Avaya Aura® Session Border Controller

Release Notes

Release 6.0.2

Issue 1

May 2011

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

Avaya shall not be 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. 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 End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked Web sites referenced within this site or documentation(s) 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 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 to Avaya customers and other parties through the Avaya Support Web site:

http://www.avaya.com/support.

Please note that if you acquired the product from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. 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 AUTHORIZED RESELLER, AND 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 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 originally sold by Avaya and ultimately utilized by End User.

License type(s)

Named User License (NU). End User may: (i) install and use the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). With respect to Software that contains elements provided by third party suppliers, End User may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickwrap" license accompanying or applicable to the Software ("Shrinkwrap License"). The text of the Shrinkwrap License will be available from Avaya upon End User's request (see "Third-party Components" for more information).

Copyright

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 regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the

Third Party Terms that apply to them is available on the Avaya Support

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

A copy of the open source licensed source code in the SDK and SBC is available via plds.avaya.com. A copy of the License text file for SBC can be found by opening the SBC web console and clicking on the link entitled '(c) 2005-2011 Acme Packet, Inc. All rights reserved'. A copy of the License text file for the SBC SDK can be found in the "LICENSE" directory contained within the post-install.tar file.

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://www.avaya.com/support. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

Avaya, the Avaya logo, Avaya Aura, one-X Portal, Communication Manager, Application Enablement Services, Modular Messaging, and Conferencing 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://www.avaya.com/support

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

Contents

Avaya Aura® Session Border Controller Template R6.0.2 Release Notes

Introduction

This document introduces the General Availability release of the Avaya Aura® Session Border Controller Template Release 6.0.2 and provides installation notes and describes known issues.

Software Release Versions

Session Border Controller Application	File Name
Avaya Aura® Session Border Controller Template	SBCT_6.0.2.0.3.iso Includes: • SBCT 6.0.2 Application software for System Platform: nnSE362p4-xen-aasbc.img.gz • SBCT 6.0.2 OVF template descriptor file for the Avaya Common Server: SBCT.ovf • SBCT 6.0.2 OVF template manifest file: SBCT.mf • SBCT 6.0.2: OVF template descriptor file for HP Procurve: SBCT_Procurve.ovf • SBCT 6.0.2 OVF template manifest file : SBCT_Procurve.mf • SBCT 6.0.2 Pre-Installation Wizard: pre-install.war • SBCT 6.0.2 Post-Installation Wizard: post-install.tar • SBCT 6.0.2 System Platform Plug-ins: sbc_plugins_https.tar • SBCT 6.0.2 Standalone Installation Wizard: SP_Pre-Installation_Wizard_5579.exe
Avaya Aura® System Platform	vsp-6.0.3.0.3.iso

Release History:

Date	Build	Change(s)
May 2011	6.0.2.0.3	Service Pack R6.0.2
November 2010	6.0.0.1.5	General Availability R6.0
August 2010	6.0.0.3.4	Controlled Introduction R6.0

New Functionality in this Release

- This release includes support for the Avaya Aura® System Platform patching mechanism.

Resolved Issues

- Disable 3PCC for all Service Provider configurations
- Update the Skype Service Provider configuration to include DoS settings
- Directive fields missing in INVITE for Digest Authentication
- If the Default Gateway for the AA-SBC is defined on the Public Interface, any change to this value following installation does not persist
- SBC: Installation of SBC gives error "Failed to create configuration file"
- Avaya Aura® Midsize Enterprise template only issue: Static Routes administered on cdom are not accepted into SBC

Further resolved issues are detailed in Acme Packet - Avaya Aura® Session Border Controller 3.6.2 p4 Build Notes

Upgrade Notes

Upgrade to this release using the Aura Aura® System Platform solution template upgrade mechanism. This upgrade process includes backup and restore of the running configuration of the Avaya Aura® Session Border Controller.

Known Issues List

This section lists in order the known issues for the Avaya Aura® Session Border Controller Template. Details on workarounds can be found further in the document. The top issues are in bold.

1. **AA-SBC LDAP support: AA-SBC does not currently support the System Platform LDAP server.**

2. **HA configuration: network connection instability problems can occur if one of the AA-SBCs resets and the Public Interface IP address has been re-used for the virtual public interface.**

3. **HA configuration: changing the IP addresses of the standby server of the AA-SBC HA cluster via the System Platform web console will result in any changes being lost as soon as the cluster synchronizes its configuration.**

Known Issues and Workarounds

1. **AA-SBC LDAP support: AA-SBC does not currently support the System Platform LDAP server.**

   - All AA-SBC accounts must be administered via the AA-SBC CLI or GUI. Default accounts of admin and cust are currently added by the AA-SBC Installation Wizard with default passwords of admin01 and cust01 respectively. These passwords must be changed manually following installation using the AA-SBC CLI or GUI.

2. **AA-SBC HA configuration: network connection instability problems can occur if one of the AA-SBCs resets and the Public Interface IP address has been re-used for the virtual public interface.**

   - When configured for HA, in the event that one of the AA-SBCs resets it pulls in the eth2 public/outside IP address information from the System Platform OVF environment file. This will cause a duplicate IP address and cause network connection instability if the same IP address has been used for the virtual public interface in the HA configuration.

     i. **Workaround:** When configuring the AA-SBC for HA use a new unique IP address for the virtual public interface IP address, i.e. don’t re-use the IP address defined for the AA-SBC’s Public Interface.

3. **AA-SBC HA configuration: changing the IP addresses of the standby server of the AA-SBC HA cluster via the System Platform web console will result in any changes being lost as soon as the cluster synchronizes its configuration**.

   - When configured for HA, changing any IP addresses via the System Platform web console should only be done to the AA-SBC Cluster Master otherwise changes will be lost when the cluster synchronizes its configuration.

     i. **Workaround:** When making changes to the IP addresses of the AA-SBCs, ensure that these are only made to the Cluster Master. Switch to the standby server by using the CLI "group-down" command.

Post Installation Notes

1. **Backup and Restore of AA-SBC configuration data**
    a. Only the System Platform backup and restore mechanism should be used for saving and retrieving AA-SBC configuration data. Other native methods present on the AA-SBC itself could cause problems if the restoration of the data is attempted on a different system to the one on which the data was originally saved, e.g. if the AA-SBC was re-installed, this would be regarded as a different system.

2. **Network changes to the AA-SBC interfaces**
    a. Following SBCT Installation, any network updates to the virtual eth0 and eth2 interfaces of the AA-SBC must be done via the System Platform web console Network Configuration page.

3. **Minimal Installation**
    a. If using the "minimal" installation option of the SBCT Installation Wizard, following installation the network values for the virtual eth2 interface of the AA-SBC must be done via the System Platform web console Network Configuration page. By default, "DHCP" will be applied to this interface until this is done.

4. **Skype Service Provider configuration**
    a. If Skype is the chosen Service Provider, the default gateway will be defined on the Public Interface following installation. As such, static routes may need to be configured on the Private Interface to ensure correct routing. This can be done via the System Platform web console Static Route Configuration page.

5. **Denial of Service (DoS) protection**
    a. Application level Denial of Service (DoS) protection is only enabled by default for the Skype Service Provider configuration. As a security measure for all other Service Provider configurations, the installation wizard configures source IP address filtering. Source IP address filtering blocks traffic from all IP addresses other than that of the service provider's POP to deter potential DoS or other similar attacks. Skype's POPs are addressed using an FQDN which prevents the wizard from configuring such a filter. More information can be found in:

        i. Avaya Aura® SBC System Administration Guide
        ii. Avaya Aura® SBC Session Services Configuration Guide

Troubleshooting

1. Loss of contact with AA-SBC
    a. General
        i. Access the AA-SBC console
            ▪ Login to Dom0 as admin
            ▪ Switch user to root: su - root
            ▪ Access the AA-SBC console: xm console sbc
            ▪ Save any console output
            ▪ Login as admin
            ▪ Issue the following command: show faults

            - If fault listed, request further assistance

   b. Following the loading of a configuration from a different installation / system
      i. Access the AA-SBC console
         - Login to Dom0 as admin
         - Switch user to root: su - root
         - Access the AA-SBC console: xm console sbc
      ii. Check the MAC address of the system
         - issue the following command to determine if the interfaces are active (where an attempt to load a configuration with an incorrect MAC address is made, no interfaces will be shown): show interfaces
         - issue the following command to determine the correct MAC address of the system and note the MAC address for eth0: show interface-details
      iii. Configure the correct MAC address by entering the following commands:
         - config cluster box 1
         - set identifier <MAC address for eth0>
         - top
         - save
         - exit

2. Revert to a previous configuration
   a. Access the AA-SBC CLI
      i. Login stage 1 using root
      ii. Login stage 2 using admin
   b. Enter the following commands in order to revert the AA-SBC to a previous configuration
      i. Show backup configuration file directory: show file-directory /cxc/backup
      ii. Replace the currently running configuration with a previous configuration: config replace /cxc/backup/cxc.cfg
      iii. Save the configuration: config save

Acme Packet - Avaya Aura® Session Border Controller 3.6.2 p4 Build Notes

This section provides the Acme Packet release notes for the Avaya Aura® Session Border Controller Template Release 6.0.2, including defects fixed from the previous release and known issues.

New Feature

- RFE 2768: Support Avaya System Platform Patch plugin.

Defects Fixed (delta from 3.6.2 p2)

- PD00017296, 18981: When SIP peer configured with FQDN rather than IP address, server failover detection does not work.
- PD00017334: When using FQDN for SIP peer, NNOS-E uses old IP address after peer address changes.
- PD00018262: Segmentation fault while tracing enabled.
- PD00018308: Policy doesn't match user-group-condition when the INVITE is to the configured UA, only when it comes from the UA.
- PD00018350: SIP segmentation fault related to DTMF translation from INFO to 2833.
- PD00018407: SIP segmentation fault related to DTMF translation from INFO to 2833.
- PD00018419: Kernel transcoding enhancements to increase internal buffer size to allow 8kHz ptimes of up to 120 msec.
- PD00018487: Segmentation fault resulting from any manipulations of the From header with header-settings would result in a fault if the original From URI was missing a tag parameter.
- PD00018365, 19265: Network-address plugin on ME system failed to update static routes or AASBC's IP addresses correctly.
- PD00016834: Failed ENUM lookup with regex matching, and creation of empty 'Request' header in response messages. (The creation of the 'Request' header is known to cause interop problems with some Genband softswitches.)
- PD00018074: *qop, cnonce* and *nc* values are missing from Authorization header for a 401/407 INVITE response with handle-challenge-locally is enabled.

Known Issues

- PD00018153: For inbound TLS connections, outbound SIP transactions attempt to create new TLS connection and fail. A configuration workaround is available for this issue.
- PD00020226: With 3PCC, outgoing INVITE incorrectly contains duplicated multipart-MIME body parts. *Note: This occurs in 3.6.2 p1, but is believed fixed in 3.6.2 p4. (Confirmation pending.)*
- PD00020518: In the Authorization header, a parameter with a quoted valued which includes a comma, for example *qop="auth,auth-int"*, will not be parsed properly, resulting in the header being ignored. To be fixed in 3.6.2 p5.