Avaya Aura® Application Server 5300
Administration
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 modify changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of 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), 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 is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicensesInfo under the link “Heritage Nortel Products” or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment.
Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

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

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

Third Party Components
“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya’s website at: https://support.avaya.com/ Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms. The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD (“AVC VIDEO”) AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

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

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

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

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

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

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

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

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

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

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

Avaya is a registered trademark of Avaya Inc.

AVAYA

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. Java is a registered trademark of Oracle and/or its affiliates.
Contents

Chapter 1: New in this release ............................................................................................................. 9
  Features .............................................................................................................................................. 9
  Document changes since last issue ................................................................................................. 9
  Other changes ................................................................................................................................. 9

Chapter 2: Introduction .......................................................................................................................... 11

Chapter 3: Backup and restore ............................................................................................................. 13
  Backup and restore overview ........................................................................................................... 13
  Backup jobs ........................................................................................................................................ 14
  Backup sets ......................................................................................................................................... 15

Chapter 4: Remote backup parameter configuration .............................................................................. 17
  Using the configuration script help ................................................................................................. 18
    Using the Configuration script help job aid ................................................................................ 18
    Using the configuration script help example job aid ................................................................... 18
  Listing backup sets for a job ............................................................................................................ 19
  Configuring remote backup and restore parameters ....................................................................... 20
  Regenerating or verifying the SSH keys for remote backup and restore ........................................ 22
  Cleaning up SSH keys ....................................................................................................................... 24
  Restoring the default backup configuration ..................................................................................... 24
  Viewing the current backup configuration ......................................................................................... 25
    Viewing the current backup configuration job aid ....................................................................... 26

Chapter 5: System backup ................................................................................................................... 27
  System backup tasks ........................................................................................................................ 28

Chapter 6: Server backup and platform backup .................................................................................. 29
  Server backup and platform backup procedures ............................................................................... 29
    Server backup and platform back up job aid ................................................................................ 29
  Backing up server data or platform data remotely ........................................................................... 30
  Backing up server data or platform data locally .............................................................................. 31
  Removing unneeded loads from the EM Servers ............................................................................ 32
    Variable Definitions ....................................................................................................................... 32

Chapter 7: Database backup ................................................................................................................. 33
  Database backup procedures ........................................................................................................... 33
  Backing up a database manually ....................................................................................................... 34
  Scheduling database backups ......................................................................................................... 35
  Removing a scheduled backup .......................................................................................................... 36

Chapter 8: FSI backup .......................................................................................................................... 37
  Backing up FSI baseline files remotely ............................................................................................ 37
  Backing up FSI baseline files locally ............................................................................................... 38

Chapter 9: Security logs backup ......................................................................................................... 39
Contents

- Backing up security logs to a remote server .......................................................... 39
- Backing up security logs locally .............................................................................. 40

Chapter 10: Backup script help .............................................................................. 41
  - Using the backup script help .................................................................................. 41
    - Using the backup script help job aid .................................................................. 41
  - Limiting bandwidth for backup operations ............................................................ 42

Chapter 11: System restore ...................................................................................... 43
  - System restore tasks ............................................................................................. 43

Chapter 12: Platform data restore ............................................................................ 45

Chapter 13: Server application data restore ............................................................ 46
  - Restoring server application data remotely ........................................................... 46
    - Restoring server application data remotely job aid ......................................... 47
  - Restoring server application data locally .............................................................. 47

Chapter 14: Non-EMS server restore ...................................................................... 49
  - Non-EMS server restore tasks .............................................................................. 49

Chapter 15: EMS server restore from an operational EMS server ......................... 52
  - EMS server restore from an operational EMS server tasks .................................. 52

Chapter 16: Double EMS server restore from a backup ........................................ 55
  - Double EMS server restore from a backup task .................................................... 55

Chapter 17: Avaya Media Server backup and restore ............................................. 58
  - Backing up an Avaya MS ...................................................................................... 58
  - Scheduling an Avaya MS backup .......................................................................... 59
  - Restoring an Avaya MS ......................................................................................... 60

Chapter 18: Common restore procedures ............................................................... 61
  - Restoring the primary EMS server ....................................................................... 61
  - Restoring the secondary EMS server ................................................................... 63
  - Synchronizing the primary and secondary databases ......................................... 64
  - Testing database replication ................................................................................ 65
  - Viewing database replication errors ..................................................................... 65
  - Restoring the database from a backup—missing data ......................................... 66
  - Restoring the database from a backup—double EMS server restore .................. 67
  - Extracting security records from a remote backup file .................................... 69
    - Extracting security records from a remote backup file job aid ....................... 70
  - Converting from a single database to a redundant database configuration ....... 70
  - Using the restore script help .............................................................................. 71
    - Using the restore script help job aid ................................................................. 72

Chapter 19: FSI restore .......................................................................................... 73
  - Restoring FSI baseline backups remotely ............................................................ 73
  - Restoring FSI baseline backups locally ............................................................... 74

Chapter 20: Application Server 5300 re-IP ............................................................ 75
  - Application Server 5300 re-IP procedures .......................................................... 75

Chapter 21: Avaya Media Server re-IP ................................................................. 77
## Chapter 22: Re-IP procedures
- Shutting down the application—core server .................................................. 80
- Shutting down the application—Avaya Media Server ...................................... 81
- Restoring the access control default configuration ......................................... 81
- Stopping the IPsec service ............................................................................... 81
- Performing a server re-IP ............................................................................... 82
- Updating IP addresses for the server ................................................................ 83
- Updating the hostname and clock source ....................................................... 83
- Updating the AS 5300 Element Manager and database IP addresses .............. 85
- Updating NE IP addresses, hostnames, and certificates .................................. 85
- Updating the Avaya Media Server IP addresses .............................................. 86
- Shutting down the application and the database ............................................ 87
- Configuring ACL ............................................................................................ 87
- Configuring IPSec ......................................................................................... 88
- Starting the application and the database ...................................................... 88

## Chapter 23: Power outage recovery
- Power outage recovery procedures .................................................................. 90
- Powering on the database server ..................................................................... 90
- Stopping and starting the database .................................................................. 91
- Verifying that the AS 5300 Element Manager processes are running ............... 92
- Stopping and starting the AS 5300 Element Manager ...................................... 92
- Verifying the status of other servers and components ..................................... 93

## Chapter 24: Network data management
- Enabling HTTP DoS mitigation ...................................................................... 97
- Enabling SIP DoS mitigation .......................................................................... 97
- Editing the IP address table ............................................................................. 97
- Configuring a trusted node ............................................................................. 98
  - Informational elements job aid ..................................................................... 99
  - Configuring a trusted node job aid ................................................................. 99
- Configuring an external node ......................................................................... 100
  - Configuring an external node job aid ............................................................. 101
- Deleting an external node ............................................................................. 101
- Configuring an informational element ........................................................... 101
  - Configuring an informational element job aid ............................................. 102
- Deleting an informational element ................................................................ 103
- Configuring an SNMP profile ....................................................................... 103
  - Configuring an SNMP Profile job aid ............................................................ 104
- Deleting an SNMP profile ............................................................................ 104
- Configuring a site .......................................................................................... 105
  - Configuring a site job aid ........................................................................... 105
- Deleting a site ............................................................................................... 106
- Updating a license key .................................................................................. 106
Querying a license key: 107

Chapter 25: Network element management: 108
- Deploying and starting the primary AS 5300 Element Manager: 108
- Starting a network element: 109
- Stopping a network element: 110
- Deploying a network element: 110
- Undeploying a network element: 111
- Restarting a network element: 111
- Killing a network element: 112
- Deleting a network element: 113

Chapter 26: Accounting management: 114
- Enabling and disabling accounting processing rules: 114
  - Enabling and disabling accounting processing rules job aid: 115
- Accessing accounting files on the Accounting Manager: 115
- Deleting files on the Accounting Manager: 116

Chapter 27: Fault management: 117
- Enabling and disabling log processing rules: 117
  - Enabling and disabling log processing rules job aid: 118
- Monitoring a server: 118
  - Variable Definitions: 118
- Monitoring the database: 119
  - Monitoring the database job aid: 119

Chapter 28: Performance management: 120
- Enabling and disabling OM processing rules: 120
  - Enabling and disabling OM processing rules job aid: 121

Chapter 29: Avaya Media Server performance management: 122
- Monitoring performance statistics on the Avaya Media Server (MS): 122
- Monitoring active sessions on the Avaya Media Server (MS): 123
  - Changing Refresh Rate for active session monitoring: 123
- Monitoring active sessions: 123
- Filtering active sessions: 124
- Releasing active sessions: 124
- Muting and unmuting active sessions on the Avaya Media Server: 125
- Changing Time Stamps for active sessions: 125
Chapter 1: New in this release

The following sections detail what is new for Avaya Aura® Application Server 5300 Administration, NN42040-600 for Avaya Aura® Application Server 5300 Release 3.0.

Navigation

• Features on page 9
• Other changes on page 9

Features

For more information about the features that are new for this release, see Avaya Aura® Application Server 5300 Release Delta, NN42040-201.

Document changes since last issue

The following changes have been made to this document since it was issued for Application Server 5300 Release 3.0 in June, 2012:

• Added a statement to Stopping a network element on page 110, indicating that stopping an Avaya MS NE causes any in-progress conference recordings to be lost.

Other changes

The following other changes were made:

Revision history

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>Updated the legal page for Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>November 2012</td>
<td>Standard 04.03. This document is issued to support Avaya Aura® Application</td>
</tr>
<tr>
<td></td>
<td>Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>October 2012</td>
<td>Standard 04.02. This document is issued to support Avaya Aura® Application</td>
</tr>
<tr>
<td></td>
<td>Server 5300 Release 3.0.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Date</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2012</td>
<td>Standard 04.01. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
</tbody>
</table>
| August 2010| Standard 02.03. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. The following sections were updated:  
  - Updating IP addresses for the server on page 83  
  - Enabling and disabling accounting processing rules on page 114  
  - Enabling and disabling log processing rules on page 117  
  - Enabling and disabling OM processing rules on page 120  
  - Querying a license key on page 107  
  - Starting the application and the database on page 88  
  - Backing up a database manually on page 34  
  - Server backup and platform back up job aid on page 29 |
| May 2010   | Standard 02.02. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. The re-IP chapter is updated. |
| April 2010 | Standard 02.01. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. |
| June 2008  | Standard 01.01. This document is new for Nortel Application Server 5300 Release 1.0. |

Updated database backup and replication procedures in the following chapters:  
- Database backup on page 33  
- Common restore procedures on page 61
Chapter 2: Introduction

This document provides the procedures that you perform to administer the Avaya Aura® Application Server 5300 (AS 5300) system. This document does not include information about Primary Rate Interface (PRI) gateway, or Integrated Access Device (IAD) administration.

⚠️ Important:
Throughout the procedures in this document, for each individual user account, the corresponding preconfigured user account appears in parenthesis ( ). For example: Log on to the server as an SSA.

For more information about individual and group (preconfigured) user accounts, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Prerequisites
- You are familiar with the AS 5300 Element Manager Console. For more information about using the AS 5300 Element Manager Console, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.
- You are familiar with the Provisioning Client. For more information about using the Provisioning Client, see Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112 and Avaya Aura® Application Server 5300 Security, NN42040-601.

Navigation
- Backup and restore on page 13
- Remote backup parameter configuration on page 17
- System backup on page 27
- Server backup and platform backup on page 29
- Database backup on page 33
- FSI backup on page 37
- Backing up security logs to a remote server on page 39
- Backup script help on page 41
- System restore on page 43
- Platform data restore on page 45
- Server application data restore on page 46
- Non-EMS server restore on page 49
- EMS server restore from an operational EMS server on page 52
Introduction

- Double EMS server restore from a backup on page 55
- Common restore procedures on page 61
- FSI restore on page 73
- Application Server 5300 re-IP on page 75
- Avaya Media Server re-IP on page 77
- Re-IP procedures on page 79
- Power outage recovery on page 90
- Network data management on page 96
- Network element management on page 108
- Accounting management on page 114
- Fault management on page 117
- Performance management on page 120
Chapter 3: Backup and restore

This chapter provides background and supporting information for backup and restore operations on the following supported hardware platforms:

- IBM System x3550
- HP ProLiant DL360 G7

Prerequisites

- The server network interfaces are configured to full-duplex, and connected by a live Ethernet connection.
- SSH is installed on the remote backup server, and pass phrase authentication is enabled. The supported operating systems (OS) for the backup server are:
  - Linux RHEL3, RHEL4, RHEL5, and Fedora Core
  - HPUX

⚠️ Important:
Because of processing capacity and space requirements, Avaya recommends that you do not use the backup server to host Application Server 5300 components.

Avaya recommends that the target directory on the remote backup server have at least 200 gigabytes (GB) of free space.

- The remote backup directory has 100 gigabytes (GB) of free space.
- The remote backup server must be a trusted node.

Navigation

- [Backup and restore overview](#) on page 13
- [Backup jobs](#) on page 14
- [Backup sets](#) on page 15

Backup and restore overview

The backup and restore command names, which appear in the following sections, are actually Linux shell aliases for commands that you invoke with sudo privileges. For example, bkupSvr is an alias for sudo /usr/local/bin/bkupSvr.pl. Sudo requires that users authenticate with a password. After successful authentication, you can use sudo (without entering your password) for a short period of...
time. After this time interval expires, you receive a prompt for the password. This behavior causes password prompting at various intervals.

Two methods exist, by which you can log on to the Application Server 5300 servers:

- A secure shell session (SSH) through the network interface of the server. If the SSH session drops, the associated process ends as well.
- The out-of-band Management Network connection to the x3550 Remote Supervisor Adapter (RSA) card.

⚠️ Important:

The first time a server communicates with another server over SSH, the following message appears:

The authenticity of host '47.104.22.132 (47.104.22.132)' can't be established.
Are you sure you want to continue connecting (yes/no)?

If the RSA fingerprint is correct, at the prompt, enter yes. If you cannot verify the RSA fingerprint, contact your system administrator for guidance.

Backups include only data that is unique to each server. Backups do not include data that you can easily retrieve from an installation CD. The restore process uses the unique previously backed up server data in conjunction with the installation CDs to perform the restore. This strategy reduces the amount of time and system resources required for backup.

⚠️ Important:

The IPv6 server and service address configuration are not part of the backup and restore process.

⚠️ Important:

Direct backup to and restore from a tape drive or CD is not supported. You can archive backup files to tape or CD by using internal site procedures.

The following list provides an overview of the backup and restore process:

- For each server, configure the remote backup parameters.
- Create primary database server backups daily.
- Create other server backups after you make major changes.
- Use the server backups to recover from a server failure, or loss of database data.

---

**Backup jobs**

Backup operations are divided into separate backup jobs. Each backup job predefines the data to be backed up and the users who can perform the backup. By default, all backup job types use a
default backup configuration, which includes the remote server address, (backup to) directory, remote user ID and pass phrase. The System Security Administrator (SSA) has the option of defining individualized backup configurations for specific backup job types.

The backup and restore jobs are:

- Platform Backup parameter configuration
- Platform Backup—performs a backup of only the platform data. This includes the contents of the /admin directory structure.
- Server Backup (svr)—backs up the data required to restore an server to an operational state. Server Backup includes the platform backup, the database backup, and the application backup. The backup also includes the configuration data for the OSSEC HIDS agent that is stored in the `/opt/mcp/ossec/etc/ossec.conf` file. The database backup includes the snapshots of the database backups stored in the `/var/mcp/db/backup` directory. You can use the database backups to restore the database if both the primary and the secondary database are lost. (You can back up the database only as part of Server Backup.)
- File System Integrity (FSI)—backs up the file system integrity baselines (not required to restore the server operating state).
- Security Log (seclog)—backs up the security logs (not required to restore the server operating state). You can expand a log backup file on a different server to view the contents.

The server and platform backup jobs are the core backup jobs that you require to complete the restore process.

Backup sets

The server backup job can create five different backup sets, and each backup set produces a tar file:

- Platform—mcpPlatform.<host name>.<date/time stamp>.tar
- Application—mcpApp.<host name>.<date/time stamp>.tar
- Load—mcpLoad.<host name>.<date/time stamp>.tar
- Database—mcpDb.<host name>.<date/time stamp>.tar
- Avaya Media Server (MS)—mcpMAS.<host name>.<date/time stamp>.tar

The server backup job creates the following three backup sets, only if the relevant information is present on the server.

- Application (mcpApp)—generated only for a server that hosts an AS 5300 Element Manager
- Database (mcpDB)—generated only for a server that hosts a database
- Avaya Media Server (MS) (mcpMAS)—generated only for a server that hosts an Avaya Media Server (MS)

The platform backup job creates one backup set that includes all the administrative data required to restore the platform to its previous state. The platform backup is provided for use when not much
has changed on the server (in the db/load area) but you require a quick backup of the administration data. The platform backup is very quick and produces a smaller amount of data than the server backup. The single backup set produces a single tar file.

The restore process allows restoration of any combination of backup sets.

**Important:**

The backup does not include the antivirus configuration.

The platform backup set includes all of the data to restore the server platform. Most of the data resides in the /admin partition, but the backup also includes the following data:

- user information
- password configuration (pwconfig settings)
- IPSec-related information
- Access Control information
- database configuration
- FCheck config file
- remote configuration parameters for backup and restore operations except for SSH keys: Remote SSH backup operation is unconfigured after restoration; the remote IP address, target directory, and remote userid are restored.
- Banners: Motd and Issue

The application backup set includes all the data in the following directories:

- /var/mcp/loads
- /var/mcp/media
- /var/mcp/install

The application backup set includes all of the data required to recreate the load and deployment information for the server if it is a primary or secondary Element Management System (EMS) server. The EMS hosts the AS 5300 Element Manager (MCP EM) network element (NE). Backup and restore of the application data for all other servers is not required.
Chapter 4: Remote backup parameter configuration

The Security System Administrator (SSA) must configure remote backup parameters before you can perform the following tasks:

- remote backup
- remote restore
- transfer of a local backup to a remote server

After you complete the remote backup parameter configuration, it applies to all subsequent remote backup and restore operations.

**Important:**

Only the owner of the backup tar file (the remote user specified during the backup configuration) can change the ownership on the contents of a tar file backed up to a remote server.

To configure remote backup parameters, you can use the configBkup script. The configBkup script configures remote parameters for all backup jobs: platform backup, server backup, file system integrity (FSI) backup, and security log backup.

Four other configuration scripts exist: configPlatformbkup, configSvrBkup, configFSIBkup, and configSecLogBkup. If an individual backup job requires unique remote backup parameters, you can run one of these four configuration scripts.

Note that the SSA must generate new SSH keys after a server restore.

**Navigation**

- Using the configuration script help on page 18
- Listing backup sets for a job on page 19
- Configuring remote backup and restore parameters on page 20
- Regenerating or verifying the SSH keys for remote backup and restore on page 22
- Cleaning up SSH keys on page 24
- Restoring the default backup configuration on page 24
- Viewing the current backup configuration on page 25

**Related links**

- Using the configuration script help on page 18
- Listing backup sets for a job on page 19
Using the configuration script help

About this task
Use this procedure to obtain help with the configuration script.

Prerequisites

- You are an SSA with sudo access.

Procedure
Use the -h command line parameter when you run the configuration script.

<table>
<thead>
<tr>
<th>Obtain help with</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring parameters for all backup jobs</td>
<td>configBkup -h</td>
</tr>
<tr>
<td>Configuring parameters for platform backups</td>
<td>configPlatformBkup -h</td>
</tr>
<tr>
<td>Configuring parameters for server backups</td>
<td>configSvrBkup -h</td>
</tr>
<tr>
<td>Configuring parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup -h</td>
</tr>
<tr>
<td>Configuring parameters for security log backups</td>
<td>configSecLogArchive -h</td>
</tr>
</tbody>
</table>

Using the Configuration script help job aid
This job aid provides additional usage information.

Usage: configBkup <-d debugLevel> <-s v[vv]> <-h>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-d &lt;0</td>
<td>1</td>
</tr>
<tr>
<td>-s&lt;SSHParm&gt;</td>
<td>Only for use by Avaya Support.</td>
</tr>
<tr>
<td>-h</td>
<td>Use to print usage information.</td>
</tr>
</tbody>
</table>

Using the configuration script help example job aid
The following job aid is an example of the screen output from the configSvrBkup script. Other backup job configuration scripts produce similar output.
Listing backup sets for a job

About this task

Use this procedure to list and view the backup sets and the list of directories backed up for each job.
Prerequisites

- You are an SSA with sudo access.

Procedure

1. Log on to the server as an SSA.
2. Run the configuration script.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure parameters for all backup jobs</td>
<td>configBkup</td>
</tr>
<tr>
<td>Configure parameters for platform backups</td>
<td>configPlatformBkup</td>
</tr>
<tr>
<td>Configure parameters for server backups</td>
<td>configSvrBkup</td>
</tr>
<tr>
<td>Configure parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup</td>
</tr>
<tr>
<td>Configure parameters for security log backups</td>
<td>configSecLogArchive</td>
</tr>
</tbody>
</table>

3. If you receive a password prompt, enter your password.
4. To list the backup sets, enter 1.

The list of backups sets appears with a list of directories included for backup for each set.

Configuring remote backup and restore parameters

About this task

Use this procedure to configure remote backup parameters (IP address, user ID, remote backup directory, and SSH keys) for the following backup and restore jobs:

- all backup jobs
- platform backup jobs
- server backup jobs
- file system integrity (FSI) baselines
- security log backup jobs

After you configure these parameters, they apply to subsequent backup and restore jobs, and transfers. Previously configured parameters are the defaults; each subsequent time you run the script, you receive a prompt to change each value.

Prerequisites

- You know the IP address, directory in which to place data, user ID, and password on the remote server.
- You are an SSA with sudo access.
- SSH is installed on the remote server and pass phrase authentication is enabled.
Procedure

1. Log on to the server as an SSA.
2. Run the configuration script:

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure parameters for all backup jobs</td>
<td>configBkup</td>
</tr>
<tr>
<td>Configure parameters for platform backups</td>
<td>configPlatformBkup</td>
</tr>
<tr>
<td>Configure parameters for server backups</td>
<td>configSvrBkup</td>
</tr>
<tr>
<td>Configure parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup</td>
</tr>
<tr>
<td>Configure parameters for security log backups</td>
<td>configSecLogArchive</td>
</tr>
</tbody>
</table>

3. If you receive a password prompt, enter your password.
4. To configure remote backup operation, enter 2.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable remote backup operation</td>
<td>Enter Y</td>
</tr>
<tr>
<td>Disable remote backup operation</td>
<td>Enter N</td>
</tr>
<tr>
<td>Accept the default</td>
<td>Press Enter</td>
</tr>
</tbody>
</table>

**Important:**
You must enable remote backup before you can configure SSH keys for server backup jobs.

5. Enter the IP address of the target backup server.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the IP address (initial configuration)</td>
<td>Enter the IP address in dot notation.</td>
</tr>
<tr>
<td>Change the existing IP address</td>
<td>Enter Y</td>
</tr>
<tr>
<td>Accept the existing IP address</td>
<td>Press Enter</td>
</tr>
</tbody>
</table>

6. Enter the full path to the backup directory located on the target backup server.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure the backup directory (initial configuration)</td>
<td>Enter the full path to the directory.</td>
</tr>
<tr>
<td>Change the existing backup directory</td>
<td>Enter Y</td>
</tr>
<tr>
<td>Accept the existing backup directory</td>
<td>Press Enter</td>
</tr>
</tbody>
</table>

7. Configure the SSH keys.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>To generate new keys</td>
<td>Enter Y</td>
</tr>
<tr>
<td>To verify the existing keys</td>
<td>Enter N</td>
</tr>
</tbody>
</table>

8. Enter the remote server user ID.
Choose to | Do this
---|---
Configure the remote server user ID. (initial configuration) | Enter the remote server user ID.
Change the remote server user ID. | Press Y
Keep the existing remote server user ID. | Press Enter

9. Generate the private key.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a pass phrase to protect the private key.</td>
<td>Enter a pass phrase that contains 6 characters (at least one digit 0–9, one uppercase letter A–Z, and one lower case letter a–z.), and proceed to 10 on page 22.</td>
</tr>
<tr>
<td>Not use a pass phrase.</td>
<td>Press Enter, and proceed to 11 on page 22.</td>
</tr>
</tbody>
</table>

**Important:**

Avaya recommends that you use a pass phrase. If you do not, the SSH key appears in plain text. The SSA must provide the pass phrase to the backup administrators and security administrators.

10. If you enter a pass phrase in 9 on page 22, enter the pass phrase again.
11. If you press Enter in 9 on page 22, press N to continue without entering a pass phrase.
12. Enter the password for the remote server user ID.
13. After the script operation is complete, check the script status report to ensure that the script completed successfully and the directory status is ACCESSIBLE.
14. To exit, enter 7.

---

**Regenerating or verifying the SSH keys for remote backup and restore**

**About this task**

Use this procedure to regenerate or verify the SSH keys for remote backup. Previously entered values are the default; each subsequent time you run the script, you receive a prompt to change them.

**Prerequisites**

- You are an SSA with sudo access.
- SSH is installed on the remote server and pass phrase authentication is enabled.

**Procedure**

1. Log on to the server as an SSA.
2. Run the configuration script.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure parameters for all backup jobs</td>
<td>configBkup</td>
</tr>
<tr>
<td>Configure parameters for platform backups</td>
<td>configPlatformBkup</td>
</tr>
<tr>
<td>Configure parameters for server backups</td>
<td>configSvrBkup</td>
</tr>
<tr>
<td>Configure parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup</td>
</tr>
<tr>
<td>Configure parameters for security log backups</td>
<td>configSecLogArchive</td>
</tr>
</tbody>
</table>

3. If you receive a password prompt, enter your password.

4. Enter 3.

   If SSH keys already exist, you receive a prompt to generate new keys.

5. Configure the SSH keys.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>To generate new keys</td>
<td>Enter Y</td>
</tr>
<tr>
<td>To verify the existing keys</td>
<td>Enter N</td>
</tr>
</tbody>
</table>

6. Confirm the remote server user ID.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change the remote server user ID.</td>
<td>Press Y</td>
</tr>
<tr>
<td>Keep the existing remote server user ID.</td>
<td>Press Enter</td>
</tr>
</tbody>
</table>

7. If you enter Y in 6 on page 23, at the prompt enter the new user ID.

8. Generate the private key.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use a pass phrase to protect the private key.</td>
<td>Enter a pass phrase that contains 6 characters (at least one digit 0–9, one uppercase letter A–Z, and one lower case letter a–z.), and proceed to 9 on page 23.</td>
</tr>
<tr>
<td>Not use a pass phrase.</td>
<td>Press Enter, and proceed to 10 on page 23.</td>
</tr>
</tbody>
</table>

9. If you enter a pass phrase in 8 on page 23, enter the pass phrase again.

10. If you press Enter in 8 on page 23, press N to continue without entering a pass phrase.

11. Enter the password for the remote backup server.

12. After the script operation is complete, check the script status report to ensure that the script completed successfully and the directory status is ACCESSIBLE.

13. To exit, enter 7.
Cleaning up SSH keys

About this task
Use this procedure to remove SSH keys from the system for security or troubleshooting purposes.

⚠ Important:
After you remove the SSH keys, you must regenerate the SSH keys to permit remote backup and restore operations.

Prerequisites
• You are an SSA with sudo access.
• SSH is installed on the remote server and pass phrase authentication is enabled.

Procedure
1. Log on to the server as an SSA.
2. Run the configuration script.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure parameters for all backup jobs</td>
<td>configBkup</td>
</tr>
<tr>
<td>Configure parameters for platform backups</td>
<td>configPlatformBkup</td>
</tr>
<tr>
<td>Configure parameters for server backups</td>
<td>configSvrBkup</td>
</tr>
<tr>
<td>Configure parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup</td>
</tr>
<tr>
<td>Configure parameters for security log backups</td>
<td>configSecLogArchive</td>
</tr>
</tbody>
</table>

3. If you receive a password prompt, enter your password.
4. To delete all SSH keys from the local machine, enter 4.
5. At the prompt to confirm the delete, enter Y.

Restoring the default backup configuration

About this task
Perform this procedure to remove remote configuration parameters for this backup job from the local machine.

Prerequisites
• You are an SSA with sudo access.

Procedure
1. Log on to the server as an SSA.
2. Run the configuration script.
<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure parameters for all backup jobs</td>
<td>configBkup</td>
</tr>
<tr>
<td>Configure parameters for platform backups</td>
<td>configPlatformBkup</td>
</tr>
<tr>
<td>Configure parameters for server backups</td>
<td>configSvrBkup</td>
</tr>
<tr>
<td>Configure parameters for file system integrity (FSI) baselines</td>
<td>configFSIBkup</td>
</tr>
<tr>
<td>Configure parameters for security log backups</td>
<td>configSecLogArchive</td>
</tr>
</tbody>
</table>

3. If you receive a password prompt, enter your password.
4. Enter 5.
5. To confirm the removal of the remote configuration parameters for this backup job, enter Y.

### Viewing the current backup configuration

**About this task**

Use this procedure to display the current configuration for the backup parameters, including the status of remote operations, remote SSH operations, and the remote backup directory.

⚠️ **Important:**

The status for the remote backup directory must always be ACCESSIBLE, and the status for remote operations must be ENABLED for remote backup operations to function. The status for remote SSH operations must be CONFIGURED for remote backup and restore to function.

⚠️ **Important:**

The status of the remote backup directory indicates the result of the last attempt to access this directory during configuration. This status can be incorrect. Subsequent system changes (for example, changes to the permissions for this remote directory or removal of the remote SSH keys) or network connectivity issues can affect the accessibility of the remote server.

**Prerequisites**

- You are an SSA with sudo access.

**Procedure**

1. Log on to the server as an SSA.
2. Run the configuration script.
3. If you receive a password prompt, enter your password.

4. Enter 6.

A list of the current backup configuration parameters appears, as well as the list of backup sets and the directories included in each backup set.

---

**Viewing the current backup configuration job aid**

This job aid is an example of the current backup configuration display for a successfully configured job.

```
**********************************************
CURRENT REMOTE BACKUP CONFIGURATION PARAMETERS
**********************************************
Local "backup to" directory : /var/mcp/os/backup/
Remote operation is : ENABLED
Remote SSH Operations are : CONFIGURED
Remote server IP Address : 47.1.2.3
Remote user login ID : johndoe
Remote "backup to" directory : /home/johndoe/bkup (ACCESSIBLE)
Current Backup Sets for Svr backup job:
Backup Set   Directories in set
----------   ------------------
MCP Platform: /admin
MCP Applications: /var/mcp/loads /var/mcp/media /var/mcp/install
```

Press <ENTER> to continue...
Chapter 5: System backup

This section provides the procedures that you perform to back up servers.
Avaya recommends that you back up the primary database server daily, and other servers after making any of the following changes:

- after you apply a patch to the Linux operating system (OS), or after you make any other major changes to configuration data—all servers
- after you add new administrators to the system—all servers
- after you apply a database patch (changes to the configuration data)—database server only
- after you install a maintenance release (MR)—Primary EMS server only

The backup process generates a snapshot of predefined directories on a server, and stores the backup in a .tar file in a storage directory.

The storage directory can be on a remote disk, the local disk, or on a local USB drive. A local USB drive is only recognized if only one USB drive is inserted into the USB port.

⚠️ Important:
- The system stores local disk backups in /var/mcp/backup/local. The directory is owned by root. The number of backups that can be stored depends on the capacity of the local disk. The SSA role administrator must monitor available disk space, and use SFTP to transfer old out-of-date backups off the server.
- The system stores USB backups in the root directory of the USB drive. The directory is owned by root. The number of backups that can be stored depends on the capacity of the USB drive. The SSA role administrator must monitor available disk space and remove old out-of-date backups. If more than 99% of this directory is in use, the backup operator receives notification and can choose whether to continue the backup. You can disable this warning by using the -silent parameter; however, the backup fails if more than 99% of the partition is in use.
- Application Server 5300 does not support direct backup to and restore from a local or remote tape drive. After backup to a remote server, you can store the backup files on tape.

Prerequisites
- [Remote backup parameter configuration](#) on page 17
System backup tasks

About this task
This work flow provides the tasks that you perform to back up the system.

Navigation
- Server backup and platform backup on page 29
- Database backup on page 33
- FSI backup on page 37
- Security logs backup on page 39
Chapter 6: Server backup and platform backup

This section provides the procedures you use to perform a server backup or a platform backup.

As explained earlier in this document, the server backup job creates up to four backup sets, but a platform backup job creates only one backup set. For more information about the differences between server backup and platform backup, see Backup sets on page 15.

Server backup and platform backup procedures

About this task

Use the procedures in this section to perform a server backup operation or a platform backup operation, and to clean up unneeded files from the servers before backing up the servers.

Navigation

- Backing up server data or platform data remotely on page 30
- Backing up server data or platform data locally on page 31
- Removing unneeded loads from the EM Servers on page 32

Server backup and platform back up job aid

This job aid provides an example of the summary of the results of a server backup, and explains the naming convention for the .tar files.

16:27:57 Summary of backup results:
16:27:57
 Backup to remote Disk => /admin/ to 47.1.2.3::/home/johndoe/bkup/mcpPlatform.zrchy0qq.2007_10_19.16_25_37.tar completed successfully
16:27:57
 Backup to remote Disk => /var/mcp/loads/ /var/mcp/media/ /var/mcp/install/ to 47.1.2.3::/home/johndoe/bkup/mcpApp.zrchy0qq.2007_10_19.16_25_39.tar completed successfully

SSHUtil: Stopping SSH-agent...
Logs are written to /home/ntsysadm/bkup_restore/bkupsvr.log.
2007_10_19.16:27:57

Each of the backup sets produces a separate backup file:

• Platform: mcpPlatform.<host name>.<date/time stamp>.tar
• Application: mcpApp.<host name>.<date/time stamp>.tar

The file name includes the type of backup (mcpPlatform or mcpApp), the host name of the server, and the date and time stamp for the backup.

In this example the server backup produced two tar files: mcpPlatform and mcpApp. A server backup produces an mcpDB tar file if the server hosts primary Database Manager, or an mcpMAS.tar file if the server hosts an Avaya Media Server (MS). For more information see Backup jobs on page 14.

# Backing up server data or platform data remotely

## About this task

Use this procedure to back up server data or platform data to a remote server.

⚠️ Important:

Avaya recommends that you store backup data in a remote location to facilitate recovery in the event of server failure.

⚠️ Caution:

**Risk of data loss**

If disk usage on the remote server is over 85%, you receive a warning and a prompt to continue. If you continue and the backup exceeds available disk space, the backup fails.

## Prerequisites

- The remote server is running SSH and pass phrase authentication is enabled.
- You are a user with a BA role or an SSA role.
- The remote backup settings for the backup script are configured as described in Remote backup parameter configuration on page 17.
- If the SSH keys are pass phrase protected, you know the pass phrase.

## Procedure

1. Log on to the server as a BA or an SSA.
2. Run the script to perform the backup.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the server</td>
<td>bkupSvr –remote</td>
</tr>
<tr>
<td>Back up the platform</td>
<td>bkupPlatform –remote</td>
</tr>
</tbody>
</table>
3. If you receive a password prompt, enter your password.

4. If the SSK keys are pass phrase protected, at the prompt, enter the pass phrase for the SSH keys.

   After the backup is complete, a summary report displays the results.

5. Check the backup summary report to verify that all backup sets complete successfully.

6. Make a note of the name and location of the tar file or tar files. (Server backup produces up to three tar files; platform backup produces one tar file.)

7. Make a note of the name and location of the log file.

   If errors occur, you can use the log file to assist with troubleshooting.

---

## Backing up server data or platform data locally

### About this task

Use this procedure to back up server data or platform data locally, to a local directory, or to a USB drive.

⚠️ **Important:**

You can also schedule local backups; however, Avaya recommends that you store backup data in a remote location to facilitate recovery in the event of system failure.

⚠️ **Important:**

To restore server data or platform data, you require a remote server running SSH.

### Prerequisites

- You are a user with a BA or an SSA role.
- For backup to a USB drive, one (and only one) USB drive must be inserted into the USB port.

### Procedure

1. Log on to the server as a BA or an SSA.

2. Run the script to perform the backup.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the server to USB drive</td>
<td>bkupSvr –usbdrive</td>
</tr>
<tr>
<td>Back up the server to local directory</td>
<td>bkupSvr –local</td>
</tr>
<tr>
<td>Back up the platform to USB drive</td>
<td>bkupPlatform –usbdrive</td>
</tr>
<tr>
<td>Back up the platform to local directory</td>
<td>bkupPlatform –local</td>
</tr>
</tbody>
</table>

   After the backup is complete, a summary report displays the results.

3. Check the backup summary report to verify that all backup sets complete successfully.
4. Make a note of the name and location of the tar file or tar files. (Server backup produces up to three tar files; platform backup produces one tar file.)

5. Make a note of the name and location of the log file.

   If errors occur, you can use the log file to assist with troubleshooting.

---

### Removing unneeded loads from the EM Servers

#### About this task

Use this procedure to remove old loads from the Element Management (EM) Servers if they are no longer needed; otherwise they are backed up as part of the Application backup set. The number of loads in the /var/mcp/loads directory should be 3 or less; when an MR with multiple Patch loads exist, keep the latest base/MR load and the latest associated patch load.

**Important:**

You must delete the loads from both Primary EM and Secondary EM simultaneously, because the Primary EM and Secondary EM monitor the loads and if the load is on one server but not the on other, the EM copies the loads back to the other EM Server.

#### Prerequisites

- You know the name of the load to remove.
- You are a user with a AA role.

#### Procedure

1. Log on to the Primary EM with the AA role (ntappadm).
2. In another window, log on to the Secondary EM with the AA role (ntappadm).
3. On the Primary EM, enter the following command:
   ```
   cd /var/mcp/loads
   ```
4. On the Secondary EM, enter the same command:
   ```
   cd /var/mcp/loads
   ```
5. On the Primary EM, type the following command (but do not press Enter):
   ```
   rm -rf <loadname>
   ```
6. On the Secondary EM, type the following command (but do not press Enter):
   ```
   rm -rf <loadname>
   ```
7. As close together as possible, press Enter in the both the Primary EM window and the Secondary EM window.

#### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;loadname&gt;</td>
<td>The name of the load to remove.</td>
</tr>
</tbody>
</table>
Chapter 7: Database backup

This section provides the procedures that you perform to back up the database.

Database backup procedures

About this task
This task flow shows you the sequence of procedures you perform to back up the database.

Navigation

- Backing up a database manually on page 34
Back up a database manually

About this task

Use this procedure to perform a manual back up of an existing database from the primary Element Management System (EMS) server.

The backup data rate for the x3550 server is approximately 300 megabytes (MB) per minute. The time to create the backup varies with the size of the database. If the database is in use during the backup, the time required to create the backup increases.

Prerequisites

- You are a user with DBA role.
- You know the name of the database that you want to back up. The system uses the name of the database to derive the directory path to the backup script.

Procedure

1. Log on to the primary EMS server as a user with DBA role.
2. Change directory:
   ```
   cd /var/mcp/run/MCP_15.1/<mcpdb>_0/bin/util
   ``
3. Run the database backup script:
   ```
   ./dbBackup.pl <BackupFileName>
   ```

   The backup destination directory is `/var/mcp/db/backup/latest`, and the backup file name is `<BackupFileName>.tar.gz`

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;BackupFileName&gt;</code></td>
<td>This value is the name assigned to the backup file.</td>
</tr>
<tr>
<td><code>&lt;mcpdb&gt;</code></td>
<td>This value is the name of the database as listed in the <code>/var/mcp/install/installprops.txt</code> file.</td>
</tr>
</tbody>
</table>
Scheduling database backups

About this task
Use this procedure to schedule automated backups for the database on the primary Element Management System (EMS) server.

⚠️ Important:
Avaya recommends that you schedule backups for off-peak hours. The default backup time is 3:30 AM.

The time required to create the backup varies with the size of the database. If the database is in use during the backup, the time required to create the backup increases.

Prerequisites
• You are a user with DBA role.
• You know the name of the database that you want to back up. The system uses the name of the database to derive the directory path to the backup script.

Procedure
1. Log on to the primary EMS server as a user with DBA role.
2. Change directory:
   ```
   cd /var/mcp/run/MCP_15.1/<mcpdb>:_0/bin/util
   ```
3. Run the script to schedule the database:
   ```
   ./scheduleDBBackup.pl
   ```
   A summary of the database backup jobs appears.
4. At the prompt to select a command, enter E.
5. Enter the time to perform the backups (hh:mm format).
6. Enter a prefix (such as dbBackup) for the backup file name.
7. At the prompt, enter Y to schedule the backup.
8. Enter Q to quit.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mcpdb&gt;</td>
<td>This value is the name of the database as listed in the /var/mcp/install/installprops.txt file.</td>
</tr>
</tbody>
</table>
Removing a scheduled backup

About this task
Use this procedure to remove a scheduled backup job (change the status to Not Scheduled).

Prerequisites
- You are a user with DBA role.

Procedure
1. Log on to the Primary database server as a user with DBA role.
2. Change directory:
   ```
   cd /var/mcp/run/MCP_15.1/<mcpdb>_0/bin/util
   ```
3. Run the script to schedule the database:
   ```
   ./scheduleDBBackup.pl
   ```
   A summary of the database backup jobs appears.
4. At the prompt to select a command, enter D to change the job status to Not Configured.
5. At the prompt, enter Y to confirm the change.
6. Enter Q to quit.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mcpdb&gt;</td>
<td>This value is the name of the database as listed in the /var/mcp/install/installprops.txt file.</td>
</tr>
</tbody>
</table>
Chapter 8: FSI backup

This section provides the procedures that you perform to back up the file system integrity (FSI) baselines. For more information about FSI baselines, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Navigation

- Backing up FSI baseline files remotely on page 37
- Backing up FSI baseline files locally on page 38

Related links

- Backing up FSI baseline files remotely on page 37
- Backing up FSI baseline files locally on page 38

Backing up FSI baseline files remotely

About this task

Use this procedure to back up the File System Integrity (FSI) baseline files to a remote server.

⚠️ Caution:

Risk of data loss

If disk usage on the remote server is over 85%, you receive a warning and a prompt to continue. If you continue and the backup exceeds available disk space, the backup fails.

Prerequisites

- SSH is installed and pass phrase authentication is enabled on the remote machine.
- You are a user with a BA role or an SSA role.
- The remote backup settings for the backup script are configured as described in Remote backup parameter configuration on page 17.
- If the SSH keys are pass phrase protected, you know the pass phrase.

Procedure

1. Log on to the server as a BA or an SSA.
2. Run the FSI backup script:
   
bkupFSI -remote
3. If you receive a pass phrase prompt, enter the pass phrase for the SSH keys. After the backup is complete, a summary report displays the results.

4. Check the summary report to verify that all backup sets complete successfully.

5. Make a note of the name and location of the tar files.

6. Make a note of the name and location of the log file.

   If errors occur, you can use the log file to assist with troubleshooting.

---

### Backing up FSI baseline files locally

**About this task**

Use this procedure to back up the File System Integrity (FSI) baseline files to a USB drive inserted in the USB port of the local server.

**Prerequisites**

- You are a user with a BA role or an SSA role.
- One (and only one) USB drive must be inserted into the USB port.

**Procedure**

1. Log on to the server as a BA or an SSA.

2. Run the FSI backup script:

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up FSI data to a USB drive</td>
<td>bkupFSI –usbdrive</td>
</tr>
<tr>
<td>Back up FSI data to local directory</td>
<td>bkupFSI –local</td>
</tr>
</tbody>
</table>

   After the backup is complete, a summary report displays the results.

3. Check the summary report to verify that all backup sets complete successfully.

4. Make a note of the name and location of the tar files.

5. Make a note of the name and location of the log file.

   If errors occur, you can use the log file to assist with troubleshooting.
Chapter 9: Security logs backup

You can back security logs up to the local drive, a local USB drive, or to a remote server so that you can view them.

Navigation

• Backing up security logs to a remote server on page 39
• Backing up security logs locally on page 40

Related links

Backing up security logs to a remote server on page 39
Backing up security logs locally on page 40

Backing up security logs to a remote server

About this task

Use this procedure to back up the security logs to a remote server.

⚠️ Important:

Only the owner of the backup tar file (the remote user specified during the backup configuration) can change the ownership on the contents of a tar file backed up to a remote server.

⚠️ Caution:

Risk of data loss

If disk usage on the remote server is over 85%, you receive a warning and a prompt to continue. If you continue and the backup exceeds available disk space, the backup fails.

Prerequisites

• SSH is installed and pass phrase authentication is enabled on the remote machine.
• You are a user with an SA role or an SSA role.
• The remote backup settings in the backup script is configured as described in Remote backup parameter configuration on page 17.
• If the SSH keys are pass phrase protected, you know the pass phrase.

Procedure

1. Log on to the server as an SA or an SSA.
2. Run the script to perform the backup.
   ```bash
   archSecLog -remote
   ```
3. If you receive a pass phrase prompt, enter the pass phrase for the SSH keys.
   After the backup is complete, a summary report displays the results.
4. Check the summary report to verify that all backup sets complete successfully.
5. Make a note of the name and location of the tar files.
6. Make a note of the name and location of the log file.
   If errors occur, you can use the log file to assist with troubleshooting.

---

Back up security logs locally

**About this task**

Use this procedure to back security logs up to the local directory or to a local USB drive.

**Prerequisites**

- You are a user with a BA role or an SSA role.
- For backup to a USB drive, one (and only one) USB drive must be inserted into the USB port.

**Procedure**

1. Log on to the server as a BA or an SSA.
2. Run the script to perform the backup.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Back up the logs to a USB drive</td>
<td><code>archSecLog –usbdrive</code></td>
</tr>
<tr>
<td>Back up the logs to local directory</td>
<td><code>archSecLog –local</code></td>
</tr>
</tbody>
</table>

   After the backup is complete, a summary report displays the results.
3. Check the summary report to verify that all backup sets complete successfully.
4. Make a note of the name and location of the tar files.
5. Make a note of the name and location of the log file.
   If errors occur, you can use the log file to assist with troubleshooting.
Chapter 10: Backup script help

This chapter contains the procedures that you use to obtain help with the backup script.

Navigation

- Using the backup script help on page 41
- Limiting bandwidth for backup operations on page 42

Using the backup script help

About this task

Use this procedure to obtain help with the backup scripts.

Prerequisites

- For bkupSvr, or bkupFSI, you are a user with a BA role or an SSA role.
- For archSecLog you are a user with a BA role, an SA role, or an SSA role.

Procedure

Use the -h command line parameter when you run the backup script.

<table>
<thead>
<tr>
<th>Obtain help with</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running the platform backup script</td>
<td>bkupPlatform -h</td>
</tr>
<tr>
<td>Running the server backup script</td>
<td>bkupSvr -h</td>
</tr>
<tr>
<td>Running the file system integrity (FSI) baselines backup script</td>
<td>bkupFSI -h</td>
</tr>
<tr>
<td>Running the &quot;archive&quot; command to back up security logs</td>
<td>archSecLog -h</td>
</tr>
</tbody>
</table>

Using the backup script help job aid

This job aid provides additional usage information.

Usage:

bkupSvr [-remote|-usbdrive]  <-silent> <-d debugLevel> <-s v[vv]> <-l bandwidthLimit> <-h>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-remote</td>
<td>Use to specify backup to a remote server (previously configured by the SSA).</td>
</tr>
<tr>
<td>-local</td>
<td>Use to specify backup to the directory on the local hard disk.</td>
</tr>
<tr>
<td>-usbdrive</td>
<td>Use to specify backup to a USB drive inserted in the USB port of the local server.</td>
</tr>
<tr>
<td>-silent</td>
<td>Use to specify silent operation (no user input required).</td>
</tr>
<tr>
<td>-d debugLevel</td>
<td>Only for use by Avaya Support.</td>
</tr>
<tr>
<td>-s vv</td>
<td>Only for use by Avaya Support.</td>
</tr>
<tr>
<td>-l bandwidthLimit</td>
<td>Use to limit the upload bandwidth (in KB/s) for the backup.</td>
</tr>
<tr>
<td>-h</td>
<td>Use to print usage information.</td>
</tr>
</tbody>
</table>

### Limiting bandwidth for backup operations

#### About this task
The default bandwidth limit during remote backups is 5000 kilobytes (KB) per second. Under normal circumstances, use the default bandwidth. Use this procedure to limit the bandwidth.

#### Procedure
Use the -l command line parameter to specify the rate in KB/s, when you run the script for a backup operation.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit upload bandwidth consumption for platform backups</td>
<td>bkupPlatform -remote [-l rate]</td>
</tr>
<tr>
<td>Limit upload bandwidth consumption for server backups</td>
<td>bkupSvr -remote [-l rate]</td>
</tr>
<tr>
<td>Limit upload bandwidth consumption for file system integrity baselines.</td>
<td>bkupFSI -remote [-l rate]</td>
</tr>
<tr>
<td>Limit upload bandwidth consumption for security logs backups</td>
<td>archSecLog -remote [-l rate]</td>
</tr>
</tbody>
</table>

**Important:**
The smaller the -l parameter, the longer the backup operation takes to complete.
Chapter 11: System restore

Restore servers to recover from a failure. The process that you follow to restore a server depends on whether or not the server is an Element Management System (EMS) server. This document defines an EMS server as a server which hosts the primary or secondary AS 5300 Element Manager and database (DB). The restore process for an EMS server depends on whether the other server (primary or secondary) and both the AS 5300 Element Manager and DB applications are fully operational.

If the primary and secondary EMS servers and application are fully operational, but the database is missing data (because of corruption or an inadvertent delete), you can restore the database from a backup.

**Important:**

Backups are server-specific. Only restore server data to the server from which you created the backup.

---

**System restore tasks**

**About this task**

This work flow provides the task flows and procedures that you perform to restore the system.
Navigation

- Using the restore script help on page 71
- Non-EMS server restore on page 49
- EMS server restore from an operational EMS server on page 52
- Double EMS server restore from a backup on page 55

⚠️ Warning:

COMPLETE LOSS OF SERVICE

Only restore both EMS servers in the event of a catastrophic failure where both servers are totally down.

- Restoring the database from a backup—missing data on page 66
- FSI restore on page 73
- Extracting security records from a remote backup file on page 69
Chapter 12: Platform data restore

To restore platform data using previously backed up platform data, you perform a reinstall of the platform software.

For information about how to install the platform using previously backed up platform data, see the 102.1.6 AS5300 3.0 AvayaMS Installation and Commissioning.
Chapter 13: Server application data restore

About this task
This section provides the procedures that you perform to restore the server application data backup. You can restore server application data remotely or locally. Restore of server application data is only required for Element Management System (EMS) servers. The EMS servers host the primary and secondary Element Managers and databases (DB).

Navigation
- Restoring server application data remotely on page 46
- Restoring server application data locally on page 47

Restoring server application data remotely

About this task
Use this procedure to restore a server application data backup remotely. This procedure is optional for any server that does not host an AS 5300 Element Manager or database (DB).

Prerequisites
- The platform is installed with a backup of the platform data. For more information, see the 102.1.1 AS5300 Server Installation.
- Platform patches are installed. For more information, see the 102.1.1 AS5300 Server Installation.
- Antivirus software is installed and configured. For more information, see Avaya Aura® Application Server 5300 Security, NN42040-601.
- The remote backup and restore parameters are configured. For more information, see Remote backup parameter configuration on page 17.
- The remote server is running SSH with pass phrase authentication enabled.
- A backup for the server application data exists on the remote server.

Procedure
1. Log on to the server as a user with SSA role and sudo access.
2. Run the restore script:
   restoreSvr -remote
3. If prompted, enter the pass phrase for the SSH keys.
4. From the list, locate the restore TAR file.
5. Enter the corresponding number for the restore TAR file.
6. Review the restore file information and enter \( \checkmark \) to confirm.
   After the restore is complete, a summary report displays the results.
7. Check the summary report to verify that all restore sets complete successfully.
8. Make a note of the name and location of the log file.
   If errors occur, you can use the log file to assist with troubleshooting.

---

**Restoring server application data remotely job aid**

This job aid provides an example of the summary of backup restore results.

16:54:48
Restore from remote Disk  (directory  /var/mcp/loads/ /var/mcp/
media/ /var/mcp/install/) completed successfully
SSHUtl: Stopping SSH-agent...
Logs are written to /home/ntsysadm/bkup_restore/restoresvr.log.
2007_10_19.16:54:48
Changing ownership of /home/ntsysadm/bkup_restore/restoresvr.log.
2007_10_19.16:54:48 to ntsysadm

---

**Restoring server application data locally**

**About this task**

Use this procedure to restore a backup of the server application data from a USB drive inserted in the USB port on the local server. This procedure is optional for any server that does not host an AS 5300 Element Manager or database (DB).

**Prerequisites**

- The platform is installed with a backup of the platform data. For more information, see the 102.1.1 AS5300 Server Installation.
- Platform patches are installed. For more information, see the 102.1.1 AS5300 Server Installation.
- Antivirus software is installed and configured. For more information, see Avaya Aura® Application Server 5300 Security, NN42040-601.
- DB is installed. For more information, see the 102.1.1 AS5300 Server Installation.
- DB patches are installed. For more information, see the 102.1.1 AS5300 Server Installation.
- Insert the USB drive that holds the local backup files into the USB port. Ensure that no other USB drive is inserted.
Procedure

1. Log on to the server as a user with SSA role and sudo access.
2. Run the restore script:
   
   `restoreSvr -usbdrive`

3. If prompted, enter the pass phrase for the SSH keys.
4. From the list, locate the restore TAR file.
5. Enter the corresponding number for the restore TAR file.
6. Review the restore file information and enter \( \text{Y} \) to confirm.

   After the restore is complete, a summary report displays the results.

7. Check the summary report to verify that all restore sets complete successfully.
8. Make a note of the name and location of the log file.

   If errors occur, you can use the log file to assist with troubleshooting.
Chapter 14: Non-EMS server restore

This section provides the procedures you perform to completely restore any server that is not an Element Management System (EMS) server. The EMS servers host either a primary or secondary AS 5300 Element Manager and database (DB).

Prerequisites

- Both the primary and secondary EMS servers and applications are fully operational. For information about how to restore either the primary or the secondary EMS server, see EMS server restore from an operational EMS server on page 52. For information about how to restore both the primary and secondary EMS servers, see Double EMS server restore from a backup on page 55.

Non-EMS server restore tasks

About this task

This work flow shows you the sequence of tasks that you perform to completely restore a server that does not host either the primary or secondary AS 5300 Element Manager and DB.
Navigation

- Install the platform using previously backed up platform data
  
  For more information, see the 102.1.1 AS5300 Server Installation.

- Apply platform patches
  
  For more information, see the 102.1.1 AS5300 Server Installation.

- Install and configure antivirus software
For more information, see your Avaya antivirus installation method and *Avaya Aura*® *Application Server 5300 Security, NN42040-601.*

- Configure the remote backup and restore parameters
  For more information, see [Configuring remote backup and restore parameters](#) on page 20.
- Restore the server application data
  For more information, see [Restoring server application data remotely](#) on page 46.
- Stop the other NEs hosted by the server
  For more information, see [Stopping a network element](#) on page 110.
- Deploy the other NEs hosted by the server
  For more information, see [Deploying a network element](#) on page 110.
- Start the other network elements hosted by the server
  For more information, see [Starting a network element](#) on page 109.
- Create a new FSI baseline
  For more information about file system integrity (FSI) baseline creation, see *Avaya Aura*® *Application Server 5300 Security, NN42040-601.*
Chapter 15: EMS server restore from an operational EMS server

This section provides the procedures that you perform to completely restore an Element Management System (EMS) server that hosts either the primary or secondary AS 5300 Element Manager and database (DB).

Prerequisites

- The replicated counterpart (primary or secondary) EMS server and the AS 5300 Element Manager and DB applications are fully operational.

EMS server restore from an operational EMS server tasks

About this task

This work flow shows you the sequence of tasks that you perform to completely restore a primary or secondary AS 5300 Element Manager and DB server.
Navigation

- Install the platform using previously backed up platform data
  For more information, see the 102.1.1 AS5300 Server Installation.
- Apply platform patches
  For more information, see the 102.1.1 AS5300 Server Installation.
- Install and configure the antivirus software
EMS server restore from an operational EMS server

For more information, see your Avaya Antivirus Installation Method and 102.1.1 AS5300 Server Installation.

- Restore the server application data For more information, see Restoring server application data remotely on page 46.

- Install DB
  For more information, see the 102.1.1 AS5300 Server Installation.

- Apply DB patches
  For more information, see the 102.1.1 AS5300 Server Installation.

- Configure the remote backup and restore parameters
  For more information, see Configuring remote backup and restore parameters on page 20.

- Restore the primary EMS server
  For more information, see Restoring the primary EMS server on page 61.

- Restore the secondary EMS server
  For more information, see Restoring the secondary EMS server on page 63.

- Stop the other NEs hosted by the server
  For more information, see Stopping a network element on page 110.

  For a two-server configuration, use the physical view of the AS 5300 Element Manager Console to identify the other NEs hosted by the server. In a four-server configuration, there are no other NEs hosted by the server.

- Deploy the other NEs hosted by the server
  For more information, see Deploying a network element on page 110.

- Start the other network elements hosted by the server
  For more information, see Starting a network element on page 109.

- Create a new FSI baseline
  For more information about creating file system integrity (FSI) baselines, see Avaya Aura® Application Server 5300 Security, NN42040-601.
Chapter 16: Double EMS server restore from a backup

This section provides the procedures that you perform to completely restore both of the Element Management System (EMS) servers after both fail. The EMS servers host the primary and secondary AS 5300 Element Manager and databases (DB).

⚠️ Important:

Only restore both EMS servers if both the primary and secondary EMS are completely out of service (for example, after a catastrophic failure where the entire site is lost.)

Double EMS server restore from a backup task

About this task

This task flow shows you the sequence of procedures that you perform to completely restore both EMS servers.
Navigation

- Install the platform using previously backed up platform data
  For more information, see the 102.1.1 AS5300 Server Installation.
- Apply platform patches
  For more information, see the 102.1.1 AS5300 Server Installation.
- Install and configure the antivirus software
For more information, see the Avaya Antivirus Installation Method and *Avaya Aura® Application Server 5300 Security, NN42040-601*.

- Restore the server application data
  For more information, see [Restoring server application data remotely](#) on page 46.

- Install DB
  For more information, see the *102.1.1 AS5300 Server Installation*.

- Apply DB patches
  For more information, see the *102.1.1 AS5300 Server Installation*.

- Configure the remote backup and restore parameters
  For more information, see [Configuring remote backup and restore parameters](#) on page 20.

- Restore the database from a backup
  For more information, see [Restoring the database from a backup—double EMS server restore](#) on page 67.

- Stop the other NEs hosted by the server
  For more information, see [Stopping a network element](#) on page 110.

  For a two-server configuration, use the physical view of the AS 5300 Element Manager Console to identify the other NEs hosted by the server. In a four-server configuration, there are no other NEs hosted by the server.

- Deploy the other NEs hosted by the server
  For more information, see [Deploying a network element](#) on page 110.

- Start the other network elements hosted by the server
  For more information, see [Starting a network element](#) on page 109.

- Create a new FSI baseline
  For information about how to create a new file system integrity (FSI) baseline, see *Avaya Aura® Application Server 5300 Security, NN42040-601*.
Chapter 17: Avaya Media Server backup and restore

This chapter provides information you can use to back up and restore an Avaya Media Server (MS).

Navigation
- Backing up an Avaya MS on page 58
- Scheduling an Avaya MS backup on page 59
- Restoring an Avaya MS on page 60

Backing up an Avaya MS

About this task
Use this procedure to back up an Avaya Media Server (MS).

The Avaya MS backup you create is stored in a TAR file, which is included in server backups made with bkupSvr.

Prerequisites
- You have SSA role or BA role.
- The server has sufficient free hard drive space to store the new backup file.

Procedure
1. Log on to the Avaya MS server as a user with BA or SSA role.
2. Enter `su` to become the root user.
3. When prompted, enter the root password.
4. Run the backup script:
   ```
   msBackup <path> <TAR_file_name>
   ```
Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;path&gt;</td>
<td>Optionally, enter the full path to the folder in which to create the TAR file. If you do not enter a path, the Avaya MS uses the folder var/mcp/ma/MAS/platdata/EAM/Backups.</td>
</tr>
<tr>
<td>&lt;TAR_file_name&gt;</td>
<td>Optionally, enter a file name for the TAR file. If you do not enter a value for &lt;TAR_file_name&gt;, the Avaya MS automatically creates a name based on the current date. If you create another backup on the same day, the same name is used, overwriting the previous file.</td>
</tr>
</tbody>
</table>

Scheduling an Avaya MS backup

About this task

Use this procedure to schedule a backup of an Avaya MS server.

Prerequisites

- You have SSA role.
- The server has sufficient free hard drive space to store the new backup file.

Procedure

1. Log on to the Avaya MS server as a user with SSA role.
2. Run the backup scheduling script:
   
   msschedulebackup

3. Enter E to edit/schedule a job.
4. Enter the time to execute the backup, in the format [hh:mm].
5. Enter Y to confirm, and save your changes.
   
   A summary of the scheduled backup is displayed.

6. Enter Q to quit the scheduling tool.

At the scheduled time, the system backs up the Avaya MS into a new TAR file in the folder /var/mcp/ma/MAS/platdata/EAM/Backups/latest, and archives existing TAR files as follows:

- If the latest folder contains any automatically-generated TAR files, the system moves them to the folder /var/mcp/ma/MAS/platdata/EAM/Backups/AUTO_history.
If the latest folder contains any manually-generated TAR files, the system moves them to the folder `/var/mcp/ma/MAS/platdata/EAM/Backups/`.

## Restoring an Avaya MS

### About this task

Use this procedure to restore a backup of an Avaya MS server.

* **Note:**

In case of server replacement or server rebuild, Avaya MS platform and applications must be installed. See *Implementing and Administering Avaya Media Server 7.5* to install MS platform and MS applications. Skip this procedure if Avaya MS platform and application already installed on the server.

### Prerequisites

- You have SSA role.

### Procedure

1. To stop Avaya MS, see *Stopping a network element* on page 110.
2. Log on to the Avaya MS server as a user with SSA role.
3. Enter `su` to become the root user.
4. When prompted, enter the root password.
5. Run the restore script:
   ```
   msRestore <TAR_file_name>
   ```
6. If you did not specify a `<TAR_file_name>`, the system prompts you to select one from a list. If this happens, select the file to restore by entering the corresponding digit.
7. To deploy the Avaya MS network element, see *Deploying a network element* on page 110.
8. To start Avaya MS, see *Starting a network element* on page 109.

### Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;TAR_file_name&gt;</code></td>
<td>Optionally, enter the path and file name for the TAR file to restore.</td>
</tr>
</tbody>
</table>
Chapter 18: Common restore procedures

This chapter contains procedures common to the restore work and task flows.

Navigation

- Restoring the primary EMS server on page 61
- Restoring the secondary EMS server on page 63
- Synchronizing the primary and secondary databases on page 64
- Testing database replication on page 65
- Viewing database replication errors on page 65
- Restoring the database from a backup—missing data on page 66
- Restoring the database from a backup—double EMS server restore on page 67
- Extracting security records from a remote backup file on page 69
- Converting from a single database to a redundant database configuration on page 70
- Using the restore script help on page 71

Restoring the primary EMS server

About this task

Use this procedure to restore the primary Element Management System from the secondary EMS server. The EMS servers host the primary and secondary AS 5300 Element Manager and primary databases (DB).

Prerequisites

- The secondary AS 5300 Element Manager and DB applications are fully operational.
- The server platform is installed using platform data from a previous backup.
- The application data for the server is restored from a previous backup.
  For more information see, Restoring server application data remotely on page 46.
- DB is installed.
- You are familiar with the procedure to synchronize the databases.
  For more information, see Synchronizing the primary and secondary databases on page 64.
Procedure

1. Log on to the primary EMS as a user with AA role.
2. Change directory:
   
   cd /var/mcp/install
3. Deploy the DB scripts:
   
   dbInstall.pl -fo
   
   The following prompt appears:
   
   Perform "Deploy Files Only" operation to Secondary DB also (Y/N)?
   [Y]: [Y]
4. Press Enter.
5. Log on to the secondary EMS server as a DBA.
6. Change directory:
   
   cd /var/mcp/run/MCP_15.1/<mcpdb_1>/bin/util
7. Run the synchronization script:
   
   ./resync.pl
8. To confirm the synchronization, press Y.
   
   The script can take several hours to complete.
9. Log on to the server that hosts the primary AS 5300 Element Manager as an AA.
10. Change directory:
    
    cd /var/mcp/install
11. Deploy and start the AS 5300 Element Manager:
    
    ./mcpUpgrade.pl

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mcpdb_1&gt;</td>
<td>This value is the name of the secondary database.</td>
</tr>
</tbody>
</table>
Restoring the secondary EMS server

About this task

Use this procedure to restore the server that hosts the secondary Element Management System (EMS) server, from the primary AS 5300 Element Manager and DB server. The EMS servers host the primary and secondary AS 5300 Element Manager and databases (DB).

Prerequisites

- The primary AS 5300 Element Manager and DB applications are fully operational.
- The server platform is installed using platform data from a previous backup.
- The application data for the server is restored from a previous backup.
  For more information see, Restoring server application data remotely on page 46.
- DB is installed.
- You are familiar with the procedure to synchronize the database. For more information, see Synchronizing the primary and secondary databases on page 64.
- You are familiar with the procedure to deploy a NE. For more information, see Deploying a network element on page 110.
- You are familiar with the procedure to start a NE. For more information, see Starting a network element on page 109.

Procedure

1. Log on to the primary EMS server as a user with AA role.
2. Change directory:
   cd /var/mcp/install
3. Deploy the DB scripts:
   dbInstall.pl –fo
   The following prompt appears: Perform "Deploy Files Only" operation to Secondary DB also (Y/N)?[Y]: [Y]
4. Press Enter.
5. Log on to the primary EMS server as a DBA.
6. Change directory:
   cd /var/mcp/run/MCP_15.1/<mcpdb_0>/bin/util
7. Run the resynchronization script:
   ./resync.pl
8. To confirm the synchronization, press Y.
   The script can take 45 minutes or more to complete.
9. Use the aAS 5300 Element Manager Console to deploy the secondary AS 5300 Element Manager.
10. Use the AS 5300 Element Manager Console to start the other NE instances on the server.

---

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;mcpdb_1&gt;</td>
<td>This value is the name of the secondary database.</td>
</tr>
</tbody>
</table>

---

**Synchronizing the primary and secondary databases**

**About this task**

In a database redundant configuration, the databases are synchronized. Use this procedure to synchronize the primary and secondary database servers.

**Prerequisites**

- You are a user with DBA role.
- The configuration includes a redundant database.
- The database is installed and deployed on both servers and the scripts are deployed.

**Procedure**

1. Log on to the server with the source database (the database from which data is copied) using an account that has the DBA role (such as ntdbadm).

2. Enter the following command to change the directory:
   ```
   cd /var/mcp/run/MCP_15.1/<dbName>/bin/util
   ```

3. Enter the following command to run the synchronization script:
   ```
   ./resync.pl
   ```

   The script copies the data from the source database to a given System Change Number (SCN) while queuing all changes made. After the transfer of the data files is complete, the script applies the queued changes to the restored database.

4. Verify the information that appears at the confirmation prompt, and press Y.

5. After the synchronization completes, enter the following command to test the database replication:
   ```
   /testReplication.pl
   ```
Testing database replication

Before you begin

• Your system has a redundant database configuration.
• You have an account with the DBA role.

About this task

Use this procedure to verify that replication is executing properly in replicated databases.

Procedure

1. Log in to the primary database server using an account that has the DBA role.
2. Enter the following command to change the directory:
   
   ```
   cd /var/mcp/run/MCP_16.0/<DBName>_0/bin/util
   ```
3. Enter the following command to test the replication:
   
   ```
   ./testReplication.pl
   ```

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DBname&gt;</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

Viewing database replication errors

Before you begin

You have an account with the DBA role.

About this task

Use this procedure to view replication errors.

Procedure

1. Log in to the primary database server as a user with as the DBA role (such as ntdbadm).
2. Change directory:
   
   ```
   cd /var/mcp/run/MCP_16.0/<DBname>_0/bin/util
   ```
3. Run the View Replication Errors script:
   
   ```
   ./viewRepErrors.pl
   ```

   The system displays replication errors, if any are found, and stores a detailed report in
   
   /var/mcp/run/MCP_16.0/<DBname>_0/work/RepErrors.

Next steps

If replication errors are reported, resynchronize the database using the steps in Synchronizing the primary and secondary databases on page 64.
Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;DBname&gt;</td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

Restoring the database from a backup—missing data

About this task

Use this procedure to restore missing database (DB) data. In this scenario, the database is corrupt or missing data after an inadvertent delete; both the primary and secondary EMS servers and applications are fully operational.

⚠️ Important:

In this case, during the restore procedure, all Application Server 5300 components connect to the secondary database, which is in read-only mode. Writing to the database during this procedure is not permitted.

⚠️ Caution:

This procedure can cause loss of data and service interruption. Only trained administrators must perform this procedure.

Prerequisites

- The current software load matches that of the load at the time the backup was created.
- The DB backup (.tar.gz file) to be restored is located in the /var/mcp/db/backup directory.
  If the backup to restore is not in this directory, retrieve it from the remote location. If necessary, you can restore the backup directory.
- You are familiar with the procedure to synchronize the databases.
  For more information, see Synchronizing the primary and secondary databases on page 64.

Procedure

1. Log on to the primary EMS as a user with DBA role.
2. Change directory:
   ```
   cd /var/mcp/run/MCP_15.1/<mcpdb>_0/bin/util
   ```
3. Run the cleanup Replication script:
   ```
   ./cleanupReplication.pl
   ```
4. Ensure that the database backup (*.tar.gz) to restore is located in /var/mcp/db/backup:
   ```
   ls /var/mcp/db/backup
   ```
5. Change directory:
cd /var/mcp/run/MCP_15.1/<mcpdb>_0/bin/util

6. Run the restore script:
   ./dbRestore.pl <backupName>

7. From the script output, verify that the restore is complete.

8. After the restore is complete, synchronize the primary to the secondary DB:
   ./resync.pl

9. Log on to the primary EMS server as a user with AA role.

10. Change directory:
    cd /var/mcp/install

11. Run the script to stop the primary AS 5300 Element Manager:
    ./emStop.pl

12. Run the script to start the primary AS 5300 Element Manager:
    ./emStart.pl

13. For a two-server configuration, use the physical view of the AS 5300 Element Manager Console to identify the other NEs hosted by the server.

   In a four-server configuration, there are no other NEs hosted by the server.

14. Use the AS 5300 Element Manager Console to restart all other NEs in the system.

---

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;loadName&gt;</code></td>
<td>The name of the load (must match the backup load).</td>
</tr>
<tr>
<td><code>&lt;backupName&gt;</code></td>
<td>The name of the backup .tar.gz file (with or without the tar.gz extension).</td>
</tr>
<tr>
<td><code>&lt;mcpdb&gt;</code></td>
<td>The name of the database.</td>
</tr>
</tbody>
</table>

---

Restoring the database from a backup—double EMS server restore

About this task

Use this procedure to restore the primary DB when you must restore both the primary and the secondary Element Management System (EMS) servers (after a double failure). The EMS servers host the primary and secondary AS 5300 Element Manager and databases (DB).
Prerequisites

- The platform is already installed with a backup of the platform data on each EMS server. For more information, see the 102.1.1 AS 5300 Server Installation.
- Platform patches are installed on each EMS server. For more information, see the 102.1.1 AS 5300 Server Installation.
- Antivirus software is installed and configured on each EMS server. For more information, see Avaya Aura® Application Server 5300 Security, NN42040-601.
- DB is installed on each EMS server. For more information, see the 102.1.1 AS 5300 Server Installation.
- DB patches are installed on each EMS server. For more information, see the 102.1.1 AS 5300 Server Installation.
- The primary AS 5300 Element Manager has the load (in /var/mcp/loads) that matches the load of the DB backup to be restored.

❗️ Important:

If the load that is currently deployed does not match the load of the DB backup, you must perform a system downgrade to match the DB load. For more information about performing a system downgrade, see the 102.2.4 AS 5300 Release Downgrade.

- The DB backup (.tar.gz file) to be restored is located in the /var/mcp/db/backup directory.

  If the backup to restore is not in this directory, retrieve it from the remote location. If necessary, you can restore the backup directory.

- You are familiar with the procedure to synchronize the databases.

  For more information, see Synchronizing the primary and secondary databases on page 64.

Procedure

1. Log on to the primary EMS server as a user with AA role.
2. Change directory:
   ```
   cd /var/mcp/install
   ```
3. Log on to the primary EMS as a user with DBA role.
4. Run the script to deploy the database load (scripts) to the Primary and Secondary DBs:
   ```
   ./dbInstall.pl -fo
   ```
5. Ensure that the database backup (*.tar.gz) to restore is located in /var/mcp/db/backup:
   ```
   ls /var/mcp/db/backup
   ```
6. Change directory:
   ```
   cd /var/mcp/run/MCP_15.1/<mcpdb>_0/bin/util
   ```
7. Run the restore script:
   ```
   ./dbRestore.pl <backupName>
   ```
8. From the script output, verify that the restore is complete.
9. After the restore is complete, synchronize the primary to the secondary DB:
   .\resync.pl

10. Log on to the primary EMS server as a user with AA role.

11. Change directory:
    cd /var/mcp/install

12. Run the script to deploy and start the primary AS 5300 Element Manager:
    .\mcpUpgrade.pl

---

### Extracting security records from a remote backup file

**About this task**

Use this procedure to extract security records on a non-Application Server 5300 server so that you can examine them manually.

During the creation of the backup file, the -p flag preserves the permissions and ownership of the logs—normally root permission with either root or ntseclog group ownership. If the administrator does not have root access to the remote server, or belong to the ntsecgroup, they cannot read the security logs. You can use the –owner parameter to change ownership of the files when you extract (untar) the security logs.

**Important:**

Never restore security log backup files to the server. The restore of security records is not supported. Perform this procedure on the server that contains the security log .tar file.

**Prerequisites**

- The security log .tar file exists on the server.

**Procedure**

1. Change directory to the directory that contains the backup .tar file:
   
   cd <secLogDir>

2. Un-tar and change the ownership of the files:
   
   tar -owner <newowner> -xvf <secLogBackupTarFileName>

---

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;secLogDir&gt;</td>
<td>This value is the full path to the directory that contains the security logs.</td>
</tr>
</tbody>
</table>

---

October 2017 Avaya Aura® Application Server 5300 Administration

Comments on this document? infodev@avaya.com
### Extracting security records from a remote backup file job aid

This job aid provides the results of an example restore operation, and the resulting file and directory hierarchy.

```bash
[johndoe@zrc2y1a0 bkup]$ tar --owner johndoe -xvf mcpSecLogs.zrchy0qq.2007_10_26.11_57_02.tar
var/log/
var/log/messages.4
var/log/cron.5
var/log/secure.2
...
var/log/spooler.7
var/log/maillog.4
var/log/faillog var/log/cron.2
```

In this example, the new owner is johndoe and the structure of the untarred files would be as follows:

```bash
[johndoe@zrc2y1a0 bkup]$ tree -afpug var
var `-- [drwxr-x--- johndoe acnd ]
var/log | -- [-rw-r----- johndoe acnd ]
var/log/anaconda.log `-- [-rw-r----- johndoe acnd ]
var/log/anaconda.syslog `-- [drwxr-x--- johndoe acnd ]
var/log/audit |   `-- [-rw-r----- johndoe acnd ]
var/log/audit/audit.log ... | `-- [-rw-r----- johndoe acnd ]
var/log/spooler.4 | `-- [-rw-r----- johndoe acnd ]
var/log/spooler.5 | `-- [-rw-r----- johndoe acnd ]
var/log/spooler.6 | `-- [-rw-r----- johndoe acnd ]
var/log/spooler.7 | `-- [-rw-r----- johndoe acnd ]
var/log/tallylog `-- [-rw-r--r-- johndoe acnd ]
var/log/wtmp
```

### Converting from a single database to a redundant database configuration

#### Before you begin
- Your system is currently configured with a Single Database configuration.
- The system is ready to support a Replicated Database configuration (this usually means that a second server/blade has been added to the system).
• The Secondary database server has the latest platform image.
• The Primary database server has an up-to-date database loaded.

**About this task**

Use this procedure to expand your system from a single database configuration to a redundant database configuration.

**Procedure**

1. Log on the primary database server using an account that has the AA role (such as ntappadm).
2. Enter the following command to change the directory: `cd /var/mcp/install`
3. Enter the following command to edit the installprops.txt file: `edit installprops.txt`
4. In the text editor, add the following line: `db.secHost=<IP address of Secondary DB>`
5. Save the installprops.txt file.
6. Enter the following command to configure database replication: `./setupDBReplication.pl`
7. After the setupDBReplication.pl script execution completes, test the replication by completing the steps in [Testing database replication](#) on page 65.

### Variable definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;IP address of Secondary DB&gt;</code></td>
<td>The IP address of the secondary database server.</td>
</tr>
</tbody>
</table>

**Using the restore script help**

**About this task**

Use this procedure to obtain help with the restore scripts.

**Prerequisites**

- You are a user with SSA role and sudo access.

**Procedure**

Use the `-h` command line parameter when you run the restore script.

<table>
<thead>
<tr>
<th>Obtain help with</th>
<th>Enter this command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Running the server restore script</td>
<td><code>restoreSvr.pl -h</code></td>
</tr>
<tr>
<td>Running the file system integrity (FSI) baselines restore script</td>
<td><code>restoreFSI.pl -h</code></td>
</tr>
</tbody>
</table>
Using the restore script help job aid

This job aid provides additional usage information.

Usage: restoreSvr.pl [-remote|-usbdrive] <-silent> <-d debugLevel> <-s v[vv]> <-l bandwidthLimit> <-h>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-remote</td>
<td>Use to specify restore from a remote server (previously configured by the SSA).</td>
</tr>
<tr>
<td>-usbdrive</td>
<td>Use to specify restore from the USB drive inserted in the USB port of the local server.</td>
</tr>
<tr>
<td>-silent</td>
<td>Use to specify silent operation (no user input required).</td>
</tr>
<tr>
<td>-d debugLevel</td>
<td>Only for use by Avaya Support.</td>
</tr>
<tr>
<td>-s v[vv]</td>
<td>Only for use by Avaya Support.</td>
</tr>
<tr>
<td>-l bandwidthLimit</td>
<td>Use to limit the bandwidth (in kB/s) for the restore. Default: 5000.</td>
</tr>
<tr>
<td>-h</td>
<td>Use to print usage information.</td>
</tr>
</tbody>
</table>
Chapter 19: FSI restore

This section provides the procedures that you perform to restore a backup of the file system integrity (FSI) baselines. You can restore the FSI baseline backups from a remote server or locally.

**Navigation**

- Restoring FSI baseline backups remotely on page 73
- Restoring FSI baseline backups locally on page 74

**Related links**

Restoring FSI baseline backups remotely on page 73
Restoring FSI baseline backups locally on page 74

---

**Restoring FSI baseline backups remotely**

**About this task**

Use this procedure to restore the file system integrity (FSI) baseline backup from a remote server. This procedure is not required to restore server operation.

**Prerequisites**

- Configure the remote backup parameters.
  
  For more information, see Configuring remote backup and restore parameters on page 20.

- SSH is running and pass phrase authentication is enabled on the remote server.

- A backup for the server must exist on the remote server.

- If the SSH keys are pass phrase protected, you know the pass phrase.

- You are familiar with the procedures to reset the FSI baselines and to verify the FSI baselines.
  
  For more information, see Avaya Aura® Application Server 5300 Security, NN42040-601.

**Procedure**

1. Log on to the server as a user with SSA role.
2. Run the FSI restore script:
   ```bash
   restoreFSI -remote
   ```
3. If you receive a pass phrase prompt, enter the pass phrase for the SSH keys.
4. From the list of backup files, choose the backup file to restore.
5. Enter the corresponding number for the backup file to restore.
6. Press \texttt{Y} to confirm the file information.
7. From the script output, verify that the restore is complete.

The FSI baselines are in the directory defined by the FSI backup set (/var/mcp/os/baselines).

---

**Restoring FSI baseline backups locally**

**About this task**

Use this procedure to restore the file system integrity (FSI) baseline backup from the local server. This procedure is not required to restore server operation.

**Prerequisites**

- Insert the USB drive that holds the local backup files into the USB port. Ensure that no other USB drive is inserted.

**Procedure**

1. Log on to the server as a user with SSA role.
2. Run the FSI restore script:
   ```bash
   restoreFSI -usbdrive
   ```
3. If you receive a pass phrase prompt, enter the pass phrase for the SSH keys.
4. From the list of backup files, choose the backup file to restore.
5. Enter the corresponding number for the backup file to restore.
6. Press \texttt{Y} to confirm the file information.
7. From the script output, verify that the restore is complete.

The FSI baselines are in the directory defined by the FSI backup set (/var/mcp/os/baselines).
Chapter 20: Application Server 5300 re-IP

This chapter provides information about the procedures that you perform to change Internet Protocol (IP) addresses for the Application Server 5300 system (perform a re-IP). For more information, see 103.1.1 AS5300 Re-IP.

Prerequisites

• Use the AS 5300 Element Manager Console to examine system certificates to determine whether new ones are required.

For more information about how to use the AS 5300 Element Manager Console, see Avaya Aura® Application Server 5300 Configuration, NN42040-500. For information about certificate management, see Avaya Aura® Application Server 5300 Security, NN42040-601.

Important:

Network elements (NE) require a new Session Initiation Protocol (SIP) certificate if the current certificate uses either the old IP address or host name for the Subject AltName or the Common Name. If you want to update any other information, a new certificate is optional. However, Avaya recommends that you obtain a new certificate to keep certificate information current.

• Obtain and install new certificates as required.

Important:

It can take some time to request and receive certificates if a certificate authority (CA) must sign them.

• Complete all three information tabs in 103.1.1_AS5300_ReIP_20100401.xls.

Application Server 5300 re-IP procedures

About this task

This task flow shows you the sequence of procedures you perform to re-IP the Application Server 5300 core servers.
Navigation

- **Shutting down the application—core server** on page 80
- **Restoring the access control default configuration** on page 81
- **Stopping the IPsec service** on page 81
- **Performing a server re-IP** on page 82
- **Updating IP addresses for the server** on page 83
- **Updating the hostname and clock source** on page 83
- **Updating the AS 5300 Element Manager and database IP addresses** on page 85
- **Updating NE IP addresses, hostnames, and certificates** on page 85
- **Updating the Avaya Media Server IP addresses** on page 86
- **Shutting down the application and the database** on page 87
- **Configuring ACL** on page 87
- **Configuring IPSec** on page 88
- **Starting the application and the database** on page 88
Chapter 21: Avaya Media Server re-IP

This chapter provides information about the procedures that you perform to change Internet Protocol (IP) addresses for an Avaya MS cluster system (perform a re-IP). For more information, see 103.1.1 AS5300 Re-IP.

Prerequisites

- Use the AS 5300 Element Manager Console to examine system certificates to determine whether new ones are required.

  For more information about how to use the AS 5300 Element Manager Console, see Avaya Aura® Application Server 5300 Configuration, NN42040-500. For information about certificate management, see Avaya Aura® Application Server 5300 Security, NN42040-601.

  Important:

  Network elements (NE) require a new Session Initiation Protocol (SIP) certificate if the current certificate uses either the old IP address or host name for the Subject AltName or the Common Name. If you want to update any other information, a new certificate is optional. However, Avaya recommends that you obtain a new certificate to keep certificate information current.

- Obtain and install new certificates as required.

  Important:

  It can take some time to request and receive certificates if a certificate authority (CA) must sign them.

- Complete all three information tabs in 103.1.1_AS5300_ReIP_20100401.xls,
Navigation

- Shutting down the application—Avaya Media Server on page 81
- Restoring the access control default configuration on page 81
- Stopping the IPsec service on page 81
- Performing a server re-IP on page 82
- Updating IP addresses for the server on page 83
- Updating the hostname and clock source on page 83
- Updating NE IP addresses, hostnames, and certificates on page 85
- Updating the Avaya Media Server IP addresses on page 86
- Shutting down the application and the database on page 87
- Configuring ACL on page 87
- Configuring IPSec on page 88
- Starting the application and the database on page 88
Chapter 22: Re-IP procedures

This chapter provides the procedures that you require to perform a re-IP of Application Server 5300 server or Avaya Media Server (MS). For more information about the order in which to perform these procedures, see the following sections:

- Application Server 5300 re-IP on page 75
- Avaya Media Server re-IP on page 77

Prerequisites

- Use the AS 5300 Element Manager Console to examine system certificates to determine whether new ones are required.

For more information about how to use the AS 5300 Element Manager Console, see Avaya Aura® Application Server 5300 Configuration, NN42040-500. For information about certificate management, see Avaya Aura® Application Server 5300 Security, NN42040-601.

⚠️ Important:

Network elements (NE) require a new Session Initiation Protocol (SIP) certificate if the current certificate uses either the old IP address or host name for the Subject AltName or the Common Name. If you want to update any other information, a new certificate is optional. However, Avaya recommends that you obtain a new certificate to keep certificate information current.

- Obtain and install new certificates as required.

⚠️ Important:

It can take some time to request and receive certificates if a certificate authority (CA) must sign them.

- Complete all three information tabs in 103.1.1_AS5300_ReIP_20100401.xls,

Insert content for the first section.

Navigation

- Shutting down the application—core server on page 80
- Shutting down the application—Avaya Media Server on page 81
- Restoring the access control default configuration on page 81
- Stopping the IPsec service on page 81
- Performing a server re-IP on page 82
- Updating IP addresses for the server on page 83
- Updating the hostname and clock source on page 83
Shutting down the application—core server

About this task
Use this procedure to shut down the application before you perform a re-IP of an Application Server 5300 core server.

Procedure

1. Use the AS 5300 Element Manager Console to stop all network element instances, except the primary AS 5300 Element Manager (EM_0).
2. Log on to the server that hosts the primary AS 5300 Element Manager instance (EM_0) as a user with AA role.
3. Change directory:
   
```
cd /var/mcp/install
```
4. Stop the primary AS 5300 Element Manager instance (EM_0):
   
```
./emStop.pl
```
Shutting down the application—Avaya Media Server

About this task
Use this procedure to shut down the application before you perform a re-IP of an Avaya MS.

Prerequisites
- You are familiar with the procedure to stop an NE. For more information, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*.
- You are familiar with Avaya MS configuration. For more information, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*.

Procedure
1. Use the AS 5300 Element Manager to stop both the primary and secondary Avaya MS.
2. Break the cluster (remove the secondary server from the primary Avaya MS configuration and make the secondary Avaya MS primary).

Restoring the access control default configuration

Use this procedure for troubleshooting purposes, to restore the default configuration for access control (trusted nodes, trusted ports, and DSCP marking).

Before you begin
- You are a user with SSA role and sudo access.

Procedure
1. Log on to the server as an SSA.
2. At the prompt, enter `iptcfg`.
3. If you receive a prompt, enter your password.
4. Enter `7` to select Restore System Defaults.
5. Enter `Y` to confirm the rollback to the system defaults.

Stopping the IPsec service

Use this procedure to stop the IPsec service.

Before you begin
- You are a user with SSA role and sudo access.
Procedure

1. Log on to the server as a user with SSA role.
2. At the command prompt, enter the following command:
   
   stopipsec

Performing a server re-IP

About this task

Use this procedure to perform a re-IP of an Application Server 5300 server, or an Avaya MS. Repeat this procedure for each server to be re-IPed.

Prerequisites

- You are familiar with the procedure to update the following addresses:
  - Internal OAM (Default) IP address
  - External OAM IP address
  - Signaling IP address
  - Media IP address

For more information, see Updating IP addresses for the server on page 83.

- You are familiar with the procedure to update the host name and the clock source for the server. For more information, see Updating the hostname and clock source on page 83.

Procedure

1. Use the console port or KVM to log on to the server as a user with SSA role.
2. If the server hosts a database, stop the database:

   stopDB

3. If the new IP address is not in the same bond or vlan interface, update the Internal OAM (Default) IP address of the server.
4. Update the hostname and the primary and secondary clock source for the server.
5. Update the External OAM Address for the server.
6. Update the Signaling IP address for the server.
7. Update the Media IP address for the server.
8. If the server hosts a database, start the database:

   startDB
Updating IP addresses for the server

About this task
Use this procedure to update each the following IP addresses for the server if the new IP addresses are not in the same bond or vlan interface:

- Internal OAM (Default) IP address
- External OAM IP address
- Signaling IP address
- Media IP address

⚠ Important:
Perform this procedure for each IP address to be updated.

Procedure

1. If the new interface does not exist, create a new bond interface:

   mcpAddBondNif [-name <name of bonded network Interface>] -slaves <name of physical Ethernet network interface> [<name of physical Ethernet network interface>]

   ⚠ Important:
   The <second slave ethernet> is optional.

2. To create a new vlan interface:

   mcpAddVlanNif -parent <name of bonded network interface> -vid <VLAN ID number>

3. Update the server address:

   mcpModIPv4Subnet -name <name of subnet> -nif <new bonded/vlan network interface> [-addr <new IPv4 address on the subnet/subnet prefix length>] [-router <new IPv4 address of subnet default router>]

   ⚠ Important:
   The <NIF Name> can be a bond interface, (for example, . bond0) or a vlan interface (for example, . bond0.123).

Updating the hostname and clock source

About this task
Use this procedure to update the hostname and clock source for a server, during the re-IP procedure.
**Procedure**

1. Use the console port or KVM to log on to the server.
2. Run the reconfigure.pl script:
   ```
   reconfigure.pl
   ```
3. At the password prompt, enter the root password.
4. Enter the new hostname.
5. To confirm this is correct, enter `Y`.
6. To use the default value for this timezone, enter `Y`.
7. At the prompt **Do you wish to configure/display the Audit configuration?**, enter `Q`.
8. At the prompt **Do you wish to configure/display the NTP configuration?**, enter `C`.
9. Specify the Clock Source (NTP) function of the server.
   - Select 1 for a Primary EM Server
   - Select 2 for a Secondary EM Server
   - Select 3 for a Network Element (NE) Server
10. At the **Select an option (E,I)** prompt, enter `I`. **Option I** configures the server to use the Internal Clock as the time source. See *Application Server 5300 Security, NN42040–601* for information about other NTP configuration options.
11. For the Primary Clock Source Server, enter the Machine Logical IP Address of the Secondary Clock Source Server -> `<New Secondary Clock Source>`.
12. For the Secondary Clock Source Server, enter the Machine Logical IP Address of the Primary Clock Source Server -> `<New Primary Clock Source>`.
13. For all other servers:
   - Enter the Machine Logical IP Address of Primary Clock Source Server -> `<New Primary Clock Source>`
   - Enter the Machine Logical IP Address of Secondary Clock Source Server -> `<New Secondary Clock Source>`
14. To skip Grub password configuration, enter `Q`.
15. To skip SysLog Configuration, enter `Q`.
Updating the AS 5300 Element Manager and database IP addresses

About this task

Use this procedure to update the IP addresses for the AS 5300 Element Manager and the database (DB), during a server re-IP.

Procedure

1. Log on to the server that hosts the EM_0 instance as a user with AA role.
2. Change directory.
   ```
   cd /var/mcp/install
   ```
3. Edit installprops.txt file as follows:
   - Update the ne.mgmt.ip field with the new IP address of the primary EM server.
   - Update the db.host field with the new Primary database IP address.
   - Update the db.sechost field with the new Secondary database IP address.
4. Run the script to deploy the database load (scripts) to the Primary and Secondary DBs:
   ```
   ./dbInstall.pl -fo
   ```
5. Run the script to deploy the software:
   ```
   ./emDeploy.pl
   ```
6. Run the script to update the IPAddr.txt file:
   ```
   ./addrListUpdate.pl -i IPAddr.txt
   ```
7. Run the script to start the AS 5300 Element Manager:
   ```
   ./emStart.pl
   ```

Updating NE IP addresses, hostnames, and certificates

About this task

Use this procedure to update the IP addresses, hostnames, and certificates for the AS 5300 Element Manager and other network elements (NE), after server re-IP.

Prerequisites

- You can access the AS 5300 Element Manager Console.
- You are familiar with the procedure to configure a server. For more information, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.
Procedure

1. Use the new service IP address of the AS 5300 Element Manager to open the AS 5300 Element Manager Console.
2. Log on to the AS 5300 Element Manager Console.
3. Update the server configuration for each server that has a new hostname.
4. Use the AS 5300 Element Manager Console to update the certificate for the AS 5300 Element Manager and for the other NEs as required.
5. Log off from the AS 5300 Element Manager Console.
6. Log on to the server that hosts the EM_0 instance as a user with AA role.
7. Change directory:
   ```
   cd /var/mcp/install
   ```
8. Stop the AS 5300 Element Manager:
   ```
   ./emStop.pl
   ```
9. Start the AS 5300 Element Manager:
   ```
   ./emStart.pl
   ```
10. Use the AS 5300 Element Manager Console to deploy and start all of the network element instances.
11. Verify the state of all network element instances.

Updating the Avaya Media Server IP addresses

About this task

Use the following procedure to update the IP addresses for each Avaya Media Server (MS). For more information about Avaya MS configuration and management, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.

Procedure

1. Log on to the AS 5300 Element Manager Console.
2. Stop the Avaya MS network element: In the Configuration view of the AS 5300 Element Manager Console, select Network Elements > NE type > NE instance > NE Maintenance. In the Maintenance pane, select the network element to stop, and click Stop.
3. In the Configuration view of the console, select Servers.
4. Update the IP Addresses:
   - Signalling: Signalling New IP Address
   - Media: Media New IP Address
• Cluster: OAM Internal New IP Address
• OAM: External OAM New IP address

5. Click **Apply**.

6. Start the Avaya MS network element: In the Configuration view of the AS 5300 Element Manager Console, select **Network Elements > NE type > NE instance > NE Maintenance**. In the Maintenance pane, select the network element to start, and click **Start**.

---

**Shutting down the application and the database**

**About this task**

Use this procedure to shut down the AS 5300 Element Manager and database (DB) before you update the Access Control List (ACL) configuration after server re-IP.

**Procedure**

1. Use the AS 5300 Element Manager Console to stop all network element (NE) instances except the EM_0 instance.
2. Log onto the server that hosts the EM_0 instance, as a user with AA role.
3. Change directory:
   
   ```bash
   cd /var/mcp/install
   ```
4. Stop the EM_0 instance:
   
   ```bash
   ./emStop.pl
   ```
5. Use the console port or KVM to log on to the server that hosts the primary database, as an SSA.
6. Stop the primary database:
   
   ```bash
   stopDB
   ```
7. Use the console port or KVM to log on to the server that hosts the secondary database, as an SSA.
8. Stop the secondary database:
   
   ```bash
   stopDB
   ```

---

**Configuring ACL**

**About this task**

After a server re-IP, you must update the Access Control List (ACL) configuration if the system uses ACL.
Prerequisites

• You have a copy of 105.13 AS5300 Security Hardening.

Procedure

To update the ACL configuration after ReIP, follow the instructions in Section 8.1.11 of 105.13 AS5300 Security Hardening.

Configuring IPSec

About this task

After a server re-IP, you must update the IP Secure (IPSec) configuration if the system uses IPSec.

Prerequisites

• You have a copy of 105.13 AS5300 Security Hardening.

Procedure

1. To update the IPSec mesh configuration, follow the instructions in IPSec configuration Section 8.1.10 of 105.13 AS5300 Security Hardening.

2. To update external node configuration, follow the instructions in IPSec external node configuration Section 9.2.2 of 105.13 AS5300 Security Hardening.

Starting the application and the database

About this task

Use this procedure to start the primary AS 5300 Element Manager, database, and other network elements (NE).

Procedure

1. Use the console port or KVM to log on to the server that hosts the primary database, as a user with SSA role.

2. Start the primary database:

   startDB

3. Use the console port or KVM to log on to the server that hosts the secondary database, as an SSA.

4. Start the secondary database:

   startDB

5. Log onto the server that hosts the EM_0 instance, as a user with AA role.
6. Change directory:
   
   cd /var/mcp/install

7. Start the EM_0 instance:
   
   ./emStart.pl

8. Log on to the AS 5300 Element Manager Console.

9. Use the AS 5300 Element Manager Console to start all of the other network element instances.

10. Use the AS 5300 Element Manager Console to verify all of the network element instances, and to ensure that there are no unacknowledged alarms.

    For more information, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*. 

   

Chapter 23: Power outage recovery

After a power outage, you power up the servers in a specific order, which is not the way the system comes up if you power on all servers at the same time.

Power outage recovery procedures

About this task
This task flow shows you the sequence of procedures you perform to recover after a power outage.
Powering on the database server

About this task
Use this procedure to fully power on the server that hosts the database and to ensure that database is running.

Procedure
1. Power on the database server fully.
   It takes from 5 to 8 minutes for the server to boot and load the database application.
2. Log on to the server as a user with DBA role.
3. Verify that the database is running by entering the following command:
   ```
   cd /opt/mcp/db/bin ./dbMonitor.pl
   ```
   The script output shows the status of the listener and the database, for example:
   ```
   [ntdbadm@zngdyljz bin]$ ./dbMonitor.pl Database is up
   ```

Stopping and starting the database

About this task
If necessary, you can stop and restart the database.

Prerequisites

⚠️ Caution:
The commands in the following procedure severely affect service.

Procedure
1. Use KVM or SSH to connect to the database server and log on as a user with SSA role.
2. Enter:
   ```
   su - root
   ```
3. Change directory:
   \cd /etc/rc.d/init.d
4. Enter the command.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start the database</td>
<td>./dbora start</td>
</tr>
<tr>
<td>Stop the database</td>
<td>./dbora stop</td>
</tr>
</tbody>
</table>

Verifying that the AS 5300 Element Manager processes are running

About this task
Verify that the AS 5300 Element Manager processes are running to control the Application Server 5300 components from the AS 5300 Element Manager Console.

Procedure
1. Use KVM or SSH to connect to the AS 5300 Element Manager/Accounting Manager server as a user with AA role.
2. Enter:
   \neinit -p
3. If the processes are running, you see output similar to the following:

```
[root@ibm5 root]# neinit -p
Release Name Pid
------- ---- ----
MCP_15.1 EM_0 2344
```

Stopping and starting the AS 5300 Element Manager

About this task
Use this procedure to start and stop the AS 5300 Element Manager on the Element Management System (EMS) server.

Prerequisites
- You are familiar with the procedure to restart a network element. For more information, see Restarting a network element on page 111.
Verifying the status of other servers and components

**About this task**
Verify the status of other servers and components.

**Procedure**

1. Launch the AS 5300 Element Manager Console.
2. In the configuration view, expand each network element.

3. To view the status of a network element, from the configuration view, select **NE Maintenance**.

4. If the clients cannot communicate with the AS 5300 Session Manager, restart the AS 5300 Session Manager.

5. If you want to watch the AS 5300 Session Manager startup logs, use KVM or SSH to connect to the AS 5300 Session Manager and log on as a user with AA role.

6. Change directory:

```bash
    cd /var/mcp/oss/log/EM/all/MCP/<NE NAME>
```

7. Enter:

```bash
    supertail -f *.active
```

8. To verify that the SNMP process is running, enter:

```bash
    ps -ef | grep snmp
```

9. If you do not see the SNMP process running, or if an alarm in the AS 5300 Element Manager Console indicates that there is a problem with the AS 5300 Session Manager SNMP, stop the process.

    The process automatically restarts in 30 seconds.

10. If you want to watch NE startup logs, use KVM or SSH to connect to the AS 5300 Element Manager server and log on as a user with AA role.

11. Change directory:

```bash
    cd /var/mcp/oss/log/EM/all/MCP/<NE NAME>
```

12. Enter:

```bash
    tail -f *.active
```

13. To verify that the SNMP process is running, enter:

```bash
    ps -ef | grep snmp
```

**Important:**

A user logged on as root can use the following command to verify that the SNMP process is running:

```bash
    service snmpd status snmpd (pid 3909) is running
```

14. If you do not see the SNMP process running, stop the process.

    The process automatically restarts in 30 seconds.

15. To verify whether the Provisioning Manager is operating properly, log on to the Provisioning Client.

16. In the **User** portlet, type the name of a user and click **Search**.
17. If the browser does not respond properly, restart the Provisioning Manager (PROV).

18. To verify that the SNMP process is running, enter:

   `ps -ef | grep snmp`

19. If you do not see the SNMP process running or if an alarm in the AS 5300 Element Manager Console indicates that there is a problem with the PROV SNMP, stop the process. The process automatically restarts in 30 seconds.
Chapter 24: Network data management

This chapter provides the procedures that you perform to manage network data (organized in the AS 5300 Element Manager Console under Network Data and Mtc). For information about how to configure network data, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500.*

**Navigation**

- [Enabling HTTP DoS mitigation](#) on page 97
- [Enabling SIP DoS mitigation](#) on page 97
- [Editing the IP address table](#) on page 97
- [Configuring a trusted node](#) on page 98
- [Configuring an external node](#) on page 100
- [Deleting an external node](#) on page 101
- [Configuring an informational element](#) on page 101
- [Deleting an informational element](#) on page 103
- [Configuring an SNMP profile](#) on page 103
- [Deleting an SNMP profile](#) on page 104
- [Configuring a site](#) on page 105
- [Deleting a site](#) on page 106
- [Updating a license key](#) on page 106
- [Querying a license key](#) on page 107

**Related links**

- [Enabling HTTP DoS mitigation](#) on page 97
- [Enabling SIP DoS mitigation](#) on page 97
- [Editing the IP address table](#) on page 97
- [Configuring a trusted node](#) on page 98
- [Configuring an external node](#) on page 100
- [Deleting an external node](#) on page 101
- [Configuring an informational element](#) on page 101
- [Deleting an informational element](#) on page 103
- [Configuring an SNMP profile](#) on page 103
- [Deleting an SNMP profile](#) on page 104
- [Configuring a site](#) on page 105
- [Deleting a site](#) on page 106
Enabling HTTP DoS mitigation

About this task
Enable Hypertext Transfer Protocol (HTTP) Denial of Service (DoS) Mitigation feature to protect the Web server from DoS attacks.

Procedure
1. From configuration view of the AS 5300 Element Manager Console, select the Provisioning Managers > <PROV> > Configuration Parameters.
2. From the Parm Group list, select HTTPDoS Parm Group.

Enabling SIP DoS mitigation

About this task
Enable the Session Initiation Protocol (SIP) DoS mitigation feature to protect the call server from DoS attacks.

Procedure
1. From the AS 5300 Element Manager Console, select the Session Managers > <SESM> > Configuration Parameters.
2. From the Parm Group list, select SIPDoS Parm Group.
3. Configure the Enable DoS filter attribute to true.

Editing the IP address table

About this task
Use this procedure to edit entries in the IPv4 or IPv6 address table.

Prerequisites
• You can access the AS 5300 Element Manager Console.
• You have AddressService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Addresses > IPv4 Addresses / IPv6 Addresses**.
2. On the IPv4/IPv6 Addresses window, select Logical Name, and click **Edit (-/+)**.
3. On the Edit IPv4/IPv6 Address window, configure the address.
4. Click **Apply**.

---

## Configuring a trusted node

### About this task
Perform this procedure to configure an Informational Element, or trusted node, and to prevent the Session Initiation Protocol (SIP) Denial of Service (DoS) mitigation feature from blocking messages generated by the external SIP proxies or SIP test tools.

### Prerequisites
• You can access the AS 5300 Element Manager Console.
• You have NodeService privileges.
• You have InfoElementService privileges.

### Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Addresses > IPv4 Addresses / IPv6 Addresses**.
2. In the IPv4/IPv6 Addresses window, click **Add (+)**.
3. Type the **Logical Name** and **IP Address**, and click **Apply**.
4. Select **External Nodes**.
5. In the External Nodes window, click **Add (+)**.
6. Type the **Name** of the external node, select an **IPv4 Address** for the external node, and optionally select an **IPv6 Address** for the external node.
7. Click **Apply**.
8. Select Informational Elements.
9. In the Informational Elements window, click **Add (+)**.
10. Configure the **ShortName**, **LongName**, **Trusted**, **ExemptDosProtection**, **Port**, and **Type** parameters.
11. In the **Transport Information** section, configure the **Node**, **Enable SIP UDP Port**, **SIP UDP Port**, **Enable SIP TCP Port**, **SIP TCP Port**, **Enable SIP TLS Port**, and **SIP TLS Port** parameters as required.
**Important:**

Systems that do not use Transport Layer Security (TLS) and Secure Real-time Transport Protocol (SRTP) use UDP and RTP. The Audiocodes Mediant 3000 does not support best effort RTP/SRTP (mixed-mode). The configuration for all endpoints must be either secure or nonsecure for media.

12. Click **Apply**.

---

**Informational elements job aid**

The following are the supported informational element types:

- Gateway: select for the IP address of a gateway such as the Communications Server 1000.
- General: select for an IP address that is not a gateway or Avaya Media Server (MS).
- Avaya MS: select for an address of a Avaya MS.
- Media Portal Resource: select for the address of a Media Portal resource.
- Pooled Media Resource: select for the address of a Pooled Media resource.

---

**Configuring a trusted node job aid**

**About this task**

The following table lists and describes the parameters for trusted node configuration.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>The name of the device.</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 6</td>
</tr>
<tr>
<td>LongName</td>
<td>The long name of the device (same as the description of a long</td>
</tr>
<tr>
<td></td>
<td>name parameter for a Network Element).</td>
</tr>
<tr>
<td></td>
<td>Maximum characters: 32</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the informational element is trusted. The informational</td>
</tr>
<tr>
<td></td>
<td>element is trusted for SIP communications only, not for any other protocol.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service</td>
</tr>
<tr>
<td></td>
<td>Protection.</td>
</tr>
<tr>
<td>Port</td>
<td>Specifies the port.</td>
</tr>
<tr>
<td></td>
<td>Range: 0– 65 534</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies the informational element type.</td>
</tr>
</tbody>
</table>

*Table continues...*
### Configuring an external node

**About this task**

Configure an external node to add multiple Informational Elements with the same IP address and different ports.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have NodeService privileges.
- The IP address of the external node exists in the address table. For more information, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > External Nodes**.
2. Click **Add** or select an entry and click **Edit**.
3. In the **Add External Node** or **Edit External Node** dialog box, configure the **Name** and **Address** parameters.
4. Click **Apply**.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>External node of the informational element.</td>
</tr>
<tr>
<td>Enable SIP UDP Port</td>
<td>Enables the SIP UDP port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP Port</td>
<td>Enables the SIP TCP port. Selected = enabled Not selected = disabled Example: 5060</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP. Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TLS Port</td>
<td>Enables the SIP TLS port. Selected = enabled Not selected = disabled</td>
</tr>
<tr>
<td>SIP TLS Port</td>
<td>Specifies the TLS port for SIP. Example: 5061</td>
</tr>
</tbody>
</table>
Configuring an external node job aid

The following table lists and describes the parameters used to configure an external node.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the device (1–16 alphanumeric characters)</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>The IPv4 address of the device (select from the list). You must configure an IPv4 address for each node.</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>The IPv6 address of the device (select from the list). This field is optional.</td>
</tr>
</tbody>
</table>

Deleting an external node

About this task

You can delete an external node that the Application Server 5300 does not use.

Prerequisites

- You have NodeService privileges.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > External Nodes.
2. From the External Nodes window, select an entry.
3. Click Delete.
4. Click Yes to confirm the delete.

Configuring an informational element

About this task

Use the following procedure to configure an informational element to provide device type information.

Prerequisites

- You have NodeService privileges.
**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Informational Elements.**
2. Click **Add** or select an entry and click **Edit.**
3. In the **Add Informational Element (IE) **dialog box, configure the **ShortName, LongName, Trusted, ExemptDoSProtection, Port, Type**, parameters.
4. In the **Transport Information** section, configure the **Node, Enable SIP UDP Port, SIP UDP Port, Enable SIP TCP Port, SIP TCP Port, Enable SIP TLS Port, and SIP TLS Port** parameters as required.
5. Click **Apply.**

---

**Configuring an informational element job aid**

This job aid lists and describes the parameters for configuring an informational element.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ShortName</td>
<td>The name of the device.</td>
</tr>
<tr>
<td>LongName</td>
<td>The long name of the device (same as the description of a long name parameter for a Network Element)</td>
</tr>
<tr>
<td>Port</td>
<td>An integer from 0 to 65 534.</td>
</tr>
<tr>
<td>Trusted</td>
<td>Specifies whether the informational element is trusted.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> The informational element is trusted for SIP communications only, not for any other protocol.</td>
</tr>
<tr>
<td>ExemptDoSProtection</td>
<td>Specifies whether the informational element is exempt from Denial of Service Protection.</td>
</tr>
<tr>
<td>Type</td>
<td>The informational element type.</td>
</tr>
<tr>
<td>Node</td>
<td>An External node configured.</td>
</tr>
<tr>
<td>Enable SIP UDP Port</td>
<td>Enables the SIP UDP port.</td>
</tr>
<tr>
<td></td>
<td>Selected = enabled</td>
</tr>
<tr>
<td></td>
<td>Not selected = disabled</td>
</tr>
<tr>
<td>SIP UDP Port</td>
<td>Specifies the UDP port for SIP.</td>
</tr>
<tr>
<td></td>
<td>Example: 5060</td>
</tr>
<tr>
<td>Enable SIP TCP Port</td>
<td>Enables the SIP TCP port.</td>
</tr>
<tr>
<td></td>
<td>Selected = enabled</td>
</tr>
<tr>
<td></td>
<td>Not selected = disabled</td>
</tr>
<tr>
<td>SIP TCP Port</td>
<td>Specifies the TCP port for SIP.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Deleting an informational element

**About this task**

You can delete informational elements that the Application Server 5300 does not use.

**Prerequisites**

- You have NodeService privileges.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Informational Elements**.
2. From the Informational Element window, select an entry.
3. Click **Delete**.
4. Click **Yes** to confirm the delete.

### Configuring an SNMP profile

**About this task**

Configure an Simple Network Management Protocol (SNMP) profile to establish consistent SNMP parameters that the AS 5300 Element Manager uses to monitor the condition of the operating system and server hardware for the managed and monitored Application Server 5300 network elements.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have SnmpProfileService privileges.
- The license key is updated. For more information about how to update the license key, see [Updating a license key](#) on page 106.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable SIP TLS Port</td>
<td>Enables the SIP TLS port.</td>
</tr>
<tr>
<td></td>
<td>Selected = enabled</td>
</tr>
<tr>
<td></td>
<td>Not selected = disabled</td>
</tr>
</tbody>
</table>

Example: 5060

<table>
<thead>
<tr>
<th>SIP TLS Port</th>
<th>Specifies the TLS port for SIP.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Example: 5061</td>
</tr>
</tbody>
</table>
Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > SNMP Profiles.

2. Click Add

   OR

   Select an entry and click Edit.

3. Configure the Profile Name, SNMP Port, Read Community String, and Write Community String parameters.

4. Click Apply.

---

Configuring an SNMP Profile job aid

The following table describes the parameters that you use to configure an SNMP profile.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>A unique name to identify the profile</td>
</tr>
<tr>
<td>SNMP Port</td>
<td>The port that SNMP uses</td>
</tr>
<tr>
<td>Read Community String</td>
<td>Public</td>
</tr>
<tr>
<td>Write Community String</td>
<td>Private</td>
</tr>
</tbody>
</table>

⚠️ Important:

For security reasons, Avaya recommends that customers change the default Read and Write Community Strings. Each value can be any string of 31 characters, composed of the following characters: a-z, A-Z, 0-9, _, -

---

Deleting an SNMP profile

About this task

You can remove Simple Network Management Protocol (SNMP) profiles that the servers do not use.

⚠️ Important:

Before deleting an SNMP Profile, edit any servers that use the profile and configure the servers to use a different SNMP Profile.

Prerequisites

- The SNMP profile must not be used by any server.
Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > SNMP Profiles**.
2. Select an entry from the SNMP Profiles window.
3. Click **Delete**.
4. Click **OK** to confirm the delete.

---

Configuring a site

**About this task**

Use the following procedure to add or edit a sites or site information about the servers.

**Prerequisites**

- You can access the AS 5300 Element Manager Console.
- You have PhysicalSiteService privileges.

**Procedure**

1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Physical Sites**.
2. Click **Add (+)**
3. Configure the **Site Name**, **Zone**, **Easting**, and **Northing** parameters.
4. Click **Apply**.

---

Configuring a site job aid

The following table lists and describes the parameters for configuring a site.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site Name</td>
<td>This parameter is a unique name identifying the site.</td>
</tr>
<tr>
<td></td>
<td>Range: 1–20 alphanumeric characters</td>
</tr>
<tr>
<td>Zone</td>
<td>This parameter is the Universal Transverse Mercator (UTM) zone location of this site.</td>
</tr>
<tr>
<td></td>
<td>Range: 1–3 alphanumeric characters</td>
</tr>
<tr>
<td>Easting</td>
<td>This parameter is the Easting of the site.</td>
</tr>
<tr>
<td></td>
<td>Range: 1–1 000 000 digits For numbers greater than 1 100, do not enter spaces.</td>
</tr>
<tr>
<td>Northing</td>
<td>This parameter is the northing of the site.</td>
</tr>
<tr>
<td></td>
<td>Range: 1–7 digits</td>
</tr>
</tbody>
</table>
Deleting a site

About this task
You can delete a site that the Application Server 5300 does not use.

⚠️ Important:
Administrators must delete all the servers and network elements of a site, before deleting the site itself.

Prerequisites
• You have PhysicalSiteService privileges.
• The site does not contain servers or network elements.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Physical Sites.
2. From the Physical Site window, select the site.
3. Click Delete.
4. Click Yes to confirm the delete.

Updating a license key

About this task
Update a license key to push the key codes automatically down to all elements with a registered interest.

Prerequisites
• You have LicenseKeyService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select Network Data and Mtc > Licensekey.
2. From the Licensekey panel, select the license that you want to update.
3. Click Edit (-/+).
4. Navigate to the license key file that is on the local computer.
5. Select the license key file.
6. Click Open.
Querying a license key

About this task
You can view version information for license keys, and the number of available license units. You can also view license information for network elements, network elements with ports, features, and feature states.

Prerequisites
• You have LicenseKeyService privileges.

Procedure
1. From the configuration view of the AS 5300 Element Manager Console, select **Network Data and Mtc > Licensekey**.
2. From the Licensekey panel, select a tab.

<table>
<thead>
<tr>
<th>Choose to view</th>
<th>Select</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version information</td>
<td>Version Info</td>
</tr>
<tr>
<td>Available license units</td>
<td>Licenseable Units</td>
</tr>
<tr>
<td>License information for network elements</td>
<td>Network Elements</td>
</tr>
<tr>
<td>License information for network elements with ports</td>
<td>Network Elements with Ports</td>
</tr>
<tr>
<td>License information for features</td>
<td>Features</td>
</tr>
<tr>
<td>License information for feature states</td>
<td>Feature States</td>
</tr>
<tr>
<td>License information for applications or services</td>
<td>Applications</td>
</tr>
</tbody>
</table>
Chapter 25: Network element management

This chapter provides the procedures you perform to manage Application Server 5300 network elements. For information about how to configure network elements, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*.

Navigation

- Deploying and starting the primary AS 5300 Element Manager on page 108
- Starting a network element on page 109
- Stopping a network element on page 110
- Deploying a network element on page 110
- Undeploying a network element on page 111
- Restarting a network element on page 111
- Killing a network element on page 112
- Deleting a network element on page 113

Related links

- Deploying and starting the primary AS 5300 Element Manager on page 108
- Starting a network element on page 109
- Stopping a network element on page 110
- Deploying a network element on page 110
- Undeploying a network element on page 111
- Restarting a network element on page 111
- Killing a network element on page 112
- Deleting a network element on page 113

Deploying and starting the primary AS 5300 Element Manager

**About this task**

Use this procedure to deploy and restart the primary AS 5300 Element Manager. The AS 5300 Element Manager must be active before you can use the AS 5300 Element Manager Console to manage the secondary AS 5300 Element Manager and other network elements (NE).
Procedure

1. Log on to the primary Element Management System (EMS) server as a user with AA role.
2. Change directory:
   `cd /var/mcp/install`
3. Run the script to deploy the software:
   `./emDeploy.pl`
4. Run the script to start the AS 5300 Element Manager:
   `./emStart.pl`

Starting a network element

About this task
Perform this procedure to start a network element instance.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Procedure

1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > `<NE type>` > `<NE instance>` > NE Maintenance.
2. In the Maintenance panel, select the network element to start, and click Start.
   The time required to complete the process depends on the network element type and the hosting server.
3. (Optional) To view the maintenance and operational states of the transition, click Details.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;NE type&gt;</code></td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td><code>&lt;NE instance&gt;</code></td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>
Stopping a network element

Perform this procedure to stop a network element instance.

⚠️ Important:
- When the AS 5300 Element Manager stops, your AS 5300 Element Manager Console window closes.
- When an Avaya MS NE stops, any conference recordings that are in progress, are lost.

⚠️ Note:

Before you begin
- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Procedure

1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance panel, select the network element to stop, and click Stop.

The time required to complete the process depends on the network element type and the hosting server.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>

Deploying a network element

About this task

Perform this procedure to deploy a network element instance.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Procedure

1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance panel, select the instance to deploy, and click Deploy.
   Software transfers from the AS 5300 Element Manager to the server associated with the
   selected network element instance.
3. (Optional) To view the maintenance and operational states of the transition, click Details.
4. If the network element is fault tolerant, select the other instance and click Deploy.

Undeploying a network element

About this task
Use this procedure to undeploy a network element.

⚠️ Important:
If you undeploy an AS 5300 Session Manager instance, IPv6 and service address
configurations are lost. You must use the ipv6config tool to reconfigure IPv6.

Prerequisites
- You can access the AS 5300 Element Manager Console.
- You have NEService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network
   Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance panel, select the instance to deploy, and click Undeploy.
   Software transfers from the AS 5300 Element Manager to the server associated with the
   selected network element instance.
3. (Optional) To view the maintenance and operational states of the transition, click Details.
4. If the network element is fault tolerant, select the other instance and click Undeploy.

Restarting a network element

About this task
The Restart operation performs a combined stop and start. During the period of the restart, the
network element instance does not provide service. There is no difference between performing a
restart, or stopping and starting a network element (NE) instance. Restart a network element
instance to apply configuration changes, or as a troubleshooting step.
Important:
You cannot restart the active AS 5300 Element Manager from the AS 5300 Element Manager Console. It can only be restarted from the command line. When the AS 5300 Element Manager stops, your AS 5300 Element Manager Console window closes.

Prerequisites
• You can access the AS 5300 Element Manager Console.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. From the Maintenance panel, select the instance to restart, and click Restart.
3. To confirm the restart, click Yes.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;NE type&gt;</td>
<td>This value is the type of network element, such as Accounting Managers.</td>
</tr>
<tr>
<td>&lt;NE instance&gt;</td>
<td>This is the network element, such as the Accounting Manager.</td>
</tr>
</tbody>
</table>

Killing a network element

About this task
Use this procedure to kill a network element (NE).

Prerequisites
• You can access the AS 5300 Element Manager Console.
• You have NEService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. In the Maintenance panel, select the network element to kill, and click Kill.
   The time required to complete the process depends on the network element type and the hosting server.
Deleting a network element

About this task
Use this procedure to delete a network element on the Application Server 5300.

⚠ Caution:
You can delete a network element on a server. However, before you remove any network element, contact your next level of support to determine the potential effect on the system.

Prerequisites
• You have NEService and NEInstanceService privileges.

Procedure
1. In the configuration view of the AS 5300 Element Manager Console, select Network Elements > <NE type> > <NE instance> > NE Maintenance.
2. From the Maintenance window, select each network element instance and click Stop.
3. Click Yes to confirm the Stop.
4. From the Maintenance window, select each network element instance and click Undeploy.
5. From the configuration view, select Network Elements > <ne_type> > <ne>> Instance to view a list of the configured network element instances for this network element.
6. From the Instance window, select each entry and click Delete.
7. To confirm the deletion, click Yes.
8. From the configuration view, select Network Elements > <ne_type>.
9. Select the network element to delete and click Delete.
10. To confirm the deletion, click Yes.
Chapter 26: Accounting management

This chapter provides the procedures that you require to perform Application Server 5300 accounting administration. For information about accounting management configuration, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.

Navigation

- Enabling and disabling accounting processing rules on page 114
- Accessing accounting files on the Accounting Manager on page 115
- Deleting files on the Accounting Manager on page 116

Related links
- Enabling and disabling accounting processing rules on page 114
- Accessing accounting files on the Accounting Manager on page 115
- Deleting files on the Accounting Manager on page 116

Enabling and disabling accounting processing rules

About this task
Enable or disable accounting processing rules to determine which rules apply.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Accounting Managers > <Accounting Manager> > RU Processing > Accounting Rules Maintenance.

2. On the Accounting Processing Rules Maintenance panel, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accounting storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>Accounting North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>Accounting FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

3. Select a rule.
Choose to | Do this
---|---
Enable the selected rule. | Click Enable.
Disable the selected rule. | Click Disable.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Accounting Manager&gt;</td>
<td>This value is the name of Accounting Manager element for which you want to enable or disable accounting processing rules. Example: AM1</td>
</tr>
</tbody>
</table>

Enabling and disabling accounting processing rules job aid

The following table lists and describes the columns that appear on the Accounting Processing Maintenance panel.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>Accounting Format</td>
<td>This column contains the names of the accounting formats associated with the processing rules (MCPV3 or MCPV4).</td>
</tr>
<tr>
<td>Admin State</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>

Accessing accounting files on the Accounting Manager

About this task

You can access accounting files on the Accounting Manager of the Application Server 5300.

Prerequisites

- You require a log on ID and password. Contact your next level of support.

Procedure

1. Establish a secure shell connection to the server.
2. To access the directory on the Accounting Manager, type all on one line:
   ```
   cd /var/mcp/oss/acct/<AM_name>/ALL/<format_path_name>/
   <Session_manager_instance_name>/
   ```
3. To see all the files in the directory, enter:
   ```
   ls
   ```
4. To view a file, enter:
   
   `more <filename>`

5. To exit the session, enter: **Exit**.

**Variable Definitions**

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>&lt;AM_name&gt;</code></td>
<td>This value is the name of the Accounting Manager.</td>
</tr>
<tr>
<td><code>&lt;format_path_name&gt;</code></td>
<td>This value is the format path name.</td>
</tr>
<tr>
<td><code>&lt;Session_manager_instance_name&gt;</code></td>
<td>This value is the name of the AS 5300 Session Manager instance.</td>
</tr>
<tr>
<td><code>&lt;file_name&gt;</code></td>
<td>This value is the name of the file.</td>
</tr>
</tbody>
</table>

**Deleting files on the Accounting Manager**

**About this task**

You can delete files on the Accounting Manager to free disk space.

⚠️ **Caution:**

Risk of data loss. Ensure that you transfer all information to a back-end billing system prior to deletion. Avaya recommends deleting the oldest files first.

**Procedure**

1. Establish a secure shell connection to the server.

2. To access the directory on the Accounting Manager, type all on one line:
   
   `cd /var/mcp/oss/acct/<AM_name>/ALL/<format_path_name>/
    <Session_manager_instance_name>/`

3. To see all the files in the directory, enter:
   
   `ls`

4. To delete a file, enter:
   
   `rm <file_name>`

5. To exit the session, enter: **Exit**.
Chapter 27: Fault management

This chapter provides the procedures that you require to perform Application Server 5300 fault management administration. For information about fault management configuration, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.

Navigation

- Enabling and disabling log processing rules on page 117
- Monitoring a server on page 118
- Monitoring the database on page 119

Enabling and disabling log processing rules

About this task
Enable or disable log processing rules to determine which rules apply.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Manager > <Element Manager> > Log Processing > Log Rules Maintenance.

2. On the Log Processing Rule Maintenance panel, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>Log North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>Log FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

3. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>
Enabling and disabling log processing rules job aid

The following table lists and describes the columns that appear on the Log Processing Maintenance panel.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>Log Format</td>
<td>This column contains the names of the log formats associated with the processing rules.</td>
</tr>
<tr>
<td>Log Filter</td>
<td>This column contains the names of the log filters associated with the processing rules.</td>
</tr>
<tr>
<td>Admin State</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>

Monitoring a server

About this task

Use this procedure to start the monitor and to view status details for a server.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Servers > <Server> > Monitor.
   The Monitor window appears in the work area and displays a summary of the statistics for CPU, Memory, Disk, and Interface usage.
2. (Optional) To view details about CPU, Memory, Disk, or Interface usage, select the corresponding tab.
3. If the Summary tab does not display data, and the status bar at the bottom of the Monitor panel indicates that the server monitor is not running, click Start Monitor.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Server&gt;</td>
<td>This value is the name of the server that you want to monitor.</td>
</tr>
</tbody>
</table>
Monitoring the database

About this task
Use this procedure to start the database monitor, and to view the capacity, disk space used, and status of the database.

Prerequisites

• You can access the AS 5300 Element Manager Console.

• Viewing the database monitor status requires an administrative role with DBMonitorService privilege.

Procedure

1. From the AS 5300 Element Manager Console configuration view, select **Database > mcpdb > Monitor**.

2. Select instance 0 or 1 from the mcpdb Monitor window and click **Monitor**.

3. Ensure that the status line at the bottom of the Monitor window indicates "The database instance monitor is running." If not, click **Start Monitor**.

Monitoring the database job aid
The default MCP DB name is mcpdb. You can configure this value as an alphanumeric string that begins with a letter and is 6 characters or less.
Chapter 28: Performance management

This chapter provides the procedures that you require to perform for Application Server 5300 performance management administration. For information about performance management configuration, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.

Navigation

• Enabling and disabling OM processing rules on page 120

Related links

Enabling and disabling OM processing rules on page 120

---

Enabling and disabling OM processing rules

About this task

Enable or disable Operational Measurement (OM) processing rules to determine which rules apply.

Procedure

1. From the configuration view of the AS 5300 Element Manager Console, select Network Elements > Element Managers > Element Manager > OM Processing > Element Manager OM Processing Rules Maintenance.

2. On the Element Manager OM Processing Maintenance panel, select a tab.

<table>
<thead>
<tr>
<th>To enable or disable</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>OM storage rules</td>
<td>Select the Storage tab.</td>
</tr>
<tr>
<td>OM North-bound Server Feed rules</td>
<td>Select the North-bound Server Feed tab.</td>
</tr>
<tr>
<td>OM FTP Push rules</td>
<td>Select the FTP Push tab.</td>
</tr>
</tbody>
</table>

3. Select a rule.

<table>
<thead>
<tr>
<th>Choose to</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable the selected rule.</td>
<td>Click Enable.</td>
</tr>
<tr>
<td>Disable the selected rule.</td>
<td>Click Disable.</td>
</tr>
</tbody>
</table>
## Enabling and disabling OM processing rules job aid

The following table lists and describes the columns that appear on the OM Processing Maintenance panel.

<table>
<thead>
<tr>
<th>Column name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This column contains the unique names of the processing rules.</td>
</tr>
<tr>
<td>OM Type</td>
<td>This column contains the names of the OM types associated with the processing rules.</td>
</tr>
<tr>
<td>Admin State</td>
<td>This column contains the administrative states of the rules. The value is either ENABLED or DISABLED.</td>
</tr>
</tbody>
</table>
Chapter 29: Avaya Media Server performance management

This chapter provides procedures that you can perform for Avaya MS performance management using AS 5300 Element Manager Console.

Navigation

- Monitoring performance statistics on the Avaya Media Server (MS) on page 122
- Monitoring active sessions on the Avaya Media Server (MS) on page 123

Related links

Monitoring performance statistics on the Avaya Media Server (MS) on page 122
Monitoring active sessions on the Avaya Media Server (MS) on page 123

Monitoring performance statistics on the Avaya Media Server (MS)

About this task

Use this procedure to start the Avaya MS Performance Monitor and view statistical information about sessions, requests, and resource utilization.

Procedure

1. Log on to the AS 5300 Element Manager Console.
2. In the AS 5300 Element Manager Console Configuration view, navigate to Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Performance Monitor .

Related links

Avaya Media Server performance management on page 122
Monitoring active sessions on the Avaya Media Server (MS)

About this task

Use the procedures in this section to monitor active sessions on the Avaya MS, and to customize the active sessions monitor display.

Related links

- Avaya Media Server performance management on page 122
- Changing Refresh Rate for active session monitoring on page 123
- Monitoring active sessions on page 123
- Filtering active sessions on page 124
- Releasing active sessions on page 124
- Muting and unmuting active sessions on the Avaya Media Server on page 125
- Changing Time Stamps for active sessions on page 125

Changing Refresh Rate for active session monitoring

About this task

Use this procedure to change the Active Sessions display rate. The refresh rate is the period of time at which the displayed results refresh and display updated results.

Procedure

1. Log on to AS 5300 Element Manager Console.
2. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions. The ActiveSessionMonitor page appears.
3. Click the Refresh Every drop down box.
4. Select the desired refresh rate period. You can select one of the following time periods: 1 second, 5 seconds, 10 seconds, 15 seconds. 30 seconds, 45 seconds, 1 minute, No Refresh. To refresh the page immediately, click Refresh. To disable auto refresh, select No Refresh from the Refresh Every drop down box.

Related links

- Monitoring active sessions on the Avaya Media Server (MS) on page 123

Monitoring active sessions

About this task

Use this procedure monitor active sessions for Avaya Media Server.
Procedure

1. Log on to AS 5300 Element Manager Console.
2. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions. The ActiveSessionMonitor page appears, and local machine’s active sessions are displayed.

Related links
Monitoring active sessions on the Avaya Media Server (MS) on page 123

Filtering active sessions

About this task

Use this procedure to display specific active sessions by using filtering in the Active Sessions display page.

Procedure

1. Log on to AS 5300 Element Manager Console.
2. In the Configuration view of the AS 5300 Element Manager Console, navigate to Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions. The ActiveSessionMonitor page appears.
3. In the Filter list, select the desired filter type to use when searching through the active sessions. Filter types are None, Global Session ID, Application, Avaya Media Server Hostname, Remote Party, Endpoint, Remote IP Address, and Time Stamp. For example, to see all active sessions that are running the Notifier application, select Application from the Filter list and enter Notifier in the Criteria field. To disable filtering, select None from the Filter list.
4. In the Criteria field, enter the desired text to search on for the filter type chosen.
5. To view the filter results, either wait until the next refresh occurs or force a refresh by clicking Refresh .

Related links
Monitoring active sessions on the Avaya Media Server (MS) on page 123

Releasing active sessions

About this task

Use this procedure to release one or more active sessions in the Active Sessions display page.

Procedure

1. Log on to AS 5300 Element Manager Console.
2. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions**. The ActiveSessionMonitor page appears.

3. Select a session from the list of displayed Active Sessions or for multiple sessions, hold down either the **Shift** key (multiple selections that are grouped together) or the **Ctrl** key (multiple selections that are randomly separated) and select the desired sessions.

4. From the **Select** list, choose either Release Selected Session or Release All Selected Sessions.

**Related links**
- Monitoring active sessions on the Avaya Media Server (MS) on page 123

---

### Muting and unmuting active sessions on the Avaya Media Server

**About this task**

Use this procedure to mute or unmute one or more sessions in the Active Sessions display page. This option is available only if the running application supports muting.

**Procedure**

1. Log on to AS 5300 Element Manager Console.

2. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions**. The ActiveSessionMonitor page appears.

3. Select a session from the list of displayed Active Sessions or for multiple sessions, hold down either the **Shift** key (multiple selections that are grouped together) or the **Ctrl** key (multiple selections that are randomly separated) and select the desired sessions.

4. From the Select list, choose **Mute Selected Session** or **Mute All Selected Sessions** to mute the selection, or **Unmute Selected Session** or **Unmute All Selected Sessions** to unmute the selection.

**Related links**
- Monitoring active sessions on the Avaya Media Server (MS) on page 123

---

### Changing Time Stamps for active sessions

**About this task**

Use this procedure to change the time zone used to display the active session timestamps.

**Procedure**

1. Log on to AS 5300 Element Manager Console.
2. In the Configuration view of the AS 5300 Element Manager Console, navigate to **Network Elements > Media Servers and Clusters > Media Servers > <Avaya MS> > Monitoring > Active Sessions**. The ActiveSessionMonitor page appears.

3. To display the active session timestamps using the local time, select the **Display All Timestamps In Local Time** check box, or to display the active session timestamps using Greenwich Mean Time (GMT) clear the **Display All Timestamps In Local Time** check box.

4. Click **Refresh**.

Related links

- [Monitoring active sessions on the Avaya Media Server (MS)](page_123) on page 123