Avaya Session Border Controller for Enterprise 7.1 Release Notes

Release 7.1
Issue 1
June 2016

Notice

While reasonable efforts were made to ensure that the information in this document was complete and accurate at the time of printing, Avaya Inc. can assume no liability for any errors. Changes and corrections to the information in this document might be incorporated in future releases.

Documentation disclaimer

Avaya Inc. is not responsible for any modifications, additions, or deletions to the original published version of this documentation unless such modifications, additions, or deletions were performed by Avaya. Customer and/or End User agree 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 the Customer or End User.

Link disclaimer

Avaya Inc. is not responsible for the contents or reliability of any linked Web sites referenced elsewhere within this documentation, and Avaya does not necessarily endorse the products, services, or information described or offered within them. We cannot guarantee that these links will work all the time and we have no control over the availability of the linked pages.

Warranty

Avaya Inc. provides a limited warranty on this product. 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 through the Avaya Support Web site: http://support.avaya.com

License

USE OR INSTALLATION OF THE PRODUCT INDICATES THE END USER'S ACCEPTANCE OF THE TERMS SET FORTH HEREIN AND THE GENERAL LICENSE TERMS AVAILABLE ON THE AVAYA WEB SITE http://support.avaya.com/LicenseInfo/ ("GENERAL LICENSE TERMS"). IF YOU DO NOT WISH TO BE BOUND BY THESE TERMS, YOU MUST RETURN THE PRODUCT(S) TO THE POINT OF PURCHASE WITHIN TEN (10) DAYS OF DELIVERY FOR A REFUND OR CREDIT.

Avaya grants End User a license within the scope of the license types described below. 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 End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware Products, originally sold by Avaya and ultimately utilized by End User.

License type(s)

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. 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 Product that permits one user to interface with the Software. Units may be linked to a specific, identified Server.

Copyright

Except where expressly stated otherwise, the Product is protected by copyright and other laws respecting proprietary rights. Unauthorized reproduction, transfer, and or use can be a criminal, as well as a civil, offense under the applicable law.

Third-party components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information identifying Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site:

http://support.avaya.com/ThirdPartyLicense/

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 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 Web site:
http://support.avaya.com

Trademarks

Avaya and the Avaya logo are either registered trademarks or trademarks of Avaya Inc. in the United States of America and/or other jurisdictions. All other trademarks are the property of their respective owners.

Downloading documents
For the most current versions of documentation, see the Avaya Support Web site:
http://support.avaya.com

Avaya support

Avaya provides a telephone number for you to use to report problems or to ask questions about your product. The support telephone number is 1-800-242-2121 in the United States. For additional support telephone numbers, see the Avaya Support Web site: http://support.avaya.com

Table of Contents

Overview

This document provides information about the new features/enhancements in ASBCE Release 7.1, and the known issues for this release.

Documentation

The latest documentation for 7.1 is available on support.avaya.com

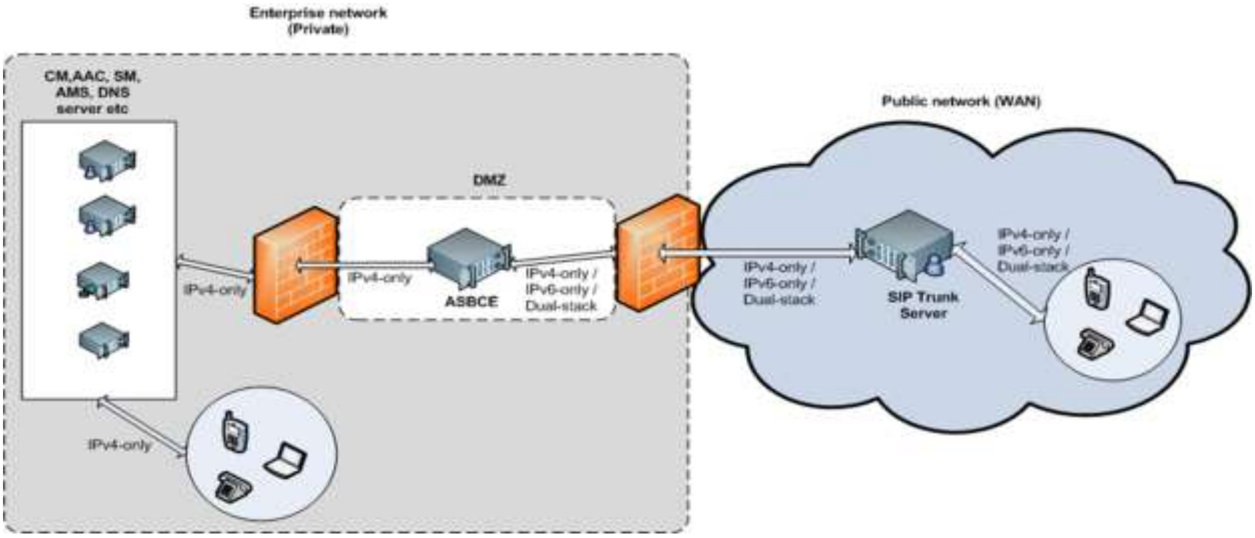
No.	Title	Link
1.	Avaya Session Border Controller for Enterprise Overview and Specification	http://support.avaya.com/css/P8/documents/101026875
2.	Deploying Avaya Session Border Controller for Enterprise	http://support.avaya.com/css/P8/documents/101026879
3.	Deploying Avaya Session Border Controller in Virtualized Environment	http://support.avaya.com/css/P8/documents/101026877
4.	Upgrading Avaya Session Border Controller for Enterprise	http://support.avaya.com/css/P8/documents/101026883
5.	Administering Avaya Session Border Controller for Enterprise	http://support.avaya.com/css/P8/documents/101001024
6.	Troubleshooting and Maintaining Avaya Session Border Controller for Enterprise	http://support.avaya.com/css/P8/documents/101026881
7.	Avaya SBCE 7.0 Security Configuration and Best Practices Guide	https://downloads.avaya.com/css/P8/documents/101014066

New features and enhancements

Following new features and enhancements are added in this release.

IPv6 Support

SBCE supports IPv6 addressing scheme towards SIP trunk servers. SBCE supports trunk deployments where enterprise (private) side is IPv4-only network and trunk (public) side is either IPv6-only network, dual stack network, IPv4-only network or mixed-mode. In this release, SBCE does not support IPv6 towards enterprise and Remote worker deployments. The following figure illustrates a typical network diagram of a trunk deployment wherein SIP Trunk connection can be IPv6, whereas enterprise is on IPv4



Management Interface IPv6 has to be in Dual-Stack Mode only. We support both IPv6 unique-local unicast address and IPv6 global unicast address configuration, besides support for convention IPv4 support on Management interface. Communication towards DNS servers, NTP server, syslog server etc. is supported over IPv6. For call processing, following is supported starting with ASBCE7.1

1. SIPv6 (SIP over IPv6 – RFC 6157)
2. SDP ANAT (Alternative Network Address Types) for SDP negotiation (RFC 4091, RFC 4092)
   ANAT semantics are defined to address scenarios that involve different network address types (e.g. different IP versions)
   ANAT semantics allow for the expression of alternative network addresses (e.g., different IP versions) for a particular media stream.
3. Video calls
4. SRTP over IPv6
5. DNS over IPv6
6. NTP over IPv6
7. Syslog over IPv6
8. HA solution

Transcoding

ASBCE 7.1 Release supports transcoding solution for audio sessions. Transcoding is the process of translating a media stream encoded using one codec into a media stream encoded using another codec. For example, translating a media stream encoded as Pulse Code Modulation u-law (PCMU) into one encoded as ITU-T G.726-32. Transcoding is supported for calls traversing the SBCE for SIP

Trunking.
Following is the list of codecs supported for Transcoding

1. OPUS
   12kbps Narrowband
   16kbps Narrowband
   18kbps Wideband
2. G.722
3. G.711ulaw
4. G.711alaw
5. G.726
6. G.729AB

Call Preservation

Call Preservation feature enables calls to be preserved across core Session Manager Failures. Not only is the voice path of a connection preserved, but agents/users can also manipulate calls with in-call signaling after a Session Manager (SM) failure. Call preservation is currently available only for SIP Routing Element (SRE) flows. Instead of the IP addresses, SM inserts Failover Group Domain Name (FGDN) in the pertinent SIP headers of the requests.

ASBCE communicates with SM using the domain names instead of IP addresses. SM FGDN resolves to an ordered set of SM instances in the order of the preferred SM instance. Upon detecting the failure of the SM instance, ASBCE shift traffic to the next SM instance. With support for mid-transaction and mid-dialog requests, mid-dialog feature invocation continues to work

Media Un-anchor/Media Release

Media release or direct media is the method for signaling the direct talk path between end points involved in the call. It is desirable to release media when possible for enhanced scalability and reduce delay. ASBCE 7.1 supports media release for non-hairpin calls. ASBCE allow direct media for all non-hairpin calls that include trunk to enterprise, enterprise to trunk, remote to enterprise and enterprise to remote. ASBCE allow direct media for any call types –audio, video and multimedia calls.

SIPREC Enhancements

Selective Recording is a feature in which recording is not invoked right from start of the call. Recording and media streaming starts when Recorder indicates to SBC to start streaming. This does optimization and performance enhancement, conserves bandwidth and this is applicable for both trunking and remote worker recording. High Availability support for selective recording is supported in this release for all media policies and rules applicable for Selective recording like codec prioritization, transcoding and SRTP/RTP

Continuous Recording Secondary Recorder will join seamlessly to ASBCE in case of load sharing or failover of primary recorder. All media rules and policies are applicable. ASBCE will start streaming media to the new recorder and this is supported after failover of ASBCE. The trigger to switch from primary recorder to secondary recorder is proprietary to recorders. No configuration required on ASBCE for the same.

Call Termination on No Recording is a feature by which call is not processed until recording does not take place for the call. Some business critical functionality may be there where recording is mandatory and in such cases, if recording does not happen call is terminated. This is applicable only for Trunk Calls for CC/UC cases from a customer and not for internal/RW workers. The Recorder may send any 4xx,5xx,6xx messages and main call will be terminated by sending CANCEL or BYE or 480 depending on the state

SIPREC for Remote Worker is a feature which enables recording of Remote Worker calls through SIPREC. High Availability supported for Remote Worker SIPREC. In case of Remote Worker – Remote Worker, if both legs are through same ASBCE it records only for the first leg. In case of Trunk – RW call, if recorder flow is configured at both legs ASBCE will send recording streams for both legs and ACR will record the stream for one leg of the call. Additional recorder flow should be made for the Remote Worker leg of call. If Aura setup is on 7.0.1, patch is required on CM for Remote worker to internal call to be recorded via SIPREC.

ASBCE 7.1 supports SIPREC with transcoding when main call is transcoded. Need to configure either transcoded codec as G729AB and/or G711 or have codec prioritization set as G729AB and/or G711MU. Assumption is that one side is transcoded and the other side needs to be on G729AB or G711 or vice-versa. Media streamed towards Recorder is either on G729AB or G711. SBCE DOES NOT support transcoding towards Recorder in this release and we need to ensure G729AB/G711 is configured on both sides of the Media rules although transcoding may be taking place with different codecs.

ASBCE 7.1 supports SIPREC with IPV6 i.e. support for SIPREC scenarios is available when main call converted from IPV6 to IPV4. Support of SIPREC when main call supports SDP-ANAT (RFC 4092). IPV6 is not supported towards Recorder and SIP signaling/RTP media towards Recorder is always IPV4, likewise ANAT is not supported towards Recorder. ANAT in media policy should be disabled for Recorder flow.

ASBCE 7.1 supports enhancement for SIPREC Recording Tone feature. Recording Tone is played towards the Trunk User and following codecs are supported for playing of Recording Tone. To configure recording tone, enable Play Recording Tone option

- G711MU, G711A, G729, G723, G726-32k, G722

The tones (preferably short beep tone) are placed in the path /usr/local/ipcs/prompt/codec_name/CALL_CONNECTING. Codec_name can be any one or all of the above codecs as per codec negotiated on the customer's network. Our recommendation is to put support for tones for all the codecs. Transcoding should include these or a subset of the codecs listed. It is the responsibility of the administrator to put a proper encoded "beep tone" in the path specific for the codec

Database Changes and EMS Active-Active

Starting with ASBCE7.1, database has been changed from SolidDB to Postgres and Configuration data for each SBCE has been moved from EMS to SBC .If the SBCEs are in HA state database replication between pair will now take place between the 2 SBCEs directly and not via EMS. EMS database will not house only global configuration and is very lightweight. EMS GUI talks directly to SBCEs via tcp port 5432. If global data is updated while one of the SBCEs is in down state, sync button will be enabled. This button needs to be clicked once SBCE is back online so that changes are pushed over to the SBCEs.

Starting with ASBCE7.1, if we have primary and secondary EMS, both EMS will be now in active state and we will be able to administer the SBCEs from any of the EMS server. There is no need to run switchover command for secondary EMS to be active in case of failure on primary EMS. GUI can be simultaneously be used from both EMS servers.

Also, starting with ASBCE7.1 OpenVPN has been removed from the EMS server and all the changes configured on EMS are pushed to SBCEs via one of the below

a. Secure DB connectivity
b. https
c. SSH

ENUM Routing

ENUM is a protocol that defines a method to convert a regular telephone number (e.g. +91 7631 987 153) into a format that can be used on the Internet within the
Domain Name System (DNS) to look up Internet addressing information such as Uniform Resource Identifiers. The problem ENUM tries to solve is the mapping between a standard telephone number and a SIP URI. Once ENUM is widely deployed, the idea is that you should be able to dial any "phone number," and have your SIP infrastructure look it up using DNS.

A simple call flow depicting the ENUM feature is represented in the diagram,

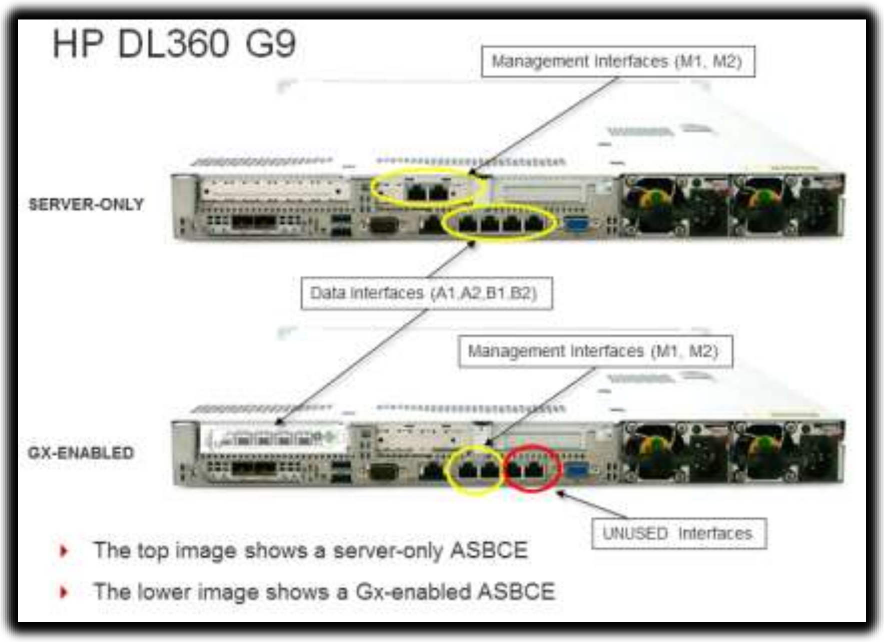
1. Let’s say user dials E.164 number (+44-20-7946-0148)
2. SBC will convert the E.164 number as per below algorithm
3. Remove all characters with the exception of the digits
4. Reverse the order of the digits by placing dots (‘.’) between each digit.
5. Append the configured ENUM suffix to the end and interpret as a domain name.
   Example: 8.4.1.0.6.4.9.7.0.2.4.4.e164.arpa (with “e164.arpa” being the suffix).
6. The result from DNS would be SIP URI which SBC uses to update the request URI in sip message.
7. SBC proceeds with the regular routing logic and route the SIP message via the internet

Tilera - Gx-Enabled Hardware Support for Scalability

For customers looking for high scalability, ASBCE7.1 now provides an option to install Hi-Capacity servers which house a Gx-Enabled PCIE Card. The purpose of this feature is to increase ASBCE capacity by adding more CPU cores to the system, in the form of a PCIe card. The PCIe card used in the ASBCE adds 36 new CPUs to the system and capacity increase is realized by offloading the ASBCE media plane (primarily RTP/SRTP) processing from the host to the card.

The Gx adapter is supported ONLY in the following servers:
HP DL360 G9
Dell R630

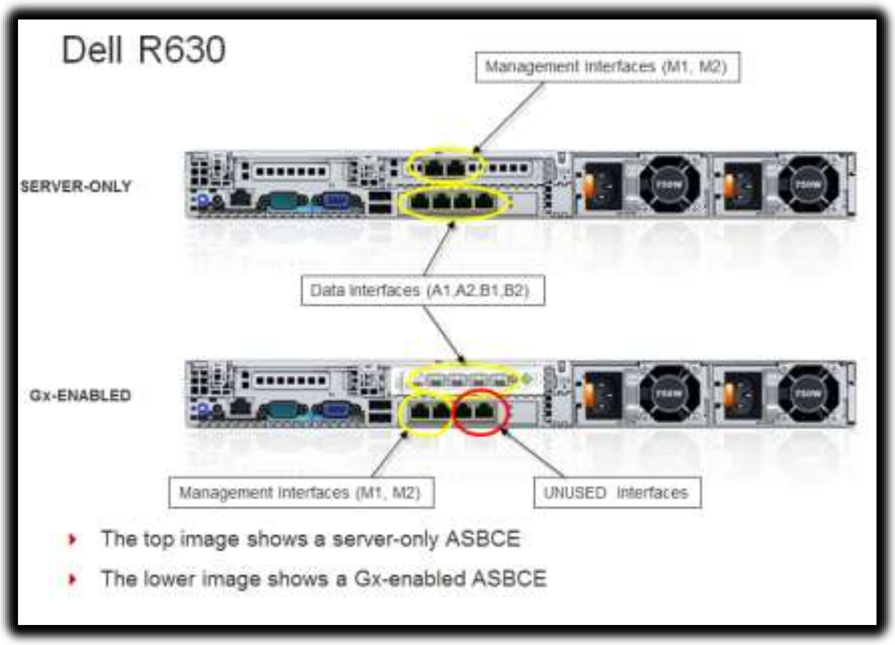
There are differences in physical network connectivity between a server-only ASBCE and a Gx-enabled ASBCE. This is because the Gx adapter, when installed, displaces an existing network card in the server



HP DL360 G9

Management Interfaces (M1, M2)
SERVER-ONLY
Data Interfaces (A1,A2,B1,B2)
Management Interfaces (M1, M2)
GX-ENABLED
UNUSED Interfaces

- The top image shows a server-only ASBCE
- The lower image shows a Gx-enabled ASBCE



Dell R630

Management Interfaces (M1, M2)
SERVER-ONLY
Data Interfaces (A1,A2,B1,B2)
GX-ENABLED
Management Interfaces (M1, M2)
UNUSED Interfaces

- The top image shows a server-only ASBCE
- The lower image shows a Gx-enabled ASBCE

Upgrade Path

Supported Upgrade path is as below:

ASBCE7.0 → ASBCE7.1

ASBCE7.0 SP1 → ASBCE7.1

ASBCE6.3 SP6 → ASBCE 7.1

7.1 build can be obtained from below Download location:

Upgrade file: ftp://customer-P:3e4rFGBV@ftp.avaya.com/incoming/guests/pndoxey/customer-P/Software/7.1-Beta/7.1.0.0-04-11122/sbce-7.1.0.0-04-11122-45a057678bff54481a5eb9ffb24707db.tar.gz
OVA file: https://Avaya.sharefile.com/d/sf0468efffa242218

- If you have ASBCE 7.0 build 6602 **OR** 6.3 SP6 build installed on the server, please ensure that GUI patch is applied on EMS for upgrade through GUI to work successfully. Procedure to apply the patch is as below:
  a. Login to EMS and become a super user
  b. Untar the patch: tar -xvf to /home/ipcs on EMS.
  c. cd upgrade-patch/
  d. sh upgrade-regex.sh

  Note: above workaround is not required if version is ASBCE 7.0 SP1. GUI patches is a pre-requisite for GUI upgrade will be made available on PLDS for both 6.3 SP6 and 7.0 GA build. Following are the pre-upgrade patch

  6.3.6-upgrade_regex_patch.tar 7.0-upgrade-regex.tar

- Upgrade from 6.3.6 or 7.0 SP1 requires pre-upgrade patch to be installed before initiating upgrade. This is to ensure that roll-back is supported post upgrade to 7.1 Release. Please following the procedure described below:

  1. Copy the 7.1 upgrade package to /archive/urpackages/

  2. Copy the patch file named “preupgrade-patch.tar.gz” to /home/ipcs

  3. As a root user, untar the patch file
     tar –xvf preupgrade-patch.tar.gz

  4. Run modify_upgrade_pkg script
     ./modify_upgrade_pkg.sh

  5. Wait for 4-5 minutes for script to work. Once patch script has been executed successfully, navigate to EMS GUI and start upgrade.
     In case of HA setup, upgrade the SBCs from EMS GUI.

- If there is a need to Roll-Back HA setup or Multi-SBCE setup from 7.1 to previous release, user can roll back EMS to previous version from GUI, however SBCE’s will need to be rolled back sequentially using CLI procedure described as below:

Rollback procedure from CLI is as below

1. Make sure that roll-back package (upgrade package of previous version) is present under /archive/urpackages/

2. As a root user delete the files /archive/temp/ directory

   ```
   rm –rf /archive/temp/
   ```

3. Create /archive/temp/ directory

   ```
   mkdir /archive/temp/
   ```

4. Untar the rollback package to /archive/temp/

   ```
   tar -xvzf /archive/urpackages/<NAME OF ROLLBACK
   PACKAGE>  -C /archive/temp/
   ```

5. Change the permission of ursbce file to make it executable

   ```
   cd /archive/temp

   chmod +x ./ursbce.py
   ```

6. Start the rollback with ursbce.py

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

Converting the Setup to IPv6 Dual stack Mode and Vice-Versa

Please navigate to "cd /usr/local/ipcs/icu/pylib" then run below command to change stack mode.

./SBCEConfigurator.py change-ip-stack-mode –I DUAL_STACK (or IPV4)

List of known issues and workarounds

- While EMS is getting upgraded, if SBCE has gone through reboot for some reason, then upgrade of SBCE through GUI will not work. Workaround for this is to upgrade the SBCE via CLI method as described in upgrade document for ASBCE

- If Data interface of ASBCE needs to be configured for IPv6, it is mandatory that management interface of SBCE has to be in configured in Dual Stack mode instead of IPv4 only mode.

- If Spirit Agent logs cause the disk space to be filled up, please follow workaround as below:

  1. Stop spiritAgent. Ensure that it is properly stopped using ps and grep for java. If OAMP is trying to start it again, stop application.
     Commad : service spiritAgent stop
  2. Delete or rename DB folder.
     Command : mv /opt/spirit/DB/agentDB /opt/spirit/DB/agentDB_old

3. Start spiritAgent (or restart application)
   Command: service spiritAgent start.

- Before upgrade make sure that /tmp directory is empty. If upgrade fails due to space issue empty the /tmp directory and run upgrade again.

- After rollback of EMS through GUI, SBCEs will be shown as having same version as that of EMS without being rolled-back. Roll-back of SBCs will need to be done through CLI with procedure described in Upgrade Path section.

- If SBCE has rebooted for some reason during or post upgrade of EMS to 7.1, upgrade of SBCEs will have to be done through CLI for each of the SBCEs. Please refer upgrade document for procedure to upgrade through CLI.

- GUI does not recover automatically after Upgrade of EMS. Please re-enter the URL of EMS in the browser to access the EMS GUI post upgrade

- Device Swap option for swapping SBC fails. Please perform workaround as below before attempting Device Swap

  1. Make sure that EMS's and SBCs are using same DB password. If not, please change the same using script SBCEConfigurator.py change-db-password.

  2. Apply the patch named "sbce-add.patch.tar.gz" on EMS and working SBCs, Restart the boxes.

  Run as root and copy the tar at /home/ipcs

  ```
  tar -xvzf sbce-add.patch.tar.gz

  cd 11127.patch

  ./install.sh
  ```

  Restart the boxes.

  3. Deploy new SBCE and add this SBCE through EMS GUI. Wait for this SBCE to get into registered state.

  4. Press on swap on newly added SBCE and swap it with the non-working SBCE

  5. Login as a root user on newly added SBCE and run command clipcs. Then run command "certsync" and "certinstall" operations to make sure certificates have been synced to newly added SBCE

  6. Reboot the new SBC

- Adding separate SBCE to existing setup may have problem for syncing global data with EMS. Please use workaround as below.

  Upload the patch named "sbce-add.patch.tar.gz" on EMS and on all SBCs and follow the procedure as below:

Run as root and copy the tar at /home/ipcs

tar -xvzf sbce-add.patch.tar.gz

cd 11127.patch

./install.sh

Restart the boxes

- Adding secondary EMS on upgraded EMS server need following workaround to get into working state:

  1. Change DB password in old EMS and SBCs to non-default password with SBCEConfigurator.py change-db-password. Please ensure that password is same on EMS and SBCE's. Basically the password has to be same for both EMS's and likewise for SBCE's in HA state.

  2. Deploy secondary EMS with changed password db password and run script named "SecondaryEMS_bdrRejoin.sh"

  3. Place the script on Secondary EMS in any directory, say /home/ipcs

  4. Become root:

  $ sudo -i

  5. Make script executable:

  # chmod 777 /home/ipcs/ SecondaryEMS_bdrRejoin.sh

  6. Execute script:

  # /home/ipcs/ SecondaryEMS_bdrRejoin.sh

  7. Now Secondary EMS should be accessible and working.