcs/patch`** to extract the patch file.

   The system extracts the patch file.
9. At the command prompt, type **`sh install.sh`** to install and run the patch file.
10. Reboot Avaya SBCE.

Next steps

- After successful completion of patch installation, go to command prompt and type **rm -rf /usr/local/ipcs/patch/*** to remove all the contents of pre-upgrade patch from /usr/local/ipcs/patch/ directory.
- From the command line, use the **ipcs-version** command to check the current version to verify whether the upgrade was successful or not.
- If pre-upgrade patch installation is successful, upgrade EMS and Avaya SBCE to Release 7.2.1.

Upgrading Avaya SBCE from Release 7.1.x to Release 7.2 by using CLI

Procedure

1. Log in to the Avaya SBCE CLI with administrative privileges.
2. Copy the tar file sbce-7.2.x.0-xx-xxxxx-<md5sum>.tar.gz to the Avaya SBCE instance that you want to upgrade.
3. Using root permissions, move the upgrade tar file from the ipcs user home directory to /archive/urpackages directory.
4. Ensure that the md5sum of the upgrade tar file matches the checksum given in the name of the file.

   You can use the **md5sum** command to verify whether the md5sum and the checksum match.
5. At the command prompt, type mkdir /usr/local/ipcs/*temp*, where *temp* is the name of the temporary directory.

   The system creates a temporary directory in the archive directory.
6. At the command prompt, type the following command:

   ```
   cd /usr/local/ipcs/temp
   ```
7. At the command prompt, type the following command:

   ```
   tar -zxvf /archive/urpackages/sbce-7.2.x.0-xx-xxxx-<md5sum>.tar.gz
   ```

   The system extracts the upgrade tar file in the temp directory.
8. At the command prompt, type the following command:

   ```
   chmod +x ursbce.py
   ```
9. At the command prompt, type the following command:

   ```
   ./ursbce.py -U --daemonize
   ```

   This step reboots the system.

⚠ **Warning:**

Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if the user is disconnected because of inactivity.

10. Wait for the system to reboot.
11. At the command prompt, type the following command and verify the version of the system:

    ```
    cat /etc/sbce-version
    ```

    The file `/archive/log/icu/upgrade.log` contains upgrade related logs.
12. At the command prompt, type `grep UPGRADE_STATE /usr/local/ipcs/etc/sysinfo` to check the upgrade status.

    The system displays the following: `UPGRADE_STATE=UPGRADE_COMPLETED` for a successful upgrade and `UPGRADE_STATE=UPGRADE_FAILED` for a failed upgrade process.

Upgrading Avaya SBCE to Release 7.2.2 using CLI

About this task

Use the following procedure to upgrade Avaya SBCE from following releases to Release 7.2.2:

- Release 6.3.6
- Release 6.3.7
- Release 7.0.2
- Release 7.2
- Release 7.2.1

Procedure

1. Log in to the Avaya SBCE CLI with administrative privileges.
2. Copy the tar file (`sbce-7.2.2.0-xx-xxxxx-<md5sum>.tar.gz`) to the Avaya SBCE instance that you want to upgrade.
3. Using root permissions, move the upgrade tar file from the ipcs user home directory to `/archive/urpackages` directory.
4. Ensure that the md5sum of the upgrade tar file matches the checksum given in the name of the file.

    You can use the **`md5sum`** command to verify whether the md5sum and the checksum match.
5. At the command prompt, type the following command:

    ```
    mkdir /usr/local/ipcs/temp
    ```

    Where, *temp* is the name of the temporary directory.

The system creates a temporary directory in the archive directory.

6. At the command prompt, type the following command:

   ```
   cd /usr/local/ipcs/temp
   ```

7. At the command prompt, type the following command:

   ```
   tar -zxvf /archive/urpackages/sbce-7.2.2.0-xx-xxxx-<md5sum>.tar.gz
   ```

   The system extracts the upgrade tar file in the `temp` directory.

8. At the command prompt, type the following command:

   ```
   chmod +x ursbce.py
   ```

9. At the command prompt, type the following command:

   ```
   ./ursbce.py -U --daemonize
   ```

   This step reboots the system.

   ⚠ **Warning:**

   Use the --daemonize option while using CLI-based upgrades over SSH. Without the --daemonize option, the upgrade fails if the user is disconnected because of inactivity.

10. Wait for the system to reboot.

11. At the command prompt, type the following command and verify the version of the system:

    ```
    cat /etc/sbce-version
    ```

    The file `/archive/log/icu/upgrade.log` contains upgrade related logs.

12. At the command prompt, type the following command to check the upgrade status:

    ```
    grep UPGRADE_STATE /usr/local/ipcs/etc/sysinfo
    ```

    The system displays `UPGRADE_STATE=UPGRADE_COMPLETED` for the successful upgrade and `UPGRADE_STATE=UPGRADE_FAILED` for a failed upgrade process.

Rolling back using web interface

About this task

Use this procedure to rollback from Release 7.2.x to Release 7.1.x and Release 7.2.2 to Release 7.2.1 and Release 7.2.0.

❗ **Important:**

If you roll back from Avaya SBCE Release 7.2.x to Release 7.1, then you cannot upgrade to Release 7.1 service pack 1. Avaya SBCE does not support this upgrade path.

Procedure

1. Log in to the EMS web interface with administrator credentials.

2. In the navigation pane, click **System Management**.

   The system displays the System Management screen.
3. Select the **Updates** tab.

   The system displays the current EMS version and the available upgrade and rollback options.
4. Click **Rollback**.
5. Select the Avaya SBCE device you want to rollback in an HA pair.

   The system displays the Rollback Status screen during rollback, and displays the **Return to EMS** tab after the rollback is complete.
6. Click the **Return to EMS** tab to log back in to the EMS web interface.

Roll back sequence in a multiserver deployment

Find the node IDs from `/usr/local/ipcs/etc/sysinfo`.

No.	Tasks	References	Notes	✔
1	Roll back Avaya SBCE with a lower node ID.	See Rolling back through CLI on page 73	-	
2	Roll back Avaya SBCE with a higher node ID.	See Rolling back through CLI on page 73	-	
3	Roll back the primary EMS server with a lower node ID.	See Rolling back through CLI on page 73	-	
4	Roll back the secondary EMS server with a higher node ID.	See Rolling back through CLI on page 73	-	

Rolling back through CLI

Before you begin

Download the Avaya SBCE tar file for the release to which you want to roll back.

About this task

You can roll back to the last Avaya SBCE release from CLI.

Procedure

1. Log on to Avaya SBCE CLI as a super user.
2. Create a temporary directory in `/usr/local/ipcs/`.

For example, type `mkdir /usr/local/ipcs/temp`, where *temp* is the name of the temporary directory.

3. Untar the package to which you want to roll back, in the temporary directory.
4. Run the following pre-rollback script:

   ```
   /usr/local/ipcs/icu/scripts/pre_rollback.sh
   ```

5. To begin rollback, type the following command:

   ```
   ./ursbce.py --rollback --daemonize
   ```

   After the rollback process is complete, you can check the rollback logs stored at `/archive/log/icu`.

Chapter 9: Licensing requirements

Avaya SBCE uses WebLM for licensing requirements. You can install the Avaya SBCE license file on Element Management System (EMS) using the System Management page. Ensure that the license file of the WebLM server displays the product code Session Border Controller E AE. Before you configure the license file, you can view the **License State**, **Grace Period State**, and **Grace Period Expiration Date** fields on the Dashboard page. To install a license file on a newly installed or upgraded EMS, you have a 30-day grace period from the day of installation or upgrade.

The license file contains the following information:

- Product name
- Supported software version
- Expiration date
- Host ID

  The primary host ID of WebLM is used for creating the license file.
- Licensed features
- Licensed capacity

All hardware Avaya SBCE devices can use a local WebLM server for licenses. However, for mixed deployment environments with EMS on VMware and Avaya SBCE on hardware, use a WebLM server installed on VMware or System Manager WebLM.

Avaya SBCE supports pooled licensing. As opposed to static license allocation, Avaya SBCE dynamically reserves and unreserves pooled licenses when needed. For example, customers with multiple Avaya SBCE devices can use a pool of licenses dynamically across the devices as required.

Avaya SBCE license features

To use a feature, you must ensure that the license file that you upload to WebLM has the appropriate licenses for the feature. You cannot configure or use a feature if the correct license for that feature is not present in the license file.

License feature	Description
VALUE_SBCE_STD_SESSION_1	Specifies the number of standard session licenses.
VALUE_SBCE_STD_HA_SESSION_1	Specifies the number of standard service HA session licenses.
VALUE_SBCE_ADV_SESSION_1	Specifies the number of session licenses for remote worker, media recording, and encryption. **Note:** You must buy and deploy a standard session license with every advanced license feature.
VALUE_SBCE_ADV_HA_SESSION_1	Specifies the number of advanced service HA session licenses.
VALUE_SBCE_VIDEO_CONF_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing session licenses.
VALUE_SBCE_VIDEO_CONF_HA_SVC_SESSION_1	Specifies the number of Avaya Scopia® video conferencing HA session licenses.
VALUE_SBCE_CES_SVC_SESSION_1	Specifies the number of Client Enablement Services session licenses.
VALUE_SBCE_CES_HA_SVC_SESSION_1	Specifies the number of Client Enablement Services HA session licenses.
VALUE_SBCE_TRANS_SESSION_1	Specifies the number of transcoding session licenses.
VALUE_SBCE_TRANS_HA_SESSION_1	Specifies the number of transcoding HA session licenses.
VALUE_SBCE_ELEMENTS_MANAGED_1	Specifies the maximum number of Avaya SBCE elements managed.
VALUE_SBCE_VIRTUALIZATION_1	Specifies that download of VMware OVA files is permitted for Avaya SBCE.
VALUE_SBCE_ENCRYPTION_1	Specifies the Avaya SBCE encryption, and is required for advanced licenses.
FEAT_SBCE_HIGHAVAILABILITY_CONFIG_1	Specifies the configuration of HA for the setup.
FEAT_SBCE_DYNAMIC_LICENSING_1	Specifies that dynamic or pooled licensing is permitted for Avaya SBCE.
VALUE_SBCE_RUSSIAN_ENCRYPTION_1	Specifies encryption Avaya SBCE encryption only for signaling.

Configuring WebLM server IP address on EMS

Before you begin

Install the Avaya SBCE license file on System Manager WebLM, local WebLM, or standalone WebLM server. For more information about installing license files, see *Administering Avaya Aura® System Manager*.

Procedure

1. Log on to the EMS web interface with administrator credentials.
2. In the left navigation page, click **System Management**.
3. On the System Management page, click the **Licensing** tab.
4. Perform one of the following tasks:
   - For a System Manager WebLM server or standalone server, in the **WebLM Server URL** field, type the URL of the WebLM server and click **Save**.

     The url format of the System Manager WebLM server is `https://<SMGR_server_IP>:52233/WebLM/LicenseServer` and the standalone WebLM server is `https://<WEBLM_server_IP>:52233/WebLM/LicenseServer`.
   - For a local WebLM server, select the **Use local WebLM server** check box and click **Save**.
5. On the Dashboard screen, check the **License State** field.

   If the configuration is successful, the **License State** field shows `OK`.
6. Click the **Devices** tab.
7. Locate the Avaya SBCE device you configured, and click **Edit**.

   The system displays the Edit Device dialog box.
8. In the **Standard Sessions**, **Advanced Sessions**, and **Scopia Video Sessions** fields, type the number of licensed sessions depending on the license you purchased.
9. Click **Finish**.

Chapter 10: Resources

Documentation

This document covers the generic procedures for Avaya SBCE upgrade. For application-specific upgrade procedures, see the product-specific document on the Avaya support site at http://support.avaya.com.

Document number	Title	Use this document to:	Audience
Understanding			
	Avaya Session Border Controller for Enterprise Overview and Specification	Describes high-level functional and technical description of characteristics and capabilities of Avaya SBCE.	Sales Engineers Solution Architects Implementation Engineers
Installing and configuring			
	Deploying Avaya Session Border Controller for Enterprise	Describes hardware installation and preliminary configuration procedures for installing Avaya SBCE	Solution Architects Implementation Engineers
	Installing Dell R620	Describes hardware installation and preliminary configuration.	Solution Architects Implementation Engineers
	Installing HP DL360 G7	Describes hardware installation and preliminary configuration.	Solution Architects Implementation Engineers
	Installing the Dell™ PowerEdge™ R630 Server	Describes hardware installation and preliminary configuration.	Solution Architects Implementation Engineers
	Installing the HP ProLiant DL360 G9 Server	Describes hardware installation and preliminary configuration.	Solution Architects

Table continues…

Document number	Title	Use this document to:	Audience
			Implementation Engineers
	Deploying Avaya Session Border Controller for Enterprise in Virtualized Environment	Describes hardware installation and preliminary configuration procedures for installing Avaya SBCE in a virtualized environment.	Solution Architects Implementation Engineers
Administering			
	Administering Avaya Session Border Controller for Enterprise	Describes configuration and administration procedures of for Avaya SBCE.	Administrators Implementation Engineers
	Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	Describes troubleshooting and maintenance procedures for Avaya SBCE.	Sales Engineers Administrators Implementation Engineers
	Administering Avaya Aura® System Manager	Describes how to perform administration tasks for System Manager and Avaya Aura® applications that System Manager supports.	System administrators

Related links

Finding documents on the Avaya Support website on page 79

Finding documents on the Avaya Support website

Procedure

1. Navigate to http://support.avaya.com/.
2. At the top of the screen, type your username and password and click **Login**.
3. Click **Support by Product** > **Documents**.
4. In **Enter your Product Here**, type the product name and then select the product from the list.
5. In **Choose Release**, select an appropriate release number.
6. In the **Content Type** filter, click a document type, or click **Select All** to see a list of all available documents.

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

Related links

Documentation on page 78

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
5U00090E	Knowledge Access: Avaya Session Border Controller
5U00160E	Knowledge Collection Access: Avaya Unified Communications Core Support

Viewing Avaya Mentor videos

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

About this task

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

Procedure

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

Note:

Videos are not available for all products.

Support

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

Related links

Using the Avaya InSite Knowledge Base on page 81

Using the Avaya InSite Knowledge Base

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

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

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

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

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

   The system displays the Avaya Support page.
3. Click **Support by Product** > **Product Specific Support**.
4. In **Enter Product Name**, enter the product, and press `Enter`.
5. Select the product from the list, and select a release.
6. Click the **Technical Solutions** tab to see articles.
7. Select relevant articles.

Related links

Support on page 81

Index