Avaya Agile Communication Environment™ Release Notes

Release 6.2.3
NN10850-019
June 2015

© 2015 Avaya Inc.
All Rights Reserved.

Notice

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

Documentation disclaimer

“Documentation” means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. 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 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: http://support.avaya.com 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.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO 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. 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 Designated Processor that hosts 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

CPU License (CP). End User may install and use each copy or Instance of the Software on a number of Servers up to the number indicated in the order provided that the performance capacity of the Server(s) does not exceed the performance capacity specified for the Software. End User may not re-install or operate the Software on Server(s) with a larger performance capacity without Avaya’s prior consent and payment of an upgrade fee.

Named User License (NU). You 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.

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 currently available for license from Avaya is the software contained within the list of Heritage Nortel Products located at http://support.avaya.com/LicenseInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants You 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.

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: http://

support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

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: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

Avaya Aura is a registered trademark of Avaya Inc.

Avaya ACE is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners. Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

See the Avaya Support website: http://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: http://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction 6
Chapter 2: Avaya ACE GA load 7
Avaya ACE GA load 7
Chapter 3: Software load lineup 8
Product compatibility 8
Chapter 4: Supported upgrade paths 10
Chapter 5: Upgrades and Migration to 6.2.3 12
Migrating to Avaya ACE release 6.2.3 12
Upgrading Avaya ACE from release 6.2.0 to release 6.2.3 13
Upgrading Avaya ACE from release 6.2.1 or 6.2.2 to release 6.2.3 13
Chapter 6: Issues resolved in release 6.2 15
Chapter 7: Capacity and traffic considerations 18
Capacity model considerations 18
Avaya ACE capacity considerations 19
Avaya ACE Foundation Toolkit capacity considerations 19
Avaya ACE Service Provider capacity considerations 19
Avaya ACE application capacity considerations 20
Chapter 8: Documentation considerations 21
Downloading ACE documents from support site 21
Chapter 9: Installation and deployment considerations 23
Avaya ACE installer claims a port is in use when it is not 23
Certificate configuration is not updated on Upgrade to 6.2.1 24
ACE Server loses connectivity to Session Manager 25
Configuring NMS locations 25
IWA configuration fails when you backup and migrate from ACE VE 6.2 to 6.2.1 26
Applying the post installation patch 26
Applying patch to prevent the Shellshock security threat 27
Chapter 10: Provisioning considerations 29
Some SIP interfaces do not use ssl 29
Unable to edit provider on Avaya ACE GUI 30
Chapter 11: Avaya ACE GUI and OAM considerations 31
Provisioning of provider in OAMP on Google Chrome does not work 31
Unreliable certificate management 31
Chapter 12: Third Party Call considerations 33
Third Party Call v2 and v3 do not support the whitespace character for the called party and second participant in the URI for WSDL requests 33
Display on the Calling and Called Party devices is incorrect when a TPC v2 call is initiated from ACE 34

Comments on this document? infodev@avaya.com

Chapter 13: Third Party Call Extensions considerations 35
Single step transfer operation on JTAPI provider in ACE succeeds but throws exceptions in the log 35
endCall does not clear all parties in a conference when the consultCall is made with conferenceOnly option 36
Missing notification events during singleStepTransfer 36
Chapter 14: Call Notification considerations 38
Third Party Call Extensions (v2.0) related Call Notifications (v3.8) for interprovider calls have improper Called Party URI 38
Call Notifications (v3.8) for interprovider calls will have calling party appended with “phone-context=dialstring” 39
ACE sends Disconnect notification to listener when Busy on a call 39
TPCv2 and Call Notification v3.8 have issues when forwarded DN is busy on Aura TR/87 and SIP one-X clients 40
Unreachable event not received when called party is unreachable in Session ID based Call Notification v3.8 40
Call ID Pariticpant based Call notifications contain multiple participant entries for PSTN numbers 41
Duplicate notifications received when using H.323 clients in singleStepTransfer 41
Call Notification clients do not receive No Answer events when a call to a transferredTo party times out 42
Wrong notification in a call forward scenario, Not Reachable instead of Busy notification 42
Chapter 15: Call Forwarding considerations 44
Incomplete notifications for Call forwarding or redirectCall 44
Chapter 16: Presence considerations 45
Chapter 17: Endpoint display considerations 46
Calling party phone does not display called party number in a TPCv2 makeCall 46
Chapter 18: Foundation Toolkit considerations 47
B2B Routing call fails when the calling and called party are sequenced to AAFT and CM 47
Chapter 19: Avaya Aura® service provider considerations 49
Avaya clients do not play Busy tone when a third party call is made to a busy line 49
SIP calls fail when AAFT and AURA SIP providers are both provisioned 50
Incorrect phone display when receiving call from thirdPartyCallController in a TPCv2/v3 makeCall 50
First call after a CTI link has been restored always fails when the call is made from Browser add-in 51
Call forwarding and redirectCall have issues when using H.323 clients 51
Chapter 20: CS 1000 service provider considerations 52
No busy notification for a network initiated call to a monitored DN on a CS 1000 TR/87 provider 52
Failed to CallSender when ACE SIP Interface makecall from CS1K set to MM then CallSender to BCM set 53
Multiple transfers on a CS1000 provider results in inconsistent behavior 53

Chapter 1: Introduction

This Release Notes document provides a brief description of operational considerations for Avaya Agile Communication Environment™ Release 6.2.x

Comments on this document? infodev@avaya.com

Chapter 2: Avaya ACE GA load

Avaya ACE GA load

Download the Avaya ACE Release 6.2.3 files from the following locations:

- Confluence: https://confluence.forge.avaya.com/display/ACE/Download+Generally+Available
- PLDS:

  ACE000000036 - ACE Core 6.2 SP (6.2.3) - LINUX OS
  ACE000000044 - ACE Core 6.2 SP (6.2.3) - WASND 8.0.0.5 V3 tar.gz
  ACE000000045 - ACE Core 6.2 SP (6.2.3) - IBM WAS for upgrade from 6.2 to 6.2.3
  ACE000000046 - ACE Core 6.2 SP (6.2.3) - AMS (Media Server) load
  ACE000000047 - ACE Core 6.2 SP (6.2.3) - Bare Metal (Non Virtual) tar.gz
  ACE000000048 - ACE Core 6.2 SP (6.2.3) - Bare Metal (Non Virtual) iso
  ACE000000049 - ACE Core 6.2 SP (6.2.3) - VE load (ova)

Chapter 3: Software load lineup

The following Avaya ACE Release 6.2.3 application and related software are available as iso images and tar files:

- Red Hat Enterprise Linux 6.0
- Avaya ACE Software and Installation Tools 6.2.3
- IBM WebSphere 8.0.0.5 V3
- Avaya Aura® Media Server (MS) 7.5.0.1299
- Avaya ACE upgrade software
- IBM Websphere upgrade software

Note:

The Websphere upgrade software is only available as a tar file.

You can download the above files from the Avaya support site at http://support.avaya.com/.

Related Links

Product compatibility on page 8

Product compatibility

The following table lists the interoperability matrix for Avaya ACE Release 6.2.3.

Avaya Aura load lineup

Product	5.2x	6.1	6.2 FP1	6.2 FP2	6.2.3
Application Enablement Services	5.2.2 Superpatch 3	6.1 SP 2 (6.1.0.20)	6.2	6.3	6.3.3 **Note:** Further, install the LSU1 and LSU2 patches as well as the

Table continues…

Comments on this document? infodev@avaya.com

Product	5.2x	6.1	6.2 FP1	6.2 FP2	6.2.3
					6.3.3 Superpatch 3.
Avaya Aura® Communication Manager	5.2.1 SP 7	6.0.1 SP 2 (00.1.510.1-18860)	6.2.0.0.3086	6.3	6.3.10
Avaya Aura® Session Manager	5.2 SP 3	6.1 SP1 (6.1.1.0.611023)	6.3.0.0-76008	6.3.2	6.3.13
Avaya Aura® System Manager	5.2 SP 2	6.1 SP1.1 (6.1.0.0.7345)	6.2	6.3.2	6.3.13
G450 Branch Gateway	Firmware 30.X.Y	G450 Firmware 31.x.y (31.18.1)		6.3	
Avaya Aura® Presence Services			6.1.5	6.2	

Non-Aura products

Product	Supported releases
Communication Server 1000	7.5, 7.6
Communication Server 2100/ CS2100 Core	SE 13.0
Cisco Unified Communications Manager	8.6
Tandberg VCS	3.0
Avaya NES Contact Center	6.0 or later

Comments on this document? infodev@avaya.com

Chapter 4: Supported upgrade paths

The following migrate/upgrade paths are supported:

Path	Migrate/Upgade	Tool to run	What is migrated
Avaya ACERelease 6.2.0 Standalone (SA) to 6.2.1 High availability (HA)	Migrate	migrate62Standalone-62HA.sh	Database data
Avaya ACERelease 6.2.1 Standalone (SA) to 6.2.1 High availability (HA)	Migrate	migrate62Standalone-62HA.sh	Database data
Avaya ACERelease 6.2.0 HA to 6.2.1 HA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACERelease 6.2.0 SA to 6.2.1 SA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACERelease 3.0.x SA to 6.2.1 HA	Migrate	migrate30Standalone-62HA.sh	Database data
Avaya ACERelease 3.0.x SA to 6.2.1 SA	Migrate	migrate30to621.sh	Database and configuration data
Avaya ACERelease 3.0.x HA to 6.2.1 HA	Migrate	migrate30to621.sh	Database and configuration data
Avaya ACE 6.2.1 SA to 6.2.2 SA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACE 6.2.1 HA to 6.2.2 HA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACERelease 6.2.2 to 6.2.3	Migrate	migrate62to623Vm.sh	Database and configuration data
Avaya ACE Release 6.2.0 SA to 6.2.3 SA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACE Release 6.2.0 HA to 6.2.3 HA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACE 6.2.1 or 6.2.2 SA to 6.2.3 SA	Upgrade	upgrade.sh	Database and configuration data
Avaya ACE 6.2.1 or 6.2.2. HA to 6.2.3 HA	Upgrade	upgrade.sh	Database and configuration data

Comments on this document? infodev@avaya.com

Note:

When you upgrade from Release 3.0 to Release 6.2.3, you must first migrate from 3.0 to 6.2.1, and then upgrade to 6.2.3.

Chapter 5: Upgrades and Migration to 6.2.3

Migrating to Avaya ACE release 6.2.3

About this task

Perform the following procedure to migrate from previous releases to Avaya ACE release 6.2.3

Procedure

1. Login to the Avaya ACE host.
2. Type **`cd /opt/avaya/ace/bin`** to change directories.
3. Initiate a backup. Do one of the following:
   - To create a backup using the default location settings, type **`./ACE_backup.sh -a`**.
   - To create a backup and specify the location, type **`./ACE_backup.sh`**
4. If you chose to specify a location for the backup, enter the path to the location where you want to store the backup files.
5. At the prompt, enter the database user name.

   The default database user name is the root database user. If you type any other name, ensure that the user has backup privileges.
6. At the prompt, type the database user password.

   The backup process starts after you enter the password.
7. Use WinSCP or a similar tool to transfer the backup to a remote location.
8. Power OFF the Virtual Machine.
9. Deploy the Avaya ACE 6.2.3 VM.
10. Copy the backup file from the remote location to the new ACE VM.
11. Type **`cd /opt/avaya/ace/bin`** to change directories.
12. Type **`./migrate62to623Vm.sh`** to migrate the data.

    Provide the backup file as the input.

Comments on this document? infodev@avaya.com

Upgrading Avaya ACE from release 6.2.0 to release 6.2.3

Procedure

1. Login to the Avaya ACE host.
2. Copy the `ACE-<new_version>.tar.gz` file to the Avaya ACE host directory, `/opt/avaya` .
3. Type **cd/opt/avaya** to change the directory.
4. Type **tar -zxvf ACE<new_version>.tar.gz** to untar the Avaya ACE file.
5. Download the WebSphere upgrade software `ACE-WASND-8.0.0.5_Upgrade_V3.tar.gz`.
6. Create the directory `/opt/avaya/was` to store the WebSphere upgrade software.
7. Type **mkdir was**.
8. Transfer the downloaded upgrade file to the `/opt/avaya/was` directory.
9. Type **cd was** to change directories.
10. Type **tar -xvf ACE-WASND-8.0.0.5_Upgrade_V3.tar.gz** to untar the Websphere files.
11. Type **cd /opt/avaya/ace-6.2.3/install** to change directories.

    Note:

    For High Availability deployments, untar the Avaya ACE file on both Host A and Host B.
12. Type **./upgrade.sh** to run the upgrade script.

    The system displays messages as the upgrade procedure proceeds. To see the Avaya ACE upgrade log file, go to `/var/avaya/ace/log/install/ACE_install.log`.

Upgrading Avaya ACE from release 6.2.1 or 6.2.2 to release 6.2.3

Procedure

1. Login to the Avaya ACE host.
2. Copy the `ACE-<new_version>.tar.gz` file to the Avaya ACE host directory, `/opt/avaya` .
3. Type **cd/opt/avaya** to change the directory.
4. Type **tar -zxvf ACE<new_version>.tar.gz** to untar the Avaya ACE file.

Comments on this document? infodev@avaya.com

Note:

For High Aavailability deployments, untar the Avaya ACE file on both Host A and Host B.

5. Type **`/opt/avaya/ace-6.2.1/install`** or **`/opt/avaya/ace-6.2.2/install`**.
6. Type **`./upgrade.sh`** to run the upgrade script.

   The system displays messages as the upgrade procedure proceeds. To see the Avaya ACE upgrade log file, go to `/var/avaya/ace/log/install/ACE_install.log`.

Comments on this document? infodev@avaya.com

Chapter 6: Issues resolved in release 6.2

The following issues, identified in the Release 3.0.2 Release Notes, have been resolved in Release 6.2.

Table 1: Installation and deployment

ACECORE-7000	Cluster Suite does not failover when power removed from active host
ACECORE-8324	MOSFET security scan warning: unsafe file mode seen in root crontab
ACECORE-9211	After uninstalling ACE, the ACE software cannot be reinstalled
ACECORE-9673	Avaya ACE support for PLDS and WebLM licenses

Table 2: Provisioning

ACECORE-10435	AS5300 is not a supported service provider in ACE release 3.0
ACECORE-4740	Limitations on Third party call (v2) and Third party call (v3) when configuring a service provider for SIP REFER or Media Server

Table 3: ACE GUI and OAM

ACECORE-7228	Database not synchronized alarm is raised when databases are synchronized

Table 4: Third party call

ACECORE-7117	Endcall on held call causes exception
ACECORE-7654	Subsequent `makecall/makecallSession` requests to calling party with identical user and host will not recognize changes to password, port, parameter or header until ACE or service provider is restarted.

Table 5: Third party call extensions

ACECORE-8117	Third party call extensions service metrics are pegged against third party call (v2) service metrics

Table 6: Call forwarding and notification

ACECORE-6738	Cannot clear call forwarding errors remotely
ACECORE-10378	Answer notification lists wrong party as called in a network initiated call resolving to a call forwarded number
ACE-12576	ACA is stuck in Calling state when a call is made from ACA or Lync to a long distance number. Connected state response is not received after the call completes.

Table 7: Foundation Toolkit

ACECORE-7482	VES create dialog method does not throw exception for invalid URI
ACECORE-7484	Subsequent requests are lost when the session manager TLS port is 5061
ACECORE-7489	The media service **`generateDtmf()`** throws `UnsupportedOperation` exception
ACECORE-7491	Foundation toolkit does not send a 408 Request Timeout response
ACECORE-8743	Foundation toolkit client application registrations and subscriptions may not be automatically renewed after two consecutive failures
ACECORE-10348	Virtual endpoint service DialogTerminationCauses are incorrect in some circumstances

Table 8: Message Drop and Message Blast

ACECORE-4255	Message Drop fails intermittently when both originating and terminating lines are off the same CS1000 PBX

Table 9: Avaya Aura service provider

ACECORE-7219	ACE nad AES sporadically lose connectivity
ACECORE-7431	Limitations on Third party call (v2) operations when configuring an Avaya Aura service provider for SIP REFER
ACECORE-7769	Communication between ACE and AES fails after switchover or restart of AES
ACECORE-11847	Upgrade to ACE 3.0.2 does not preserve certificates

Table 10: CS 1000 service provider

ACECORE-4262	The `getCallForwarding` WSDL operation returns truncated Avaya CS1000 phone numbers after ACE restart
ACECORE-4491	Calling party does not hear `busy/invalid` number tones during `makecall/makeCallSession` using third party call(v3) with SIP.
ACECORE-10695	CS1000 release 6.0 is now end of life and is no longer supported

Comments on this document? infodev@avaya.com

Table 11: Turret

ACECORE-6655	No provider out-of-service alarm for turret provider configured with wrong IP

Table 12: IBM Lotus Sametime

ACECORE-4096	Users will be considered as non Avaya users if they have a duplicate IBM Lotus Sametime contact ID in their ACE user profile

Table 13: Security

	Fixed the Poodle SSLv3 vulnerability (CVE-2014–3566).
	Fixed the leap second issue.

Chapter 7: Capacity and traffic considerations

Related Links

Capacity model considerations on page 18
Avaya ACE capacity considerations on page 19
Avaya ACE Foundation Toolkit capacity considerations on page 19
Avaya ACE Service Provider capacity considerations on page 19
Avaya ACE application capacity considerations on page 20

Capacity model considerations

Determining the Avaya ACE system capacity model is based on the following:

- Number of devices that will be integrated with Avaya ACE for each user (for example, telephone, video device, soft clients)
- Number of users integrated with Avaya ACE
- What the users are doing which would require Avaya ACE resources
- How often they are doing it
- Capacity of the communication network

Actual traffic rates may vary depending on the type of hardware and operating system Avaya ACE is installed on, network conditions and other non-ACE related applications running on the Avaya ACE server. A typical Avaya ACE deployment with 15000 Avaya ACE users using ThirdPartyCall (v2), Presence and Call Notification (v2.3) with a 2-3 minute call duration can expect their traffic capacity to fall in the 6-15 calls per second range. Each Avaya ACE deployment should work with Avaya Professional Services (APS) to have an architect identify the addressable capacity for the deployment.

Related Links

Capacity and traffic considerations on page 18

Avaya ACE capacity considerations

Avaya ACE can support a maximum of 45,000 SIP subscriptions (these are consumed by either SIP SUBSCRIBE or SIP REFER transactions) and 30,000 SIP call legs (these are consumed by SIP INVITE transactions and released by SIP BYE transactions). These limitations are used to determine how many SIP/TR87 contacts an Avaya ACE user can have and how many concurrent SIP calls can be made.

Avaya ACE on VMware capacity considerations

Avaya ACEon VMware supports a maximum of 15000 users with call rate of 18 call per second where each call consists of make call session, presence update and a call notification.

Related Links

Capacity and traffic considerations on page 18

Avaya ACE Foundation Toolkit capacity considerations

Foundation Toolkit supports a call rate of 20 calls per second.

Related Links

Capacity and traffic considerations on page 18

Avaya ACE Service Provider capacity considerations

SIP B2BUA

The maximum verified sustainable rate of Avaya ACE-initiated SIP B2BUA calls is 18 calls per second with 15,000 Avaya ACE users using the ThirdPartyCall (v2) web service or ThirdPartyCall (v3) web service with sufficient media server capacity and an average call duration of 3 minutes.

TR87 (CTI)

The maximum verified sustainable rate of Avaya ACE-initiated TR87 (CTI) calls is 18 calls per second with 15,000 Avaya ACE users using ThirdPartyCall (v2), Presence and Call Notification (v3.2 or v3.8) web services and an average call duration of 3 minutes.

JTAPI

The maximum verified sustainable rate of Avaya ACE-initiated calls is 6 calls per second on JTAPI (all service providers combined) per Avaya ACE server with 5000 Avaya ACE users using Third Party Call (v2) and Third Party Call extensions (v2) web services and an average call duration of 3 minutes.

Cisco Unified Communication Manager using AXL

The maximum verified sustainable rate of Avaya ACE-initiated AXL calls is 18 calls per second per Avaya ACE server with 15,000 Avaya ACE users using the Call Forward web services and average call duration of 3 minutes.

Avaya NES Contact Center

The maximum verified sustainable rate of Avaya ACE-initiated calls is 3 calls per second on the Avaya NES Contact Center using Third Party Call (v2), Call History and Call Notification (v3.8) web services using 5000 Avaya ACE-users with average call duration of 3 minutes.

Related Links

Capacity and traffic considerations on page 18

Avaya ACE application capacity considerations

Message Drop and Message Blast

The Message Blast traffic rate is one call per second, with a maximum of 180 concurrent blast participants and a call duration of three minutes.

Click-to-Dial with Message Drop, Message Drop and Leave:

- 4 Click-to-Dials per second, where 0.5 calls per second is a Message Drop, 1.5 calls per second is a Message Drop & Leave and the call duration is 2.5 minutes.
- The traffic mixture for this model is:
  - CS 1000 Click-to-Dial: one call per second, where 0.25 calls per second is a Message Drop and 0.25 calls per second is a Message Drop andamp; Leave.
  - Avaya Aura Click-to-Dial: 1 call per second call, where 0.25 calls per second is a Message Drop and 0.25 calls per second is a Message Drop & Leave.
  - Turret Click-to-Dial: 2 calls per second, where 1.0 call per second is a Message Drop & Leave.

Related Links

Capacity and traffic considerations on page 18

Comments on this document? infodev@avaya.com

Chapter 8: Documentation considerations

The Avaya Agile Communication Environment™ (ACE) software ships with the documentation available when the software is built. The following documents have been updated for the official ship date of Avaya ACE™ release 6.2.

- *Avaya Agile Communication Environment™ Overview and Specification*
- *Avaya Agile Communication Environment™ Planning and Installation* (NN10850-004)
- *Avaya Agile Communication Environment™ Web Services* (NN10850-007)
- *Avaya Agile Communication Environment™ Troubleshooting* (NN10850-026)

The following documents have been added:

- *Avaya Agile Communication Environment™ User and Security Administration* (NN10850-010)
- *Avaya Agile Communication Environment™ using VMware in the Virtualized EnvironmentDeployment Guide* (NN10850–065)

The following document has been renamed:

from *Avaya Agile Communication Environment™ Administration* (NN10850-005)

to *Avaya Agile Communication Environment™ Service Provider Administration* (NN10850-005)

Updated documents can be identified by the issue number on the front cover, located after the document number. The second number indicates how many times the document has been reissued within a software release. For example, the original document is labelled XX.01. The second issue is labelled XX.02.

Current documents can be obtained from the Avaya support site at https://support.avaya.com. See Downloading ACE documents from support site on page 21 .

Related Links

Downloading ACE documents from support site on page 21

Downloading ACE documents from support site

Use the following procedure to download ACE documents from the Avaya support site.

Procedure

1. On your web browser, enter the Avaya support site URL, https://support.avaya.com.

2. Click **Downloads & Documents**.
3. Enter `Avaya Agile Communication Environment` in the **Enter Your Product Here** field.
4. In the **Choose Release** drop down menu, select the release.
5. In the Select the content type section, select **Documents** and click **Enter**.
6. In the resultant page, do one of the following:
   - Filter the documents displayed based on the type of document you require. To filter, select the type of document you want from the list.
   - Click **Select All** to display all the documents pertaining to the release.
7. From the documents displayed, click the document you want.

Related Links

Documentation considerations on page 21

Comments on this document? infodev@avaya.com

Chapter 9: Installation and deployment considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) installation and deployment.

Related Links

Avaya ACE installer claims a port is in use when it is not on page 23
Certificate configuration is not updated on Upgrade to 6.2.1 on page 24
ACE Server loses connectivity to Session Manager on page 25
Configuring NMS locations on page 25
IWA configuration fails when you backup and migrate from ACE VE 6.2 to 6.2.1 on page 26
Applying the post installation patch on page 26
Applying patch to prevent the Shellshock security threat on page 27

Avaya ACE installer claims a port is in use when it is not

While Installing ACE, the installer displays an error message stating that a specific port is already in use and the installation fails even though the port is free. This happens if the ACE server has a connection established with a remote server and the remote server port matches with the specific port used by ACE.

Expected result:

Installation should not fail as the port is used on the remote server and not the ACE server.

Actual result:

Installation fails with the error that a specific port is already in use.

Tracking number

ACECORE-12885/ACE-11687

Impact

ACE cannot be installed if some port needed by ACE is used by any remote server to connect to ACE server.

Workaround

1. Reboot the ACE server.
2. Run the command: `netstat –nat | grep port`

   Ensure that the command returns no entries. This implies that the port is not assigned to any other service.
3. Restart the installation.

Related Links

Installation and deployment considerations on page 23

Certificate configuration is not updated on Upgrade to 6.2.1

Tracking number

ACE-12530

Description

Applicable when you upgrade from ACE 6.2.0 or ACE-6.2.1-SNAPSHOT to ACE 6.2.1. After the upgrade is completed, user-provisioned certificates from the previous release are not used. This is applicable for System Manager certificates and for self-signed certificates.

Impact

Service providers using certificates will go OOS after upgrade.

Workaround

1. Run the **`/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/wsadmin.sh -user <was_admin_username> -password <was_admin_password> –f/opt/avaya/ace/bin/modifySSLConfig.py <host_type> <certificate_alias>`** command in the Linux console of your ACE machine.

Here, was_admin_username is the IBM Websphere admin user name,

was_admin_password is the password for the IBM Websphere admin user

host_type is the Avaya ACE host type, as present in /etc/host_type

certificate_alias is the alias of the certificate to be used. The certificate is present in *CellDefaultKeyStore*. To view the certificates, on IBM Websphere GUI navigate to **Security** > **SSL Certificate**, **Key Management** > **Key Stores**, and **Certificates** > **CellDefaultKeyStore** > **Personal certificates**.

Note:

If you have configured the AAFT service provider, delete, and reconfigure the certificate from the Avaya ACE GUI.

Related Links

Installation and deployment considerations on page 23

ACE Server loses connectivity to Session Manager

Description

The ACE SIP component loses connectivity to Session Manager, though this is not propagated back. An alarm is not raised on ACE OAM. The SIP container threads go into a dead lock. This scenario occurs when ACE connects to CS1k through Session Manager, which acts as a proxy.

Tracking number

ACE-12319

Impact

All applications using an ACE SIP provider will not be able to make any call related operation.

Workaround

You must install an additional IBM Websphere Application server patch. You must perform the following procedure post installation, post upgrade, and post an inrelease upgrade.

1. Download `WASPatch621v3.tar.gz` from PLDS. The ID is **ACE000000039**.
2. Create the `/opt/avaya/was` directory using the **`mkdir /opt/avaya/was`** command. Upload `WASPatch621v3.tar.gz` to this location.
3. Type the **`tar -xvf WASPatch621v3.tar.gz`** command to explode the tarball.
4. Type the **`./installPatch6.2.1.sh`** command to install the patch.

You must apply this patch to both the standalone and high-available deployments. For high availability scenarios, you must apply the patch to Node A and then Node B.

Related Links

Installation and deployment considerations on page 23

Configuring NMS locations

Description

While configuring NMS locations, non-numeric characters are accepted for **Port Number**.

Tracking number

ACE-12529

Impact

While configuring NMS locations, non-numeric characters are accepted for **Port Number** and notifications are not sent to the NMS locations

Workaround

None. You must enter a numeric value for NMS port number.

Related Links

Installation and deployment considerations on page 23

IWA configuration fails when you backup and migrate from ACE VE 6.2 to 6.2.1

Description

IWA configuration fails when you backup and migrate from ACE VE 6.2, in which IWA is configured, to 6.2.1.

Tracking number

ACE-12532

Impact

When you upgrade from ACE VE 6.2, in which IWA is configured, to 6.2.1, the keytab file is not present in the backup file. As a result, IWA configuration fails.

Workaround

- Ensure that you backup the keytab file. Transfer the keytab file to a local computer before you power off the 6.2 virtual machine.
- Deploy the 6.2.1 OVA file.
- Transfer the keytab file from the local computer to the 6.2.1 OVA. Copy the keytab file at the same location as before.
- Upgrade to ACE 6.2.1.

Related Links

Installation and deployment considerations on page 23

Applying the post installation patch

Note:

The following procedure is applicable only for users with Israel Daylight Saving Time.

About this task

You must perform the following procedure after you install or upgrade Agile Communication Environment™ 6.2.1.

To install Israel Daylight Saving Time settings on ACE 6.2.x, an additional RHEL rpm is required. You must also update the Java version.

Procedure

1. Download **ACE_DST_Updatev1.tar.gz** from PLDS. The ID is ACE000000040.
2. Create the `/opt/avaya/dst` directory, type the **`mkdir`** command.
3. Upload **ACE_DST_Updatev1.tar.gz** to `/opt/avaya/dst`.
4. Type the **tar -xvf ACE_DST_Updatev1.tar.gz** command to explode the tarball.

Comments on this document? infodev@avaya.com

5. Download *jtzu-1.6.13d.zip* from http://www.ibm.com/developerworks/java/jdk/dst/jtzu.html.
6. Copy the zip file to `/opt/avaya/dst/ACE_DST_Updatev1` and type the **`unzip jtzu-1.6.13d.zip`** command to unzip *jtzu-1.6.13d.zip*.
7. Type the **`cd /opt/avaya/dst/ACE_DST_Updatev1`** command to change the directory.
8. Type the **`./UpgradeACEDSTv1.sh`** command to install the DST patch.

Note:

You must apply this patch to both standalone and high-available deployments. For high availability deployment, you must apply the patch to Node A and then Node B.

Related Links

Installation and deployment considerations on page 23

Applying patch to prevent the Shellshock security threat

About this task

You must perform this task to prevent the security threat posed by Shellshock Bash injection.

Note:

You must apply this patch to both the standalone and high-available deployments. For high availability deployments, you must apply the patch to Node A and then to Node B.

Procedure

1. Download `ACEShellShockFix.tar.gz` from the PLDS website.

   The ID is **ACE000000050**.
2. Login to the Agile Communication Environment™ terminal by using PUTTY or a similar software.
3. Do one of the following:
   - Use sysadmin credentials to login to root, and enter **`su -`**.
   - If you do not use sysadmin credentials, login to the terminal using root credentials.
4. Go to **`cd /opt/avaya`**.
5. Upload the Agile Communication Environment™ tar ball to `cd /opt/avaya`.

   Use WinSCP or a similar client to upload the file.
6. Run the **tar -xvf ACEShellShockFix.tar.gz** command.
7. Go to `cd /opt/avaya/ACEShellShockFix`.
8. Run the **`./fixShellShock.sh`** command.

Related Links

Installation and deployment considerations on page 23

Comments on this document? infodev@avaya.com

Chapter 10: Provisioning considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) provisioning.

Related Links

Some SIP interfaces do not use ssl on page 29
Unable to edit provider on Avaya ACE GUI on page 30

Some SIP interfaces do not use ssl

Currently some of the SIP interfaces on ACE do not use secure signaling.

The requirement for using secure signaling is applicable for the AS5300 and CS2100 network elements that ACE interfaces with.

It is not applicable to the Cisco Unified Communications Manager since it is not an Avaya product.

Tracking number

ACECORE-13417/ACE-11717

Impact

You cannot add a white space character in the URI request for the following parameters,:

- called party parameter of a Third party Call (v2)
- second participant of a Third Party Call (v3)

Workaround

None

Related Links

Provisioning considerations on page 29

Unable to edit provider on Avaya ACE GUI

After posting the list of provisioned ACE service providers, unable to edit provider on Avaya ACE GUI by clicking the enabled **Edit** button, regardless of whether the provider status is `In Service` or `Disabled`.

In addition, after posting the edit page for some providers, the **Update** button on said page is enabled despite not having the ability to edit any settings.

Tracking number

ACECORE-12988/ACE-11595

Impact

The user thinks he can update the provider configuration but some provider configuration fields are not editable. This would misleading for user.

Workaround

None

Related Links

Provisioning considerations on page 29

Comments on this document? infodev@avaya.com

Chapter 11: Avaya ACE GUI and OAM considerations

There are no known issues related to Avaya Agile Communication Environment™ (ACE) graphical user interface (GUI) and operations, administration, and maintenance (OAM) tasks performed using the ACE GUI.

Related Links

Provisioning of provider in OAMP on Google Chrome does not work on page 31
Unreliable certificate management on page 31

Provisioning of provider in OAMP on Google Chrome does not work

Although the provisioning of a provider (AURA - SIP TLS) on the oamp is successful, the provider does not appear on OAM.

Tracking number

ACECORE-13289/ACE-11532

Impact

None.

Workaround

None. Google Chrome is not a supported browser. For a list of supported browsers, see, *Avaya Agile Communication Environment™ Planning and Installation* (NN10850–004).

Related Links

Avaya ACE GUI and OAM considerations on page 31

Unreliable certificate management

ACE OAMP (GUI) became inaccessible after a certificate deletion from the GUI.

Scenario:

- Administrator logs on to ACE console via https://<ip_or_fqdn>:9449/oamp>
- Navigates to **Security** > **Certificate management** > **System Manager Certificates**.
- Clicks **Delete** on the page.

Result:

Page goes inaccessible

Tracking Number

ACE-11659

Impact

Administrator will not be able to use the Operation and Management console of ACE.

Workaround

Perform the following steps:

1. Connect to terminal session of the ACE machine. For example, through a PuTTY session.
2. Enter the credentials.
3. Type the following commands:
   a. `cd /opt/avaya/ace/bin`
   b. `./deleteCertificates.sh <was_admin_id> <was_admin_password>`

   Where, *was_admin_id* is the Websphere administrator user name and *was_admin_password* is the associated password.

The above shell script displays success message on the console.

Key output statements to be looked at on the console are :

```
ACE ssl configuration is modified to default
SMGR CA certificate and SMGR personal certificate are deleted
```

Related Links

Avaya ACE GUI and OAM considerations on page 31

Comments on this document? infodev@avaya.com

Chapter 12: Third Party Call considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) Third Party Call web service.

Related Links

Third Party Call v2 and v3 do not support the whitespace character for the called party and second participant in the URI for WSDL requests on page 33

Display on the Calling and Called Party devices is incorrect when a TPC v2 call is initiated from ACE on page 34

Third Party Call v2 and v3 do not support the whitespace character for the called party and second participant in the URI for WSDL requests

For the called party in Third Party Call v2 and the second participant in Third Party Call v3, having a %20 (whitespace) in the URI will cause the URI to be recognized as invalid. For example:

```
<loc:calledParty>sip:steve@avaya.com?user=dave%20lee</loc:calledParty>
```

Tracking number

ACECORE-7030/ACE-11633

Impact

Customers will currently be unable to have whitespace for called party in Third Party Call v2 and second participant in Third Party Call v3 in the URI for WSDL requests.

Workaround

No workaround at this time.

Related Links

Third Party Call considerations on page 33

Display on the Calling and Called Party devices is incorrect when a TPC v2 call is initiated from ACE

Tracking number

ACE-11516

Impact

The display on the Calling and Called Party devices is incorrect when a TPC v2 call is initiated from ACE. This is applicable for the TR/87 provider using AES / CS1K configuration.

This issue affects:

- Calls between SIP client to H.323 client. Here, only the SIP client has the issue.
- Call forward, redirect, consult & single step transfer scenarios as well.

This issue does not affect:

- Calls between a H.323 client to a SIP client
- Calls between two H.323 clients
- TPCv2 makeCall (H.323 to H.323) scenarios

Workaround

None

Related Links

Third Party Call considerations on page 33

Chapter 13: Third Party Call Extensions considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) Third Party Call Extensions web service.

Related Links

Single step transfer operation on JTAPI provider in ACE succeeds but throws exceptions in the log on page 35
endCall does not clear all parties in a conference when the consultCall is made with conferenceOnly option on page 36
Missing notification events during singleStepTransfer on page 36

Single step transfer operation on JTAPI provider in ACE succeeds but throws exceptions in the log

Scenario:

Set up CCM JTAPI service provider

Make Call from A to B, send Answer Call on B

Single Step Transfer B to C

all operations work, but exception is thrown in `cmf/JtapiCcm.log`

Tracking number

ACECORE-13293

Impact

There is no functionality impact but exception gets printed in the log.

Workaround

None

Related Links

Third Party Call Extensions considerations on page 35

endCall does not clear all parties in a conference when the consultCall is made with conferenceOnly option

In a **consultCall** operation using conferenceOnly as the consultOption with stations A, B and C.

A - CS1k, B - Aura SIP, C - Aura SIP.

ACE **endCall** does not clear all parties in the conference, leaving A and C still on call.

Scenario:

Perform the TPCv2 operation, **makeCall**, between Party A(CS1k) and Party B(Aura) (CallID 1) using ACE.

Perform the TPCExtensions operation, **consultTransfer** with conferenceOnly from Party B(Aura) to Party C(Aura)(CallID 2)

Perform the TPCExtensions operation, **consultComplete**

Perfom **endCall**(CallID 1)

Tracking number

ACECORE-13400/ACE-11572

Impact

Applications using ACE **consultTransfer** or **consultComplete** using a CS1k DN as the Calling party will see two parties still on call (A and C) after using ACE **endCall**.

Workaround

None

Related Links

Third Party Call Extensions considerations on page 35

Missing notification events during singleStepTransfer

Setup:

- Configure Aura TR87 service provider for **singleStepTransfer** and for callID-based notifications
- Configure CS1000 v2 SIP service provider for TPCv2 **makeCall**
- H.323 endpoints: DN2, DN3
- CS1000 endpoint: DN1
- Make TPCV2 **makeCall** between DN1 and DN2 and start callID based notifications **startCallNotification**
- Answer DN2 -Do **consultationCall** (DN2 to DN3), do not answer DN3

Comments on this document? infodev@avaya.com

- Do **consultationComplete**, do not answer DN3
- Do an **endCall** using the callID from notification event for DN2

Expected result:

After **endCall**, entire call should be terminated and there should be no active call on DN1, DN2 and DN3

Actual result:

Call is terminated on DN1 but call is still active between DN2 and DN3. When DN2 is hung up DN3 still rings.

Tracking number

ACECORE-13315/ACE-4

Impact

The **endCall** operation does not terminate the entire call.

Workaround

Manually disconnect the call from the phone.

Related Links

Third Party Call Extensions considerations on page 35

Comments on this document? infodev@avaya.com

Chapter 14: Call Notification considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) Call Notifications web service.

Related Links

Third Party Call Extensions (v2.0) related Call Notifications (v3.8) for interprovider calls have improper Called Party URI on page 38

Call Notifications (v3.8) for interprovider calls will have calling party appended with “phone-context=dialstring” on page 39

ACE sends Disconnect notification to listener when Busy on a call on page 39

TPCv2 and Call Notification v3.8 have issues when forwarded DN is busy on Aura TR/87 and SIP one-X clients on page 40

Unreachable event not received when called party is unreachable in Session ID based Call Notification v3.8 on page 40

Call ID Pariticpant based Call notifications contain multiple participant entries for PSTN numbers on page 41

Duplicate notifications received when using H.323 clients in singleStepTransfer on page 41

Call Notification clients do not receive No Answer events when a call to a transferredTo party times out on page 42

Wrong notification in a call forward scenario, Not Reachable instead of Busy notification on page 42

Third Party Call Extensions (v2.0) related Call Notifications (v3.8) for interprovider calls have improper Called Party URI

Call Notifications regarding TPCV2 Extension services (`ConsultCall`, `CallForward` and `SingleStepTransfer`) have HLOC prefixed to called party number and missing URI scheme (tel).

Tracking number

ACECORE-6295/ACE-11774

Impact

For inter provider calls, `ConsultCall`, `CallForward` and `SingleStepTransfer` operations fail.

Workaround

Add Reverse Translation rule which removes HLOC and prefixes URI Scheme.

1. On the Avaya Avaya ACE GUI, under the **Configuration** menu, select **Service Providers**.
2. Select the service provider and then click **Rules**.
3. Select the **Reverse Transformation** check box and complete the required fields.

Related Links

Call Notification considerations on page 38

Call Notifications (v3.8) for interprovider calls will have calling party appended with “phone-context=dialstring”

When subscribing for notifications (DN based or callid based) using the default address direction Called, the calling party notifications have `";phone-context=dialstring"` appended to the URI.

Tracking number

ACECORE-6294/ACE-11886

Impact

Call Notification (v3.8) display contains extra characters.

Workaround

No workaround at this time.

Related Links

Call Notification considerations on page 38

ACE sends Disconnect notification to listener when Busy on a call

When a call is made to a DN which is Busy (already in another call), Busy followed by Disconnect notifications are sent to the calling party listener. However, after about 25 seconds a Disconnect notification is also sent for the called party listener even though that party never entered the call. This Disconnect event has the call ID of the failed call.

Tracking number

ACE-11684

Impact

The application listening to events on the called party might be confused with the unexpected Disconnect event and might consider it to be a Disconnect for the ongoing call.

Workaround

Applications should consider the call ID field along with the type of event.

Related Links

Call Notification considerations on page 38

TPCv2 and Call Notification v3.8 have issues when forwarded DN is busy on Aura TR/87 and SIP one-X clients

In a **`CallForward`** scenario with Party B forwarded to Party C with Call Notification subscriptions to all parties, when an ACE **`makeCall`** is made between Part A and Party B, **`getCallInformation`** reports `CallingPartyBusy` as the Call termination reason.

Tracking number

ACECORE-12399/ACE-11519

Impact

Application listeners trying to verify the status of the call will receive wrong notifications about the status of Party A.

Workaround

None

Related Links

Call Notification considerations on page 38

Unreachable event not received when called party is unreachable in Session ID based Call Notification v3.8

On Aura TR87 and SIP One-X clients, an ACE MakeCall to an unreachable number using Session Id based embedded TPC notifications, an unreachable participant event is not notified to the listener.

Tracking number

ACECORE-12401/ACE-11604

Impact

Application listeners will not receive the NotReachable CallEvent

Comments on this document? infodev@avaya.com

Workaround

None.

Related Links

Call Notification considerations on page 38

Call ID Pariticpant based Call notifications contain multiple participant entries for PSTN numbers

`redirectCall` and **`consult Call`** Call ID Pariticpant based Call notifications contain multiple participant entries for PSTN numbers

Tracking number

ACECORE-13235/ACE-11587

Impact

There will be an additional participant in the call that might confuse to the Applications call modelling.

Workaround

None.

Related Links

Call Notification considerations on page 38

Duplicate notifications received when using H.323 clients in singleStepTransfer

In an Aura TR/87 ACE call with **`singleStepTransfer`** and CallId based notifications, after **`singleStepTransfer`**, there is a set of duplicate notifications sent to the client, with the new *participant*(transferred-to) as *CallParticipantInitial*.

Scenario:

Third Party Call v2**`makeCall`** (A(Aura) to B(Aura))

`startCallNotification` (addresses: callID, criteria: Participant)

Make sure call is connected

`singleStepTransfer` (B to C)

Make sure call is connected

endCall

stopCallNotification

Tracking number

ACECORE-13308/ACE-11675

Impact

Client application listeners will see a set of duplicate notifications when Party C rings.

Workaround

No work around yet.

Applications can have a logic to ignore events if they are the same as the one received previously.

Related Links

Call Notification considerations on page 38

Call Notification clients do not receive No Answer events when a call to a transferredTo party times out

In a single step transfer call scenario, where A calls B, B transfers the call to C, and the call times out, the notification listener against party A does not get the No Answer event when the call times out.

Tracking Number

ACE-12553

Impact

ACE call notification clients on single step transfer event calls.

Workaround

None

Related Links

Call Notification considerations on page 38

Wrong notification in a call forward scenario, Not Reachable instead of Busy notification

In a Call Forward - MakeCall scenario, party A calls Party B, and B has set call forward to Party C. If Party C is busy on all lines, the notification ACE sends is *Not Reachable* instead of *Busy*.

Tracking Number

ACE-12542

Impact

ACE call notification clients who receive *Busy* notification.

Workaround

None

Related Links

Call Notification considerations on page 38

Chapter 15: Call Forwarding considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) Call Forwarding web service.

Related Links

Incomplete notifications for Call forwarding or redirectCall on page 44

Incomplete notifications for Call forwarding or redirectCall

Call ID based notifications for the call forwarded or redirected SIP calls are not supported. This means that the notification events will not contain the **`forwarded To`** party information.

Tracking number

ACECORE-13187/ACE-11570

Impact

Any SIP call forwarded calls subscribing for call-id based notifications will not get the **`forwarded To`** party information in the Call notification events.

For example:

- DN2 has set call forward or redirect to DN3
- DN1 calls DN2

Call notification events contain DN2 instead of DN3 that answered the call.

Note:

Avaya ACE does not support Call forwarding for SIP providers. The scenario mentioned here is when the Call Forwarding is done at the PBX level itself. For more information on services supported by various service providers, see *Tables of Avaya ACE supported services by service provider type* in *Avaya Agile Communication Environment™ Web Services* (NN10850–007).

Work around

None.

Related Links

Call Forwarding considerations on page 44

Chapter 16: Presence considerations

There are no known issues related to Avaya Agile Communication Environment™ (ACE) Presence web service.

Comments on this document? infodev@avaya.com

Chapter 17: Endpoint display considerations

This section contains information about all known issues related to endpoint displays.

Related Links

Calling party phone does not display called party number in a TPCv2 makeCall on page 46

Calling party phone does not display called party number in a TPCv2 makeCall

In an Aura TR/87 ACE **`makeCall`** between a CS1k DN (Calling party) and Aura DN (Called party), the display of Calling Party (CS1k) does not get updated properly.

Scenario:

`makeCall` from A (CS1k) to B (Aura), make sure call is connected.

`endcall`

Tracking number

ACECORE-13258/ACE-11716

Impact

Calling party phone does not display the called party number in ringing and connected state.

Workaround

None

Related Links

Endpoint display considerations on page 46

Comments on this document? infodev@avaya.com

Chapter 18: Foundation Toolkit considerations

This section contains information about known issues related to Avaya Agile Communication Environment™ (ACE) Foundation Toolkit.

Note:

If the Foundation Toolkit is deployed with Avaya Aura® Communication Manager, the Communication Manager must be at release 6.0.1 or higher.

Related Links

B2B Routing call fails when the calling and called party are sequenced to AAFT and CM on page 47

B2B Routing call fails when the calling and called party are sequenced to AAFT and CM

User setup:

calling party originating sequence: aaft client app + CM

calling party terminating sequence: CM

called party originating sequence: CM

called party terminating sequence: CM + aaft client app

AAFT client application uses B2B routing service.

When calling party calls called party, it gets a busy signal , or the call is setup briefly, then terminated.

Tracking number

ACECORE-10586/ACE-11601

Impact

The MAS media server does not support appending to a recording and therefore, this functionality cannot be exercised using the Foundation Toolkit API.

Workaround

None

Related Links

Foundation Toolkit considerations on page 47

Comments on this document? infodev@avaya.com

Chapter 19: Avaya Aura® service provider considerations

This section contains information about known issues related to the Avaya Aura® service provider.

Related Links

Avaya clients do not play Busy tone when a third party call is made to a busy line on page 49

SIP calls fail when AAFT and AURA SIP providers are both provisioned on page 50

Incorrect phone display when receiving call from thirdPartyCallController in a TPCv2/v3 makeCall on page 50

First call after a CTI link has been restored always fails when the call is made from Browser add-in on page 51

Call forwarding and redirectCall have issues when using H.323 clients on page 51

Avaya clients do not play Busy tone when a third party call is made to a busy line

Avaya clients do not play busy tone when a Third Party Call is established to a busy terminating line. This issue only affects Avaya service providers configured to use the `"Invite;Answer;Refer"` Make Call Sequence. Scenarios in which the terminating side of the call provides in-band busy treatment will also be unaffected.

Tracking number

ACECORE-4933/ACE-11631

Impact

The problem manifests as follows:

- Third Party Call is initiated through Avaya ACE, between an Avaya client and a busy subscriber.
- The originating Avaya client rings and the originating user answers. Call immediately drops and the originating client's display goes to an idle state, with no destination busy notification presented to the user.
- Desired behavior is that the Avaya client should present busy treatment to the user, in the form of a busy tone and optionally a message on the Avaya client's screen.

Workaround

None

Related Links

Avaya Aura service provider considerations on page 49

SIP calls fail when AAFT and AURA SIP providers are both provisioned

SIP calls fail with `Indeterminate originating entity` error when AAFT and AURA SIP providers are both provisioned.

Tracking number

ACECORE-12641/ACE-11636

Impact

Network initiated SIP calls will fail for Aura SIP provider when an Aura FT provider is also provisioned on ACE. Though ACE initiated calls work fine it is recommended to disable Aura FT provider while using Aura SIP provider.

Workaround

- Disable Aura FT provider while making SIP calls using Aura SIP provider.
- When using AAFT applications ensure that the entity-link created from Session Manager uses the port 5063 on ACE.

Related Links

Avaya Aura service provider considerations on page 49

Incorrect phone display when receiving call from thirdPartyCallController in a TPCv2/v3 makeCall

When a TPC call is made from ACE using Aura v2 SIP TLS service provider ,calling party shows an incorrect display name.

Tracking number

ACECORE-13092/ACE-11520

Impact

It will be not known from where the call has come from.

Workaround

None. CM ticket raised for this issue.

Comments on this document? infodev@avaya.com

Related Links

Avaya Aura service provider considerations on page 49

First call after a CTI link has been restored always fails when the call is made from Browser add-in

First call fails from the browser add-in when CTI link in CM is brought down. End user must launch a second call before the functionality is restored.

Tracking number

ACECORE-13038/ACE-11580

Impact

First call will always fail after the CTI link is down.

Workaround

None.

Related Links

Avaya Aura service provider considerations on page 49

Call forwarding and redirectCall have issues when using H.323 clients

When a CallForward is set on Party B to Party C and an ACE TPC v2 makeCall is made between Party A and Party B, the calling party display phone shows Party B as Called instead of Party C. The Called party, Party C, display phone shows Party B as Calling instead of Party A.

Tracking number

ACECORE-13133/ACE-11616

Impact

ACE applications and OneX soft or hard clients will be notified incorrectly about the other connection involved in the call.

Workaround

None.

Related Links

Avaya Aura service provider considerations on page 49

Chapter 20: CS 1000 service provider considerations

This section contains information about known issues related to the Avaya Communication Server 1000 service provider.

Related Links

[No busy notification for a network initiated call to a monitored DN on a CS 1000 TR/87 provider](#) on page 52
[Failed to CallSender when ACE SIP Interface makecall from CS1K set to MM then CallSender to BCM set](#) on page 53
[Multiple transfers on a CS1000 provider results in inconsistent behavior](#) on page 53

No busy notification for a network initiated call to a monitored DN on a CS 1000 TR/87 provider

If a user makes a network initiated call to a monitored DN, the call fails to establish when the DN is busy. However, no Call Notification Busy event is sent to the application monitoring this DN. Instead, a disconnect event is sent when the call fails.

This issue only occurs on the CS 1000 TR/87 provider.

Tracking number

ACECORE-7681

Impact

The application does not receive the Busy event, and does not know why the call was terminated.

Workaround

No workaround at this time.

Related Links

[CS 1000 service provider considerations](#) on page 52

Failed to CallSender when ACE SIP Interface makecall from CS1K set to MM then CallSender to BCM set

Configuration:

1. Configure SIP trunk from CS1K7.6 to SM
2. ACE SIP Interface

Procedure:

1. Construct and send makeCallSession request to ACE to make call between CS1K DN and Modular Messaging
2. CS1K user logins its mailbox on MM to check message then presses 88 to make call back to the called through CallSender application to BCM EndPoint that had left a voicemail
3. BCM DN answers the call.

Observation: Call is dropped immediately.

Tracking number

ACECORE-13161/ACE—11678

Impact

Can not initiate a call back through ACE between CS1K DN & MM to reach back to the caller.

Workaround

This issue doesn't happen when CS1K DN calls directly to MM without ACE.

Related Links

CS 1000 service provider considerations on page 52

Multiple transfers on a CS1000 provider results in inconsistent behavior

Description

When multiple transfers are made on a CS 1000 service provider, the original participants of the call are shown as active praticipants in the call, even though they are no longer in the call.

Tracking number

ACE-12457

Impact

If the customer is using the GoogleApps integration feature of ACE with Esna software and if there are multiple transfers performed in the same call, the ILync client pop ups are inconsistent and end call operation from ILync client fails.

Workaround

None

Related Links

CS 1000 service provider considerations on page 52

Comments on this document? infodev@avaya.com