



# **Maintaining and Troubleshooting Avaya IQ**

Release 5.2  
April 2012

## Notice

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

## Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya generally makes available to users of its 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 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 Web sites 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 its Hardware and Software ("Product(s)"). Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this Product while under warranty is available to Avaya customers and other parties through the Avaya Support Web site: <http://support.avaya.com>. Please note that if you acquired the Product(s) from an authorized Avaya reseller outside of the United States and Canada, the warranty is provided to you by said Avaya reseller and not by Avaya.

## Licenses

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

Avaya grants End User a license within the scope of the license types described below. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a

different number of licenses or units of capacity is specified in the Documentation or other materials available to End User. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Software" means the computer programs in object code, originally licensed by Avaya and ultimately utilized by End User, whether as stand-alone Products or pre-installed on Hardware. "Hardware" means the standard hardware originally sold by Avaya and ultimately utilized by End User.

## License types

**Designated System(s) License (DS).** End User may install and use each copy of the Software on only one Designated Processor, unless a different number of Designated Processors is indicated in the Documentation or other materials available to End User. Avaya may require the Designated Processor(s) to be identified by type, serial number, feature key, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

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

**Database License (DL).** End User may install and use each copy of the Software on one Server or on multiple Servers provided that each of the Servers on which the Software is installed communicate with no more than a single instance of the same database.

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

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

**Shrinkwrap License (SR).** Customer may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License"). (see "Third-party Components" for more information).

## Copyright

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

the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

### **Third-party components**

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements (“Third Party Components”), which may contain terms that expand or limit rights to use certain portions of the Product (“Third Party Terms”). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: <http://support.avaya.com/Copyright>.

### **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 Web site: <http://support.avaya.com>. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: [securityalerts@avaya.com](mailto:securityalerts@avaya.com).

### **Trademarks**

The trademarks, logos and service marks (“Marks”) displayed in this site, the Documentation and Product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation 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.

Aura is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners, and “Linux” is a registered trademark of Linus Torvalds.

### **Downloading Documentation**

For the most current versions of Documentation, see the Avaya Support Web site: <http://support.avaya.com>.

### **Contact Avaya Support**

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



# Contents

<b>Chapter 1: Troubleshooting recommendations.....</b>	<b>11</b>
Avaya IQ software troubleshooting.....	11
Hardware troubleshooting.....	11
Database troubleshooting.....	12
Network troubleshooting.....	13
Avaya data source troubleshooting.....	13
Vendor software troubleshooting.....	14
InSite Knowledge Management.....	14
<b>Chapter 2: Data flows.....</b>	<b>17</b>
System startup data flow.....	17
All-in-One host, Single host, or Dual host data flow.....	18
Multiple Hosts data flow.....	18
Overview of events and administration data flow.....	19
Historical data flow.....	20
Real-time data flow.....	20
Events data flow.....	21
Administration data flow.....	23
Key management.....	27
<b>Chapter 3: Common troubleshooting tasks.....</b>	<b>29</b>
Verifying system status.....	29
Running a ping test.....	29
Stopping Avaya IQ on an application host.....	30
Starting Avaya IQ on an application host.....	30
Running the Pump-up Monitoring tool.....	31
Overview.....	31
Pump-Up Command.....	31
Running the pump-up monitoring tool.....	33
Running the pump-up monitoring tool in the background.....	34
Stopping the pump-up monitoring tool running in the background.....	34
Managing Oracle database and database server stability.....	35
About database monitoring diagnostics.....	35
About the database diagnostic tool.....	36
Using database diagnostic tool.....	37
General Tool Use.....	38
Oracle Tablespace Conditions.....	38
Archive Log management.....	41
Redo Log Management.....	44
Database Server Resource Conditions.....	44
Oracle Alert Log Management.....	46
Oracle Backup Management.....	47
Database Interfaces.....	47
Administrative Functions.....	48
Performance Metrics.....	50
Custom Conditions.....	51

<b>Chapter 4: Log files.....</b>	<b>53</b>
Viewing log files.....	53
Enabling log messages.....	53
Log file descriptions.....	53
Enabling and viewing report usage information.....	57
Enabling RTD report usage monitoring.....	58
Disabling RTD report usage monitoring.....	58
Enabling standard real-time report usage monitoring.....	58
Disabling standard real-time report usage monitoring.....	59
Sending logs to Avaya.....	59
<b>Chapter 5: Containers and PEs.....</b>	<b>61</b>
Troubleshooting concepts.....	61
Mapping of containers and PEs.....	62
All Functions host.....	62
Administration host.....	63
Data Processing host.....	63
Data Collection host.....	64
Reporting host.....	64
RTD host.....	64
PE descriptions.....	65
Alarm Config Service.....	65
Alarm Retriever Service.....	65
PE Alarm Service.....	65
PE Authorization Service.....	65
PE Host Log Retriever Server.....	66
PE Network Log Retriever Server.....	66
PE Host Log Server.....	66
PE Network Log Service.....	66
PE OAM.....	66
PE SDAS.....	67
PE Event Processor.....	67
PE Recorder.....	67
PE CM Adapter.....	67
PE PDS Adapter.....	68
PE Aggregation.....	68
PE HDAPR Entity Monitor.....	68
PE HDR Entity Monitor.....	68
PE IRS.....	69
PE Key Authority.....	69
PE Load Date.....	69
PE Message Broker.....	69
PE RDAPR Entity Monitor.....	70
PE RDR Entity Monitor.....	70
PE Real Time Report Service.....	70
Data Export (optional).....	70
PE Reporting Web.....	71
PE Reporting Application.....	71

PE Admin Recorder.....	71
PE Scheduler.....	71
Container descriptions.....	72
<b>Chapter 6: OAM pages for troubleshooting.....</b>	<b>73</b>
Host View and Container View icons.....	73
Host View page.....	74
How containers and PEs are grouped.....	74
Subsystem descriptions.....	75
Processing Element Status Information page.....	77
Container View.....	77
Edit Container page.....	77
Ping Host page.....	77
Ping Host field descriptions.....	77
<b>Chapter 7: Synchronization.....</b>	<b>79</b>
Synchronization.....	79
Synchronization terms.....	79
Synchronization types.....	79
What data gets synchronized?.....	80
Communication Manager and Proactive Contact.....	81
Initiating synchronizations manually.....	82
Synchronization data flow.....	82
Phase 1.....	82
Phase 2.....	83
Phase 3.....	84
Phase 4.....	85
Phase 5.....	86
Phase 6.....	87
Synchronization verification.....	88
Ensuring that data is getting processed.....	89
Checking reports.....	89
Checking container logs.....	90
Checking Communication Manager hexadecimal logs.....	90
Checking Proactive Contact logs.....	91
Troubleshooting the ETL application for Voice Portal.....	91
<b>Chapter 8: Maintenance activities.....</b>	<b>93</b>
Differences between software-only and turnkey maintenance.....	93
Recommendations for monitoring logs and alarms.....	94
Cleaning up user accounts.....	94
Changing the password for the administration user in Tomcat.....	95
Restarting, rebooting, and power-cycling hosts.....	96
Defining restarts, reboots, and power-cycling hosts.....	96
Restarting application hosts.....	98
Restarting the Database host.....	98
Rebooting hosts.....	99
Performing a routine system restart.....	99
Power-cycling hosts.....	103
Licensing.....	106

About licensing.....	106
Acquiring and installing license files.....	110
Maintaining license files.....	112
Installing updates.....	113
Editing properties.....	114
Adding or changing the reporting e-mail server.....	114
Changing the reporting host used for aggregation.....	116
Changing the association between the RTD host and the Reporting host.....	117
Changing host names and IP addresses.....	118
Admonishments for changing host names and IP addresses.....	118
Considerations for changing host names and IP addresses.....	118
Prerequisites for changing host names and IP addresses.....	119
Using the centralized process to change the host names or IP addresses.....	120
Using the centralized host name and IP address changes rollback process.....	124
Using the manual process to change the host names or IP addresses.....	126
Troubleshooting changes to host names and IP addresses.....	131
Starting Avaya IQ services after changing the host name or IP address.....	132
Installing trusted server certificates after changing host names or IP addresses.....	132
Updating associations between sources and hosts.....	134
Considerations for customers.....	134
Modifying the parameters of an existing Communication Manager source association.....	134
Moving the association of a Communication Manager source from one host to another host.....	135
Removing Communication Manager source associations.....	138
Deleting a Communication Manager source from OAM.....	138
Resolving error conditions when modifying or removing associations.....	141
Adjusting the parameters for communication with Proactive Contact cron jobs.....	143
Managing the external application URL links.....	144
Loading the date and time zone data.....	147
Date and time zone command options.....	148
Using the date and time zone command.....	149
Verifying date, time, and NTP status.....	150
Changing the database user names or passwords.....	150
Changing the SDS password on Avaya IQ.....	151
Changing a user name or password on Avaya IQ.....	151
Avaya IQ OAM connection names and corresponding database user names.....	154
Database management.....	154
Data removal.....	155
Removing data from all fact tables.....	155
Removing data from a single fact table.....	156
Removing obsolete users from RCL tables.....	156
Database schema and metadata sanity check.....	157
Reinitializing user service.....	157
Administering certificates.....	157
Planning for certificate installation.....	158
Backing up the existing certificates.....	159
Generating Certificate Signing Requests.....	160
Submitting CSRs to a Certificate Authority.....	162



Installing server certificates.....	163
Establishing the chain of trust.....	168
Manually adding the certificate name for the OAM certificate.....	168
Manually adding the certificate name for the Reporting certificate.....	169
Manually adding the certificate name for the RTD certificate.....	170
Individual certificate management procedures.....	171
Troubleshooting server certificates.....	177
Updating data source releases.....	178
Adjustment for Daylight Saving Time correction.....	179
Tuning parameters to prevent overload during pump-up.....	180
<b>Chapter 9: Troubleshooting activities.....</b>	<b>183</b>
InputTranslator component becomes full during pumpup.....	183
Cognos fails to start during turnkey installation.....	184
Report input page does not display any data.....	185
IQIA data source does not display entities.....	185
Report does not display any data.....	186
Status of PE IQ Input Adapter_<AACC source name> does not change.....	187
ARConnector initialization fails.....	188
SEILink does not receive heartbeat messages.....	190
SEILink logs CORBA errors.....	191
IQIA does not receive JMS messages.....	191
IQIA logs linkdown message and raises an alarm.....	192
IQIA pump-up request fails.....	193
ARConnector stops posting JMS messages.....	193
Changing the default Avaya Aura® Contact Center ARC, HEP and REP expiration values for spec contact sessions.....	194
IQ pump-up request fails.....	195
Deleting buffer storage and index files after making changes in the Data Processing dispatcher persistence configuration.....	196
<b>Chapter 10: Backing up system and database data.....</b>	<b>199</b>
Backup strategies.....	199
Backing up Avaya IQ data in a software-only deployment.....	202
Backing up the operating system in a software-only deployment.....	203
Backing up the database in a software-only deployment.....	203
Backing up custom reports.....	204
Backing up Avaya IQ data in a turnkey deployment.....	204
About enabling backups.....	206
Backup worksheet.....	206
Verifying the backup mount point on an application and database host.....	207
Setting the NFS mount point for backups.....	208
Activating the backup feature.....	209
Running an on-demand backup.....	210
Confirming a successful system data backup on an application host.....	212
Confirming a successful database data backup on the database host.....	213
Backing up custom reports.....	214
Backing up Avaya IQ data on Windows.....	214
<b>Chapter 11: Restoring system and database data.....</b>	<b>217</b>
Reasons for restoring Avaya IQ.....	217

Overview of Avaya IQ data restores.....	217
Restored directories and files.....	218
Prerequisites for restoring Avaya IQ data.....	218
Restoring Avaya IQ and data for a software-only deployment.....	219
RMAN.....	219
Restoring Avaya IQ in a software-only deployment.....	219
Recovering and restoring the database host.....	222
Selectively restoring Avaya IQ files or directories.....	224
Restoring custom reports.....	225
Restoring data on a turnkey deployment.....	225
Restore scenarios.....	226
Gathering recovery information.....	227
Restoring data after a software failure.....	228
Disk layouts on Avaya S8800 and IBM EXP3000 turnkey systems.....	230
Installing replacement disks when single disks in a mirrored pair fails.....	231
Replacing one or more mirrored pairs of system disks on an application/database host in a single host deployment.....	232
Replacing one or more mirrored pairs of system disks on an application host in a dual host or multi-host deployment.....	245
Replacing one or more mirrored pairs of system disks on the database host in a dual host or multi-host deployment.....	257
Restoring disk arrays.....	270
Restoring a replacement S8800 host computer.....	276
Confirming a successful restore.....	276
Restoring back to Avaya IQ 5.1.1.....	280
Selectively restoring Avaya IQ files or directories.....	291
Restoring custom reports.....	292
<b>Index.....</b>	<b>293</b>

# Chapter 1: Troubleshooting recommendations

---

## Avaya IQ software troubleshooting

### About this task

Follow these recommendations if you have any issues with the Avaya IQ application software.

### Procedure

1. Run alarm and log reports and look for messages that relate to your problem.  
For more information, see *Running a log report* or *Running an alarm report* in *Avaya IQ Alarms and Logs*.
2. Check your SNMP trap server for any alarm messages.
3. Go to <http://support.avaya.com> and type your support question.

**+ Tip:**

Include “Avaya IQ” or “IQ” along with your question in the question box.

If your problem has been documented, follow the troubleshooting procedures.

4. Contact Avaya technical support.  
For more information about maintenance offers and contacting support, see Support in *Avaya IQ Overview*.

---

## Hardware troubleshooting

### About this task

It is your responsibility to troubleshoot the hardware you obtained for the Avaya IQ software. If you have hardware-related issues with Avaya IQ, perform the following tasks on all Avaya IQ application hosts and the database host:

## Procedure

1. Check the cable connections.
2. Verify that the hardware has power.
3. Run alarm and log reports and look for messages that relate to your problem.  
For more information, see *Running a log report* or *Running an alarm report* in *Avaya IQ Alarms and Logs*.
4. Check your SNMP trap server for any alarm messages and for hardware MIBs.
5. Contact your IT department, or hardware supplier.  
You can be charged for any additional support by Avaya.
6. For turnkey deployments, see *Installing and Maintaining Dell Hardware for Avaya IQ Turnkey Deployments* for additional troubleshooting information.
7. To determine the version of the firmware BIOS on an application or database host, enter:  

```
dmidecode | grep "BIOS Information" -A3
```

---

## Database troubleshooting

### About this task

Avaya support representatives can assist you with any database issues by verifying that data is passing from the Avaya IQ software to the database. It is your responsibility to troubleshoot the database hardware and software. If you have database issues with Avaya IQ, Avaya has the following recommendations:

### Procedure

1. Run alarm and log reports and look for messages that relate to your problem.  
For more information, see *Running a log report* or *Running an alarm report* in *Avaya IQ Alarms and Logs*.
2. Check your SNMP trap server for any alarm messages.
3. Contact your database administrator.

 **Caution:**

If you have to shut down Avaya IQ and the database, restart the database *before* restarting Avaya IQ to ensure that all the Avaya IQ Processing Elements (PEs) start correctly.

## Result

Depending on your deployment and maintenance agreement, you can be charged for any additional support by Avaya.

---

# Network troubleshooting

## About this task

It is your responsibility to troubleshoot your network. If you have network issues with Avaya IQ, Avaya has the following recommendations.

## Procedure

1. Check the cable connections for the Avaya IQ hardware.
2. Verify that the network devices have power, and appear to be functioning correctly.
3. Use the `ping` command to determine if there are any network issues with the Avaya IQ application host computers, database host computer, or data sources.  
For more information, see [Ping Host page](#) on page 29.
4. Run alarm and log reports and look for messages that relate to your problem.  
For more information, see *Running a log report* or *Running an alarm report* in *Avaya IQ Alarms and Logs*.
5. Contact your network administrator.  
There might be an existing network issue, or changes were made to the network configuration. You can be charged for any additional support by Avaya.

---

# Avaya data source troubleshooting

## About this task

If you have any issues with the Avaya data sources, Avaya has the following recommendations.

## Procedure

1. Check the cable connections.
2. Verify that the hardware has power.
3. Run alarm and log reports and look for messages that relate to your problem.

4. Go to <http://support.avaya.com> and type your support question.

**+ Tip:**

Include “Avaya IQ” or “IQ” along with your question in the question box.

If your problem has been documented, follow the troubleshooting procedures.

5. Contact technical support.

For more information about maintenance offers and contacting support, see the *Support* topic in *Avaya IQ Overview*.

---

---

## Vendor software troubleshooting

### About this task

If you have any issues with any software that supports Avaya IQ but is not provided by Avaya, Avaya has the following recommendations.

### Procedure

1. Run alarm and log reports and look for messages that relate to your problem.  
For more information, see *Running a log report* or *Running an alarm report* in *Avaya IQ Alarms and Logs*.
  2. Contact your IT department, or software supplier.  
You can be charged for any additional support by Avaya.
- 

---

## InSite Knowledge Management

InSite Knowledge Management is a Web-based search engine that provides:

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

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the InSite Knowledge Management Web application at no extra cost. You must have a login account and a valid Sold-To number.

You can access InSite Knowledge Management at <http://support.avaya.com>.





# Chapter 2: Data flows

Data flows through an Avaya IQ system help you to understand and interpret log and alarm messages and troubleshoot problems. For more information, see [Synchronization data flow](#) on page 82.

---

## System startup data flow

Avaya IQ can be started after implementation, after a service interruption, or after a manual restart of the Avaya IQ system. The following processes are started in the following order:

1. Service Locator  
Used by other Avaya IQ processes to locate published services.
2. Lifecycle Manager  
Used to manage the starting and stopping of Avaya IQ containers and Processing Elements (PEs).
3. ActiveMQ  
Third-party service used to manage the messaging between Avaya IQ components.
4. All remaining components are started asynchronously. The remaining components retry the connections to each other until all are running and the system starts completely.  
  
If there are container or service unavailability errors, these errors are collected in log files until the needed components are working.
5. The following containers on each host are started in the following order based on the defined order in the `watchd.conf` file. You might not have all these containers on your system.
  - a. CS Tomcat or CS Tomcat Basic
  - b. Admin JBoss
  - c. Data Processing JBoss or Data Collection JBoss
  - d. Realtime Dashboard
  - e. Reporting UI
  - f. Reporting Application Service

## g. Reporting Web Service

For more information, see [Container descriptions](#) on page 72.

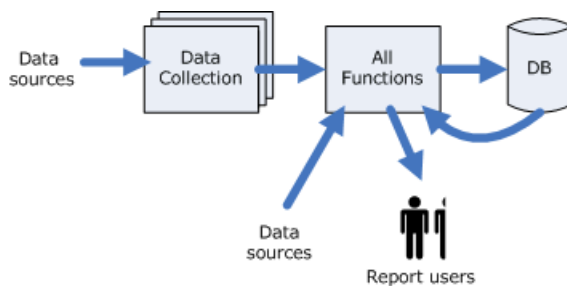
---

## All-in-One host, Single host, or Dual host data flow

An All-in-One host, Single host or Dual host deployment pattern can have more than one data flow strategy:

- One or more data sources can initiate the data flow through one or more Data Collection hosts
- One or more data sources can initiate the data flow through the All Functions host
- All of the above

A data source can be Communication Manager, Avaya Aura® Contact Center, Proactive Contact, and Voice Portal systems. The following diagram describes all of the possible data flows in a Dual Hosts deployment pattern.



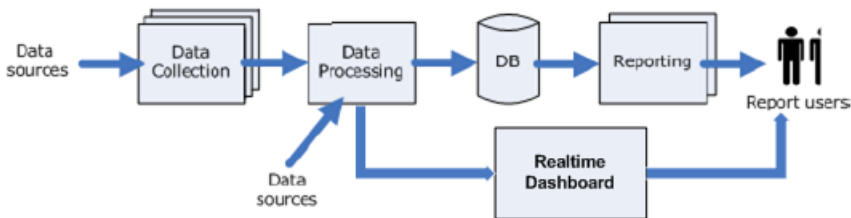

---

## Multiple Hosts data flow

A Multiple Hosts deployment pattern can have more than one data flow strategy:

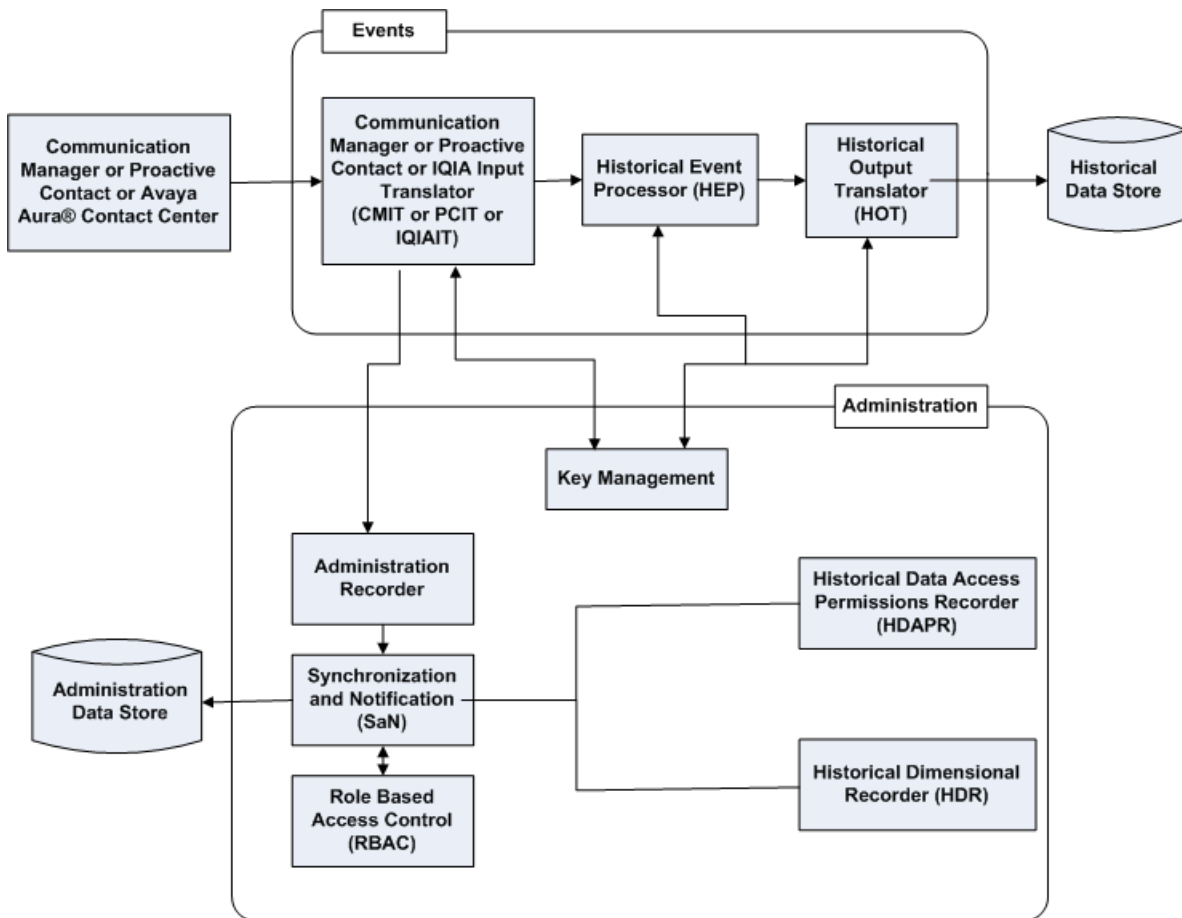
- One or more data sources can initiate the data flow through one or more Data Collection hosts
- One or more data sources can initiate the data flow through the Data Processing host
- All of the above

A data source consists of one Communication Manager and zero or more Proactive Contact systems. The following diagram describes all of the possible data flows in a Multiple Hosts deployment pattern.



## Overview of events and administration data flow

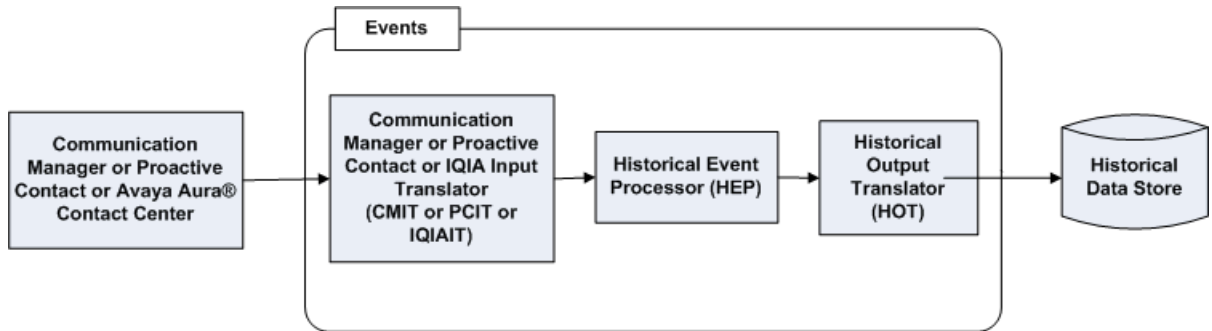
The following diagram describes how events data and administration data flow in an Avaya IQ system. For simplicity, this diagram shows only the process for historical data. The process of real-time data flow is similar to the process of historical data flow. The only difference is that in real-time data flow the data flows from ROT to both Real time data store and Real-time Dashboard. For example, Communication Manager > CMIT > REP > ROT > Real-time Data Store and Realtime Dashboard.



---

## Historical data flow

The following diagram describes how historical data flows through Avaya IQ. This diagram applies to both a Dual Hosts and a Multiple Hosts deployment. In a Dual Hosts deployment, the All Functions host contains the Administration, Data Collection, and the Data Processing functions. In a Multiple Hosts deployment, the Administration, Data Collection, and the Data Processing functions are on separate hosts.

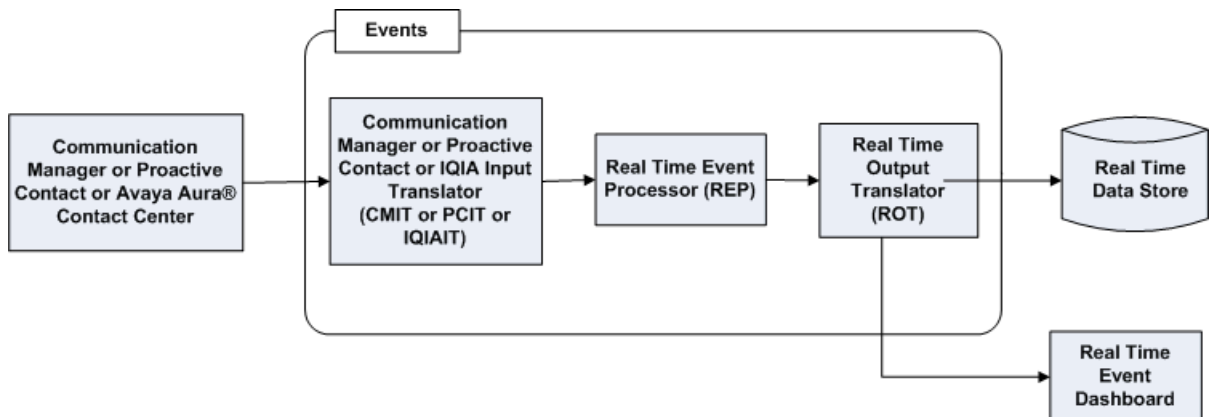


For more information, see [Events data flow](#) on page 21.

---

## Real-time data flow

The following diagram describes how real-time data flows through Avaya IQ. This diagram applies to both a Dual Hosts and a Multiple Hosts deployment. In a Dual Hosts deployment, the All Functions host contains the Administration, Data Collection, and the Data Processing functions. In a Multiple Hosts deployment, the Administration, Data Collection, and the Data Processing functions are on separate hosts.

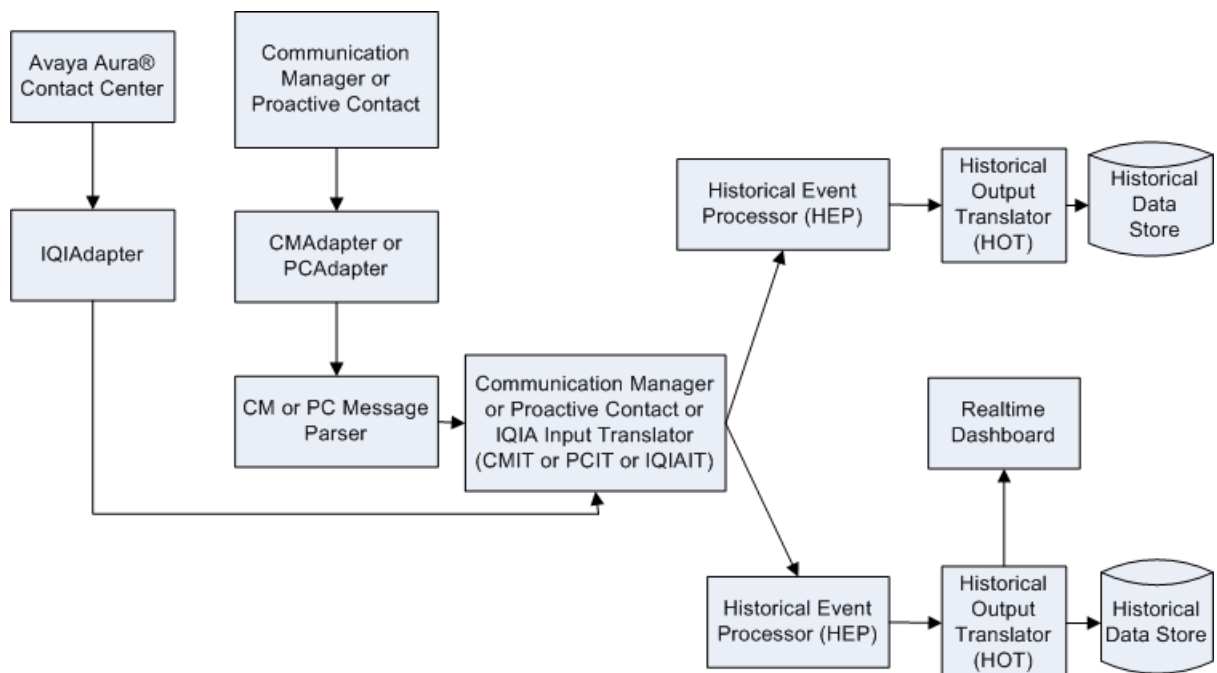


For more information, see [Events data flow](#) on page 21.

## Events data flow

The following diagram describes how data processing events are processed and stored in Avaya IQ.

Event sources consist of one Communications Manager and zero or more Proactive Contact systems. Although this represents one logical event source, events are collected from each separate Communication Manager and Proactive Contact system and then blended together in the Real Time and Historical Event Processors. Event sources can also consist of one Communication Manager and zero or more Avaya Aura® Contact Center systems. Events represent the start and end of the different states that each contact, such as inbound and outbound calls, passes through from start to finish. These events are translated by the IT (for example, CMIT, PCIT and IQIAIT) into a normalized format that the REP and HEP then convert into database insert and update messages that are processed by the ROT and HOT.



<p>CMAAdapter</p>	<p>The CMAAdapter implements the protocol that manages the communications link between Communication Manager and Avaya IQ. More specifically, the CMAAdapter prepares the data stream for event processing. One CMAAdapter monitors one Communications Manager. Your Avaya IQ system must have one or more CMAAdapters. Messages that occur between Communication Manager and the CMAAdapter are collected in the <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCE_NAME&gt;/hex_dump_all.log</code>.</p>
-------------------	---

PCAdapter	<p>The PCAdapter implements a protocol that manages the communications link between Proactive Contact and Avaya IQ. More specifically, the PCAdapter prepares the data stream for event processing. Your Avaya IQ system can have zero, one, or multiple PCAdapters. Every PCAdapter must have a corresponding CMAAdapter.</p> <p>Messages that occur between and the PCAdapter are collected in the <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/hex_dump_all.log</code>.</p>
CM Message Parser	<p>The CM Message Parser decodes Communication Manager events from their original binary hexadecimal format into a format suitable for the Communication Manager Input Translator (CMIT).</p> <p>Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_cmmsgs.log</code></p>
PC Message Parser	<p>The PC Message Parser decodes Proactive Contact events from their original binary hexadecimal format into a format suitable for the Proactive Contact Input Translator (PCIT).</p> <p>Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_pcmsgs.log</code></p>
CMIT	<p>The Communication Manager Input Translator (CMIT) normalizes event content coming from Communication Manager before sending it to the Avaya IQ historical and real-time event processors. Standardizing content can include performing calculations, filling in missing fields, and so on.</p> <p>Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_cmit.log</code>.</p>
PCIT	<p>The Proactive Contact Input Translator (PCIT) normalizes event content coming from Proactive Contact before sending it to the Avaya IQ historical and real-time event processors. Normalizing content can include performing calculations, filling in missing fields, and so on.</p> <p>Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_pcit.log</code></p>
HEP	<p>The Historical Event Processor (HEP) applies the business rules for processing historical events, such as changes in state, durations, when sessions start and end, and so on.</p> <p>Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_hep.log</code>.</p>
HOT	<p>The Historical Output Translator (HOT) reads events received from the Historical Event Processor (HEP) and performs database insertion and update operations.</p>

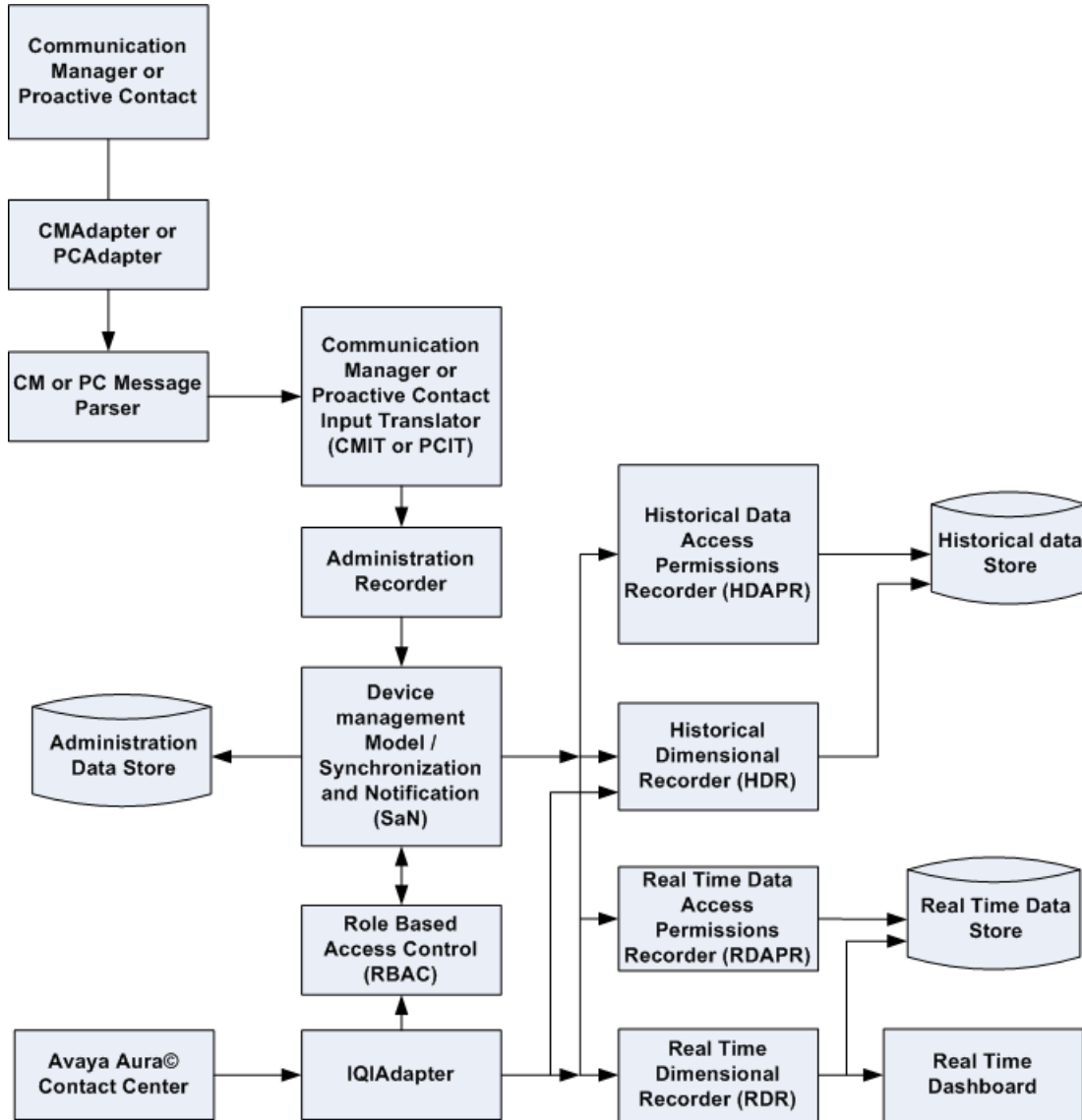
	Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_hot.log</code> .
Historical Data Store	This Historical Data Store is the database that contains historical detail and summary data for reporting.
IQIAdapter	The IQIAdapter implements the protocol that manages the communications link between Avaya Aura® Contact Center and Avaya IQ. More specifically, the IQIAdapter prepares the data stream for event processing. One IQIAdapter monitors one Avaya Aura® Contact Center. Your Avaya IQ system can have one or more IQIAdapter. Messages that occur between Avaya Aura® Contact Center and the IQIAdapter are collected in the <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_iqiait.log</code> .
IQIAIT	The IQIA Input Translator (IQIAIT) normalizes the event content coming Avaya Aura® Contact Center before sending it to the Avaya IQ historical and real-time event processors. Normalizing content can include performing calculations, filling in missing fields, and so on. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_iqiait.log</code> .
REP	The Real Time Event Processor (REP) applies the business rules for processing real-time events, such as changes in state, durations, when sessions start and end, and so on. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_rep.log</code> .
ROT	The Real Time Output Translator (ROT) reads events received from the Real Time Event Processor and performs database insertion and update operations. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;/messages_rot.log</code> .
Real-time Dashboard	Realtime dashboard contains real time data in memory, and generates real time dashboard report content.
Real Time Data Store	This Real Time Data Store is the database that contains real time data.

---

## Administration data flow

The following diagram describes how administration events on Communication Manager, Proactive Contact, and Avaya Aura® Contact Center are processed and stored in Avaya IQ.

Avaya IQ requests administration data from each Communication Manager and Proactive Contact system when a link is established. Administration events are also generated and sent to Avaya IQ by the Communication Manager as a result of administration activities. Examples of administration activities include the addition, deletion, and modification of agents on Communication Manager.



<p>CMAadapter</p>	<p>The CMAadapter implements the protocol that manages the communications link between Communication Manager and Avaya IQ. More specifically, the CMAadapter prepares the data stream for event processing. One CMAadapter monitors one Communications Manager. Your Avaya IQ system must have one or more CMAapters. Messages that occur between Communication Manager and the CMAadapter are collected in the <code>/var/log/Avaya/CCR/</code></p>
-------------------	--



	DataProcessingJBoss_<SOURCENAME>/hex_dump_all.log.
PCAdapter	The PCAdapter implements a protocol that manages the communications link between Proactive Contact and Avaya IQ. More specifically, the PCAdapter prepares the data stream for event processing. Your Avaya IQ system can have zero, one, or multiple PCAdapters. Every PCAdapter must have a corresponding CMAAdapter. Messages that occur between Proactive Contact and the PCAdapter are collected in the /var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/hex_dump_all.log.
CM Message Parser	The CM Message Parser decodes Communication Manager events from their original binary hexadecimal format into a format suitable for the Communication Manager Input Translator (CMIT). Messages from this step in the process are collected in /var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/messages_cmmsgs.log
PC Message Parser	The PC Message Parser decodes Proactive Contact events from their original binary hexadecimal format into a format suitable for the Proactive Contact Input Translator (PCIT). Messages from this step in the process are collected in /var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/messages_pcmsgs.log
CMIT	The Communication Manager Input Translator (CMIT) normalizes event content coming from Communication Manager before sending it to the Avaya IQ historical and real-time event processors. Standardizing content can include performing calculations, filling in missing fields, and so on. Messages from this step in the process are collected in /var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/messages_cmit.log.
PCIT	The Proactive Contact Input Translator (PCIT) normalizes event content coming from Proactive Contact before sending it to the Avaya IQ historical and real-time event processors. Normalizing content can include performing calculations, filling in missing fields, and so on. Messages from this step in the process are collected in /var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/messages_pcit.log
Administration Recorder	The Administration Recorder takes administration data collected from one or more external data sources and records it to the database.
Device Management Model	The Device Management Model (DMM) manages data received from sources such as Communication Manager or Proactive Contact and forwards it to other Avaya IQ administration components.
SaN	Synchronization and Notification (SaN) provides mechanisms for communicating information about the configuration data associated with the data sources. Avaya IQ components that are interested in

	administrative data can register with SaN for updates to administrative data when changes occur.
Administration Data Store	The Administration Data Store is a database that contains Avaya IQ and external data source administration and configuration information. The data stored in this database is processed and stored separately from the data stored in the Historical Data Store and the Real Time Data Store so that the data can be managed differently. This data store is used by SaN to alert registered clients of administrative changes.
RBAC	Role Based Access Control (RBAC) processes the administration of user-assigned roles. The assigned roles determine access to Avaya IQ operations and reports.
HDAPR	The Historical Data Access Permissions Recorder (HDAPR) processes administrative data about user access to Avaya IQ, and records it in the Historical Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/REPORTING_RECORDERS/messages_hdapr.log</code> .
HDR	The Historical Dimensional Recorder (HDR) processes administrative name data collected from one or more external data sources and records it in the Historical Data Store. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/REPORTING_RECORDERS/messages_hdr.log</code> .
Historical Data Store	This Historical Data Store is the database that contains historical detail and summary data for reporting.
RDAPR	The Real Time Data Access Permissions Recorder (RDAPR) processes administrative data about user access to Avaya IQ, and records it in the Real Time Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/REPORTING_RECORDERS/messages_rdapr.log</code> .
RDR	The Real Time Dimensional Recorder (RDR) processes administrative name data collected from one or more external data sources and records it in the real time database. Messages from this step in the process are collected in <code>/var/log/Avaya/CCR/REPORTING_RECORDERS/messages_rdr.log</code> .
Real Time Data Store	This Real Time Data Store is the database that contains real time data.
IQIAdapter	The IQIAdapter implements the protocol that manages the communications link between Avaya Aura® Contact Center and Avaya IQ. More specifically, the IQIAdapter prepares the data stream for event processing. One IQIAdapter monitors one Avaya Aura® Contact Center.

	Your Avaya IQ system can have one or more IQIAdapter. Messages that occur between Avaya Aura® Contact Center and the IQIAdapter are collected in the <code>/var/log/Avaya/CCR/DataProcessingJBoss_&lt;SOURCENAME&gt;</code>
--	---

---

## Key management

Key management provides services for linking together the individual segments of contact processing. By using these services, event processing can identify, join together, and blend complex call scenarios.



# Chapter 3: Common troubleshooting tasks

---

## Verifying system status

### Procedure

1. From the Avaya IQ OAM, navigate to **Enterprise > Sites > [site name] > [host name]**.
2. In the Host View page, expand all subsystems by selecting the green triangles in the left column.
3. Ensure that all Processing Elements (PEs) have green indicators on the left.
4. If you see a red indicator or a question mark indicator, wait for some time and refresh the Host View page in the browser.

**\* Note:**

Red indicators or question mark indicators can be signs of problems. However, it is normal for PEs to be in an unknown or starting state for a time before showing a green indicator. Red or question mark indicators are usually the result of a busy system, or because the OAM status query times out before the request is completed.

5. If you still have a red indicator or question mark indicator after several minutes, you might have a PE that cannot start correctly.  
If so, try starting the PE from the OAM interface and then by using the Lifecycle script `/opt/Avaya/CCR/bin/pecon.sh`. Use the `-?` option to get a command usage statement.

---

### Related topics:

[Synchronization verification](#) on page 88

---

## Running a ping test

### Procedure

1. From the Avaya IQ OAM, navigate to **Tasks > Utility > Run Ping Test**.

2. Enter an IP address or a host name in the **Host/IP** field and click **Ping**.

---

**Related topics:**

[Ping Host page](#)

[Ping Host field descriptions](#) on page 77

---

## Stopping Avaya IQ on an application host

### About this task

The following procedure stops all Avaya IQ processes on a specific application host. If you want to stop, start, or restart a single container or Processing Element (PE), see [Managing PEs and containers](#).

You should stop hosts in a multi-host deployment in the following order:

1. RTD host
2. Reporting hosts
3. Data Collection hosts
4. Data Processing hosts
5. Administration host

### Procedure

1. On the application host you want to stop, log in as root or as a root sudo user.
2. Enter the following command:  

```
service wdinit stop
```
3. To restart Avaya IQ processes, continue to [Starting Avaya IQ on an application host](#) on page 30.

---

## Starting Avaya IQ on an application host

### About this task

The following procedure starts all Avaya IQ processes on a specific application host.

You should start hosts in a multi-host deployment in the following order:

1. Administration host
2. Data Collection hosts
3. Data Processing hosts
4. Reporting hosts
5. RTD host

### Procedure

1. On the application host you want to start, log in as root or as a root sudo user.
2. Enter the following command:

```
service wdinit start
```

The wdinit service interacts with the Lifecycle watchdog (watchd) process that monitors the Avaya IQ startup. If any Avaya IQ processes fail, watchd immediately restarts the processes.

---

### Related topics:

[Initiating synchronizations manually](#) on page 82

---

## Running the Pump-up Monitoring tool

---

### Overview

The Pump-up Monitoring tool is developed to track the Pump-up status of Communication Manager and the synchronization status of Avaya IQ Administration with RDR/HDR/RDR\_JMS components and RBAC. Avaya service engineers can use this tool to track the Pump-up and synchronization status to troubleshoot customer issues.

This tool must be run post Avaya IQ installation on the Administration host to view the status of the Communication Manager pump-up and synchronization. Pump-up monitoring tool can also run in the background and can be revoked to view the latest status. The status is displayed once the call traffic commences through the Communication Manager and Avaya IQ users are authenticated with their respective permissions

---

### Pump-Up Command

The `pu_monitor.sh` command tracks the pump-up status of Communication Manager synchronization.

## Syntax

```
$CCR_HOME/bin/pu_monitor.sh -servicename avayaiq -numofdays <xxx> -refreshmin <x> -cm '<aaa|bbb|ccc>'
```

**servicename** This is a required parameter and is available from \$ORACLE\_HOME/network/admin/tnsnames.ora file.

**\* Note:**

If there is no entry pointing to the Avaya IQ database in this file, you must work with your customer's IT staff to add entry to this file. This entry must match the entry in this file on the Database host.

**-numberofdays** When supplied with this value, the tool displays values for the specified number of days to go back. The tool can go back up to 999 days. When this parameter is not used, the tool displays the latest status of the day. This parameter is optional and the tool runs even without this value.

**-refreshmin** This parameter sets the refresh rate in minutes. If this parameter is not used, the tool refreshes the status every five minutes. This parameter is optional and the tool runs even without this value.

**-cm** List of CM names as they were entered in the Input ID field during flavoring. This string must be enclosed by single quotes and delimited by the pipe symbol. When this parameter is not used, the tool displays the status for all Communication Managers administered.

## Description

This command must be run on the Avaya IQ Administration or Data Processing host. The required and optional parameters of this command are described in this section.

## Return values

**Please enter the SDS database password:** Displays when you run the tool. This is the password to the SDS database.

**CM Pumpup Status:** Displays the status of the pump-up data (dimensional data) received from the Communication Manager (or the switch).

**Names Pumpup Status:** Displays the status of synchronization between Avaya IQ Administration and RDR/HDR/RDR\_JMS components.

**Permission Pumpup Status:** Displays the status of synchronization between Avaya IQ Administration and RBAC for permission data.

## Example

```
>>>>>===== Wed Mar 31 12:08:02 MDT 2010 =====<<<<<<
PUMPUP MONITORING TOOL SHOWING STATUS FOR THE PAST 30 DAYS:
CM Pumpup Status:
2010-03-31 00:08:06 CM Started, logged by ruffles.dr.avaya.com
2010-03-31 00:08:15 CM Finished, logged by ruffles.dr.avaya.com
2010-03-31 00:08:18 CM Started, logged by ruffles.dr.avaya.com
```



```

2010-03-31 00:08:27 CM Finished, logged by ruffles.dr.avaya.com
-----
Names Pumpup Status:
>>> Historical Names Pumpup:
2010-03-30 23:42:12 Reporting Started
2010-03-30 23:42:17 Reporting Finished
2010-03-30 23:42:41 Reporting Started
2010-03-30 23:43:42 Reporting Finished
2010-03-31 00:07:52 CM Started
2010-03-31 00:08:08 CM Finished
2010-03-31 00:08:08 CM Started
>>> RealTime Names Pumpup:
2010-03-30 23:42:14 Reporting Started
2010-03-30 23:42:17 Reporting Finished
2010-03-30 23:42:36 Reporting Started
2010-03-30 23:44:14 Reporting Finished
2010-03-31 00:07:52 CM Started
2010-03-31 00:08:08 CM Finished
2010-03-31 00:08:08 CM Started
>>> RealTime Dashboard Names Pumpup:
2010-03-30 23:42:14 Reporting Started
2010-03-30 23:42:17 Reporting Finished
2010-03-30 23:42:36 Reporting Started
2010-03-30 23:44:14 Reporting Finished
2010-03-31 00:07:52 CM Started
2010-03-31 00:08:08 CM Finished
2010-03-31 00:08:08 CM Started
-----
Permission Synchronization Status:
>>> Historical Permission:
2010-03-30 23:42:18 Started
2010-03-30 23:42:36 Finished
>>> RealTime Permission:
2010-03-30 23:42:17 Started
2010-03-30 23:42:31 Finished
>>> RealTime Dashboard Permission:
2010-03-30 23:42:17 Started
2010-03-30 23:42:31 Finished
>>>>>NEXT REFRESH WILL BE 5 MINUTES FROM NOW

```

---

## Running the pump-up monitoring tool

### Procedure

1. Log on to the Administration or Data Processing host.
2. Run the following commands to start the pump-up monitoring tool:

```

cd $CCR_HOME/bin

./pu_monitor.sh -servicename avayaiq -numofdays <xxx> -
refreshmin <x> -cm <'aaa|bbb|ccc'>

```

The system asks for the SDS database password.
3. Enter the SDS database password and press **Enter**.  
The Pump-up status is displayed based on the parameters that you have provided.

**\* Note:**

Using `Ctrl+C` after step 3 completely terminates the tool.

---

## Running the pump-up monitoring tool in the background

### Before you begin

You must have the tool running before attempting to run it in the background.

### Procedure

1. On the command prompt, press `Ctrl+Z`.
2. Run the following commands:

```
bg
```

```
ps -ef | grep pu_mon
```

The system displays two output lines before returning to the command prompt. For example:

```
root      18702   5253  14 12:28 pts/0    00:00:02 /bin/bash /opt/Avaya/CCR/
bin/pu_monitor.sh
-servicename avayaig -numofdays 99999
root      22039   5253   0 12:28 pts/0    00:00:00 grep pu_mon
```

3. Run the following commands:

```
<the PID returned for pu_monitor.sh>
```

```
disown
```

In context with the example used above, this command can be written as:

```
disown 18702
```

This runs the pump-up monitoring tool in the background.

**\* Note:**

If you run the tool in the background, you cannot break out of any command using `Ctrl+C`. You must stop the background process to stop the tool.

---

## Stopping the pump-up monitoring tool running in the background

### Before you begin

You must have the tool running in the background.

## Procedure

On the command prompt, run the following commands:

```
ps -ef | grep pu_mon
```

```
kill -9 kill -<'the PID returned for pu_monitor.sh'>
```

For example, in context with the example cited in [Running the pump-up monitoring tool in the background](#) on page 34, the stop command can be written as:

```
kill -9 18702
```

---

---

## Managing Oracle database and database server stability

A set of tools is provided on an Avaya IQ 5.1 Turnkey database server to monitor conditions that are important to Oracle and database server stability. The tools are:

- Database monitoring diagnostics
- Database diagnostic tool.

These tools provide the capability to manage potentially negative database conditions before Avaya IQ operational issues take place.

With database diagnostics, you can accomplish the following:

- Monitor primary database server conditions and database server failures. The diagnostics tool performs auto-correction activities.
- Get alarms automatically when problems that cannot be corrected with the auto-correction activities occur.
- Set values for executing the diagnostic tests on a periodic basis.
- View detailed information about a problem.
- Configure thresholds for certain monitoring conditions.
- Run fixes for the identified problems.

---

## About database monitoring diagnostics

Database monitoring diagnostics are automatically performed once the system has been installed. Oracle and Database Server conditions are monitored and alarms are generated for conditions that exceed acceptable operational thresholds. This identifies pre-cursor and potential failure conditions. The focus is on alarming pre-cursor conditions prior to encountering a failure condition. The alarms are accessible via the Avaya IQ Administration client and on an administered SNMP application client. The default monitoring takes place hourly at 5

minutes past the hour. The monitoring execution time and frequency can be adjusted using the database diagnostic tool.

The following database server alarm conditions are reported:

**\* Note:**

Alarms marked with \* have automatic correction activities.

- \*ACOREE00137 DATABASE\_SERVER Archive Log Disk space usage exceeds level1 threshold (default 80%)
- \*ACOREE00138 DATABASE\_SERVER Archive Log Disk space usage exceeds level2 threshold (default 90%)
- ACOREE00139 DATABASE\_SERVER Disk space for Database Fast Recovery Area exceeds level1 threshold (default 80%)
- ACOREE00140 DATABASE\_SERVER Disk space for Database Fast Recovery Area exceeds level2 threshold (default 90%)
- ACOREE00141 DATABASE\_SERVER Database Full Backup failed
- ACOREE00142 DATABASE\_SERVER Database Incremental Backup failed
- \*ACOREE00143 DATABASE\_SERVER Database Archive Log Backup failed
- ACOREE00144 DATABASE\_SERVER Database internal error
- ACOREE00145 DATABASE\_SERVER Database critical internal error
- ACOREE00146 DATABASE\_SERVER CPU Occupancy exceeds level1 threshold (default 80%)
- ACOREE00147 DATABASE\_SERVER Memory usage exceeds level1 threshold (default 90%)
- ACOREE00148 DATABASE\_SERVER I/O Wait exceeds level1 threshold (default 20%)
- ACOREE00149 DATABASE\_SERVER Network issue
- ACOREE00150 DATABASE\_SERVER Database excessive redo log switching
- ACOREE00151 DATABASE\_SERVER Database performance issue
- ACOREE00152 DATABASE\_SERVER Database critical performance issue
- ACOREE00153 DATABASE\_SERVER Database is down
- ACOREE00154 DATABASE\_SERVER Database listener is down
- \*ACOREE00155 DATABASE\_SERVER Database parameter setting requires update

**\* Note:**

The system generates alarms even for the automatic correction conditions. After performing a auto correction, if an alarm occurs again in the next monitor period, it indicates that the corrective action did not fully address the condition and further investigation is required.

---

## About the database diagnostic tool

Avaya IQ 5.1 provides a diagnostic tool to help maintain a stable database. The database diagnostic tool is used in conjunction with the database monitoring diagnostics. This tool helps

you execute Oracle diagnostics that in turn enable you to run various diagnostic tests to identify the errors and fix them as needed. You can also use this tool to determine the state of the database server, investigate alarm conditions, and run on-demand backups.

**\* Note:**

You can use run the `db_diagnostic_mgr.sh` diagnostic tool only on the database host of a Turnkey deployment. However, the system automatically monitors the database host on a periodic basis to identify database errors and notify them to the user.

You can run `db_diagnostic_mgr.sh` diagnostic tool to monitor the following conditions:

- Oracle Tablespace Conditions
- Archive Log Management
- Redo Log Management
- Database Server Resource Conditions
- Oracle Alert Log Management
- Oracle Backup Management
- Database interfaces
- Administrative functions

---

## Using database diagnostic tool

### Procedure

1. Log on to the database host as root or a root-level user.
2. Enter the following commands to run the database diagnostic tool:

```
cd /avaya/bin
sh db_diagnostic_mgr.sh
```

The following menu is displayed:

```
Last Complete Detection at: <date><time>
Oracle supportability and support
Select:
a. Oracle Tablespace Conditions
b. Archive Log Management
c. Redo Log Management
d. Database Server Resource Conditions
e. Oracle Alert Log Management
f. Oracle Backup Management
g. Database Interfaces
h. Administrative Functions
i. Performance Metrics
j. Custom Monitoring
x. Exit
```

**\* Note:**

An asterisk displayed next to an option indicates that the system has generated alarm for that particular condition. Last Complete Detection indicates the time of the last monitoring execution.

3. Enter the required letter and press `Enter`. Submenus corresponding to the selected option is displayed.
4. Enter the letter for the required action and press `Enter`.

## General Tool Use

The following basic commands exist for condition investigation.

Display Last Execution Results	Displays the results of last monitoring/detection. Monitoring results are from the last diagnostic execution. Detection results are a manual execution of Run a Detection.
Compare Last Two Execution Results	Compares the last two monitoring or detection results of execution of this tool. This option is useful to determine if the condition has been fixed after execution of Run a Fix.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	If a fix is available, executes the fix. An execution can only occur if an error condition has been detected. This option indicates if monitoring auto-correction is executed.
Recommendation	If a fix is not available, a recommendation is provided to facilitate investigation and fix the problem. Auto-correction will not occur.
Investigate	Utilities are provided to investigate the condition. Auto-correction will not occur.

## Oracle Tablespace Conditions

Checks the threshold conditions related to Oracle Tablespace on the turnkey database server. It checks if tablespace autoextend mode is active, tablespace size is approaching the maximum size, tablespace parameters are set correctly and so on.

Tablespaces backup mode	
Verifies if each tablespace is not in backup mode. This issue occurs as a result of an explicit Oracle hot backup. This issue may rarely occur.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.

<b>Tablespaces backup mode</b>	
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	Removes the tablespace from backup mode. This results in incomplete hot backup. Automatic correction occurs.

<b>Tablespaces can not extend</b>	
Checks that each tablespace is online and in auto extend mode. The tablespaces are configured online and in autoextend mode. Tablespace modification causes these issues. It also verifies if there is enough space in the filesystem for the next datafile extend. File system space issues causes this issue.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Recommendation	Displays recommendations to correct this issue. Report this issue immediately to Avaya to determine if additional disk space is required. This condition is detected before the disk space for database approaches this level.

<b>Tablespace parameters</b>	
<p>Check each tablespace to verify that:</p> <ul style="list-style-type: none"> <li>• Logging is active</li> <li>• extent_mgmt=LOCAL</li> <li>• allocation_type=SYSTEM</li> <li>• segment_space_mgmt=AUTO</li> <li>• BIGFILE=YES</li> </ul> <p>The tablespaces are configured with these settings. Tablespace modification can cause this problem</p>	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Recommendation	Modify Tablespace Configuration parameters to align with recommendation for proper data management.

<b>Disk space for database is approaching a limit</b>	
<p>Checks if the disk space for database tablespace location exceeds a disk size threshold. The default thresholds are 80%, 85%, and 90% full. You can configure the thresholds to customize the alarming model. For example, if you know purge execution is maintaining data at 85% full, increase FS_disk_space_1 to 87, FS_disk_space_2 to 90 and FS_disk_space_3 to 95 to generate alarms based on your configuration requirements.</p>	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Investigate	Determine file system with space issue. You can get this information by viewing Display Last Execution Results. Use the following options to investigate:
Disk space for trace,audit,log,etc. files needs cleaning	<ol style="list-style-type: none"> <li>1. Run detection to identify Oracle files that consume extraneous space.</li> <li>2. Run fix to remove the identified files. This approach has limited opportunity for space gain since automatic Oracle file removal takes place.</li> <li>3. Enter (y) to rerun detection and return to previous menu.</li> <li>4. View Display Last Execution Results to determine if sufficient space is recovered.</li> <li>5. Enter (x) to return to previous menu without detect.</li> </ol>
Identify /u01 candidate big files for delete	<ol style="list-style-type: none"> <li>1. Search for large files that are a candidate for delete. If identified files are determined dispensable, remove the files from the shell.</li> <li>2. Enter (y) to rerun detection and return to previous menu.</li> </ol>
Identify /u02 candidate big files for delete	<ol style="list-style-type: none"> <li>3. View Display Last Execution Results to determine if sufficient space is recovered.</li> <li>4. Enter (x) to return to previous menu without detect.</li> </ol>
Recommendation	Contact Avaya technical support to determine if additional disk space is required. Enter (x) to return to previous menu without detect.

<b>Disk space for trace, audit, log, etc. files needs cleaning</b>	
<p>Identifies extraneous Oracle trace, audit, and log files that exceed the retention threshold. You can adjust the threshold to increase or decrease based on your system needs. For example, you may need to increase retention of Oracle log files to facilitate database troubleshooting.</p>	
Display Last Execution Results	Displays the results of last monitoring/detection execution.



Disk space for trace, audit, log, etc. files needs cleaning	
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	Removes identified Oracle trace, audit, log files. On running a fix, the issue is automatically corrected.

## Archive Log management

Checks the threshold conditions related to an archive log and backup settings on the Avaya IQ turnkey database server. It checks for problems in archive log mode settings, archiver process settings, fast recovery area configuration and disk space, and so on. It is very important to immediately address Archive Log alarms and conditions. Database server operations can stop if archive log conditions are not fixed. If Fast Recovery settings are not addressed, backups are likely to fail.

**\* Note:**

It is important to execute the backup setup procedures to enable database recovery after a failure occurs.

Database archive log mode settings	
Verifies that the database is on archive log mode. This error occurs until the execution of backup setup procedures.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Recommendation	Execute backup setup procedures to properly configure the Archive Log Mode settings.

Archiver Process Settings	
Verifies that the archive log settings are configured properly and the database is configured with the proper setting. Database modification can cause this issue.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.

<b>Archiver Process Settings</b>	
Run a Fix	Fixes archive log process setting. On running a fix, the issue is automatically corrected.

<b>Archive log destination parameter settings</b>	
Verifies proper archive log destination settings and that the database is configured with the proper setting. Modifications in the database can cause this issue.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	Fixes archive log destination setting. On running a fix, the issue is automatically corrected.

<b>Disk space for Archive log area is approaching a limit</b>	
Checks if the disk space for database archive log area exceeds a disk size threshold. The default thresholds are 80%, 85%, and 90% full. You can configure the threshold to customize the alarming model.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	Execute archive log backup to free space in archive log area for automatic correction. If issue persists after running the fix: <ol style="list-style-type: none"> <li>1. Go to Oracle Tablespace &gt; Disk space approaching limit &gt; Investigate&gt; Identify /u01 big file candidates.</li> <li>2. Go to Administrative Functions&gt; Adjust backup schedule&gt; Archive Log backup and increase the daily backup frequency.</li> </ol>

<b>Fast Recovery Area configuration</b>	
Verifies proper Fast Recovery Area (backup related) settings. This error occurs until the execution of backup setup procedures.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.

<b>Fast Recovery Area configuration</b>	
Run a Detection	Runs the tool to detect errors for this condition.
Recommendation	Execute backup setup procedures to properly configure the Fast Recovery Area settings.

<b>Fast Recovery Area is approaching a limit</b>	
Verifies that the Oracle Fast Recovery Area (backup related) space available is less than threshold . The default threshold is 80% full. you can configure the threshold to customize the Fast Recovery Area alarming model. This is an internal Oracle configuration attribute. High volume backup activity may require increase of this attribute.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Run a Fix	Allocates additional space to Fast Recovery Area.

<b>Disk space for Fast Recovery Area is approaching a limit</b>	
Checks if disk space for Fast Recovery Area (backup location) exceeds a disk size threshold. The default thresholds are 80%, 85%, and 90% full. You can configure the threshold to customize the alarming model.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run a Detection	Runs the tool to detect errors for this condition.
Investigate	Provides the following options:
Disk space for trace, audit, log, etc. files needs cleaning	Does not impact Fast Recovery Area disk space recovery.
Identify /u01 candidate big files for delete	Does not impact Fast Recovery Area disk space recovery.
Identify /u02 candidate big files for delete	<ol style="list-style-type: none"> <li>1. Search for large files that are candidates for delete. If the identified files are determined dispensable, remove these files from the shell.</li> <li>2. Enter y to re-execute detect and return to previous menu.</li> </ol>

Disk space for Fast Recovery Area is approaching a limit	
	3. View Display Last Execution Results to determine if sufficient space is recovered. 4. Enter x to return to previous menu without detect.
Recommendation	Contact Avaya technical support to determine if additional disk space is required. Enter x to return to previous menu without detect.

## Redo Log Management

Checks if the redo logs are switching appropriately and notifies if the frequency of redo logfile rollover is excessive. This verification is designed to disregard spike redo log rollover situations.

Redo logs are switching appropriately	
Verifies the optimum redo log switching frequency. Frequent Redo log switches can impact database performance. The default detection criteria is 10 redo logfile rollovers per hour for 5 consecutive hours. You can adjust the threshold to customize redo switch alarming model.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Recommendation	Contact Avaya technical support to determine if the database performance is impacted.

## Database Server Resource Conditions

Checks the threshold conditions related to CPU utilization, memory utilization, I/O wait time.

CPU Occupancy	
Checks if the database server CPU utilization exceeds the CPU threshold. To eliminate alarms due to spike condition, the average CPU utilization must exceed the threshold for an hour. The default thresholds is 80% and 95%. You can also adjust the thresholds to customize CPU alarming model.	
<p><b>* Note:</b></p> Detect is averaged over an hour so a CPU reducing activity (kill active consumer) takes an hour to reduce the CPU utilization average (at the shell execute top to determine immediate impact)	

CPU Occupancy	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Investigate	Displays top CPU consumers processes. Look for high CPU consumer (%CPU) processes that are not oracle or on single host, IQ processes (avayaiq). After it is determined that the process is not important, stop the identified process . For example, to stop the process, execute the following command at the shell: <code>kill -9 realPID</code> .

Memory Usage	
<p>Checks if the database server memory occupancy exceeds the memory threshold. To eliminate alarms due to spike condition, the average memory occupancy must exceed the threshold for an hour. The default threshold is 90%. You can adjust the threshold to customize server memory alarming model.</p> <p><b>* Note:</b>  Detect is averaged over an hour so a memory reducing activity (kill active consumer) takes an hour to reduce the memory occupancy average (at the shell execute top to determine immediate impact).</p>	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Investigate	Displays top CPU consumers processes. Look for high memory consumer (RSZ) processes that are not oracle or on single host, IQ processes (avayaiq). After it is determined that the process is not important, stop the identified process. For example, to stop the process, execute the following command at the shell: <code>kill -9 realPID</code>

I/O Wait Time	
<p>Checks if the database server I/O wait time exceeds the threshold. To eliminate alarms due to spike condition, the average I/O wait time must exceed the threshold for an hour. The</p>	

I/O Wait Time	
default threshold is 20%. You can adjust the threshold to customize server I/O wait alarming model. <b>* Note:</b> Detect is averaged over an hour so a I/O reducing activity (kill active consumer) takes an hour to reduce the I/O wait average (at the shell execute <code>iostat -dkx</code> to determine immediate impact).	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Investigate	Displays I/O wait statistics. A wait greater than 20 indicates that the disk is active. Contact Avaya technical support if there is associated Database performance issues and sustained I/O wait exists.

---

## Oracle Alert Log Management

Detects and allows display of detected Oracle warnings and failures. The detected conditions are:

- ORA-00257
- ORA-00270
- ORA-00272

If you want to monitor other Oracle conditions, you must add them to the detection list. To do this, add a line consistent with the existing format which identifies the ORA-error to the file `/avaya/Avaya_IQ/services/env/ALERTS`. This option provides an interface to view Oracle Alert Logs

Oracle Alerts	
Display Today's Errors	Displays ORA conditions detected today in Oracle Alert logs.
Display Yesterday's Errors	Displays ORA conditions detected yesterday in Oracle Alert logs.
Run Detection	Detects if Alert Logs contain designated Oracle warnings and failures.
Investigate	Provides access to Oracle Alert Logs.

---

## Oracle Backup Management

Checks for Oracle backup (full, incremental, archive) failures. Allows to view last backup results and re-initiate backup.

<b>RMAN Backups – Database</b>	
Manage full and incremental database backups. The backups fails if the backup setup procedures are not executed.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Run a Fix	Provides interface to execute an on-demand backup. It is initiated in the background. Use View last backup to view the status.
View last backup	Displays last backup log. Scroll to the bottom of the log to quickly determine the status.

<b>RMAN Backups – Archive logs</b>	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Run a Fix	Provides interface to execute an on-demand backup. The on-demand backup is initiated in the background. Use View last backup to view status. On running a fix, the issue is corrected automatically.
View last backup	Displays last backup log. Scroll to the bottom of the log to quickly determine the status.

---

## Database Interfaces

Enables you to monitor the status of the database instances and the oracle listener.

<b>Database status</b>
Detects database down status. Provides interface to view status and start/stop database.

Database status	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Investigate	To investigate the issue, perform the following actions: <ul style="list-style-type: none"> <li>• Startup – start Oracle listener</li> <li>• Shutdown – stop Oracle listener</li> <li>• Status – displays Oracle listener status</li> </ul>

Listener status	
Detects listener down status. Provides interface to view listener status and start/stop listener.	
Display Last Execution Results	Displays the results of last monitoring/ detection execution.
Compare Last Two Execution Results	Compares the last two monitoring /detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Investigate	To investigate the issue, perform the following actions: <ul style="list-style-type: none"> <li>• Startup – start Oracle listener</li> <li>• Shutdown – stop Oracle listener</li> <li>• Status – displays Oracle listener status</li> </ul>

---

## Administrative Functions

Administrative functions enable you to:

- Start or stop monitoring processes.
- Start or stop backups and backup processes.
- Set frequencies for monitoring and backup processes
- Set threshold values for database diagnostic data retention, disk space, memory usage, and so on.



Options	Description
Start/Stop Monitoring	<p>Enables you to starts or stops the following monitors:</p> <ul style="list-style-type: none"> <li>• Detection_Monitor</li> <li>• Default Monitoring</li> </ul> <p><b>* Note:</b> The default monitoring process monitors the system every hour.</p>
Adjust Monitoring schedule	<p>Enables you to modify the frequency for executing Detection_Monitor. You can set values for the following options:</p> <ul style="list-style-type: none"> <li>• day of the week</li> <li>• month of the year</li> <li>• day of the month</li> <li>• on the hours</li> <li>• on the minutes</li> </ul> <p><b>* Note:</b> To execute every day of the week, set these values to *.</p>
Start/Stop backups	<p>Enables you to start or stop backups for:</p> <ul style="list-style-type: none"> <li>• Archive Log</li> <li>• Full Database</li> <li>• Incremental Database</li> <li>• Set default backup schedule</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>• Full Sun 22:45</li> <li>• Incr Mon-Sat 22:45</li> <li>• Arch daily every 6 hrs</li> </ul>
Adjust backup schedule	<p>Enables you to modify the frequency for executing Archive_Log_Backup, Full_Database_Backup, and Incremental_Database_Backup. You can set values for the following options:</p> <ul style="list-style-type: none"> <li>• day of the week</li> <li>• month of the year</li> <li>• day of the month</li> <li>• on the hours</li> <li>• on the minutes</li> </ul>

Options	Description
	<p><b>* Note:</b> To execute every day of the week, set these values to *.</p>
Adjust thresholds	<p>Enables you to set threshold values for:</p> <ul style="list-style-type: none"> <li>• Desired percentage of space to stay below within fast recovery area</li> <li>• Days to keep database diagnostic data</li> <li>• Redo log attributes</li> <li>• Disk space usage warning levels                             <ul style="list-style-type: none"> <li>- Tablespace usage levels</li> <li>- Fast Recovery Area</li> <li>- Archive Log area</li> </ul> </li> <li>• CPU usage warning levels</li> <li>• Memory usage</li> <li>• I/O Wait</li> </ul>
Most recent alarms	Displays the alarms generated from the last complete monitor and recent manual detections.

## Performance Metrics

Checks the threshold conditions related to performance metrics on the turnkey database server. It checks if sessions, processes and open\_cursors internal Oracle parameters are approaching maximum size.

Sessions allocated	
Verifies if the active sessions is approaching Oracle limit. The threshold is 90% of the Oracle sessions parameter setting. The default is 1105. A key contributor to a large number of sessions is Real-time Report use and RTD Report use.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Recommendation	Report issue immediately to Avaya technical support to determine if system use is normal and increase this parameter. A database restart will be required.

<b>Processes allocated</b>	
Verifies if the active processes is approaching Oracle limit. The threshold is 90% of the Oracle processes parameter setting. The default is 1000. A key contributor to a large number of sessions is Real-time Report use and RTD Report use.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Recommendation	Report issue immediately to Avaya technical support to determine if system use is normal and increase this parameter. A database restart will be required.

<b>Open cursors</b>	
Verifies if the active cursors is approaching Oracle limit. The threshold is 90% of the Oracle processes parameter setting. The default is 2000. A key contributor to a large number of sessions is Real-time Report use and RTD Report use.	
Display Last Execution Results	Displays the results of last monitoring/detection execution.
Compare Last Two Execution Results	Compares the last two monitoring/detection results of execution of this tool.
Run Detection	Runs the tool to detect errors for this condition.
Recommendation	Report issue immediately to Avaya technical support to determine if system use is normal and increase this parameter. A database restart will be required.

---

## Custom Conditions

This feature provides the capability to monitor any condition on the database server. Templates are provided for various condition management options. Use this feature to add monitoring capability for system conditions that require monitoring.



# Chapter 4: Log files

---

## Viewing log files

### Procedure

To view log files, go to `/var/log/Avaya/CCR`.

---

---

## Enabling log messages

### About this task

By default, all logs are enabled, but are not set to the debug level. Enabling the debug level creates overhead on systems that process a high rate of call traffic.

### Procedure

To enable the debug level, you must edit an XML file and run the risk of invalidating the XML instance. Contact support personnel for this information or if you have access, see internal documentation.

---

---

## Log file descriptions

### \* `_console.log`

Contains messages for the console output for the associated process.

### `activemq.log`

Contains logged events in the Messaging subsystem.

The Messaging subsystem and the Message Broker PE control the ActiveMQ messaging service between Avaya IQ components. For more information about ActiveMQ, you can search the internet.

## **ADMIN/\***

This directory contains log files associated with the components that run under the CS Tomcat container.

**ADMIN.log:** Contains logged events from all components in the CS Tomcat container.

## **avaya.hostlogserver.log**

Contains all the information levels and messages logged by the components on a particular application host. Every Avaya IQ host has this file.

## **avaya.networklogserver.log**

Contains all the information levels and messages for all Avaya IQ hosts on the system. The Log Viewer retrieves only the entries stored in this log.

## **coreservices**

This directory contains log files used for the Core Services software functions that are reused across Avaya IQ and other Avaya products.

**lcm.log:** Contains errors and events related to Lifecycle processes. Lifecycle starts and stops Avaya IQ components.

**wdlog and wdlog\_p:** Contains errors and events related to the starting and stopping of watched managed components that start and stop Avaya IQ, and monitor and restart failed processes.

## **DataCollectionJBoss\_SOURCENAME/\***

This directory contains log files associated with the components that run under the Data Collection JBosscontainer.

**DataCollectionJBoss.log:** Contains logged events from all components in this container.

**hex\_dump\_all.log:** If enabled, contains all hexadecimal messages received from Communication Manager. Currently, there is no hex\_dump\_all.log file for Proactive Contact. Use the pcit and pcmsgs logs to monitor synchronization.

**messages\_cmit.log:** If enabled, contains all messages sent to and received by the CMIT. The CMIT normalizes event content coming from Communication Manager before sending it to the Avaya IQ historical and real-time event processors. Normalizing content includes performing calculations, filling in missing fields, and so on.

**messages\_cmmsgs.log:** If enabled, contains all messages sent to and received by the CM Message Parser. The CM Message Parser decodes Communication Manager events from their original binary hexadecimal format into a format suitable for the CMIT.

**messages\_pcit.log:** If enabled, contains all messages sent to and received by the PCIT. The PCIT normalizes event content coming from Proactive Contact before sending it to the Avaya IQ historical and real-time event processors. Normalizing content includes performing calculations, filling in missing fields, and so on.

**messages\_pcmsgs.log:** If enabled, contains all messages sent to and received by the PC Message Parser. The PC Message Parser decodes Proactive Contact events from their original binary hexadecimal format into a format suitable for the PCIT.

**pu\_admin\_full.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to a full translation (RFTB) synchronization

**pu\_admin\_name.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to a name synchronization.

**pu\_oper.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to an operational (RLTB) synchronization.

**traffic\_data.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to call traffic after a synchronization completes.

### **DataProcessingJBoss\_SOURCENAME/\***

This directory contains log files associated with the components that run under the Data Processing JBoss container.

**DataProcessingJBoss.log:** Contains logged events from all components in the Data Processing JBoss container.

**hex\_dump\_all.log:** If enabled, contains all hexadecimal messages received from Communication Manager. Currently, there is no hex\_dump\_all.log file for Proactive Contact. Use the pcit and pcmgs logs to monitor synchronization.

**messages\_cmit.log:** If enabled, contains all messages sent to and received by the CMIT. The CMIT normalizes event content coming from Communication Manager before sending it to the Avaya IQ historical and real-time event processors. Normalizing content can include performing calculations, filling in missing fields, and so on.

**messages\_cmmsgs.log:** If enabled, contains all messages sent to and received by the CM Message Parser. The CM Message Parser decodes Communication Manager events from their original binary hexadecimal format into a format suitable for the CMIT.

**messages\_hep.log:** If enabled, contains all messages sent to and received by the HEP. The HEP applies the business rules for processing historical events, such as changes in state, durations, when sessions start and end, and so on.

**messages\_hot.log:** If enabled, contains all messages sent to and received by the HOT. The HOT reads events received from the HEP and performs database insertion and update operations.

**messages\_pcit.log:** If enabled, contains all messages sent to and received by the PCIT. The PCIT normalizes event content coming from Proactive Contact before sending it to the Avaya IQ historical and real-time event processors. Normalizing content can include performing calculations, filling in missing fields, and so on.

**messages\_pcmgs.log:** If enabled, contains all messages sent to and received by the PC Message Parser. The PC Message Parser decodes Proactive Contact events from their original binary hexadecimal format into a format suitable for the PCIT.

**messages\_rep.log:** If enabled, contains all messages sent to and received by REP. The REP applies the business rules for processing real-time events, such as changes in state, durations, when sessions start and end, and so on.

**messages\_rot.log:** If enabled, contains all messages sent to and received by ROT. The ROT reads events received from the Real Time Event Processor and performs database insertion and update operations.

**pu\_admin\_full.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to a full translation (RFTB) synchronization.

**pu\_admin\_name.hex :** If enabled, contains all hexadecimal messages from Communication Manager that correspond to a name synchronization.

**pu\_oper.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to an operational (RLTB) synchronization.

**traffic\_data.hex:** If enabled, contains all hexadecimal messages from Communication Manager that correspond to call traffic after a synchronization has completed.

**security/avaya.security.log :** Contains logged events associated with the security components of Avaya IQ. The security log contains an audit trail of security events, such as invalid login attempts.

### **dbsetup/dbsetup.log**

Contains messages created when Avaya IQ is installed.

### **deployJBoss.log**

Contains messages created when Avaya IQ is initially configured.

### **MSGBROKER/\***

This directory contains log files associated with the components that run under the Message Broker Service container.

**MSGBROKER.log:** Contains logged events from all components in the Message Broker Service container.

### **Reporting\_Execution/\***

This directory contains log files associated with the components that run under the Reporting Application Service container.

### **REPORTING\_RECORDERS/\***

This directory contains log files associated with the components that run under the Admin JBoss container. If this directory does not exist, check the \*\_console log.

**Reporting\_Recorders.log:** Logged events from all components in the container.

**messages\_hdapr.log:** If enabled, contains messages associated with Historical Data Access Permissions Recorder (HDAPR). The HDAPR processes administrative data about user access to Avaya IQ, and records it in the Historical Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified.

**messages\_hdr.log:** If enabled, contains messages associated with HDR. The Historical Dimensional Recorder (HDR) processes administrative name data collected from one or more external data sources and records it in the Historical Data Store.

**messages\_rdapr.log:** If enabled, contains messages associated with RDAPR. The Real Time Data Access Permissions Recorder (RDAPR) processes administrative data about user



access to Avaya IQ, and records it in the Real Time Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified.

**messages\_rdr.log:** If enabled, contains messages associated with the RDR. The Real Time Dimensional Recorder (RDR) processes administrative name data collected from one or more external data sources and records it in the real time database.

### **Reporting\_UI/\***

This directory contains log files associated with the components that run under the Reporting UI container.

**Reporting\_UI.log:** Contains logged events from all components in the Reporting UI container.

**dataexport.log:** Contains logged exceptions and issues associated with data export.

**RealtimeRptSummary.log:** If enabled, contains hourly summary of active real-time reports.

### **RTD/\***

This directory contains log files associated with the Dashboard Engine that runs in the Realtime Dashboard tomcat container.

**RTD.log:** Contains logged events from Dashboard Engine in the Realtime Dashboard tomcat container.

**messages\_rtd.log:** If enabled, contains all messages received by Realtime Dashboard. Realtime Dashboard Engine processes these messages, and stores the results in memory.

**rtdPerf.log:** If enabled, contains report latency related performance information.

**rtdReportUsage.log:** If enabled, contains hourly summary of the number of executions of each report. Real-time dashboard report usage monitoring impacts RTD container memory usage and therefore enable the report usage logging for limited period. For example, to profile report use during peak periods or for troubleshooting.

---

## **Enabling and viewing report usage information**

You can enable logging to create logs on an hourly basis. These logs provide summarized Avaya IQ report usage information for the real-time dashboard reports (RTD) and the standard real-time reports. RTD report usage provides details about the number of sessions and the RTD reports generated per session. The standard real-time report usage provides details about the active reports at a point in time.

### **\* Note:**

The logs generated while monitoring the RTD report usage are placed in the RTD container and affects the container memory usage. Therefore, Avaya recommends you to enable logging for a limited period whenever required. For example, you can enable logging for monitoring report usage during the busy hours or for troubleshooting purpose.

---

## Enabling RTD report usage monitoring

### About this task

To enable RTD report usage monitoring:

### Procedure

1. On the All Function, or RTD host, open the file `/opt/Avaya/CCR/data/RTD/log4j.properties`.
2. Uncomment the lines under the `Definition` for the RTD report usage `Logger` section by removing the preceding `#`.

**\* Note:**

Note that the logs generated during the hourly logging are appended to the `/var/log/Avaya/CCR/RTD/rtdReportUsage.log` file.

---

---

## Disabling RTD report usage monitoring

### About this task

To disable RTD report usage monitoring:

### Procedure

1. On the All Function or RTD host, open the file `log4j.logger.com.avaya.reporting.rtd.reportUsage`.
  2. Change the value `ALL,rtdReportUsageLogger` to `INFO,rtdReportUsageLogger`.
- 

---

## Enabling standard real-time report usage monitoring

### About this task

To enable standard real-time report usage monitoring:

### Procedure

On the All Functions host or on each Reporting host, enter the following commands:

```
cd /opt/Avaya/CCR/bin
```

```
sh RTReportSummary.sh install
```

**\* Note:**

Note that the logs generated during the hourly logging are appended to the following file:

```
/var/log/Avaya/CCR/Reporting_UI/RealtimeRptSummary.out
```

---

---

## Disabling standard real-time report usage monitoring

### About this task

To disable standard real-time report usage monitoring:

### Procedure

On the All Functions host or on each Reporting host, enter the following commands:

```
cd /opt/Avaya/CCR/bin
sh RTReportSummary.sh uninstall
```

---

---

## Sending logs to Avaya

### About this task

Avaya support personnel can create a set of log files and mail the files to the support team for analysis.

### Procedure

1. Enter the following commands to run the log utility command:

```
cd /opt/Avaya/CCR/bin
sh logUtility.bin
```

2. Select option 1 to gather the logs.
3. Select the set of logs to be collected.
4. Once the logs are collected, select `quit`.
5. Enter the following command to run the log utility command:  

```
sh logUtility.bin
```
6. Select option 2 to FTP the logs to a remote machine.

7. Provide the FTP site information, including the machine name, user name, password, customer name, and case ID.

The log files are sent using FTP to the selected machine.

---

# Chapter 5: Containers and PEs

---

## Troubleshooting concepts

### Processing Element

A low-level software component that implements a piece of Avaya IQ functionality. Processing Elements (PEs):

- Are subcomponents of Avaya IQ functionality.
- Run under the control of a container process.
- Are organized logically under subsystems.

You can view the grouping of PEs in relation to containers using the following Lifecycle script:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

You can start and stop containers either from the OAM interface or by using a Lifecycle script.

### Container

A process that provides an environment for a Processing Element (PE) to run. Containers:

- Are based on the physical deployment of PEs on an application host.
- Can span subsystems. For example, an application host can have one Tomcat container that contains PEs from more than one subsystem.

**! Important:**

Do not confuse subsystem names with containers.

- Can have more than one instance of the same PE.

You can view the grouping of PEs in relation to containers using the `sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status` command. You can start and stop containers either from the OAM interface or by using the `pecon.sh` command.

### Subsystem

A logical grouping of PEs that work together to provide a major capability in Avaya IQ, such as Real Time Data Consolidation. A subsystem can have multiple PEs that can be spread over several processing containers. You can view the grouping of PEs in relation to subsystems from the Host View page in the OAM.

For more information, see Subsystems in *Avaya IQ Overview*.

## Host

A computer where software used for Avaya IQ is installed. An application host refers to one of the computers where the Avaya IQ software is installed. An application host can be an All Functions, Administration, Reporting, Data Collection, or Data Processing host. The database host computer refers to the computer where the third-party database software used for Avaya IQ is installed. The database host computer is always installed on a host computer that is physically separate from the application host computers.

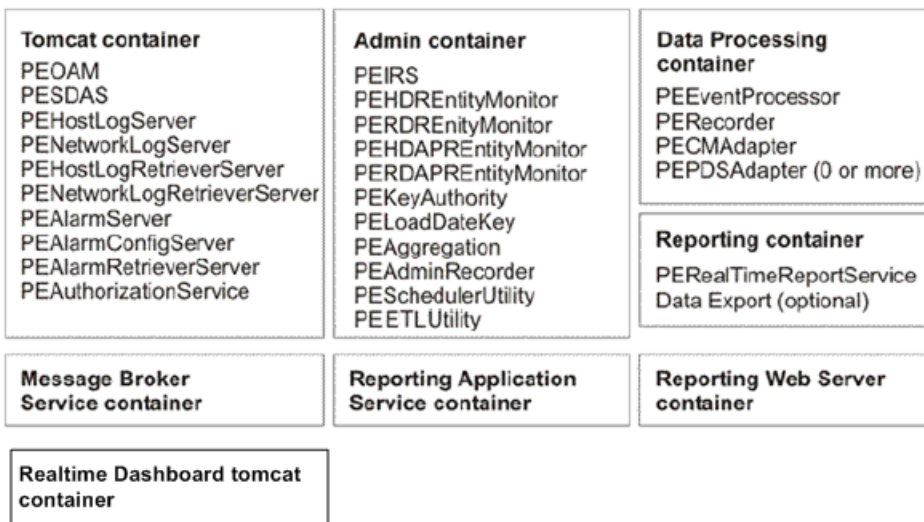
For more information, see Host function descriptions in *Avaya IQ Overview*.

## Lifecycle manager

Controls the starting and stopping of containers and the PEs within containers. Use the Lifecycle `pecon.sh` command to view PE and container groupings and to start and stop processes when the OAM is unavailable.

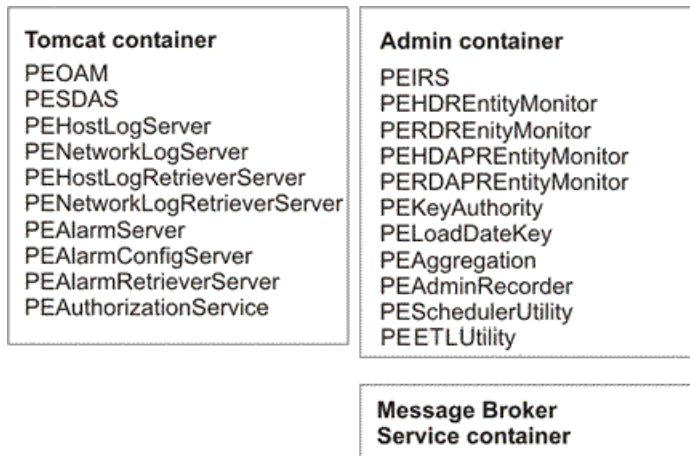
# Mapping of containers and PEs

## All Functions host



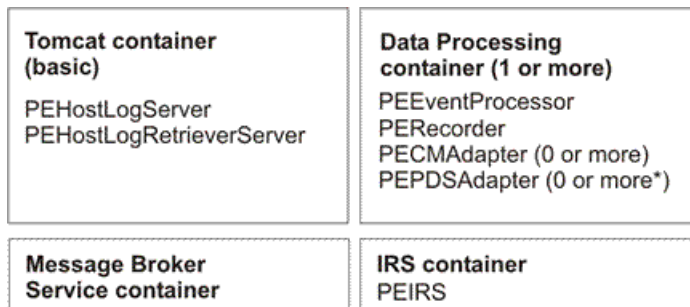
---

## Administration host




---

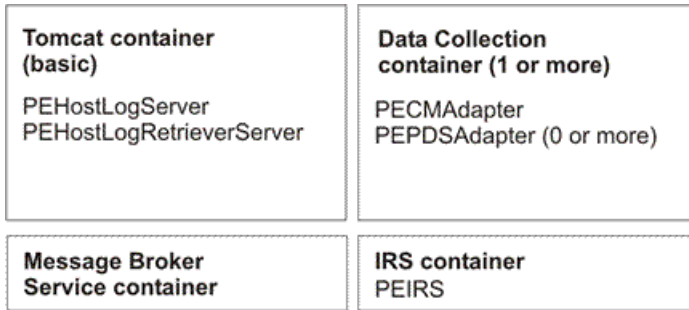
## Data Processing host



\* Every PEPDSAdapter must have a corresponding PECMAdapter.

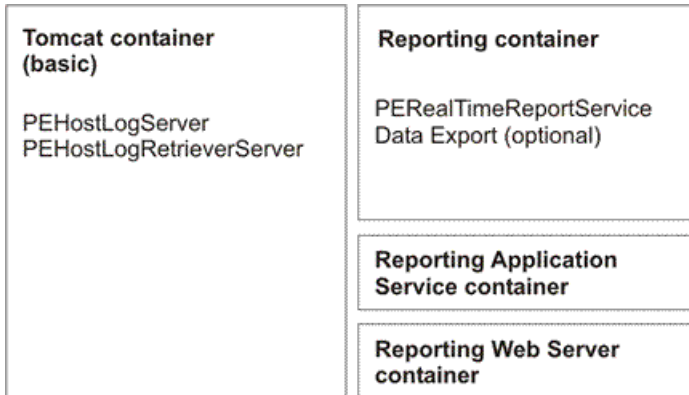
---

## Data Collection host



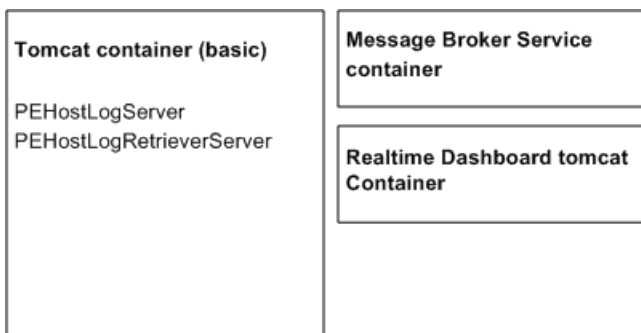
---

## Reporting host



---

## RTD host





---

## PE descriptions

---

---

### Alarm Config Service

Also called “PE Alarm Config Server”. Provides services to get, create, update, or delete the alarm configuration data stored in the EventMapAlarm, ThresholdMap, AlarmCodeListenerLink, and AlarmListener tables.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** This PE is currently not used by Avaya IQ.

---

### Alarm Retriever Service

Also called *PE Alarm Retriever Server*. Retrieves alarm records based on various filters.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** The Alarm Viewer does not function and you cannot clear alarms.

---

### PE Alarm Service

Also called *PE Alarm Server*. Responsible for alarm generation, alarm persistence, alarm state management, and alarm notification.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** Alarms are not logged and SNMP events are not propagated.

---

### PE Authorization Service

Manages Role Based Access Control (RBAC). An internet search can provide you with more information about RBAC.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** Alarms are not logged and SNMP events are not propagated.

---

## PE Host Log Retriever Server

Retrieves logs from the application host used by the Log Viewer page.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** This PE is currently not used by Avaya IQ.

---

## PE Network Log Retriever Server

Retrieves system wide logs from an application host used by the Log Viewer page.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** This PE is currently not used by Avaya IQ.

---

## PE Host Log Server

Provides centralized logging for a single application host.

**Container:** CS Tomcat Basic or CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** The affected application host cannot report log messages to both of the following log files: `/var/log/Avaya/CCR/avaya.debug.log`, `/var/log/Avaya/CCR/avaya.hostlogserver.log`.

---

## PE Network Log Service

Also called *PE Network Log Server*. Provides centralized logging on a single application host for all Avaya IQ.

**Container:** CS Tomcat Basic or CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** There is no centralized logging for Avaya IQ and nothing is logged to: `/var/log/Avaya/CCR/avaya.networklogserver.log`.

---

## PE OAM

Manages the main OAM Web services.

**Container:** CS Tomcat - also called “Admin Tomcat”.

**If this PE fails:** You cannot log into the Avaya IQ OAM interface.

---

## PE SDAS

Manages access to system configuration data.

**Container:** CS Tomcat - also called "Admin Tomcat".

**If this PE fails:** Avaya IQ components cannot retrieve configuration information and cannot start.

---

## PE Event Processor

Manages event processing and processes normalized events from the PE CM Adapter and PE PD Adapter. Records real-time data to the Real Time Data Store.

**Container:** Data Processing JBoss.

**If this PE fails:** Data is lost. If this PE shuts down, the PE CM Adapter and the PE PDS Adapter also shut down. If a remote PE Event Processor stops running, the PE CM Adapter and the PE PDS Adapter buffer some data, but eventually drop the overflow data.

---

## PE Recorder

Records fact data to the Historical Data Store.

**Container:** Data Processing JBoss.

**If this PE fails:** Historical data does not flow into the Historical Data Store, thereby affecting the data in the historical reports. Avaya IQ buffers a large amount of data before it gets recorded to disk if the PE Recorder has stopped. However, overflow data is discarded after the disk buffer is full.

---

## PE CM Adapter

Monitors the CMAAdapter.

The CMAAdapter implements the protocol that manages the communications link between Communication Manager and Avaya IQ. More specifically, the CMAAdapter prepares the data stream for event processing. One CMAAdapter monitors one Communications Manager. Your Avaya IQ system must have one or more CMAAdapters.

**Container:** Data Processing JBoss and Data Collection JBoss.

**If this PE fails:** Call event data between Communication Manager and Avaya IQ is lost.

---

## PE PDS Adapter

Monitors the PCAdapter.

The PCAdapter implements a protocol that manages the communications link between Proactive Contact and Avaya IQ. More specifically, the PCAdapter prepares the data stream for event processing. Your Avaya IQ system can have zero, one, or multiple PCAdapters. Every PCAdapter must have a corresponding CMAAdapter.

**Container:** Data Processing JBoss and Data Collection JBoss.

**If this PE fails:** Outbound call event data between Proactive Contact and Avaya IQ is lost.

---

## PE Aggregation

Periodically creates summaries of historical data.

**Container:** CS Tomcat - also called "Admin Tomcat".

**If this PE fails:** Data is missing from summary historical reports.

---

## PE HDAPR Entity Monitor

Manages the HDAPR.

The Historical Data Access Permissions Recorder (HDAPR) processes administrative data about user access to Avaya IQ, and records it in the Historical Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified.

**Container:** Admin JBoss.

**If this PE fails:** Historical user permission data is not recorded. Historical user permission data includes initial synchronization information and updates to user permissions.

---

## PE HDR Entity Monitor

Monitors the HDR.

The Historical Dimensional Recorder (HDR) processes administrative name data collected from one or more external data sources and records it in the Historical Data Store.

**Container:** Admin JBoss.

**If this PE fails:** Historical administration data is not recorded. Historical administration data includes initial synchronization information and updates to names of agents, queues, routing points, and so on.

---

## PE IRS

Manages the Identity Resolution Service (IRS) that provides a unique EID for each entity in the system.

**Container:** Admin JBoss and IRS JBoss.

**If this PE fails:** Data flow through the system eventually stalls. The PE IRS must function correctly to process events. Data is buffered for a time while the PE IRS is down, but not indefinitely.

---

## PE Key Authority

Associates the correct surrogate key to an EID.

**Container:** Admin JBoss.

**If this PE fails:** The PE Key Authority cannot receive key values generated and forwarded by the IRS component. Key lookups by the event processor fail. Data flow through the system eventually stalls. The PE Key Authority must function correctly to process events. Data is buffered for a time while the PE Key Authority is down, but not indefinitely.

---

## PE Load Date

Also called “PE Load Date Key”. Updates an internal table with an integer that identifies a current point in time down to the minute. This table is used by reports to select the time for a report.

**Container:** Admin JBoss.

**If this PE fails:** Reports contain erroneous or missing data. You might also see error messages while trying to run reports.

---

## PE Message Broker

Controls the ActiveMQ messaging service between Avaya IQ components. An internet search can provide you with more details about ActiveMQ.

**Container:** Message Broker Service.

**If this PE fails:** The processing of initial synchronization fails, as does the processing of administration and user permission data. Avaya IQ cannot function without the PE Message Broker.

---

## PE RDAPR Entity Monitor

Monitors the RDAPR.

The Real Time Data Access Permissions Recorder (RDAPR) processes administrative data about user access to Avaya IQ, and records it in the Real Time Data Store. This data is processed only during initial synchronization, and when user permissions are added, deleted, or modified.

**Container:** Admin JBoss.

**If this PE fails:** Real time user permission data is not recorded. Real time user permission data includes initial synchronization information and updates to user permissions.

---

## PE RDR Entity Monitor

Monitors the RDR.

The Real Time Dimensional Recorder (RDR) processes administrative name data collected from one or more external data sources and records it in the real time database.

**Container:** Admin JBoss.

**If this PE fails:** Real time administration data is not recorded. Real time administration data includes initial synchronization information and updates to names of agents, queues, routing points, and so on.

---

## PE Real Time Report Service

Provides reporting user interface services.

**Container:** Reporting UI - also called "Reporting JBoss".

**If this PE fails:** The Avaya IQ reporting user interface is disabled and the Avaya IQ reporting Web page cannot be found.

---

## Data Export (optional)

Provides external applications access to historical and real-time data.

**Container:** Reporting UI - also called "Reporting JBoss".

**If this PE fails:** External applications cannot access Avaya IQ data.

---

## PE Reporting Web

Controls the starting and stopping of the Apache Web server required for Avaya IQ reporting.

**Container:** Reporting Web Service.

**If this PE fails:** You might be able to log into the reporting user interface but reports cannot run.

---

## PE Reporting Application

Controls the starting and stopping of the Avaya IQ Reporting Model.

**Container:** Reporting Application Service.

**If this PE fails:** You might be able to log into the reporting user interface but reports cannot run.

---

## PE Admin Recorder

The Administration Recorder takes administration data collected from one or more external data sources and records it to the database.

**Container:** Admin JBoss.

**If this PE fails:** Administrative synchronization and update data is not propagated through the system causing missing names for agents, queues, routing points, and so on.

---

## PE Scheduler

Also called "PE Scheduler Utility". Provides a mechanism to run tasks on a scheduled basis.

**Container:** Admin JBoss.

**If this PE fails:** Scheduled jobs do not run. This includes the real time and historical Date/Timezone extender jobs required for reporting functions.

---

## Container descriptions

The following table describes each container in an Avaya IQ system. Your system may not contain all the following containers.










Container	Description
Admin JBoss	Provides the processing of administrative data and scheduling.
CS Tomcat	Provides services for configuration, logging, alarming, and so on for the Administration or All Functions host.
CS Tomcat Basic	Provides services for configuration, logging, and alarming, and so on for all application hosts except the Administration and All Functions host.
Data Collection JBoss	Controls the preservation of events and data from the data sources.
Data Processing JBoss	Contains the data source adapters and the event processing for fact data.
IRS JBoss	Controls the Identity Resolution Service (IRS) that provides a unique EID for each entity in the system.
Message Broker Service	Controls the ActiveMQ messaging service between Avaya IQ components. An internet search can provide you with more information about ActiveMQ.
Realtime Dashboard	Contains real time data in memory, and generates real time dashboard report content.
Reporting Application Service	Contains the reporting application components of Avaya IQ.
Reporting JBoss	Provides services for the reporting user interface.
Reporting Web Service	Controls the starting and stopping of the Apache Web server required for Avaya IQ reporting.









# Chapter 6: OAM pages for troubleshooting

## Host View and Container View icons

The icons seen on the Host View and Container View pages are described in the following table.

Icon or indicator	Name	Description
green 	Active	The associated subsystem, PE, or container is active and the process is running.
red 	Inactive	The associated subsystem, PE, or container is inactive or stopped.
green red 	Starting	The current state of the PE or container is in a transitional starting state. If a PE or container remains in this state, check the log files for more information.
green red 	Stopping	The current state of the PE or container is in a transitional stopping state. If a PE or container remains in this state, check the log files for more information.
	Collapsed	Indicates that the current view is collapsed. Clicking this icon expands the list.
	Expanded	Indicates that the current view is expanded. Clicking this icon collapses the list.
	Unknown	Avaya IQ cannot determine the state of this subsystem, PE, or container.
	Edit	Opens the appropriate page to change the provisioning for the highlighted subsystem, PE, or container. This icon is enabled only when the subsystem, PE, or container is highlighted.
	Show status - Opens new window	Opens the <a href="#">Processing Element Status Information page</a> on page 77 for the highlighted PE. This page provides detailed information about the PE.

Icon or indicator	Name	Description
	Start	Starts the highlighted PE or container. This icon is enabled only when the PE or container is highlighted and currently inactive.
	Restart	Restarts, or reboots, the highlighted PE or container. This icon is enabled only when the PE or container is highlighted and currently active.
	Stop	Stops the highlighted PE or container. This icon is enabled only when the PE or container is highlighted and currently active.
	Synchronize	Refreshes the display. Not all PEs can be refreshed. This icon is not active unless a PE that can be refreshed is highlighted.
	Stop All	From the Container View page, stops the container and all associated PEs. This icon is enabled only when a process and subsystem are highlighted and currently active.
	Start All	From the Container View page, starts the container and all associated PEs. This icon is enabled only when a process and subsystem are highlighted and currently inactive.

---

## Host View page

Use the Host View page to view, restart, start, and stop the Processing Elements (PEs).

---

## How containers and PEs are grouped

In the Host View page, PEs are grouped by subsystem function and not grouped by container.

The best way to determine which PEs are grouped under which containers is to use the following command:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

**! Important:**

Do not confuse subsystem names with containers.

## Subsystem descriptions

The following subsystems and PEs are displayed on the Host View page.

Subsystem or PE	Description
CS Foundation This subsystem includes the following PEs:	Contains the common services, or Core Services (CS), that are reused across Avaya IQ and other Avaya products.
Alarm Config Service	
Alarm Retriever Service	
PE Alarm Service	
PE Authorization Service	
PE Host Log Retriever Server	
PE Host Log Server	
PE Network Log Retriever Service	
PE Network Log Service	
PE OAM	
PE SDAS	
Data Collection This subsystem includes the following PEs:	Preserves the events and data from the data sources. Data Collection will be available in a future release.
PE CM Adapter	
PE PDS Adapter	Processes the events and data used for historical and real-time reporting and stores this data in the database.
Data Processing This subsystem includes the following PEs:	
PE Event Processor	
PE Recorder	
PE CM Adapter	
PE PDS Adapter	Writes historical data received from other subsystems and sends it to the historical data store.
Historical Data Consolidation This subsystem includes the following PEs:	
PE Aggregation	

Subsystem or PE	Description
PE HDAPR Entity Monitor	
PE HDR Entity Monitor	
Key Management This subsystem includes the following PEs:	Manages the Entity Identifiers (EIDs) and surrogate keys to identify the entities coming from the data sources, such as the agent login ID on Communication Manager or the agent extension on Proactive Contact.
PE IRS	
PE Key Authority	
PE Load Date	
Messaging This subsystem includes the following PE:	
PE Message Broker	
Real Time Data Consolidation This subsystem includes the following PEs:	Provides a consolidated view of real-time data received from multiple real-time data collection subsystems.
PE RDAPR Entity Monitor	
PE RDR Entity Monitor	
Real Time Report Execution This subsystem includes the following PEs:	Manages the execution and display of real-time reports that automatically refresh.
PE Real Time Report Service	
Data Export (optional)	
Report Gateway This subsystem includes the following PE:	
PE Reporting Web	
Report Management This subsystem includes the following PE:	Allows users to view, create, manage, and distribute reports.
PE Reporting Application	
System Management This subsystem includes the following PEs:	Provides the Avaya IQ OAM capabilities for Avaya IQ and Call Center administration.
PE Admin Recorder	
PE Scheduler	
Realtime Dashboard	Contains real time data in memory, and generates real time dashboard report content.

---

## Processing Element Status Information page

If you click the **Show status - Opens new window** icon from the Host View page, the Processing Element Status Information page opens with detailed information about the PE you highlighted.

**General tab:** Provides the PE name, the IP address of the system where the PE is running, and the port number where it listens for requests. Knowing the IP address and the port number is useful for troubleshooting potential port conflicts.

**Advanced tab:** Contains a snapshot of the internal state and statistics for the PE. There can also be a summary of connection status to other components. This connection status is useful because some components do not connect to other components as clients so they may not track connection status information.

---

## Container View

Use the Container View page to view, restart, start, and stop the containers.

---

## Edit Container page

The Edit Container page is used to change the name, host, and port for a container. Customers must take assistance from Avaya support personnel to change any of these values.

---

## Ping Host page

Use the Ping Host page to determine if the host name or IP address you specify exists and is accepting requests.

---

## Ping Host field descriptions

The following table provides field descriptions for the **Tasks > Utility > Run Ping Test** page.

Name	Description
<b>Host/IP</b>	Use this field to enter the host name or the IP address you want to ping.
<b>Packet Count Size: 64</b>	A display line to indicate that Avaya IQ is sending a 64-byte packet to the host name or IP address you specify. You cannot change this value.
<b>Packet Count: 5</b>	A display line to indicate that Avaya IQ is sending 5 packets to the host name or IP address you specify. You cannot change this value.

**Related topics:**

[Running a ping test](#) on page 29

# Chapter 7: Synchronization

---

## Synchronization

Avaya IQ synchronizes translation data in the Avaya IQ databases with the translation data in the data source databases to keep Avaya IQ reports current.

---

## Synchronization terms

<b>Administrative data</b>	Data about how routing points, agent IDs, splits, trunks, skills, and so on are administered. Also called “RFTB”.
<b>Operational state data</b>	Data that reflects the current state of all active entities. For example, an agent in AUX mode. Also called “RLTB”.
<b>Contact data</b>	Data that records call center contact information. For example, the telephone number of a caller.
<b>Names data</b>	Data about how vectors, trunk groups, hunt groups, routing points, and agents are named. For example, the name that identifies an agent, such as Alice Smith. Names synchronization also synchronizes permission information about all administered agents, including agents not logged in.

---

## Synchronization types

Avaya IQ has the following types of synchronizations.

### Initial

Occurs during implementation when the Avaya IQ databases are getting built. During initial synchronization, report users cannot access the user interface or generate reports for up to 20 minutes. This type of synchronization is commonly referred to as “pump-up”.

Initial synchronizations involve more activity than subsequent synchronizations. All administration data from the data sources are synchronized. In addition, all Role Based Access

Control (RBAC) permissions are synchronized, which includes queues, agents, and routing points.

### **Subsequent**

Occurs when the existing databases need to be updated because a change occurred in Avaya IQ or in the data source. Avaya IQ monitors translation data and initiates synchronizations when it discovers changes in Avaya IQ or in the data sources. On large data source systems, synchronization takes about 5 minutes. Synchronization times are significantly shorter on smaller systems. Even though report users still have access to Avaya IQ reports during synchronization, reports do not contain the updated data until synchronization is complete. Report users also cannot run reports on new Communication Manager entities for up to 30 minutes.

In subsequent synchronizations, all administration data and operational state data is synchronized. Only changes made to RBAC permissions are synchronized. RBAC permissions are processed out of a queue that is separate from the data flowing from the data sources.

Avaya IQ also initiates a synchronization after network interruptions. After the network is restored, if Avaya IQ detects any changes in the data source, administration and operational state data are synchronized. If Avaya IQ does not detect any changes, only operational state data is synchronized.

#### **\* Note:**

Subsequent synchronizations between CMS and Communication Manager work the same as subsequent synchronizations between Avaya IQ and Communication Manager.

### **Names**

Unlike CMS, Avaya IQ also performs a names synchronization with Communication Manager after the initial or subsequent synchronization is complete. The names synchronization can take some time to complete. Currently, the names in Communication Manager translation data can synchronize with Avaya IQ but not vice versa.

---

## **What data gets synchronized?**

### **From Communication Manager**

The following data gets synchronized:

- Administration data (RFTB) for routing points, agent IDs, splits, trunks, skills, and so on.
- Operational state data (RLTB) for data that reflects the current state of all active entities.
- Contact data for data that records call center contact information.
- Names data for vectors, trunk groups, hunt groups, routing points, and agents.



**From Proactive Contact**

The following data gets synchronized:

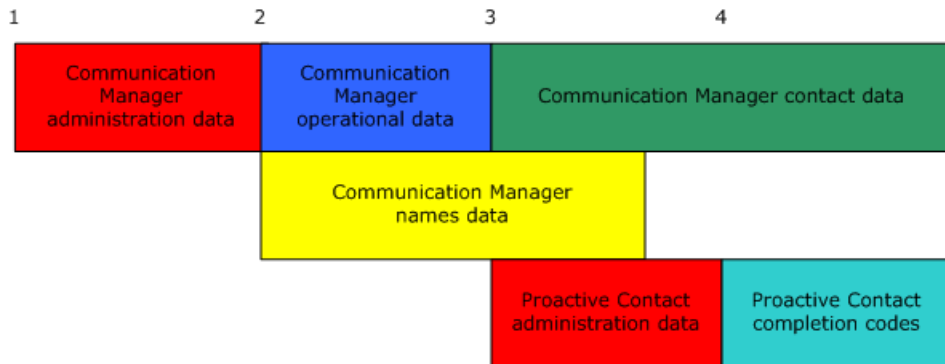
- Administration data (RFTB)
- Completion codes

**From Avaya IQ**

RBAC permission data. This data is not synchronized from a data source. Role permissions are defined for resources associated with data sources, but are assigned and maintained by Avaya IQ.

## Communication Manager and Proactive Contact

The following diagram describes how simultaneous synchronizations between Avaya IQ and Communication Manager, and between Avaya IQ and Proactive Contact are processed.



**Table 1: Figure notes:**

<ol style="list-style-type: none"> <li>1. Communication Manager administration synchronization starts.</li> <li>2. Once all Communication Manager administration messages are stored in the queue, Communication Manager names synchronization starts and Communication Manager operational synchronization is requested. Names synchronization is non-blocking and is interrupted until operational synchronization completes.</li> </ol>	<ol style="list-style-type: none"> <li>1. When Communication Manager operational synchronization completes, Communication Manager contact synchronization starts and gets recorded to the database, while names synchronization continues. At the same time, Proactive Contact administration synchronization starts.</li> <li>2. Proactive Contact administration synchronization completes and Proactive Contact completion code synchronization starts.</li> </ol>
--	---

---

## Initiating synchronizations manually

### Procedure

You can initiate a synchronization manually by temporarily disabling the link between the data source and Avaya IQ, by restarting Avaya IQ, or by restarting the PE CM Adapter or PE PDS Adapter on the Data Processing container.

---

### Related topics:

[Starting, stopping, and restarting a PE](#)

[Starting Avaya IQ on an application host](#) on page 30

---

## Synchronization data flow

The following diagrams describe each phase in a synchronization data flow between Avaya IQ and Communication Manager. In a Multiple Host deployment, the Data Processing and Administration functions are on separate application hosts. In an All Functions deployment, both functions are on the same application host. For simplicity, these diagrams show only the process for historical data. The process of real-time data flow is similar to the process of historical data flow. The only difference is that in real-time data flow the data flows from ROT to both Real time data store and Real-time Dashboard. For example, Communication Manager > CMIT > REP > ROT > Real-time Data Store and Realtime Dashboard.

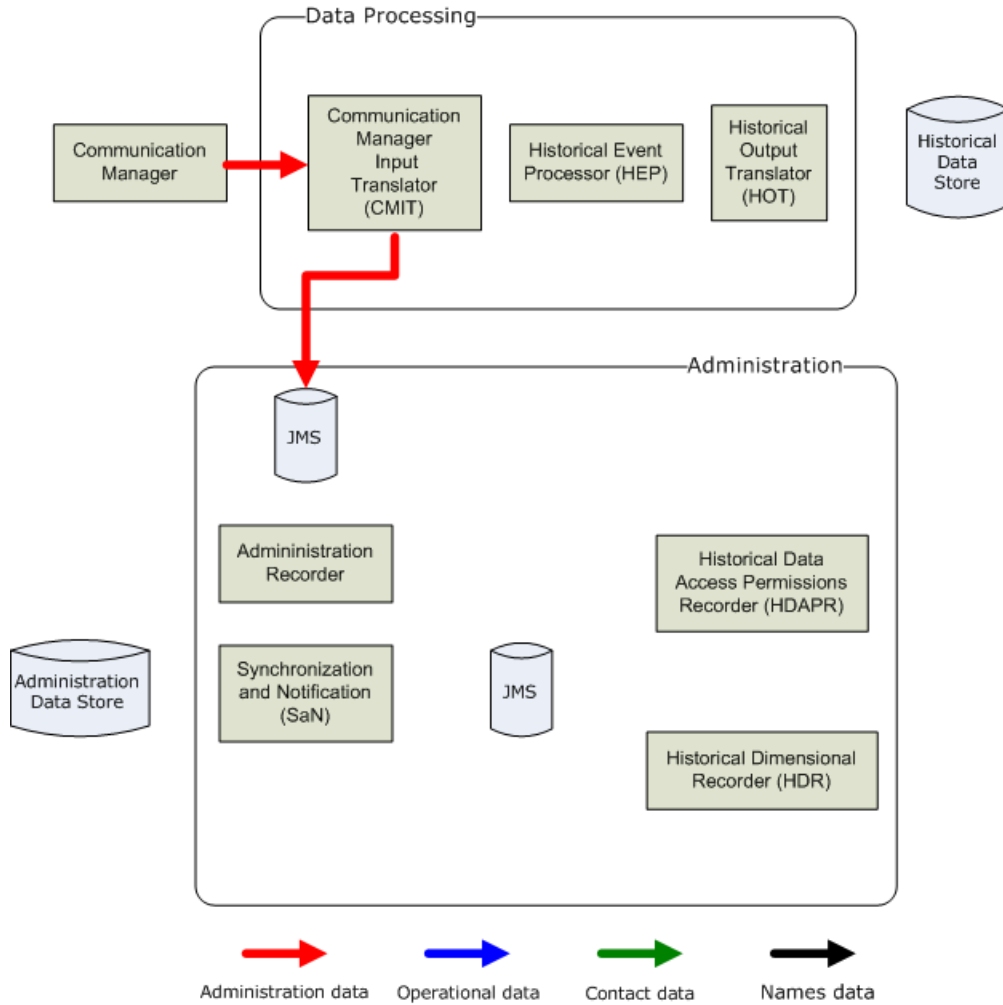
### Related topics:

[Data flows](#) on page 17

---

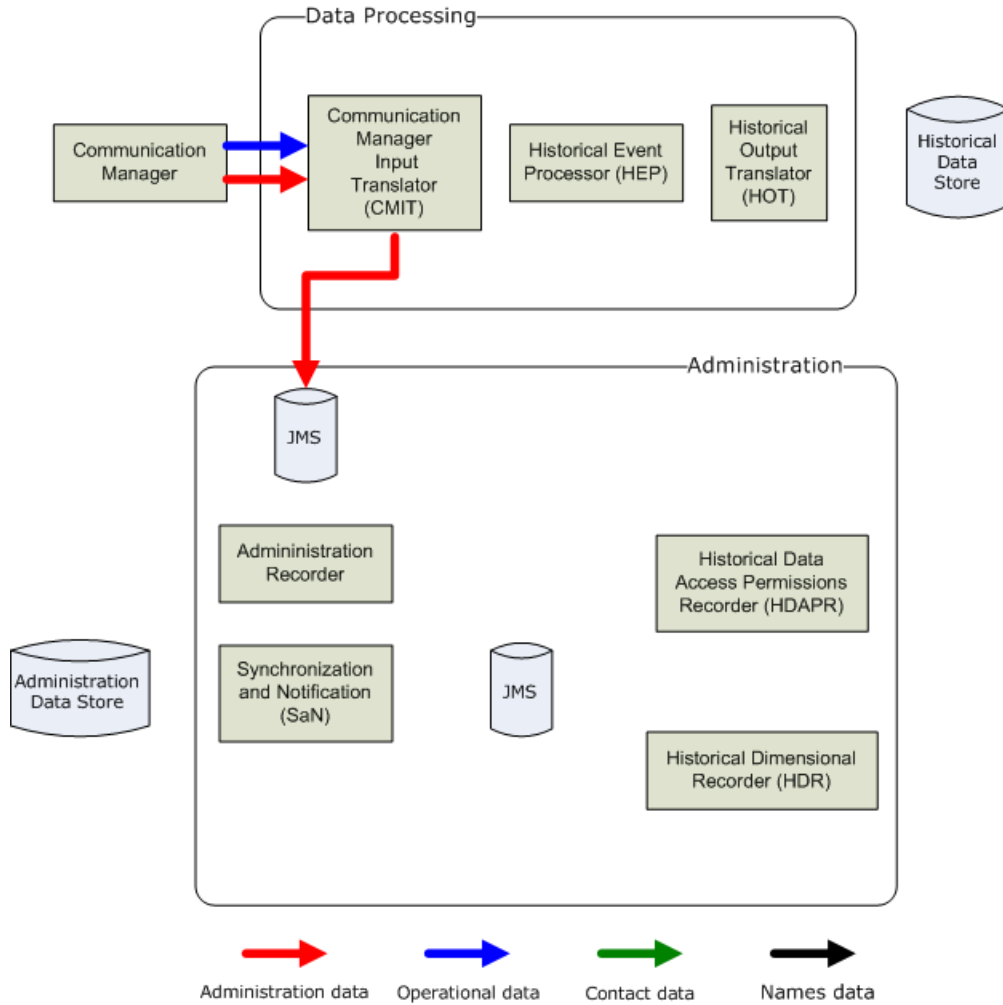
## Phase 1

The CMIT receives administration messages and delivers all messages to the administration Java Messaging Service (JMS) input queue.



## Phase 2

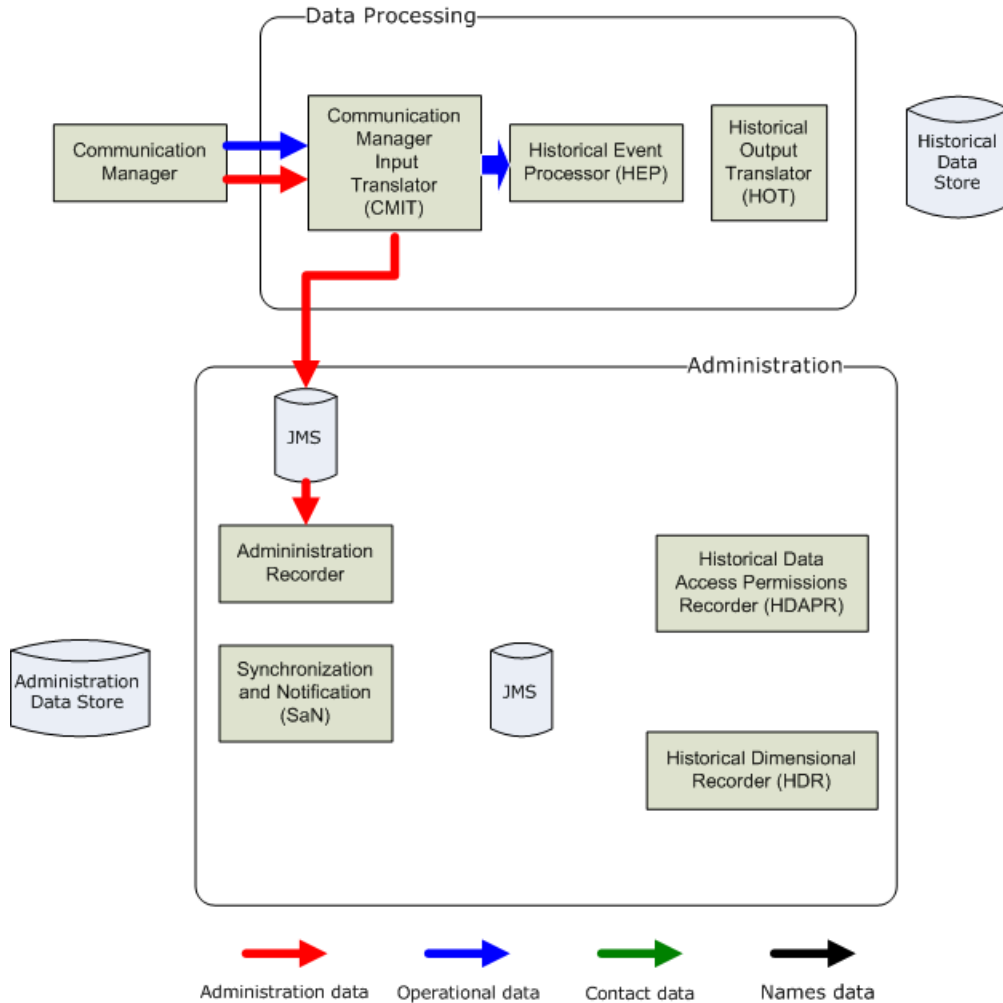
The CMIT receives operational data.



---

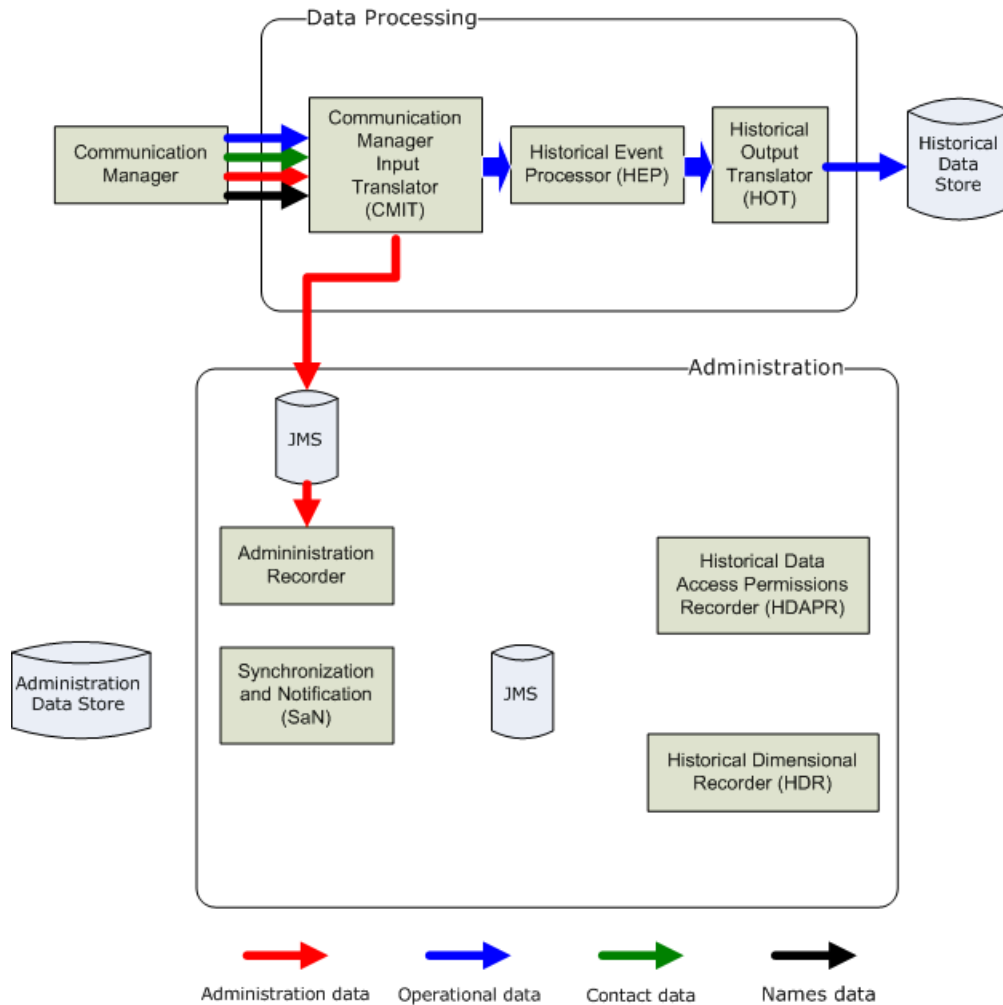
## Phase 3

Administration messages are processed off the JMS queue while the HEP receives operational data messages.



## Phase 4

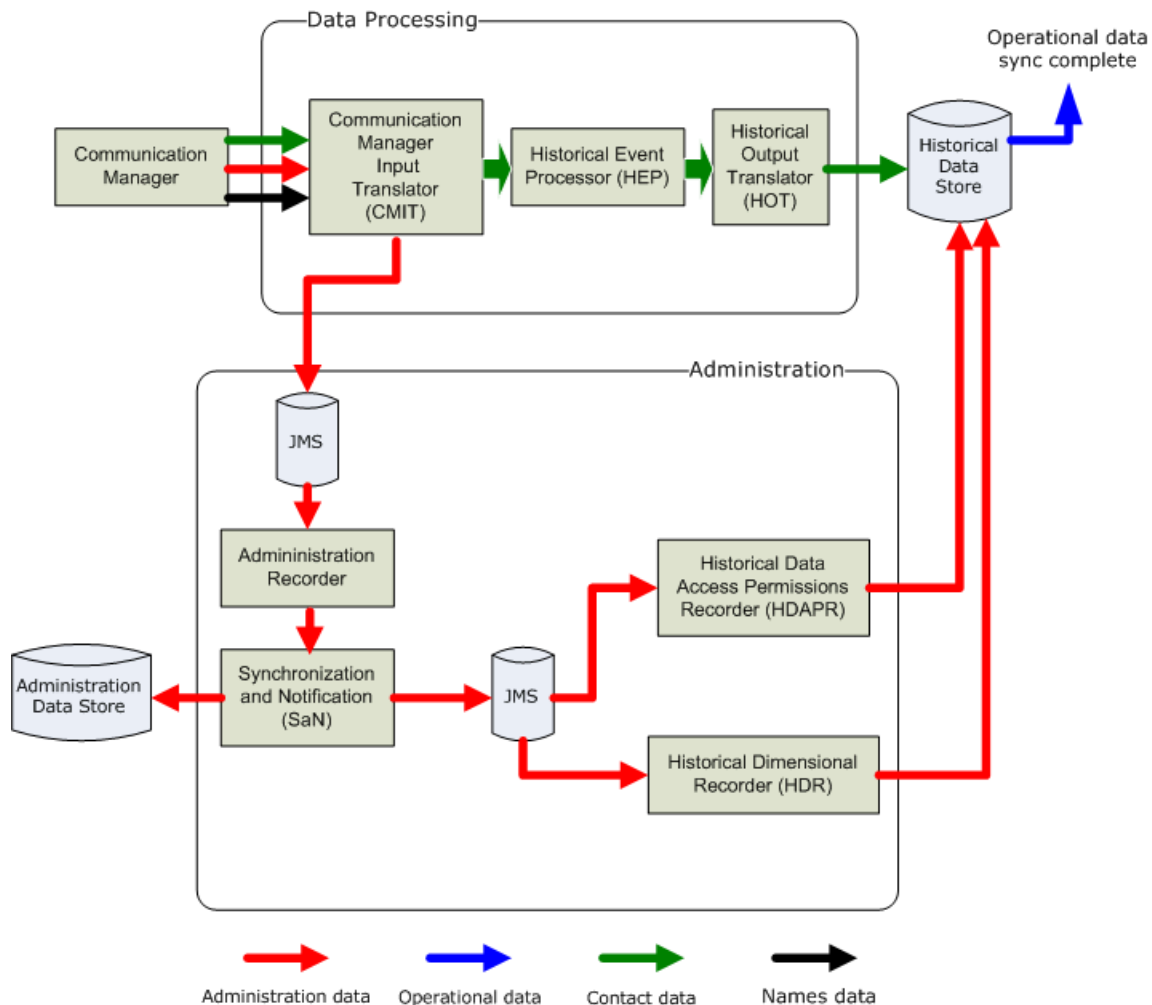
Operational data synchronization completes while the CMIT receives contact data and names synchronization data.



## Phase 5

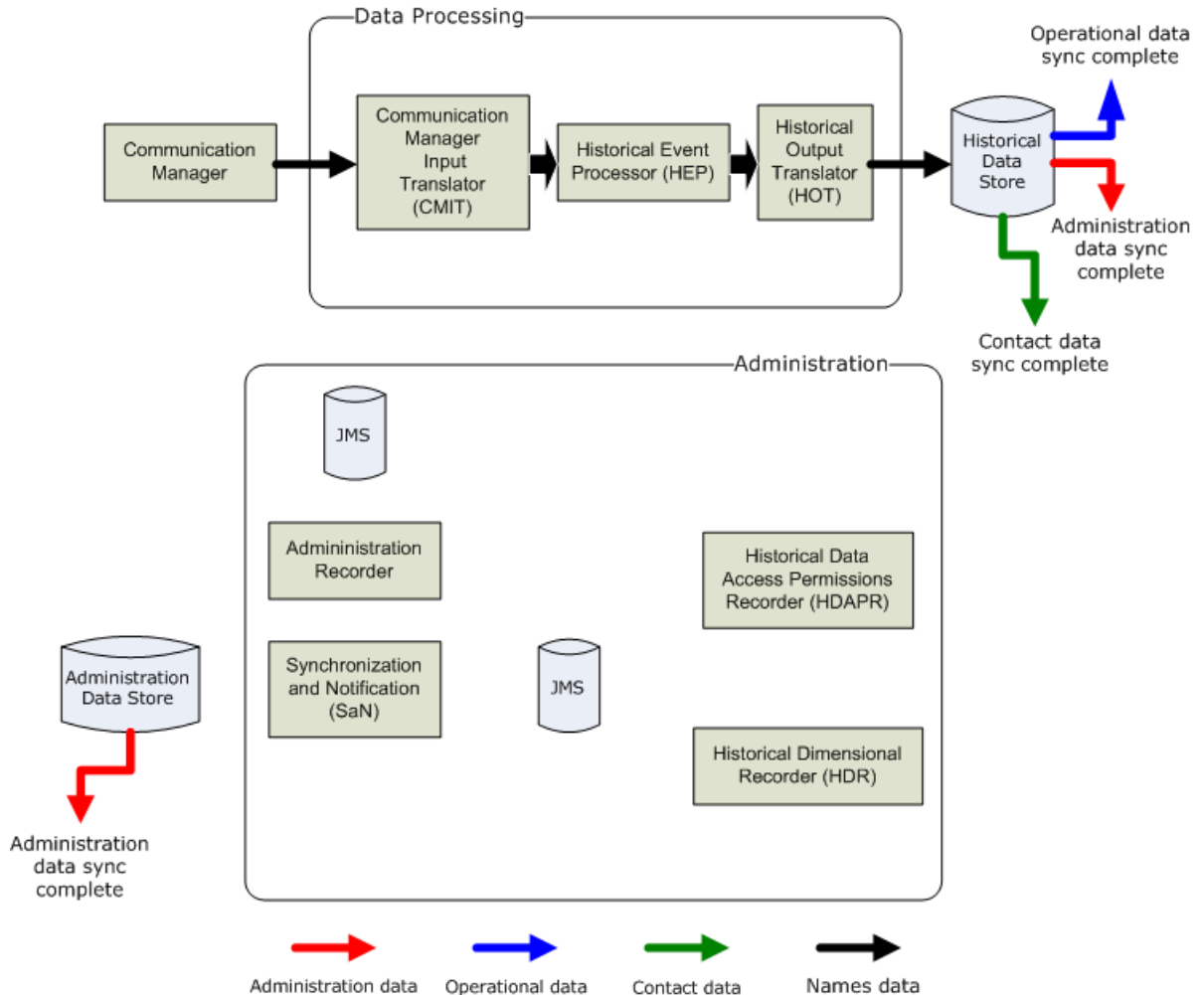
Administration data flows through the administration functions to the Historical Data Store. At the same time, contact data flows through the data processing functions.

Contact data is not blocked while administration data flows through the administration functions. Avaya IQ uses temporary IDs for the administration entities such as routing points and trunks, until each entity is added to the historical data store.



## Phase 6

Names data flows through data processing and completes.



## Synchronization verification

Usually, your synchronization completed successfully when you have green indicators next to all PEs and containers in the OAM. For more information, see [Verifying system status](#).

Do any of the following tasks if you must do further checking:

- [Ensuring that data is getting processed](#) on page 89
- [Checking reports](#) on page 89
- [Checking container logs](#) on page 90
- [Checking Communication Manager hexadecimal logs](#) on page 90
- [Checking Proactive Contact Llogs](#) on page 91



**Related topics:**

[Verifying system status](#) on page 29

---

## Ensuring that data is getting processed

### About this task

Ensure that administrative data and current call traffic is getting processed by checking the database (software-only customers) or by checking the Data Stream indicator (software-only and turnkey customers).

### Procedure

1. For administrative data, software-only customers can check the historical ROUTINGCONSTRUCTDIM and the PARTYDIM tables.  
Administrative data is getting processed if you see data.
2. For call traffic, software-only customers can check the historical AGENTSTATEFACT and real-time RTAGENSTATEFACT tables.  
Call traffic is getting processed and records are being added if you see data.
3. For software-only and turnkey customers, you can log in to either reporting interface (Standard Reports or the Avaya IQ Performance Center) to see the status of the Data Stream indicator.
  - In the Standard Reports interface, the chevron on the title bar of the window indicates where data is flowing from the source system to Avaya IQ. If the chevron is pointing up, the Avaya IQ system is receiving and processing data.
  - In the Avaya IQ Performance Center interface, if the check mark is displayed, the Avaya IQ system is receiving and processing data.

---

## Checking reports

### Procedure

Set up reporting groups and run a few reports.

---

---

## Checking container logs

### About this task

Check the following container logs for messages with exceptions, or messages with severities of error:

### Procedure

1. `/var/log/Avaya/CCR/REPORTING_RECORDERS>/REPORTING_RECORDERS.log`
  2. `/var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/DataProcessingJBoss_<SOURCENAME>.log`
- 

---

## Checking Communication Manager hexadecimal logs

### About this task

Check the Communication Manager synchronization status by monitoring the growth of the hexadecimal log files.

### Procedure

1. Go to `/var/log/Avaya/CCR/DataProcessingJBoss_<SOURCENAME>/*` and view each hexadecimal log:
    - `hex_dump_all.log`
    - `pu_admin_full.hex`
    - Full synchronization is bracketed by `XOPEN20 FULLXLATION ... XCLOSE20 FULLXLATION`
    - `pu_admin_name.hex`
    - `pu_oper.hex`
    - Full synchronization is bracketed by `XOPEN20 LOGONSTATUS ... XCLOSE20 LOGONSTATUS`
    - `traffic_data.hex`

For more information, see Log file descriptions.
  2. Go to `/var/log/Avaya/CCR/DataCollectionJBoss_<SOURCENAME>/*` and view each hexadecimal log.
-

---

## Checking Proactive Contact logs

### About this task

There are currently no hexadecimal log files for Proactive Contact. Instead, you can determine the status of a Proactive Contact synchronization by looking at the pcmsgs and pcit logs.

### Procedure

1. Go to `/var/log/Avaya/CCR/DataProcessingJBoss_<SOURCE_NAME>/messages_pcmsgs.log`.
2. Look for the following indicators:
  - LINK\_UP
  - PUMPUP\_ADMIN\_START
  - PUMPUP\_ADMIN\_END

These messages indicate a successful connection to Proactive Contact.

3. Go to `/var/log/Avaya/CCR/DataProcessingJBoss_<SOURCE_NAME>/messages_pcit.log`.
4. Look for the following indicators:
  - LINK\_UP
  - PUMPUP\_ADMIN\_START
  - PUMPUP\_ADMIN\_END
  - OUTPUTS of SourceSynchronizing
  - OUTPUTS of SourceOperational
  - OUTPUTS of SourceSynchronized

These messages indicate that the PCIT is correctly processing events.

---

---

## Troubleshooting the ETL application for Voice Portal

Every time the Extract Load Transform (ELT) application is run, the logs are appended. ETL application logs are written to:

```
$CCR_HOME/etl/Avaya/ETLApps/VoicePortal/Logs
```

You can use logs to diagnose whether ETL was able to connect to your Voice Portal database and Avaya IQ database. Logs also display the row level imports.

## Synchronization

For information on the transformation when Voice Portal data is transferred to the ETL tables, and eventually into reporting tables, some transformation may not appear as expected. To diagnose this problem, you can use the Tomcat logs located at:

```
/var/log/Avaya/CCR/TOMCAT_x
```

where *x* is the unique ID of the Tomcat container.

Tomcat log level can be changed by modifying the following file:

```
/opt/Avaya/CCR/data/TOMCAT_x/log4j.properties
```

# Chapter 8: Maintenance activities

---

## Differences between software-only and turnkey maintenance

If your Avaya IQ system uses hardware that you purchased yourself, you need software-only maintenance. If Avaya provided the hardware for your system, you need turnkey maintenance. In most cases, the routine maintenance for both is similar. This section describes the major differences in routine maintenance for the two deployments.

### Software-only maintenance

You can use all the procedures listed in the chapter “Maintenance activities” in a software-only deployment, except the procedures designated for customers using the turnkey deployment. This is especially true for the backup procedures for which you must only use the following procedures:

- [Backing up Avaya IQ data in a software-only deployment](#) on page 202
- [Backing up the operating system in a software-only deployment](#) on page 203
- [Backing up the database on a software-only deployment](#) on page 203

### Turnkey maintenance

You can use all the procedures listed in the chapter “Maintenance activities” in a turnkey deployment, except the procedures designated for customers using the software-only deployment. This is especially true for the backup procedures for which you must only use the following procedures: [Data backups and database maintenance for a turnkey deployment](#) on page 204.

The following are some more maintenance issues related to a turnkey deployment.

**Linux and Oracle updates:** You must install only the Linux or Oracle patches that Avaya provides. Avaya will contact you for the forthcoming patches to be installed on your system.

**Access to Oracle software:** In the Avaya contract for turnkey deployments, Avaya specifies that you cannot gain access to the Oracle software directly, either through command line application or a commercial Oracle client application. In addition, you cannot use the Oracle database for any applications other than Avaya IQ. As a turnkey customer, you can use the utilities that Avaya provides to run the basic database functions without being directly exposed

to the Oracle utilities that exist on the turnkey system. The Avaya utilities include the following functions:

- Backup
- Restore
- Purge data
- Rebuild index

---

## Recommendations for monitoring logs and alarms

To ascertain the frequency with which you should monitor your log and alarm files, perform the following actions:

- Conduct a risk analysis based on the nature of your business. Take into consideration the type of data that the log and alarm files contain and how critical the application is to your business.
- Think about the damage or repercussions that particular types of undetected events may cause.

In view of the findings from the above analysis, you must:

- Determine if you must perform weekly, daily, or continuous monitoring of an event.
- Create your own policy regarding different monitoring intervals for different events.
- Check the admin access log.
- Check the security access log.

For detailed information about how to monitor logs and alarms, see *Avaya IQ Alarms and Logs*.

---

## Cleaning up user accounts

### Before you begin

Before you remove users from Avaya IQ, User Management, or the Enterprise Directory, you must first clean up the user account. If you do not clean up, the scheduled reports or administration jobs of the user may use up a lot of system processing time and waste storage space.

Before you delete the user from the Enterprise Directory or from the Common User Service directory through the User Management administration, change the user password.

## Procedure

1. Log in to Reporting as the user using the new password.
  2. Delete the existing content from the **My Folders** directories of the user, including any scheduled report jobs.  
Copy custom reports or report definitions of value, if any, to **Custom Reports** folder and then move the reports to your own **My Folders** directory. Delete all the scheduled jobs of the user.
  3. Log in to Administration as the user using the new password.
  4. Delete any scheduled jobs the user created.  
Make sure no other user or system needs the scheduled job.
  5. After you delete the user jobs and folders, you can delete the user from the Enterprise Directory or the Common User Service directory.
- 

---

# Changing the password for the administration user in Tomcat

## Before you begin

For Avaya IQ 5.1 onwards, you need to have encrypted versions of the passwords.

Backup all the files before editing them.

## Procedure

1. Enter:
 

```
cd $CATALINA_HOME/bin
pwd /opt/coreservices/tomcat5/bin
./digest.sh -a SHA <defaultpassword>
```

 where *<defaultpassword>* is your new administration password.
2. Open the `/opt/coreservices/tomcat-5.5.27/conf/tomcat-users.xml` file. Search for the line `user name="admin"` and replace the value of the attribute `password` with the encrypted password.
3. Open the `/opt/coreservices/tomcat-5.5.27/tomcat-users.xml` file. Search for the line `user name="admin"` and replace the value of the attribute `password` with the encrypted password.
4. Edit the lifecycle files in the `/opt/coreservices/lifecycle/persistence` directory for all the PEs under tomcat. Search for the line `<entry key="TomcatPassword">` and replace the existing text value with your default

administration password. Ensure that you change the password in all ten files in the `/opt/coreservices/lifecycle/persistence` directory.

5. Stop and then restart the administration tomcat container using the following command:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
```

6. Enter the following commands:

```
/opt/coreservices/watchd/shutdownproc LCM
```

```
/opt/coreservices/watchd/addproc LCM
```

---

---

## Restarting, rebooting, and power-cycling hosts

---

### Defining restarts, reboots, and power-cycling hosts

There are two reasons why you should restart, reboot, or power-cycle hosts in your deployment:

- When failures occur on a host and you must restart, reboot, or power-cycle a host to recover.
- When you perform a routine system restart based on recommended best practices.

To better understand when you should perform a restart, a reboot, or a power-cycle procedure, you must first understand the purpose and consequences of doing each procedure.

#### **Caution:**

Restart, reboot, and power-cycle procedures cause loss of data and will interrupt users. Perform these procedures during low or no traffic periods. Schedule the procedure and notify users that the system will not be available during the procedure. It takes about 15 minutes to restart, reboot, or power-cycle each host.

#### **Restarts**

Restarts are used to stop the application or database software and restart the software. Restarts do not bring the OS to the init 0 (power-off) state. This means that a host can still be reached over the network and that on-site personnel are not required to restart the host.

#### **Reboots**

Reboots take a host to the OS init 0 shutdown state, then brings the host back up to the init 5 operating state. At the same time, the application software and database software are stopped and restarted. Should the host not reboot to the init 5 state, you may need on-site personnel to manually power-down and power-up the host.



## Power-cycling hosts

Power-cycling hosts is the most severe method available to restart and reboot a host. A power-down is done using the `shutdown` command or, if required, by pressing the power button on the host. After this is done, on-site personnel must manually press the power button to power-up the host.

### Impacts when restarting, rebooting, or power-cycling hosts

The following table describes the impacts of restarting, rebooting, or power-cycling various hosts.

Scenario	Severity	Description	Impact of the Outage
A	High	Data collection from data sources stops	<ul style="list-style-type: none"> <li>• Loss of data</li> <li>• Real-time reports will not show current statistics</li> <li>• Historical reports will show a gap or incomplete statistics during the outage</li> </ul>
B	Medium	Voice portal data streaming stops	<ul style="list-style-type: none"> <li>• Loss of data</li> <li>• Voice portal reports (Process Performance) will not show data during the outage</li> </ul>
C	Medium	Access to the administration interface is not possible	Cannot log in to or make administrative changes on the system
D	Medium	Access to the standard reporting interface is not possible	Cannot log in to or run standard reports
E	Medium	Access to the real-time dashboard reports is not possible	Cannot log in to or run real-time dashboard reports

When restarting application hosts, for example, an All Functions host, an Administration host, or a Reporting host, certain features will not be available to users during the restart. Use the following table to define the impacts when restarting, rebooting, or power-cycling different hosts.

Host type	Scenario
All Functions	A, B, C, D, E
Administration	B, C, D, E
Data Processing	A

Host type	Scenario
Data Collection	A
Reporting	D, E
RTD	E

---

## Restarting application hosts

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the application host.
  2. Enter:  

```
service wdinit stop
```

This stops the application software.
  3. Enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

Confirm that all processing elements and containers are in the STOPPED state.
  4. Enter:  

```
service wdinit start
```

This starts the application software.
  5. Enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

Confirm that all processing elements and containers are in the STARTED state. You may have to wait a few minutes for all processing elements and containers to start.
- 

---

## Restarting the Database host

When restarting the Database host, reporting features are not available.

### Before you begin

Notify users to log out of the system before starting this procedure.

## Procedure

1. Log on as root or a root-level user on the database host.
  2. Enter:  

```
service dbora stop
```

This stops the database software.
  3. Enter:  

```
service dbora start
```

This starts the database software.
- 

---

## Rebooting hosts

Rebooting takes a host from its normal operating state to its init0 state, restarts the OS, and also restarts the application and database software. When doing a reboot, you are not required to manually stop and start the application or database software.

**! Important:**

Rebooting a host is an extreme measure that should only be done when directed by Avaya support personnel.

For procedures that require a reboot, see [Performing a routine system restart](#) on page 99.

---

## Performing a routine system restart

Avaya recommends that you restart all hosts in your system once every three months as a preventative maintenance best practice.

**⚠ Caution:**

Restart procedures cause loss of data and will interrupt users. Perform these procedures during low or no traffic periods. Schedule the restart and notify users that the system will not be available during the restart. It takes about 15 minutes to restart a host.

**\* Note:**

Restarting your hosts is not a requirement. However, periodic restarting of your hosts is a recommended procedure targeted at minimizing the risk of a system failure. Restarting your hosts lessens the possibility of your system being adversely impacted by anomalies such as memory leaks, packet loss, un-released file locks, data inconsistency, data corruption, and storage space fragmentation. These types of problems are known to occur on any computer system.

Avaya offers a High Availability (HA) solution if data loss from a host restart is a concern. The HA solution provides an uninterrupted data stream between a Communication Manager data

source and two HA hosts. If you use the HA solution, restart each host complex at a different time to prevent data loss.

Avaya support personnel who are performing system maintenance work may require you to restart your system. If Avaya support personnel require you to restart your system, they will work with you to determine the best time to perform the restart. Avaya support personnel will make every attempt to determine the root cause of any problem that might require a restart.

Hosts within your deployment are viewed as a system in which all the hosts must be restarted in the specific sequence described in this procedure.

## Restarting a single or All-in-One host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the All Functions host. This host also serves as the Database host.
  2. Enter:  

```
service wdinit stop
```

This stops the application software.
  3. Enter:  

```
service dbora stop
```

This stops the database software.
  4. Enter:  

```
reboot
```

This reboots the host.
  5. Log on as root or a root-level user on the All Functions host.
  6. Enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```
  7. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.
- 

## Restarting a dual host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

## Procedure

1. Log on as root or a root-level user on the All Functions host.
  2. Enter:  

```
service wdinit stop
```

This stops the application software.
  3. Log on as root or a root-level user on the Database host.
  4. Enter:  

```
service wdinit stop
```

This stops the application software.
  5. Enter:  

```
service dbora stop
```

This stops the database software.
  6. On the Database host, enter:  

```
reboot
```

This reboots the Database host. Wait at least 15 minutes for the Database host to start up before rebooting the All Functions host.
  7. On the All Functions host, enter:  

```
reboot
```

This reboots the All Functions host. The application software starts automatically.
  8. On the Administration host, enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```
  9. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.
- 

## Restarting a multi-host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the RTD host.
2. Enter:  

```
service wdinit stop
```

This stops the application software.

3. Repeat Steps 1 and 2 for all application hosts in the deployment in the following order:
    - a. Reporting hosts
    - b. Data Collection hosts
    - c. Data Processing hosts
    - d. Administration host
  4. Log on as root or a root-level user on the Database host.
  5. Enter:

```
service wdnit stop
```

This stops the application software.
  6. Enter:

```
service dbora stop
```

This stops the database software.
  7. On the Database host, enter:

```
reboot
```

This reboots the Database host. Wait at least 15 minutes for the Database host to start up before rebooting the Administration host.
  8. On the Administration host, enter:

```
reboot
```

This reboots the Administration host. The application software starts automatically.
  9. Repeat Step 8 for all application hosts in the deployment in the following order:
    - a. Data Processing hosts
    - b. Data Collection hosts
    - c. Reporting hosts
    - d. RTD host
  10. After the hosts reboot, log on as root or a root-level user on each host.
  11. Enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```
  12. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.
-

---

## Power-cycling hosts

Should it be necessary to cycle power on the hosts, use the procedures given in this section to gracefully power-down and power-up the hosts.

 **Caution:**

Power-cycling procedures cause loss of data and will interrupt users. Perform these procedures during low or no traffic periods. Schedule the power-cycling and notify users that the system will not be available during the procedure. It takes about 15 minutes to power-cycle a host.

 **Important:**

Power-cycling procedures require that you have personnel on-site when powering-up the hosts.

Avaya offers a High Availability (HA) solution if data loss from a host power-cycling is a concern. The HA solution provides an uninterrupted data stream between a Communication Manager data source and two HA hosts. If you use the HA solution, power-cycle each host complex at a different time to prevent data loss.

Avaya support personnel who are performing system maintenance work may require you to power-cycle your system. If Avaya support personnel require you to power-cycle your system, they will work with you to determine the best time to perform the procedure. Avaya support personnel will make every attempt to determine the root cause of any problem that might require a power-cycling.

Hosts within your deployment are viewed as a system in which all the hosts must be power-cycled in the specific sequence described in this procedure.

## Power-cycling a single or All-in-One host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the All Functions host. This host also serves as the Database host.
2. Enter:  

```
service wdinit stop
```

This stops the application software.
3. Enter:  

```
service dbora stop
```

This stops the database software.

4. Enter:  
`shutdown -h`  
This halts and shuts down the host.
  5. Press the power button on the host.
  6. After the host powers up, log on as root or a root-level user on the All Functions host.
  7. Enter:  
`sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status`
  8. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.
- 

## Power-cycling a dual host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the All Functions host.
2. Enter:  
`service wdninit stop`  
This stops the application software.
3. Log on as root or a root-level user on the Database host.
4. Enter:  
`service wdninit stop`  
This stops the application software.
5. Enter:  
`service dbora stop`  
This stops the database software.
6. On the Database host, enter:  
`shutdown -h`  
This halts and shuts down the Database host.
7. Press the power button on the Database host. Wait at least 15 minutes for the Database host to start up before power-cycling the All Functions host.
8. On the All Functions host, enter:  
`shutdown -h`



This halts and shuts down the All Functions host.

9. Press the power button on the All Functions host.
  10. After the host powers up, log on as root or a root-level user on the All Functions host.
  11. Enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```
  12. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.
- 

## Power-cycling a multi-host deployment

### Before you begin

Notify users to log out of the system before starting this procedure.

### Procedure

1. Log on as root or a root-level user on the RTD host.
2. Enter:  

```
service wdinit stop
```

This stops the application software.
3. Repeat Steps 1 and 2 for all application hosts in the deployment in the following order:
  - a. Reporting hosts
  - b. Data Collection hosts
  - c. Data Processing hosts
  - d. Administration host
4. Log on as root or a root-level user on the Database host.
5. Enter:  

```
service wdinit stop
```

This stops the application software.
6. Enter:  

```
service dbora stop
```

This stops the database software.
7. On the Database host, enter:  

```
shutdown -h
```

This halts and shuts down the Database host.

8. Press the power button on the Database host. Wait at least 15 minutes for the Database host to start up before power-cycling the All Functions host.

9. On the Administration host, enter:

```
shutdown -h
```

This halts and shuts down the Administration host.

10. Repeat Step 9 for all application hosts in the deployment in the following order:

- a. Data Processing hosts
- b. Data Collection hosts
- c. Reporting hosts
- d. RTD host

11. Press the power button on the Administration host.

12. Repeat Step 11 for all application hosts in the deployment in the following order:

- a. Data Processing hosts
- b. Data Collection hosts
- c. Reporting hosts
- d. RTD host

13. After the hosts power-up, log on as root or a root-level user on each host.

14. Enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

15. Confirm that all processing elements and containers have started. You may have to wait a few minutes for all processing elements and containers to start.

---

## Licensing

---

### About licensing

Licensing ensures that customers have the permission to use only the product functionality for which they have paid and obtained a license. To generate and acquire the license files for Avaya IQ, use the Avaya Product Licensing and Delivery System (PLDS) process. To install the license file, use the Web License Manager (WebLM) tool.

The following features are licensed for Avaya IQ. Features are licensed by a count (for example, a number of agents) or whether the feature is turned on or off.

The following features are licensed by count:

- Number of concurrent agents
- Number of concurrent report users

The following features are licensed by being on or off:

- Support for connections to one or more Communication Manager data sources
- Support for connections to one or more Proactive Contact data sources
- Support for connections to one or more Voice Portal data sources
- Support for connections to one or more Avaya Aura® Contact Center data sources
- Advanced Reporting with Avaya Aura® Contact Center
- Custom reports
- Data imports
- Historical data export
- Real-time data export
- High Availability Primary
- High Availability Secondary
- Survivability with Communication Manager systems

The system enforces licensing in the following manner:

- At start up, the system checks the existence of a valid license file. In the operational stage, whenever you access a licensed feature or attempt to acquire a licensed resource, license management verifies that a license is available.
- The system raises a CRITICAL alarm and denies all subsequent license requests if the following happens:
  - A valid license file does not exist.
  - The installed product name does not match the licensed name.
  - The license has expired.
  - The product version is older than the version specified in the license file.
- If the system does not find an expected licensed feature in the license file, the system denies the license request.
- During normal operation, if a feature that uses licensing subsequently determines that the license server is unavailable, the system initiates a 30-day grace period and raises a MINOR alarm daily during the grace period. If the grace period is in effect and the condition that caused the grace period to start is resolved, the system clears the grace period alarm, and no further alarms are raised until a new condition for alarm occurs.

- When the license file expiration date falls within 30 days of the current date, the system raises a MINOR alarm daily to warn that the license file will expire soon.
- When the grace period expires, the system raises a CRITICAL alarm and stops all data source connections such as Communication Manager and Proactive Contact.
- When the license file expires, the system raises a CRITICAL alarm and stops all data source connections such as Communication Manager and Proactive Contact.
- The system allocates the Data source licenses only when you associate a data source with a host. You can create multiple data sources, but the system counts the license only when you associate a data source with a host.
- When an agent state changes from logged out to logged in, the system acquires a license for that agent. When an agent state changes from logged in to logged out, the system releases the license for that agent. When the link to a data source terminates, the system releases all the licenses. The system releases the unused licenses every 5 minutes.
- If the system cannot acquire a license for an agent after three consecutive requests every 5 minutes, the system raises a MINOR alarm. However, the system recognizes the agent as being logged in and tracks data for that agent.
- In Avaya Performance Center, when you logs in with permission to access reports, the system acquires a report user license. If the system cannot access the report user license, you cannot launch any report Activities. You can still access Avaya IQ Administration, Avaya IQ Reporting, and change their default settings. If you logs out of Avaya Performance Center, the system releases the license immediately. Otherwise, the system releases the license after 10 minutes.

In Avaya IQ Reporting, if the system cannot acquire a report user license, you cannot log in to Avaya IQ Reporting. If you logs out of Avaya IQ Reporting, the system releases the license immediately. Otherwise the system releases the license based on session time-out set for Avaya IQ Reporting.

- When a scheduled report is ready to run, the system attempts to acquire a report user license. If the system cannot acquire a report user license, the report still runs, but the system generates a MINOR alarm.
- When a Report Designer user or a custom report creator logs in, the system attempts to acquire a license for that user. If the system cannot acquire a custom reports license, the system still grants a license to the user and generates a MINOR alarm.
- If a valid license file is not available, attempts to add a data source, such as Communication Manager or Proactive Contact, fail and the system displays an error to the user. However, the system permits administration to add a site and a host.
- Before establishing a connection with a Communication Manager or Proactive Contact data source, the system makes a request to acquire a license. If the system cannot acquire the license, the system raises a MAJOR alarm but establishes the connection anyway. However, if license renewal fails, the system terminates the connection.

- When the system starts a data export API session, the system queries the license for the data export feature. If the feature is on, the operation continues. If the feature is off, the system returns an error to the API user indicating to purchase the feature.
- If you attempt to use more than the purchased number of licenses, the system displays a message indicating that all licenses are in use and that you cannot access reports at this time.

#### Licensing scenarios for Avaya IQ Reporting and Avaya IQ Performance Center

Avaya IQ Reporting and Avaya IQ Performance Center use the same license to authenticate a valid user. Avaya IQ calculates the license based on the system IP address and the user name.

If the number of users accessing Avaya IQ Reporting or Avaya IQ Performance Center exceeds the number of licenses that the organization purchased, the system displays a message stating that all the licenses are in use.

#### \* **Note:**

When you try to log on to Avaya IQ Reporting, the system displays the message that all licenses are in use. When you log on to Avaya IQ Performance Center, the system displays this message when you try to create a new activity or launch a report and not at the time of logging in.

The following scenarios help you to understand how Avaya IQ counts the license.

- If a user logs on to Avaya IQ Reporting and Avaya IQ Performance Center through multiple browser windows on the same system, it means the user is using a single license.
- If a user logs in to Avaya IQ Reporting and Avaya IQ Performance Center through multiple browser windows on the same system, the user should log out from both Avaya IQ Reporting and Avaya IQ Performance Center to release the license. If the user logs out from only one application, it means the user is still using a license.
- If a user logs on to Avaya IQ Reporting and Avaya IQ Performance Center from two systems, it means the user is using two licenses.
- If a user logs on to Avaya IQ Reporting or Avaya IQ Performance Center from two different systems, it means the user is using two licenses.
- Multiple users can log on to Avaya IQ Reporting or Avaya IQ Performance Center from the same system. The number of users accessing Avaya IQ Reporting or Avaya IQ Performance Center is directly proportionate to the number of licenses purchased by your organization.
- For example, if your organization has purchased five licenses, five users can log on to Avaya IQ Reporting or Avaya IQ Performance Center from the same system. The sixth user may receive a message stating that all licenses are in use.
- If a user closes the browser window without logging out, the license acquired by the user is locked for session time-out for 90 minutes.

**Note:**

You can set the session time-out duration from the Avaya IQ Administration interface.

- If your configuration has Avaya IQ hosts located in both the intranet and extranet, some proxy settings will cause the user to acquire a license for both Avaya IQ Performance Center and Avaya IQ Reporting. If your browser proxy settings are configured to bypass the proxy server, you must also configure the exceptions such as the IP subnet (for example, 192.168.\*) as well as the sub domain (for example, \*.company.com). For Firefox, use dot notation for the domain names (for example, .company.com) and *IPAddress/MaskBits* (for example, 198.162.0.0/16) to define your IP address range. For example, a subnet mask of 255.255.0.0 corresponds to 16 mask bits and a subnet mask of 255.255.255.0 corresponds to 24. Consult your system administrator for the proper mask bits value.

---

## Acquiring and installing license files

### Acquiring a license file

#### About this task

To acquire a license file, an Avaya representative or Avaya Partner representative uses the PLDS feature. The Avaya employee or Avaya Partner must be certified to use the PLDS feature. For information about PLDS training, certification, and how to acquire a license file, select **Tools > Manage Licensing** on the Avaya Support site:

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

#### Procedure

1. To acquire a license file, provide the following information to the Avaya representative or Avaya Partner representative:
  - Host ID - MAC address or HWaddr of the host. The system installs All Functions or Administration host function and WebLM and the license file at this location. To display the Host ID, use the Linux `ifconfig` command. On a Dell server with the iDRAC feature installed, you can display the MAC address for the NIC1 ethernet port on the **Properties > System Details** screen.
  - SAP order number
  - Avaya Partner Tier I and Tier II information, if applicable
  - Customer contact information
2. Download the license file to a PC that you will use to access the WebLM tool.

The PC must have Web access to the All Functions host or the Administration host.

## Installing a license file

### Procedure

1. From the PC where you have the license file, open a Web browser and enter:  
`https://AdminHost:8443/WebLM/`  
 where *AdminHost* is the name of the All Functions or Administration host.
2. On the WebLM login dialog box, log on with the `admin` ID and password. The initial password is `weblmadmin`.
3. Select **Login**.

**\* Note:**

The first time you access WebLM, you must change the initial password and log back in before you continue.

4. On the Install License dialog box, determine if a license file already exists. Look for products listed under **Licensed Products**. If a license file already exists, you must uninstall the current license file:
  - a. Select **Uninstall License**.  
The system displays the current licenses.
  - b. Select the license to uninstall. The system has only one license for Avaya IQ.
  - c. Select the **Uninstall** button.  
The system displays a confirmation dialog box.
  - d. Confirm the license uninstall.
5. On the Install License dialog box, select **Browse** to locate the license file.
6. On the Choose File dialog box, browse through the file system on the PC to select the license file.
7. When the system displays the license file, select **Install** to install the license file.

**\* Note:**

When you install or upgrade a license, the SID number changes on the screen. This is a random number and is not important to the license.

8. After you install the license, restart the Tomcat services on the Administration or All Functions host:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
restartRequest for service has been accepted and is being processed.
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STOPPING
```

```
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STOPPING
Pending status for AdminTomcat is STARTING
Pending status for AdminTomcat is STARTED
```

9. If you have made associations with the Communication Manager systems, enter the following command to restart the DataProcessingJBoss container on the Data Processing or All Functions hosts:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w DataProcessingJBoss
restart
```

10. If the All Functions or Reporting hosts have been administered, restart the ReportingJBoss container on the Reporting or All Functions hosts by entering the following command:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss restart
```

---

**Related topics:**

[Replacing a license file](#) on page 113

---

## Maintaining license files

### Checking the status of a license

#### About this task

The status of a license includes the expiry date, the number of licensed features, the number of features currently acquired on the system, and the peak usage for measured features. For example, if you are licensed for 400 agents, the license status shows the current number of agents with a license.

#### Procedure

1. Open a Web browser and enter:  
`https://administration_host:8443/WebLM/`  
where *administration\_host* is the name of the host administered with All Functions or Administration.
2. On the WebLM login dialog box, log-in with the admin login ID and password.
3. On the Install License dialog box, select **Licensed Features > Avaya IQ**.  
The system displays the status of the licensed features.
4. To display the peak usage for measured features, select **View Peak Usage**.  
The system displays the peak usage for the measured features.



## Replacing a license file

### Before you begin

Acquire a new license file. For more information, see [Acquiring a license file](#)

### Procedure

1. From the PC where you have the license file, open a Web browser and enter:  
`https://administration_host:8443/WebLM/`  
 where *administration\_host* is the name of the host administered with All Functions or Administration.
2. On the WebLM login dialog box, log on with the admin login ID and password.
3. On the Install License dialog box, select **Uninstall License**.  
 The Uninstall License dialog box lists the licenses installed on this system.
4. Select the installed license from the list and select **Uninstall**.
5. Select **Install License**.
6. On the Install License dialog box, select **Browse** to locate the new license file.
7. On the Choose File dialog box, browse through the filesystem on the PC to select the license file.
8. After you locate the license file, select **Install** to install the license file.
9. You must stop and restart the AdminTomcat, DataProcessingJBoss, and ReportingJBoss services by entering the following commands:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w DataProcessingJBoss
restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss restart
```

### Related topics:

[Installing a license file](#) on page 111

---

## Installing updates

### About this task

You should regularly check for product updates, security updates, and security advisories at the Avaya Support Web site at <http://support.avaya.com/download>

Install any required updates to the installed version of the software. Installation instructions are provided with every update. Before you install an update, you should back up your system as described in the following sections:

### Procedure

1. [Backup strategies](#) on page 199
  2. [Backing up Avaya IQ data in a software-only deployment](#) on page 202
  3. [Backing up the operating system in a software-only deployment](#) on page 203
  4. [Backing up the database on a software-only deployment](#) on page 203
- 

---

## Editing properties

All processing elements within Avaya IQ have many editable property values. These property values control all facets of how the processing elements communicate with other elements. Most of the properties should never require changes. The *Maintaining and Troubleshooting Avaya IQ* guide provides detail information of the properties that require changes. Qualified Avaya personal or Business Partner personnel should only change these property settings.

 **Note:**

The container controls the PEs residing within it. Therefore, the PEs inherit the state of the container. For example, if the container is in the running state, the PEs are also in the running state, and you cannot configure the PEs to stop. You must stop the container if you want to stop the PEs. This is because the watchdog controls the container, and the life cycle controls the PEs.

---

## Adding or changing the reporting e-mail server

### About this task

When your system was installed, an e-mail server may have been administered to e-mail reports to users. If your e-mail server or user changes, you can add or change an e-mail server.

 **Caution:**

Change your e-mail options during low or no traffic periods. For the change to take effect, stop and restart an Avaya IQ process.

### Procedure

1. Log on to the administration interface.

2. On the **Enterprise** tab, select **Sites > HostSites > HostName**, where *HostSites* is the name of your sites and *HostName* is the name of your All Functions host or your Reporting hosts.
3. In the Host View dialog box, expand the **Real Time Report Execution** subsystem.  
The system displays the **Reporting JBoss** container.
4. Select the **Reporting JBoss** container.
5. In the Reporting JBoss dialog box, select the **PE Real Time Report Service** process.
6. Select **Edit**.
7. In the Edit Container dialog box, scroll down to the e-mail server and user options.
8. Add or change the server and user options as shown in the following description:
  - **Email Server Name:** The name of the SMTP e-mail server of the customer. The SMTP e-mail server delivers reports saved to e-mail for report users. During host administration on an All Functions or Reporting host, you must define an e-mail account for mailing Avaya IQ reports to Avaya IQ report users. You can create a new email account, or an existing e-mail account can already exist on a customer e-mail server that supports SMTP mail service. Customers can create account with specific names that help user recognize that an e-mail from that account contains Avaya IQ reports. Note that you cannot create this e-mail account on an Avaya IQ host because Avaya IQ hosts do not support SMTP operation.

Based on your business needs, you can enable SMTP Relaying on your e-mail server for the All Functions host in a dual-host configuration or Reporting hosts in a multihost configuration. With this, your e-mail server can relay e-mails from Avaya IQ report e-mails to e-mail recipients inside as well as outside the e-mail server domain address. If you do not enable this feature, you can only send e-mail reports internally within your e-mail server domain limits.
  - **Email Port:** The SMTP port number used to communicate with the e-mail server. The default value is 25. Change this value if your e-mail server uses a different SMTP port.
  - **Email User Name:** The nonprivileged user on the SMTP e-mail server. If the SMTP server requires authentication to send e-mail, you require an e-mail user. An e-mail user name cannot include white spaces.
  - **Email User Password:** The password for the e-mail user. You must reenter password to verify that you have entered the correct password. The system do not verify whether the user name and password are valid for the e-mail server.
9. Select **OK**.

10. In the Reporting JBoss container dialog box, highlight the **PE Real Time Report Service** process.
  11. Select **Stop All**.  
The system displays the Reporting JBoss container dialog box. The processing element status icon shows *Stopping*.
  12. Refresh the browser window.  
The system displays the Reporting JBoss container dialog box. The processing element status icon shows *Stopped*.
  13. Highlight the **PE Real Time Report Service** process.
  14. Select **Start All**.  
The system displays the Reporting JBoss container dialog box. The processing element status icon shows *Active*.
  15. On the **Enterprise** tab, select the host you just administered.
  16. In the Host View dialog box, confirm that the **Real Time Report Execution** subsystem is active.
  17. Repeat this procedure for all Reporting hosts.
  18. Run a test report and verify that the new e-mail service is working.
- 

---

## Changing the reporting host used for aggregation

### About this task

If your configuration uses two reporting hosts, aggregation runs on only one of those hosts. The system uses the first administered reporting host on the system as the host for running aggregation. If you want to change which host runs aggregation, use the procedure shown in this section. You can change the aggregation host if one host is out of service or you want to replace the host.

#### **Caution:**

Change your aggregation during low or no traffic periods. For the change to take effect, stop and restart an Avaya IQ process.

### Procedure

1. Log in to the administration interface.
2. On the **Enterprise** tab, select **Sites > HostSites > HostName**, where *HostSites* is the name of your sites and *HostName* is the name of your All Functions or Reporting hosts.

3. In the Host View dialog box, expand the **Historical Data Consolidation** subsystem.  
The system displays the related processing elements.
  4. Select to highlight the **PE Aggregation** processing element.
  5. Click **Edit**.
  6. In the Edit Processing Element dialog box, scroll down to the aggregation IP address and port options.
  7. Change the IP address of the new Reporting host where you want to run aggregation.  
Do not change the default port number of 9300.
  8. Click **OK**.
  9. In the Host View dialog box, expand the **Historical Data Consolidation** subsystem.  
The system displays the related processing elements.
  10. Select to highlight the **PE Aggregation** processing element.
  11. Click **Restart**.
  12. Click **OK** to confirm the restart.  
The system displays the Host View dialog box.
  13. Confirm that the Historical Data Consolidation subsystem is started.
- 

---

## Changing the association between the RTD host and the Reporting host

### About this task

#### Important:

After you have made changes to the newly associated RTD host, you must log off and log back in to the system.

### Procedure

1. Log on to the Avaya IQ administration interface.
2. On the **Enterprise** tab, select **Sites**, and select the All Functions or Reporting host that you want to associate with the RTD host.
3. On the **Host View** page, expand the **Real Time Report Execution** Subsystem or process.

4. Click the **Reporting JBoss** container.
  5. On the **Container View** page, click the **PE Real Time Report Service** process, and then click the **EditContainer** pencil icon.
  6. On the **General** tab, enter the following in the **Realtime Dashboard Report URL** field:  
`https://RTD_Host_FQDN:38443/RTD`
  7. Click **Apply** and then click **OK** to complete the process.
- 

---

## Changing host names and IP addresses

Use the following procedures for changing the host name and IP address of your Avaya IQ system and rolling back to the earlier host name and IP address if you face any problem. You can either use the centralized or the manual process to change the host name and IP address.

---

## Admonishments for changing host names and IP addresses

**! Important:**

You must do a full backup of the Avaya IQ data and database. Keep these backups at a safe location.

**! Caution:**

The Avaya IQ data or database backup that you take before you change the host name or IP change will not work with the Avaya IQ that has the new host name or IP address. If you want to restore the Avaya IQ system, then you must revert to the old host name or IP address before you restore Avaya IQ.

---

## Considerations for changing host names and IP addresses

**! Important:**

If you use the rollback host name or IP address option, you will be able to roll back the changes that you made in the last run of the tool. For example, if you change host name or IP address of the Administration host and then the Reporting host, and then use the rollback option, the tool will roll back the changes made on the Reporting host.

The current version of the tool does not support the host name and IP address change of the Oracle rac database.

---

## Prerequisites for changing host names and IP addresses

### Prerequisites

- You must ensure that the Avaya IQ database is connected to the Administration host or All Functions host and the Avaya IQ deployment is operating properly.
- You must ensure that your Avaya IQ system is functional and all the services are functional before you change the host name or IP address.
- You must log in as root to the system and then run this tool.
- You must ensure that you know the new host name or IP address before you run the tool.
- You should contact a network administrator after changing the host name or IP address for further infrastructure and network support.
- You must change the host name or IP address of only one host at a time. Ensure that all the Avaya IQ services are functional on all the hosts before you change the host name or IP address of another host in case of multi host deployment.
- You must ensure the following before you use the centralized process to change or rollback the host name or IP address:
  - All the hosts in your deployment can communicate with each other.
  - Run this tool from an Administration host or All Functions Host.
  - Run this tool from Putty and not from any other SSH Client.
  - You have the root passwords for all Avaya IQ servers in your deployment.
- You must ensure that you have the following required RPMs:
  - `dialog-1.0.20051107-1.2.2.x86_64.rpm`
  - `expect-5.43.0-5.1.x86_64.rpm`
  - `perl-5.8.8-27.el5.x86_64.rpm`
- You must ensure that the following directories have the corresponding free disk space:
  - `/opt` - 100 MB
  - `/tmp` - 10 MB
  - `/var` - 10 MB

### Log files

- When you run the host name and IP address change scripts, you can find the log files at the following location on all the hosts:  
`/var/log/Avaya/CCR/ip_hostname_change/change_ip_hostname.log`
- Once the tool runs successfully, the tool copies all the log files from all the hosts to the local host where you run the tool. You can find log directory at the following location:

```
/opt/Avaya/CCR/bin/ip_hostname_change/log/<corresponding time stamp>
```

- You can find directories with all the host IP addresses at the above location and you can find the corresponding log files for each host in every directory.

---

## Using the centralized process to change the host names or IP addresses

### Procedure

1. Log in as root on the Administration host or All Functions host.
2. From the Linux command line, enter the following commands:

```
cd /opt/Avaya/CCR/bin
```

```
chmod 755 ip_hostname_change.bin
```

**\* Note:**

In software-only deployment, the `ip_hostname_change.bin` file is not available at the `cd /opt/Avaya/CCR/bin` location on database host.

Copy the file from any other host in the deployment, to the following to the `/root` directory and unpack it using the following command:

```
sh ip_hostname_change.bin -unpack
```

3. To run the change host name or IP address script, enter the following command:

```
sh ip_hostname_change.bin
```

**\* Note:**

- If you run the process on the same host and it is not yet complete, the system displays the Program Already Running page. The tool also displays the process id. Ensure that the validity of the earlier process and then exit the current process.

- Close all processes from the current terminal, or open a new terminal and close all the processes. To close the earlier session, enter the following command:

```
kill -9 <process id(s)>
```

Where, `<process id(s)>` is the ID or the list of IDs displayed on the Program Already Running page.

- After closing all the sessions, select **Proceed** on the Program Already Running page.

4. On the Welcome page, select **Next**.



**\* Note:**

To exit the process before the Summary page, press `Escape` or `Control + C`. Do not press `Control + Z`, to prevent the process from closing abruptly and damaging your Avaya IQ deployment.

5. On the Menu page, select **Change**. Select **Next**.
6. On the Confirmation page, select **Yes**.

**\* Note:**

- You will not see the Confirmation page if you run the tool for the first time or if you have used the roll back option previously.
  - Ensure that your Avaya IQ system is functional before changing the host name or IP address. You cannot roll back any changes that you did before the last run of the script.
7. On the Select Host page, the system displays all the hosts in your Avaya IQ set up. Select the host to change the IP address or host name, or both.
  8. Select **Next**.
    - For an All-in-one or single host setup, the system displays following options:
      - xxx.xxx.xxx.xxx All Functions host
    - For a dual host setup, the system displays the following options:
      - xxx.xxx.xxx.xxx All Functions host
      - xxx.xxx.xxx.xxx Database host
    - For a multi host setup, the system displays the following options:
      - xxx.xxx.xxx.xxx Administration host
      - xxx.xxx.xxx.xxx Reporting host
      - xxx.xxx.xxx.xxx Data Processing host
      - xxx.xxx.xxx.xxx Data Collection host
      - xxx.xxx.xxx.xxx RTD host
      - xxx.xxx.xxx.xxx Database host

**! Important:**

You must change the host name or IP address of only one host at a time.

9. The tool prompts you for the root password of all hosts except the Administration host or All Functions host. Enter the passwords for the hosts in your Avaya IQ system.

**\* Note:**

- The system allows you three attempts to enter your password. After exceeding this limit, you will see a warning window. Select **Yes** to enter the password again or select **No** to exit.
  - For software-only deployments, the tool will ask you to enter the Oracle user name for database host .
10. On the New Values page, enter the new host name (Fully Qualified Domain Name) or the new IP address. Ensure that you enter either the new host name or the new IP address. If you leave either of the fields blank, the system will retain either the old host name or IP address. Select **Next**.

**! Important:**

- Ensure that you follow the standard guidelines to enter values for the IP address, DNS, subnet mask and gateway fields.
  - For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.
  - After changing the host name or IP address, if the domain name or subnet changes, then the tool will ask you to enter the new DNS, Gateway and subnet values.
  - If you see any trailing characters when you enter the new DNS value, clear the input field and enter the value again.
11. On the Summary page, verify the details that you have entered. Select **Back** to change the values that you entered or **Next** to proceed.
12. On the Confirmation page, select **Yes** to change the host name or IP address. If you get the warning `Getting the log file from <xxx.xxx.xxx.xxx> failed`, select **OK** to ignore the message and check the log file from the following location:
- ```
/var/log/Avaya/CCR/ip_hostname_change/change_ip_hostname.log
```
13. Once all the scripts run successfully, you will see the following message: `IP hostname changed successfully - Restarting network services.`

**\* Note:**

After changing the IP address of any host, the local host may not be able to communicate with the remote host after you restart the network or you may not be able to connect to Putty or SSH client. In that case, verify the following items:

- Database listener status, on the database host in case you change the IP or host name of database host, using the following command:

```
su - <Oracle User> -c "lsnrctl status"
```

- If the above command displays the old host name or IP address, enter the following command on the database host:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

```
sh dbRestart.sh <Oracle User>
```

- If you are unable to locate the `dbRestart` script, run the `ip_hostname_change.bin` file using the following command:

```
sh ip_hostname_change.bin -unpack
```

- Check the listener status again and ensure that you get the new host name or IP address in the result.

14. To start the Avaya IQ services, enter:

```
service wdninit start
```

Run this command on all hosts in the following sequence:

- Database host (turnkey deployments only)
- Administration host
- Data Processing host
- Data Collection host
- Reporting host
- RTD host

---

## Next steps

### ! Important:

If you are using the High Availability feature, you must recreate the High Availability connection when you change the IP address or host name of the Administration host or Database host. For more information, see *Avaya IQ High Availability and Survivability*.

- When you change the host name or IP address on the primary server, then you must log in to Avaya IQ OAM and then recreate the High Availability connection on the secondary server.
- When you change the host name or IP address on the secondary server, then you must log in to Avaya IQ OAM and then recreate the High Availability connection on the primary server.
- When you change the host name or IP address on the primary server and the secondary server, you must recreate High Availability connection on both the servers.

If you are using Voice Portal, you must reconfigure the Voice Portal connection after you change the host name or IP address. For more information, see the “Administering an ETL application source on the IQ Administration host” section in *Administering Avaya IQ*.

After changing the host name or IP address, you must manually re-administer the data source connections (like Communication Manager, Proactive Contact or Voice Portal) to the Data Collection host.

For software-only deployment, after you change the host name or IP address of the database, you must reconfigure all the applications that use the same database.

## Verifying successful change of host name or IP address

### About this task

Verify the following:

- All the Hosts are in network and can communicate with each other.
- The host name and IP address of the host where you have changed the host name or IP address.
- The connection of the Avaya IQ system with the database host.

### Procedure

1. To verify the change in host name or IP address, open the Linux command line and enter:  

```
$CSBASE/lifecycle/bin/lc ls
```
  2. Ensure that all the Avaya IQ services are functional.
  3. Use the new host name or IP address to log in Avaya IQ OAM, and verify basic reports like agent performance, queue group performance.
  4. Use the new host name or IP address to log in to Avaya IQ Reporting, and verify basic reports like agent performance, queue group performance.
- 

---

## Using the centralized host name and IP address changes rollback process

### Procedure

1. On the Menu page, to roll back the host name or IP address that you changed previously, select **Rollback**.
2. Select **Next**.
3. On the Summary page, verify the details and select **Next**. The system changes the host name or IP address to the earlier host name or IP address.
4. Once all the scripts run successfully, you will see the following message: `IP hostname changed successfully - Restarting network services.`

**\* Note:**

After you roll back the IP address of any host, the local host may not be able to communicate with the remote host after you restart the network or you may not be able to connect to Putty or SSH client. Verify the following:

- Database listener status, on the database host in case you roll back the IP or host name of database host, using the following command:

```
su - <Oracle User> -c "lsnrctl status"
```

- If the above command displays the modified host name or IP address, enter the following command on the database host:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
sh dbRestart.sh <Oracle User>
```

- If you are unable to locate the `dbRestart` script, run the `ip_hostname_change.bin` file using the following command:

```
sh ip_hostname_change.bin -unpack
```

- Check the listener status again and ensure that you get the old host name or IP address in the result.
- Verify whether Avaya IQ services are running using the following command on all hosts:

```
service wdinit status
```

If the services are not running then enter the following command to restart the services:

```
service wdinit start
```

---

## Verifying successful rollback of host name or IP address

### About this task

Verify the following:

- All the Hosts are in network and can communicate with each other.
- The host name and IP address of the host where you have changed the host name or IP address.
- The connection of the Avaya IQ system with the database host.

### Procedure

1. To verify the rollback in host name or IP address, open the Linux command line and enter:  

```
$CSBASE/lifecycle/bin/lc ls
```
2. Ensure that all the Avaya IQ services are functional.
3. Use the new host name or IP address to log in Avaya IQ OAM, and verify basic reports like agent performance, queue group performance.

4. Use the new host name or IP address to log in to Avaya IQ Reporting, and verify basic reports like agent performance, queue group performance.

---

## Using the manual process to change the host names or IP addresses

### Generating control Files

#### About this task

**!** Important:

Before generating control files, ensure that you have database connectivity with the Administration host or All Functions host.

#### Procedure

1. Log in as root on the Administration host or All Functions host.
2. Enter the following command on all the hosts, to unpack the `ip_hostname_change.bin` file:

```
cd /opt/Avaya/CCR/bin
sh ip_hostname_change.bin -unpack
```

**\* Note:**

In software-only deployment, the `ip_hostname_change.bin` file is not available at the `cd /opt/Avaya/CCR/bin` location on database host.

Copy the file from any other host in the deployment, to the following to the `/root` directory and unpack it using the following command:

```
sh ip_hostname_change.bin -unpack
```

3. Enter the following command on the Administration host or All Functions host:  

```
sh ip_hostname_change.bin -manual
```
4. On the Welcome page, select **Next**.
5. On the Menu page, select **Change**. Select **Next**.

**\* Note:**

You must select **Change** for creating control files.

6. On the Select Host page, the system displays all the hosts in your Avaya IQ deployment. Select the host to change the host name or IP address, or both.

7. The tool prompts you for the root password of all hosts except the Administration host or All Functions host. Enter the passwords for the hosts in your Avaya IQ system.

**\* Note:**

- The system allows you three attempts to enter your password. After exceeding this limit, you will see a warning window. Select **Yes** to enter the password again or select **No** to exit.
  - For software-only deployments, the tool will ask you to enter the Oracle user name for database host.
8. On the New Values page, enter the new host name (Fully Qualified Domain Name) or the new IP address. Ensure that you enter either the new host name or the new IP address. If you leave either of the fields blank, the system will retain either the old host name or IP address. Select **Next**.

**! Important:**

- Ensure that you follow the standard guidelines to enter values for the IP address, DNS, subnet mask and gateway fields.
  - For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.
  - After changing the host name or IP address, if the domain name or subnet changes, then the tool will ask you to enter the new DNS, Gateway and subnet values.
  - If you see any trailing characters when you enter the new DNS value, clear the input field and enter the value again.
9. On the Summary page, select **Next**.
  10. On the Status page, select **OK**.
  11. On the Confirmation page:
    - a. To create a control file for another host, select **Yes**.

**\* Note:**

- You must ensure that you know the hosts where you want to change the host name or IP address.
- b. If you want to change host name or IP address on multiple hosts, select another host and select **Yes**.

**\* Note:**

- If you select the existing host, the tool recreates the control file and overwrites the earlier entries.
- c. After creating control files for all the hosts, to create a control file only for the host that you have selected, select **No**.

12. The tool creates a `.tar` file that contains the SQL queries for changing host name and IP address and for rolling back the host name of IP address changes, in the following directory:

```
/opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

13. Copy the `.tar` file in the following directory of all the hosts:

```
/opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

14. Enter the following command to unpack the file:

```
tar -xvf ip_hostname_control.tar
```

---

## Changing the host names or IP addresses

### Procedure

1. Log in as root on the Administration host or All Functions host.

2. From the Linux command line, enter the following commands:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

```
chmod 755 *.sql
```

```
cp *.sql to /home/oracle
```

```
su - oracle -c "sqlplus <sdsuser>/<password>@<servicename>  
@change_sds.sql ;"
```

```
su - oracle -c "sqlplus <rcluser>/<password>@<servicename>  
@change_rcl.sql ;"
```

Where `<servicename>` is `avayaiq` for turnkey deployments and for software only, you can find the service name in the `tnsnames.ora` file

3. To stop the Avaya IQ services, enter:

```
service wdninit stop
```

Run this command on all hosts in the following sequence:

- RTD host
- Reporting host
- Data Collection host
- Data Processing host
- Administration host
- Database host (turnkey deployments only)

4. On all the Avaya IQ hosts including the database host, enter the following command:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```



```
sh manual.sh -c
```

On the Confirmation page, select **Y**. The Confirmation page is displayed for all the hosts that you select for changing host name or IP address.

**\* Note:**

If you select **No** after the first confirmation screen, then you must revert to the earlier host name and IP address changes. To revert to the earlier host name and IP address, enter the following command:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
sh manual.sh -r
```

5. To restart the network services on the hosts where you have changed the host name or IP address, enter the following command:

```
service network restart
```

**\* Note:**

If you change the host name or the IP address of the host, you can get disconnected from the current session. Log in to the host with the new host name or IP address.

6. If you change the host name or IP address on the database host, enter the following commands on the database host:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
sh dbRestart.sh <oracle_username>
```

7. To start the Avaya IQ services, enter:

```
service wdinit start
```

Run this command on all hosts in the following sequence:

- Database host (turnkey deployments only)
- Administration host
- Data Processing host
- Data Collection host
- Reporting host
- RTD host

---

## Next steps

**! Important:**

After changing the host name or IP address, you must manually re-administer the data source connections (like Communication Manager, Proactive Contact or Voice Portal) to the Data Collection host.

For software-only deployment, after you change the host name or IP address of the database, you must reconfigure all the applications that use the same database.

## Using the manual host name and IP address changes rollback process

### Procedure

1. Log in as root on the database host.

2. Enter the following commands:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

```
chmod 755 *.sql
```

```
cp *.sql to /home/oracle
```

```
su - oracle -c "sqlplus <sdsuser>/<password>@<servicename>  
@change_sds.sql ;"
```

```
su - oracle -c "sqlplus <rcluser>/<password>@<servicename>  
@change_rcl.sql ;"
```

Where *<servicename>* is *avayaiq* for turnkey deployments and for software only, you can find the service name in the *tnsnames.ora* file

3. To stop the Avaya IQ services, enter:

```
service wdinit stop
```

Run this command on all hosts in the following sequence:

- RTD host
- Reporting host
- Data Collection host
- Data Processing host
- Administration host
- Database host (turnkey deployments only)

4. On all the Avaya IQ hosts including the database host, enter the following commands:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
```

```
sh manual.sh -r
```

5. To restart the network services on the hosts where you have changed the host name or IP address, enter the following command:

```
service network restart
```

**\* Note:**

If you change the host name or the IP address of the host, you can get disconnected from the current session. Log in to the host with the new host name or IP address.

6. If you change the host name or IP address on the database host, enter the following commands on the database host:

```
cd /opt/Avaya/CCR/bin/ip_hostname_change/scripts/
sh dbRestart.sh <oracle_username>
```

7. To start the Avaya IQ services, enter:

```
service wdinit start
```

Run this command on all hosts in the following sequence:

- Database host (turnkey deployments only)
- Administration host
- Data Processing host
- Data Collection host
- Reporting host
- RTD host

---

## Troubleshooting changes to host names and IP addresses

### Database troubleshooting

- Verify connection to SQLplus using the following command:

```
su - oracle -c "sqlplus <sdsuser>/<password>@<servicename>
```

- Check Oracle listener status using the following command:

```
lsnrctl -status
```

- If the listener is not functioning properly, restart the database using the following command:

```
dbshut
```

```
dbstart
```

### DNS troubleshooting

- After you change the host name and IP address of your Avaya IQ system, check the `resolv.conf` file at the following location:

```
/etc/
```

- If the file has wrong DNS server entries or if it has no DNS server entries, you must add or edit the DNS server entries manually.

---

## Starting Avaya IQ services after changing the host name or IP address

### About this task

After running the change host name or IP address scripts, you will have restarted Avaya IQ services as described in each procedure. However, if the `MessageBrokerService` service does not start after running the scripts, do the following procedure:

### Procedure

1. Check whether `activemq` service is active.
2. If the `activemq` service did not started because of lock file, delete the `activemq` data directory in `/opt/coreservices/activemq-4.0.1/` and the `activemq` file in `/var/lock/subsys` by using the following commands:
  - `rm -rf /opt/coreservices/activemq-4.0.1/activemq-data/`
  - `rm -rf /var/lock/subsys/activemq`
3. Enter the following command to restart the ActiveMQ service:

```
service activemq restart
```
4. If the `ReportingApplicationService` service does not start automatically, enter the following command to restart the `CSTomcatBasic_Key` service:

```
/opt/coreservices/lifecycle/bin/lc restart  
<CSTomcatBasic_Key service id>
```
5. If the `ReportingApplicationService` service does not start even after restarting the `CSTomcatBasic_Key` service, enter the following command to restart the Avaya IQ services:

```
service wdinit restart
```

---

## Installing trusted server certificates after changing host names or IP addresses

### About this task

When you run the change host name or IP address scripts, the system stores the trusted server certificates with the old host names and you cannot access the Avaya IQ Performance Center user interface and the Real Time Data user interface. Use the following steps to create new trusted server certificates with new host names:

On the Administration host or All Functions host:

1. Create a backup of the `/opt/coreservices/avaya/certs` directory.
2. Use the following commands to delete `CCRAAdmin.pfx` and `CCRReport.pfx` from `/opt/coreservices/avaya/certs/pfxs` directory:
 

```
rm -f /opt/coreservices/avaya/certs/pfxs/CCRAAdmin.pfx
rm -f /opt/coreservices/avaya/certs/pfxs/CCRReport.pfx
```
3. Use the following commands to delete `CCRAAdmin.cer` and `CCRReport.cer` from the `/opt/coreservices/avaya/certs/server` directory:
 

```
rm -f /opt/coreservices/avaya/certs/server/CCRAAdmin.cer
rm -f /opt/coreservices/avaya/certs/server/CCRReport.cer
```
4. Use the following commands to delete `CCRAAdmin.key` and `CCRReport.key` from the `/opt/coreservices/avaya/certs/private` directory:
 

```
rm -f /opt/coreservices/avaya/certs/private/CCRAAdmin.key
rm -f /opt/coreservices/avaya/certs/private/CCRReport.key
```
5. To create the OAM certificate, enter the following command:
 

```
sh /opt/Avaya/CCR/data/install/createOAMCert.sh
```
6. To create the RPT certificate, enter the following command:
 

```
sh /opt/Avaya/CCR/data/install/createRPTCert.sh
```
7. Restart the Avaya IQ services using the following command:
 

```
service wdinit restart
```

On the Reporting host and RTD host:

1. Create a backup of the `/opt/coreservices/avaya/certs` directory.
2. Delete `CCRReport.pfx` file from the `/opt/coreservices/avaya/certs/pfxs` directory:
 

```
rm -f /opt/coreservices/avaya/certs/pfxs/CCRReport.pfx
```
3. Delete the `CCRReport.cer` file from the `/opt/coreservices/avaya/certs/server` directory:
 

```
rm -f /opt/coreservices/avaya/certs/server/CCRReport.cer
```
4. Delete the `CCRReport.key` file from the `/opt/coreservices/avaya/certs/private` directory:
 

```
rm -f /opt/coreservices/avaya/certs/private/CCRReport.key
```
5. To create the RPT certificate, enter the following command:
 

```
sh /opt/Avaya/CCR/data/install/createRPTCert.sh
```
6. Restart the Avaya IQ services using the following command:
 

```
service wdinit restart
```

---

## Updating associations between sources and hosts

---

### Considerations for customers

When you change source associations, reporting group setup needs to be examined by the customer. For example, if the customer is consolidating two Communication Manager systems into one, data for only one system will now be collected by Avaya IQ. The customer needs to adjust their reporting group setup to take this change into account. For example, the customers can create or rename categories for the reporting groups associated with the retired source system, such as *SourceNameConsolidationAgentsDate*, where *SourceName* is the name of the earlier Communication Manager system and *Date* is the date when the system was retired.

---

### Modifying the parameters of an existing Communication Manager source association

#### About this task

When you want to modify the parameters of an existing Communication Manager association, you can use the **Modify CM Association** option. For example, if you want to modify the Proactive Contact system that is currently assigned to a Communication Manager system or the Data Processing host to be used with the Communication Manager system, you can use the procedure in this section.

#### Procedure

1. Under the **Enterprise** tab, select **Sites > HostSite > HostName**, where *HostSite* is the name of the site and *HostName* is the name of the host for which you want to modify the Communication Manager associations.
2. In the Host View dialog box, highlight the **Data Collection** subsystem.
3. Select **Edit**.
4. In the Edit Subsystem dialog box, on the **General** tab, scroll down to the bottom of the screen.
5. Select **Modify CM Association**.  
The system displays the CM association wizard.
6. In the Communication Manager field, select the Communication Manager system you want to modify.
7. Select **Next**.

The system displays the dialog box to select a Data Processing host and Proactive Contact systems is displayed.

8. Do one or both of the following tasks:
  - Select a different Data Processing host to use with the Communication Manager system.
  - Change the Proactive Contact system assigned to the Communication Manager system. You can either add a new Proactive Contact system if one was not administered, or you can unassociate a Proactive Contact system and add in a new Proactive Contact system.

**\* Note:**

If you have not created your Proactive Contact systems, select **Create Proactive Contact**.

9. After selecting a Data Processing host and a Proactive Contact system, select **Next**.
  10. In the Finish Up dialog box, select **Finish**.
  11. Repeat this procedure for each Communication Manager system you need to modify.
  12. When finished modifying the Communication Manager associations, select **OK**.
- 

## Moving the association of a Communication Manager source from one host to another host

### Before you begin

When you want to move the association of a Communication Manager system from one host to another host, you must first remove the old association and then make a new association.

**⚠ Caution:**

When you remove a Communication Manager system from one host to another host, you will lose any data being generated by the Communication Manager system while the system has no association.

### Procedure

1. Under the **Enterprise** tab, select **Sites > HostSite > HostName**, where *HostSite* is the name of the site and *HostName* is the name of the host to which the Communication Manager system is currently associated.
2. In the Host View dialog box, highlight the **Data Collection** subsystem.
3. Select **Edit**.

4. In the Edit Subsystem dialog box, on the **General** tab, scroll down to the bottom of the screen.
5. Select **Remove CM Association**.  
The system displays the Communication Manager association wizard.
6. In the **Communication Manager** field, select the system you want to remove from this host.
7. Select **Remove Communication Manager**.
8. When you are prompted to confirm, select **OK**.  
When you remove the Communication Manager systems, the system displays the Edit Subsystem dialog box. If you get an error message indicating that a container or processing element must be manually deleted, see [Resolving error conditions when modifying or removing associations](#) on page 141.
9. Under the **Enterprise** tab, select **Sites > HostSite > HostName**, where *HostSite* is the name of the site and *HostName* is the name of the host to which you want to reassign the Communication Manager system.  
The Host View dialog displays several subsystems and processes that make up the host.
10. In the Host View dialog, highlight the **Data Collection** subsystem.
11. Select **Edit**.
12. Edit Subsystem dialog, on the **General** tab, scroll down to the bottom of the screen.
13. Select **Add CM Association**.  
The system displays the Communication Manager association wizard.
14. In the **Communication Manager** field, select the Communication Manager system you want to associate with the host.
15. Select **Next**.  
The system displays the dialog to select a host and, optionally, a Proactive Contact system.
16. Select the All Functions, Data Processing, or Data Collection host you want to associate with the Communication Manager system.
17. If there are any Proactive Contact systems in your deployment, you can also associate one of those systems with a Communication Manager system at the same time.  
Highlight the system in the **Created Proactive Contact System** shuttle box and move it to the **Associated Proactive Contact System** shuttle box.
18. After selecting a host and any Proactive Contact systems, select **Next**.
19. In the Finish Up dialog, select **Finish**.



20. Repeat this procedure for each Communication Manager system you need to reassign.
21. When finished making Communication Manager associations, select **OK**.

---

### Next steps

When you change host associations for Communication Manager systems, you may need to change the buffering policy on the Communication Manager system.

Systems associated with All Functions and Data Processing hosts must use the **memory** buffering policy. Systems associated with Data Collection hosts must use the **disk** buffering policy.

If you move a Communication Manager system from an All Functions or Data Processing host to a Data Collection host, or from a Data Collection host to an All Functions or Data Processing host, you must change the buffering policy.

To change the buffering policy on a Communication Manager system:

1. Under the **Tasks** tab, select **Connection Management > Administer Connections**.  
The system displays the All Connection Types dialog.
2. Select **Communication Manager**.  
The system displays the Connection Resources dialog. The system displays the list of administered Communication Manager systems.
3. Select the Communication Manager system you moved from one host to a different host.
4. Select **Edit**.  
The system displays the Edit Resource dialog.
5. Scroll down the options until you find the **Buffering Policy** option.
6. Change the buffering policy option to the setting appropriate for the host type.
  - Select **memory** if the source system is connected to an All Functions or Data Processing host.
  - Select **disk** if the source system is connected to a Data Collection host. This prevents data loss if the link between the Data Collection and Data Processing hosts is down for a significant period of time.
7. Select **OK**.  
The system displays the Connection Resources dialog after changing the buffering policy.
8. Repeat this procedure for any other Communication Manager systems you reassigned to a different host.

---

## Removing Communication Manager source associations

### Procedure

1. Log on to the administration interface.
  2. Under the **Enterprise** tab, select **Sites** > **HostSite** > **HostName**, where *HostSite* is the name of the site and *HostName* is the name of the host.
  3. In the Host View dialog box, highlight the **Data Collection** subsystem.
  4. Select **Edit**.
  5. In the Edit Subsystem dialog box, on the **General** tab, scroll down to the bottom of the screen.
  6. Select **Remove CM Association**.  
The Communication Manager association wizard is displayed.
  7. In the **Communication Manager** field, select the Communication Manager system you want to remove.
  8. After selecting a Communication Manager system, select **Remove Communication Manager**.  
The system displays a confirmation dialog box.
  9. Select **OK**.  
When the Communication Manager systems have been removed, the Edit Subsystem dialog is displayed. If an error message is displayed indicating that a container or processing element must be manually deleted. Note which container must be manually deleted and continue with [Resolving error conditions when modifying or removing associations](#).
  10. Repeat this procedure for any other Communication Manager systems you want to remove.
  11. When finished removing Communication Manager associations, select **OK**.
- 

---

## Deleting a Communication Manager source from OAM

This procedure describes how to delete a Communication Manager source from the OAM interface.

 **Caution:**

You must restart the All Functions, Data Processing, or Data Collection hosts while doing this procedure. Call data will be lost while restarting the host. Perform this procedure when there is little or no traffic.

## Before you begin

Confirm that the source has been unassociated from the host. For this procedure, see [Removing Communication Manager source associations](#) on page 138.

## Procedure

1. Log on to the Administration or All Functions host as root or root-level user.
2. Enter the following commands to edit the `cm.xml` file.
 

```
cd /opt/Avaya/CCR/data/admin/sdl/resource
vi cm.xml
```
3. Search for the line `deleteEnabled="false"`.
4. Change the attribute to `"true"`.
5. Enter the following command to save and close the file:
 

```
:wq!
```
6. Enter the following commands to edit the `configureSDLData.sh` file.
 

```
cd /opt/coreservices/cs_mgmt/bin/linux
vi configureSDLData.sh
```
7. Find the lines near the end of the file that start with `#JVMPROPERTIES`.
8. Remove the `#` symbol at the beginning of each line.
9. Enter the following command to save and close the file:
 

```
:wq!
```
10. Enter the following command to update the SDL data in the database:
 

```
sh configureSDLData.sh
```
11. Enter the following command to restart the AdminTomcat container:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w Admin restart
```

One of the following occurs:

  - If only one Admin container exists, the AdminTomcat container is restarted.
  - If more than one Admin container exists, select the AdminTomcat container from the list of containers. The AdminTomcat container is restarted.
12. Log on to the OAM interface.
13. Under the **Tasks** tab, select **Connection Management > Administer Connections**.
14. Select the **Communication Manager** option.
15. Select the Communication Manager system you want to delete.
16. Select Delete to remove the Communication Manager system.
17. For a Single, All-in-One, or Dual host deployment, do the following steps:

- a. Log on to the All Functions host as root or root-level user.
- b. To display the UUID values for containers and processing elements, enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

Take note of the UUIDs for the following container and processing elements associated with the Communication Manager system you just removed:

- DataProcessingJBoss container
  - PECMAAdapter
  - PEEventProcessor
  - PERRecorder
- c. Enter:  

```
service wdinit stop
```
  - d. Enter:  

```
cd /opt/coreservices/lifecycle/persistence
```
  - e. To remove the files for these UUIDs, enter the following commands:  

```
rm PERRecorderUUID  
rm PEEventProcessorUUID  
rm PECMAAdapterUUID  
rm DataProcessingJBossUUID
```
  - f. Enter:  

```
cd /opt/coreservices/watchd/conf
```
  - g. To remove the Data Processing JBoss container lifecycle management configuration file if it exists, enter:  

```
rm W*_DataProcessingJBossUUID_LCM.conf
```
  - h. Enter:  

```
service wdinit start
```

18. For a Multi-host deployment, do the following steps:

- a. Log on to the Data Processing or Data Collection host as root or root-level user that had the associated Communication Manager system you deleted.
- b. To display the UUID values for containers and processing elements, enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

Take note of the UUIDs for the following container and processing elements associated with the Communication Manager system you just removed:

- DataProcessingJBoss container
  - PECMAAdapter
  - PEEventProcessor
  - PERRecorder
- c. Enter:

- ```
service wdinit stop
```
- d. Enter:
 

```
cd /opt/coreservices/lifecycle/persistence
```
  - e. To remove the files for any UUIDs displayed, enter the following commands:
 

```
rm PErrecorderUUID
rm PEEventProcessorUUID
rm PECMAAdapterUUID
rm DataProcessingJBossUUID
```
  - f. Enter:
 

```
cd /opt/coreservices/watchd/conf
```
  - g. To remove the Data Processing JBoss container lifecycle management configuration file if it exists, enter:
 

```
rm W*_DataProcessingJBossUUID_LCM.conf
```
  - h. Enter:
 

```
service wdinit start
```
- 

## Resolving error conditions when modifying or removing associations

### About this task

When modifying or removing the Communication Manager source associations, you may receive an error message indicating that certain processing elements and containers may not have been deleted. You must check to see whether they were deleted. If they were not deleted, you must manually delete the processing elements and containers to complete the modify or remove operation.

### Procedure

1. Log in as root to the operating system on the host indicated in the error message.
2. Enter the following command:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

A list of active services is displayed. The left-justified services are the containers. The indented services are the individual processing elements.

```
List of services :
```

```
0789d60629cf676e0129cf6777150003 : MessageBrokerService : STARTED
0789d60629cf767c0129cf7f46d700ab : ReportingApplicationService : STARTED
0789d60629cf767c0129cf7f46e900af : ReportingWebServer : STARTED
0789d60629cf767c0129cf7f470100b3 : RTDTomcat : STARTED
0789d60629cf676e0129cf67772c0008 : AdminTomcat : STARTED
    0789d60629cf676e0129cf677730000b : PEOAM_key : STARTED
    0789d60629cf676e0129cf6777890018 : PESDAS_key : STARTED
    0789d60629cf676e0129cf67778d001b : PEHostLogServer : STARTED
```

```

0789d60629cf676e0129cf67779c001f : PENetworkLogServer_key : STARTED
0789d60629cf676e0129cf6777a10023 : PEHostLogRetrieverServer : STARTED
0789d60629cf676e0129cf6777a60027 : PENetworkLogRetrieverServer_key :
STARTED
0789d60629cf676e0129cf6777ab002b : PEAlarmServer_key : STARTED
0789d60629cf676e0129cf6777b0002f : PEAlarmConfigServer_key : STARTED
0789d60629cf676e0129cf6777b50033 : PEAlarmRetrieverServer_key : STARTED
0789d60629cf676e0129cf6777ba0037 : PEAuthorizationServiceKey : STARTED
0789d60629cf767c0129cf7f44e10050 : AdminJBoss : STARTED
0789d60629cf767c0129cf7f44ec0053 : PEKeyAuthority : STARTED
0789d60629cf767c0129cf7f44fa0057 : PEIRS : STARTED
0789d60629cf767c0129cf7f4505005c : PEHDREntityMonitor : STARTED
0789d60629cf767c0129cf7f45180068 : PERDREntityMonitor : STARTED
0789d60629cf767c0129cf7f452b0075 : PEHDAPREntityMonitor : STARTED
0789d60629cf767c0129cf7f453f0082 : PERDAPREntityMonitor : STARTED
0789d60629cf767c0129cf7f4551008f : PELoadDateKey : STOPPED
0789d60629cf767c0129cf7f45580092 : PEAggregation : STARTED
0789d60629cf767c0129cf7f455f0096 : PEAdminRecorder : STARTED
0789d60629cf767c0129cf7f456b009d : PESchedulerUtility_key : STARTED
0789d60629cf767c0129cf7f457100a0 : PEETL : STARTED
0789d60629cf767c0129cf7f457700a3 : ReportingJBoss : STARTED
0789d60629cf767c0129cf7f46c800a7 : PERealTimeReportService : STARTED
0789d60629cf767c0129cf8bb5b30a28 : DataProcessingJBoss_CM : STARTED
0789d60629cf767c0129cf8bb5c00a2c : PECMAadapter_CM : STARTED
0789d60629cf767c0129cf8bb5c90a33 : PEEventProcessor_CM : STARTED
0789d60629cf767c0129cf8bb6000a56 : PERecorder_CM : STARTED

```

3. Inspect the display and complete one of the following steps:

- If the processing elements and containers indicated in the error message are not displayed, the processing elements and containers were automatically deleted and do not need to be deleted manually. Skip to step 5.
- If the processing elements and containers indicated in the error message are displayed, continue with Step 4 to manually delete the processing elements and containers.

4. Delete the processing elements and containers:

- a. Make sure the container is started. If the container is not started, enter:

```
cd /opt/coreservices/lifecycle/bin
./lc start UUID
```

*UUID* is the 32 character string of the container.

- b. Enter the following commands to stop and remove each processing element associated with the container:

```
./lc stop UUID
./lc remove UUID
```

*UUID* is the 32 character string of the processing element.

- c. Enter the following commands to stop and remove the container:

```
./lc stop UUID
./lc remove UUID
```

*UUID* is the 32 character string of the container.

- d. Enter the following command to confirm that the processing elements and container have been removed:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

5. Repeat the previous steps until the indicated containers and processing elements are removed.

---

## Adjusting the parameters for communication with Proactive Contact cron jobs

### About this task

If you change Proactive Contact maintenance cron jobs or decrease the wait recovery time for cron jobs from the default of 67 minutes to a different value, the PCAdapter processing element parameters on Avaya IQ may need adjustments to better communicate with the Proactive Contact jobs. If this situation occurs, use the procedure in this section to adjust the processing element parameters. These changes are made using the administration interface.

### Procedure

1. Under the **Enterprise** tab, select **Sites > > SiteName > HostName**.
2. Expand the **Data Collection** subsystem.
3. Select to highlight the **PE PC Adapter** associated with the Proactive Contact system where the cron jobs were changed.
4. Locate the **Maximum Bad Callbacks** option.

The default option is 100. This value indicates the number of faulty callbacks. If a connection is lost, the faulty callback counter increases every 40 seconds up to the maximum default value of 100. When the counter reaches the maximum value, the PCAdapter restarts. You can set this value to 20 to decrease the wait time for recovery.
5. If you modify the **Maximum Bad Callbacks** option to a value less than 100, you must also modify the delay time for the login. To do this, you must edit the `StateMachineConfig.xml` file located in `/opt/Avaya/CCR/data/eventmgt/XML`. The file and directory are located on the application host where PCAdapter runs.
  - a. Enter:

```
cd /opt/Avaya/CCR/data/eventmgt/XML
```
  - b. Enter:

```
vi StateMachineConfig.xml
```
  - c. Search for `State Key="Logging In"`.

d. Within this state definition, change the following values:

- `<ActionRetryCount>10</ActionRetryCount>` to `<ActionRetryCount>60</ActionRetryCount>`
- `<DelayBetweenRetriesInMSeconds>20000</DelayBetweenRetriesInMSeconds>` to `<DelayBetweenRetriesInMSeconds>120000</DelayBetweenRetriesInMSeconds>`

This change ensures that the Proactive Contact system has time to initialize its own services before the PCAdapter attempts to log in.

---

## Managing the external application URL links

When using Avaya IQ Performance Center, you can access several related user interfaces using an administered link. These links are available under the **Applications** menu of the Avaya IQ Performance Center user interface. The following procedure describes how to administer those links.

**\* Note:**

This feature is also known as the “click through to administration” feature.

### Before you begin

Before using this procedure, you should be comfortable editing XML code. Contact Avaya support if you need any assistance with this feature.

In your Web browser, go to **Tools > Internet Options**, select the **Advanced** tab, scroll down and select the **Enable native XMLHTTP support**, and select **OK** to save your change.

### Procedure

1. Open your Web browser and enter the following URL:  
`https://HostName:28443/Admin/ApcApplicationLink.html`  
where *HostName* is the host name of the Administration or All Functions host.
2. In the **IQ Admin URL** field, verify that the URL you just accessed is shown in the field:  
`https://HostName:28443/Admin/Private/Property`  
where *HostName* is the host name of the Administration or All Functions host.
3. In the **Login ID** and **Password** fields, enter the valid details of an Avaya IQ user assigned to the default System Administrator role. When you use a user ID from an enterprise directory, you must provide the fully qualified user login ID. For example, `mylogin@mydomain.mycompany.com`.



4. In the **Select the desired Action** field, select the actions that you want to perform with the link.

You can perform the following actions in the Avaya IQ Performance Center user interface:

- **Add:** To create an application link.
- **Retrieve all:** To display the application links previously administered using this feature.
- **Update:** To update an existing application link.
- **Delete:** To remove an application link.

To update or remove an application link, use **Retrieve all** to display all the administered application links, and use **Update** or **Delete** to update or delete a link. The results open in a separate browser window. You can copy the appropriate portion of the XML document and paste into the Application text area, replacing the default template. For updates, change the Application content to reflect the desired changes as described in the following steps.

5. In the **Application** text area, update the XML template to manage the application links.

To manage the application links, edit the XML template using the following information:

- `<ApcWebApplications>` - This is a required container for the XML template and therefore, you must not modify this tag.
- `<id>` - This tag identifies the XML document. Use a unique ID to identify a group of folders and application links. Do not use blank spaces in an ID. For example, *mycompanycontactcenterapplications*.
- `<folder>` - This is an optional element that identifies the root folder that contains other folders or application links or both. The use of folders creates a hierarchy in the **Applications** menu of the Avaya IQ Performance Center user interface. For example, The *Workforce Optimization* folder may contain the following application links:
  - Agent Scheduling: To set up agent schedules
  - Quality Management: To review recordings
  - Schedule Adherence: To monitor the efficiency with which the agent adheres to the schedule
  - Scorecard: To monitor agent statistics and measure agent performance

If you do not want to define a folder, then you must remove the `<folder>` tag from the default template and also the following child tags and the corresponding closing tags:

- `<id>`: This tag is a unique identifier for each folder within the XML document. For example, *wfoapplicationlinks*.

- `<displayName>`: This tag identifies the locale specific display-names that the system uses in the **Applications** menu of the Avaya IQ Performance Center user interface.
- `<locale>`: Including the locale `<id>` and `<name>`: These tags identify each supported locale. Avaya IQ Performance Center currently supports the following locales:
  - zh\_CN: Chinese, Simplified
  - en-us: English, USA
  - fr: French
  - de: German
  - it: Italian
  - ja: Japanese
  - ko: Korean
  - pt-br: Portugese, Brazil
  - ru: Russian
  - es-co: Spanish, Colombia

**\* Note:**

Application links support all the above languages. If the entry for one of the associated entries is missing from the XML document, Avaya IQ Performance Center will choose English. If English is missing from the XML document, then Avaya Performance Center uses the first locale from the set of locales. If no locales are available, then Avaya IQ Performance Center uses an empty string.

- `<apcWebApplication>` - this tag contains the details for each application link that you include in the Avaya IQ Performance Center **Applications** menu. This tag may be included in the `<folder>` container, or the tag may exist directly within the `<ApcWebApplications>` container. This tag contains the following child tags:
  - `<id>`: This tag is a unique identifier for each application entry, application link, or an `<apcWebApplication>` instance within the XML document. For example, *wfoscheduleadherence*.
  - `<url>`: This tag contains the URL associated with the Web application.
  - `<icon>`: This tag displays an icon next to the Web application's display name. Currently, the only available option is: `/assets/images/adminIcon2.png`.
  - `<displayName>`: This tag identifies the locale-specific display name to be used in the **Applications** menu of the Avaya IQ Performance Center. The specific `<locale>` and `<id>` tags identify each supported locale.

- `<description>`: This tag contains the tooltip information for the application link. The description must reflect the application associated with the link. Similar to the `<displayName>` tag, `<description>` contains `<locale>` specific values.

**\* Note:**

To update and remove application links, and to retrieve the applications entered earlier, use the **Retrieve all** option and then click **Submit**. A separate browser window displays the results. To replace the default template, you can copy the appropriate portion of the XML document and paste it in the **Application** text area. Ensure that you remove any dashes (-, -) from the **Application** text area.

6. After you update the XML document in the **Application** text area, click **Submit**. The system displays one of the following return codes:
  - **20x OK**: This error code indicates a successfully updated XML template.
  - **404 Not Found**: This error code indicates that the update failed and the plug-in with the given ID is not registered. Ensure that your content follows the defined XML format.
  - **400 Bad Request**: This error code indicates that the update failed due to *given* error message. For example, *XML validation error*. Ensure that your content follows the defined XML format.
  - **500 Internal Error**: This error code indicates a problem with the service or that the Avaya IQadministration database is unavailable.

For failed submissions, adjust the inputs and submit again.

---

## Loading the date and time zone data

To properly display report data, you must add date and time zone data to your configuration. Load the data on an All Functions host with a Remote Data Collection deployment or on an Administration host in a Multiple-host deployment. Loading the date and time zone data populates the historical and real-time databases with the date and time values.

If all of your agents are in one location, you should only load a single time zone to represent that location. If your agents are spread across several locations, you should load the time zone for each location where you have agents.

To load the date and time zone data for any available time zone, use the `dtzcli` command. By default, the command loads 3 months of time zone data for the historical schema and 4 hours of time zone data for the real-time schema. During implementation, the command loads the UTC time zone with 10 days of data for the historical schema and one hour of data for the

real-time schema. With this, you have enough time zone data to run test reports during implementation.

Since you can load data for more than 500 time zones, you should only load the time zones for which you want reports. For example, if your users require reports for U.S. Eastern time, U.S. Pacific time, and Central European time, you only need to load data for those time zones. You can always load additional date and time zones as needed.

**\* Note:**

The start times set by the `dtzcli` command have nothing to do with the starting times of the reports.

---

## Date and time zone command options

Name	Description
<p><b>List available time zones</b></p>	<p>Lists all available time zone definitions. One location may have more than one time zone definition. For example, if you have to report on agents located in Chicago, Illinois, USA, you can load any of the following time zones:</p> <ul style="list-style-type: none"> <li>• <b>America/Chicago</b></li> <li>• <b>Etc/GMT-6</b></li> <li>• <b>US/Central</b></li> </ul> <p>Select the time zone that best matches the name of the reporting location. In this example, the time zone definition named America/Chicago is the most appropriate choice.</p>
<p><b>List administered time zones</b></p>	<p>Lists the time zones that are currently loaded on the system. If a time zone is currently loaded and active, do not attempt to reload the time zone.</p>
<p><b>Add a new time zone</b></p>	<p>Allows you to add new time zone data. With this option, you can add new time zone data using the following information:</p> <ul style="list-style-type: none"> <li>• <b>Time zone ID</b> Displayed when you use the ? option. Enter the time zone ID exactly as the list of available time zone IDs show.</li> <li>• <b>Time zone prompt</b> The time zone prompt that displays in report input pages and on reports. Select a prompt name that report users easily understand.</li> <li>• <b>Historical schema and range of dates</b></li> </ul>

Name	Description
	<p>This determines if you load time zone data for the historical schema and how much data will be loaded. To change the amount of data, specify a different range of dates.</p> <ul style="list-style-type: none"> <li>• Real-time schema This determines if you load time zone data for the real-time schema.</li> </ul>
<b>Activate a time zone</b>	Activate a time zone that is currently deactivated. The system automatically extends the time zone data for all active time zones.
<b>Deactivate a time zone</b>	Deactivate a time zone when do not run reports for that time zone and save space in the database.
<b>Extend time zone data forward</b>	<p>Manually extend the time zone data for 3-5 months for the historical schema and 4 hours for the real-time schema. This option extends the time zone data for all administered time zones. Two system-scheduled jobs regularly extend the time zone data forward in addition to the manual extensions you make.</p> <ul style="list-style-type: none"> <li>• <b>sys_dtzCheck</b>: Extends historical time zone data and runs daily.</li> <li>• <b>sys_rtdtzCheck</b>: Extends real-time time zone data and runs hourly.</li> </ul>
<b>Extend time zone data backward</b>	Manually extends the time zone data for the historical schema to a specific date in the past. This option extends the time zone data for all administered time zones.
<b>Quit</b>	Use this option to move out of the command..

---

## Using the date and time zone command

### Procedure

1. Log on to the OS as root or as a user with root-level permissions.
2. Maximize the size of your terminal window to view all three columns of the available time zones.
3. On the console, enter:  
`cd /opt/Avaya/CCR/bin`
4. On the console, enter:

```
./dtzcli.sh
```

5. Select an option from the list of command options the system displays.
  6. Answer the prompts based on the option descriptions in the date and time zone command options.
  7. Repeat this procedure for all time zones that you have to load.
- 

---

## Verifying date, time, and NTP status

### About this task

Verify that the date and time are synchronized on all hosts in the deployment. Verify that NTP operates correctly on all hosts and sources in the deployment. For example, Communication Manager and Proactive Contact.

---

## Changing the database user names or passwords

### Important:

For a turnkey deployment, use the procedure in [Changing database user password](#).

Avaya IQ communicates with the database with user names and passwords that you created when you installed the database and Avaya IQ. The database user names and passwords were created on the database and that information was configured on Avaya IQ. If the database user names or passwords are changed on the Avaya IQ host, they must be changed on the database host. Conversely, if the database user names or passwords are changed on the database host, you must update the user names or passwords on the Avaya IQ host. You must remedy the following conditions where the user names or passwords do not match:

- When you manually change the password for the SDS or core database user or the database host password expires, the administration interface cannot communicate with the database. You cannot fix any other expired database passwords.
- When you manually change the remaining database user names or passwords on the Avaya IQ host or the database host, you must update the user names or passwords on the associated Avaya IQ or database host.

To remedy both the earlier conditions, use the following procedures:

- [Changing The SDS password on Avaya IQ](#) on page 151
- [Changing a user name or password on Avaya IQ](#) on page 151

**! Important:**

Do not change database user names. If you must change database user names, request an experienced DBA to make the change.

**⚠ Caution:**

When you change the database user or password, Avaya IQ cannot communicate with the database for a period of time.

---

## Changing the SDS password on Avaya IQ

Use this procedure to update the password of the SDS or core database user on Avaya IQ after the password expires or you changed the password on the database host.

**Procedure**

1. Log on to the OS on your All Functions or Administration host.
2. To stop the system, enter:

```
service wdninit stop
```

3. To recreate the database user that existed when you first installed the system, use the following commands:

```
cd $CCR_HOME/data/install./changeBootstrapDB.sh -dbUser
UserName -dbPassword Password
```

The variable *UserName* is the SDS (core) connection name and *Password* is the user password. You can find the output of this command in `$CCR_HOME/install_logs/config.log`.

4. Use the following command to restart the system:
- ```
service wdninit start
```
5. Verify that the Tomcat process is running:
- ```
ps -ef | grep tomcat
```
6. If you need to change any other database user names or passwords, use the procedure in [Changing a user name or password on Avaya IQ](#) on page 151.

---

## Changing a user name or password on Avaya IQ

First change a non-SDS or core database user or password on an Avaya IQ host and then make the change on the database host.

## About this task

### ! Important:

Do not use this procedure if the SDS or core database user name or password is already changed on the database host. Use the procedure in [Changing the SDS password on Avaya IQ](#) on page 151.

## Procedure

1. Log on to the OS on your All Functions or Administration host.
2. Before you make any changes, use the following procedure to test the database connection:
  - a. Enter:

```
sqlplus IQ_Connection_Name/IQ_Connection_Name_DB_Pwd@DB_User_Machine
```

Example: `sqlplus iq/password@dbhost`
  - b. To exit SQL Plus, enter:

```
exit
```
3. Log in to the administration interface of Avaya IQ.
4. On the **Tasks** tab, select **Connection Management > Administer Connections**.
5. in the All Connection Types dialog box, select **Database Connection**.  
The system displays the Connection Resources dialog box. See OAM connection names and corresponding database user names for the list of database names.

### \* Note:

In some installations, the same historical database user is associated with the CCR, CCRR, and CCRW connection names and the same real-time database user is associated with the CCRRT, CCRRTW, and CCRTR connection names. If you change the password on the database host for any one of the three historical or real-time database users, you must also change the password for all three connection names on the Avaya IQ host.

6. Select to highlight one of the connection names.
7. Select **Edit**.
8. On the Edit Resource dialog box, scroll down in the dialog and find the **User Name** and **User Password** fields.
9. Change the user name and password as needed.
10. Select **Apply**.
11. Select **OK**.  
The system displays the Connection Resources dialog box.
12. If you change the password for SDS on Avaya IQ first, you must immediately log out of administration, shut down the All Functions or Administration host immediately, and run an Oracle script. To do this, enter the following commands:

```
service wdinit stop
```



```
cd $CCR_HOME/data/install
./changeBootstrapDB.sh -dbUser UserName -dbPassword Password
```

The variable *UserName* is the core connection name and *Password* is the user password.

13. Log on to the OS on your All Functions or Administration host.
14. Use the following command to shut down the host:
 

```
service wdninit stop
```

If you have a Multi-host configuration, shut down all hosts in the configuration using this same command. Verify that all hosts are shut down.
15. Log in to your database host and change the database password for the same user you changed earlier in this procedure.
 

Use the table above to find the Oracle database user associated with the Avaya IQ user just changed. If the account is locked, log in as sysdba and unlock the account.
16. Log on to the OS on your All Functions or Administration host.
17. Use the following command to restart the host:
 

```
service wdninit start
```

If you have a multiple host configuration, restart all hosts in the configuration using this same command. Verify that all hosts are restarted.
18. When Avaya IQ restarts on all hosts, confirm that the system can communicate with the database.
19. Test the database connection using the following procedure:
  - a. Enter:
 

```
sqlplus IQ_Connection_Name/  
IQ_Connection_Name_DB_Pwd@DB_User_Machine
```

Example: `sqlplus iq/password@dbhost`
  - b. To exit SQL Plus, enter:
 

```
exit
```
20. Repeat this procedure for any other non-SDS (core) database user names or passwords that require changes.

---

**Related topics:**

[Avaya IQ OAM connection names and corresponding database user names](#) on page 154

---

## Avaya IQ OAM connection names and corresponding database user names

Avaya IQ OAM Connection name	Oracle database user name	Database user name
CCR	CCR	RPT_HIST_OWNER_USR
CCRCSC	CCRPT	RPT_CONTENT_USR
CCRR	CCR	RPT_HIST_RO_USR
CCRRT	CCRRT	RPT_RT_USR
CCRRTW	CCRRT	RPT_RT_RW_USR
CCRTR	CCRRT	RPT_RT_RO_USR
CCRUI	CCRCL	RPT_UI_USR
CCRW	CCR	RPT_HIST_RW_USR
core	CCRSDS	RPT_SDS_USR

### Related topics:

[Changing a user name or password on Avaya IQ](#) on page 151

---

## Database management

To manage your database, perform the following actions:

- Use the management tools and recommendations your database software provider provides.
- Monitor your tablespace usage to ensure that you have enough space.
- If you shut down the database host, make sure that you shut down the Avaya IQ hosts before you restart the database host. After the database host is operating normally, you can restart the Avaya IQ hosts.

Avaya IQ buffers events from data sources if the system encounters a problem. For example, if the database is currently unavailable, the system should be able to buffer for a short time given the buffer configuration administrated during installation. During such outages, buffering continues until maximum capacity. Typically a `Threshold exceeded` notification log message is given prior to reaching buffer capacity. You can gain access to this message in the log file of the host system for the Data Processing Container or through the Log Viewer. In addition, once capacity is reached, an Alarm is generated indicating `Persistence store has reached its limit`. This message will also be available in the Log Viewer and the

Alarm Manager To prevent loss of events from data sources, your DBA needs to investigate ways to make the disk I/O operate faster.

---

## Data removal

The Avaya IQ data model is based on standard data warehouse design principles.

Dimension tables store administered entities, such as agents, queue groups, or routing point groups. Fact tables store measurements on the administered entities, such as contact counts and time durations. Fact tables generally store significantly more data than the dimension tables. The Data removal feature removes data only from the database fact tables.

Remove unneeded fact table data from your database regularly by using the **fact\_data\_purge** command. You can remove old data from all fact tables at the same time, or you can remove data from individual fact tables one at a time.

The **fact\_data\_purge** command deletes data for the date you enter and any data older than that date. For example, if you enter 11/12/2005 in the command, the system removes all fact table data for November 12, 2005, and earlier.

 **Caution:**

Only remove data for which you no longer wish to run reports. Do not remove data you need for reports.

---

## Removing data from all fact tables

### Procedure

1. Log on to the All functions or Administration host.
2. Connect to the database so you can run database commands.
3. Enter:

```
/opt/Avaya/CCR/bin/fact_data_purge.sh MM/DD/YYYY
```

where *MM* is the two-digit month, *DD* is the two-digit day, and *YYYY* is the four-digit year of the date.

The system deletes the data from all fact tables from that date and earlier.

---

---

## Removing data from a single fact table

### Procedure

1. Log on to the All functions or Administration host.
2. Connect to the database so you can run database commands.
3. Enter:

```
/opt/Avaya/CCR/bin/fact_data_purge.sh MM/DD/YYYY fact_table
```

where *MM* is the two-digit month, *DD* is the two-digit day, *YYYY* is the four-digit year of the date, and *fact\_table* is the individual fact table.

The data is deleted from the specified fact table from that date and earlier.

---

---

## Removing obsolete users from RCL tables

### About this task

If an Avaya IQ user quits the organization or the user name and password to access the Reporting user interface is corrupt, use the RCL data purge utility to delete the user from the RCL tables.

### Procedure

1. Open the `/opt/Avaya/CCR/jars/UI` directory.
  2. Enter:
- ```
sh deleteUser.sh <LogfileName>
```
3. Enter one or more user names that you want to delete.
  4. Enter `.` at the end of the user name list.

For example, if you want to:

- Delete User A, then you must enter `User A.`
- Delete User A, User B, and User C, then you must enter `User A, User B, User C.`

5. Enter `y` to delete the users.

The system deletes the users. For more information, see the log file.

---

---

## Database schema and metadata sanity check

To verify consistency between the database schema information of the historical report tables and the metadata records, the system performs a verification check every day. If the system finds an inconsistency, the system raises an alarm and logs the inconsistency in the Scheduler container log files located at:

```
/var/log/Avaya/CCR/SCHED_UUID/
```

The `_UUID` variable represents a dynamically generated container UUID directory. The name preceding the UUID identifies the container function. In this case, the name is the Scheduler container.

The following is an example of a Scheduler container UUID directory:

```
SCHED_0789038d09d500320109d50323b70003
```

Depending on the error, you may need assistance from Avaya. For inconsistencies such as dropped tables, your database administrator can add those tables back into the database. For errors in the metadata, you must contact Avaya for assistance.

---

## Reinitializing user service

### Procedure

1. On the **Tasks** tab, select **System Configuration > Manage Administrative Data > Reinitialize User Service**.
  2. Select **Reinitialize**.
- 

---

## Administering certificates

Avaya IQ is installed on your system with default self-signed certificates for accessing the browser-based administration, reporting, and Avaya IQ Performance Center user interfaces. To provide secure access to these user interfaces, you must configure Avaya IQ to use digital server certificates. You can obtain the server certificates from an internal company Certificate Authority (CA) or purchased from an external public CA.

The required number of server certificates depends on the deployment:

- For an All-in-One, Single, or Dual host deployment, you need one server certificate.
- For a Multi-host deployment, you need separate server certificates for the Administration host, each Reporting host, and the RTD host.

To administer server certificates, use the Avaya IQ administration interface and commands run from the Linux command line interface.

**! Important:**

The customer must work with the provisioning team during the installation of Avaya IQ when it is time to purchase or obtain and install server certificates. The customer must be prepared to purchase the server certificates in accordance with the installation procedures being used by the provisioning team. The customer must decide which CA to use, an internal CA or an external CA.

---

## Planning for certificate installation

### Before you begin

You must have access to the Internet to purchase or obtain certificates from a Certificate Authority (CA). After you request the certificates, you will need Internet access to verify the validity of the certificate.

Before you attempt to purchase certificates, you must have a payment method in place. Most CA companies accept credit cards over the internet.

**⚠ Caution:**

During the process of importing certificates, you will stop and start system processes. This process logs off administration, reporting, and Avaya IQ Performance Center users from the system. Do this work during no or low traffic periods.

### Replacing expired certificates

There are two scenarios to consider when replacing expired certificates:

- If the root and intermediate certificates expire but the SSL certificate has not expired, the system will continue to operate until the SSL certificate expires.
- If the SSL certificate expires but the root and intermediates have not expired, the system will not operate properly. You must complete the process for requesting and installing new certificates.

When you replace a server certificate, you must do the following:

- Take note of the Distinguished Name (DN) that you used for the last certificate. This information must match exactly when you request a renewal certificate from the same CA. If you are obtaining a certificate from a different CA, the DN does not have to match.

To determine the names of your certificates, see [Listing trusted certificates](#) on page 171 and [Listing server certificates](#) on page 174.

- Delete the existing certificates on the host. The steps to delete a certificate are included within the procedure for installing new certificates.

### About this task

The following procedures provide the steps for configuring Avaya IQ to use server certificates issued by a CA. These procedures include:

- Before you request and import new certificates, you must back up your current configuration. Follow the procedures shown in [Backing up the existing certificates](#) on page 159.
- To request certificates, you must generate a Certificate Signing Request (CSR). The CSR contains information about your host to the CA so that the CA can provide a certificate that is linked securely to your host. See [Generating Certificate Signing Requests](#) on page 160.

#### Important:

Take note of the Distinguished Name (DN) that you use for this request. If you request a replacement certificate from the same CA, this information must match exactly.

- After you generate a CSR, you will submit the CSR to a CA to request a certificate. Remember that you will have multiple CSRs for a Multi-host deployment. See [Submitting CSRs to a Certificate Authority](#) on page 162.
- After you receive your certificates from the CA, you must install them on your hosts by importing them using the Avaya IQ administration interface. The certificates are sent to you embedded in an e-mail or made available from a URL link at the CA Web site.

The certificates that CAs send you will vary. Some CAs do not provide intermediate certificates. Some CAs provide more than one intermediate certificate. The CA might only provide an SSL certificate. If this occurs contact your CA and obtain the CA's root certificate.

When installing the certificates, you import the root and intermediate certificates as trusted certificates and the chained SSL, intermediate, and root certificates as a server certificate that links all three certificates together. See [Installing server certificates](#) on page 163.

- When you import the SSL, Intermediate, and root certificates as a group, a chain of trust between the certificates is automatically established. However, some customer IT departments that follow a different standard will not import the certificates as a group. If the certificates are imported individually, you must manually establish the chain of trust. See [Establishing the chain of trust](#) on page 168 for this optional procedure.

---

## Backing up the existing certificates

### Procedure

1. Log on to the All Functions or Administration host as root or a root-level user.

2. Enter the following commands to make a copy of the directory:

```
cd $CSBASE/avaya  
cp -rfp certs certs.old
```

---

## Generating Certificate Signing Requests

### Procedure

1. Log on to the OAM interface.
2. On the **Tasks** tab, select **Security > Administer Server Certificates**.  
The system displays the Server Certificates page.
3. Use the **Host** drop-down menu to select the name of the host for which you want to generate a Certificate Signing Request (CSR) . The host you select depends on your deployment:
  - To generate a CSR for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
  - To generate a CSR for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host.

 **Caution:**

Do not select **localhost**.

4. Select **Switch To**.
5. Select **Add**.  
The system displays the Add Server Certificate page.
6. Enter values for the following options as described in this table:

 **Important:**

Take note of the Distinguished Name (DN) that you use for this request. If you request a replacement certificate from the same CA, this information must match exactly.

| Option                   | Definition                                                                                                                                                                                                                                                                               |
|--------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Certificate Alias</b> | Enter a name for the certificate. Include the host name in the alias name. For example, for an Administration host, you might name it <i>HostNameAdminCert</i> to specify that it is to be installed on the Administration host named <i>HostName</i> . The name cannot have any spaces. |



| Option                                | Definition                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Create Self-Signed Certificate</b> | Clear this check box. Make sure it is not selected.                                                                                                                                                                                                                                                                                                                                                                                                                    |
| <b>Enrollment Method</b>              | Select <b>Manual</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| <b>Encryption Algorithm</b>           | Select <b>3DES</b> .                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Password</b>                       | Enter and re-enter the string <code>password</code> into this field.                                                                                                                                                                                                                                                                                                                                                                                                   |
| <b>Key Size</b>                       | Enter the desired Key Size. You can select from 1024, 1536, and 2048. The default is 1024.                                                                                                                                                                                                                                                                                                                                                                             |
| <b>Certificate Validity (Days)</b>    | Use the default value. The actual valid length of the certificate is based on the purchase price of the certificate from an external CA or is based on policy established by an internal CA.                                                                                                                                                                                                                                                                           |
| <b>Distinguished Name (DN)</b>        | <p>Enter a string that represents a unique identifier for the host. For example, <code>OU=OrganizationUnit, O=CompanyName, CN=machine.company.com, L=Location, ST=State, C=Country</code></p> <p><b>! Important:</b><br/>The CN value <i>must</i> be the fully qualified domain name (FQDN) for the host. The ST value <i>must</i> be the full state name, not the abbreviated name. The C value <i>must</i> be the two-character country name, not the full name.</p> |
| <b>Challenge Password</b>             | Leave these fields blank. These fields are only used when requesting a certificate from an internal CA using SCEP, which is not the standard process for Avaya IQ.                                                                                                                                                                                                                                                                                                     |
| <b>Key Usage</b>                      | Do not select an option. This option is used only when requesting self-signed certificates, which is not the standard process for Avaya IQ.                                                                                                                                                                                                                                                                                                                            |
| <b>Extended Key Usage</b>             | Do not select an option. This option is used only when requesting self-signed certificates, which is not the standard process for Avaya IQ.                                                                                                                                                                                                                                                                                                                            |

| Option                      | Definition                                                                                                                                                                          |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>SCEP Server URL</b>      | Leave this field blank. This field is only used when requesting a certificate from a Simple Certificate Enrollment Protocol (SCEP), which is not the standard process for Avaya IQ. |
| <b>CA Certificate Alias</b> | Leave this field blank. This field is only used when requesting a certificate from an SCEP, which is not the standard process for Avaya IQ.                                         |
| <b>CA Identifier</b>        | Leave this field blank. This field is only used when requesting a certificate from an SCEP, which is not the standard process for Avaya IQ.                                         |

7. Select **Apply**.
8. On the Server Certificate Request page, the **Certificate Request PEM** (Privacy Enhanced Mail) is highlighted for easy copying. Use Ctrl-C to copy the **Certificate Request PEM** text and paste it into a text editor. You will send this Certificate Request PEM to a CA.

**! Important:**

Use a text editor that does not add formatting to the content of the PEM. Some editors, such as Notepad, will insert special characters for carriage returns and may show the entire certificate on a single line. If the PEM has formatting characters, use a command such as “certutil” to remove formatting from the PEM.

You can view the Certificate Request PEM from **Security > Administer Server Certificates > View Pending Certificate Requests**.

9. Select **Close**.
10. For a Multi-host deployment, repeat this procedure for each Reporting host and the RTD host.
11. Retain a record and receipt for each certificate you request. You will need this information when you request replacement certificates.

## Submitting CSRs to a Certificate Authority

### Procedure

1. Contact a CA to request a server certificate. When requesting a server certificate, you will send them the PEM from the All Functions, Administration, Reporting, and RTD hosts. Follow the instructions from the CA when making your request. Each

CA operates differently, so specific procedures are not given here. If server or host information is requested by the CA, use the following information:

- Enter "Apache Tomcat Version 5.5.27" to request a certificate for an Administration host or an RTD host.
  - Enter "JBoss Application Server - Version JBossAS-4.0.3 SP1" to request a certificate for a Reporting host.
  - Enter both of the above to request a certificate for an All Functions host.
2. Submit your request to the CA. When the CA responds to your request, you will receive the certificate information in e-mail or you will receive a link to a URL where you can copy and paste the certificate information. You will receive the following information:
    - SSL Certificate
    - Root Certificate
    - Intermediate Certificate

**! Important:**

The certificates that CAs send you will vary. Some CAs do not provide intermediate certificates. Some CAs provide more than one intermediate certificate. The CA might only provide an SSL certificate. If this occurs contact your CA and obtain the CA's root certificate.

After receiving the certificate information, you may need to access the CA over the Internet to verify the validity of the certificate. The information from the CA will tell you if you must do this before you import the certificates.

3. Retain a record and receipt for each certificate you receive. You will need this information when you request replacement certificates.

---

## Installing server certificates

### About this task

This procedure has three distinct sections:

- Importing the root certificate
- Importing the intermediate certificate
- Importing the SSL certificate

The certificates that CAs send you will vary. Some CAs do not provide intermediate certificates. Some CAs provide more than one intermediate certificate. The CA might only provide an SSL certificate. If this occurs contact your CA and obtain the CA's root certificate. If you cannot obtain a root or intermediate certificate, skip the portion of the procedure for the root or intermediate procedure and continue with the next portion.

## Procedure

1. Log on to OAM on the Administration or All Functions host.
2. On the **Tasks** tab, select **Security > Trusted Certificates**.  
The system displays the Trusted Certificates page.
3. If you are replacing an expiring root certificate, perform the following steps. Otherwise, skip to Step 4.
  - a. From the **Host** drop-down menu, select the name of the host where you want to delete the root certificate. The host you select depends on your deployment:
    - If you are deleting a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
    - If you are deleting certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host just before you install the new root certificate.

 **Caution:**

Do not select **localhost**.

- b. Select **Switch To**.
  - c. Select the root certificate you want to delete.
  - d. Select **Delete**.  
The system displays a confirmation dialog box.
  - e. Select **OK**.  
The system displays the Trusted Certificates page.
4. If you are replacing an expiring intermediate certificate, perform the following steps. Otherwise, skip to Step 5.
    - a. From the **Host** drop-down menu, select the name of the host where you want to delete the intermediate certificate. The host you select depends on your deployment:
      - If you are deleting a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
      - If you are deleting certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host just before you install the new root certificate.

 **Caution:**

Do not select **localhost**.

- b. Select **Switch To**.
- c. Select the intermediate certificate you want to delete.
- d. Select **Delete**.  
The system displays a confirmation dialog box.
- e. Select **OK**.

The system displays the Trusted Certificates page.

5. If you received a root certificate from the CA, perform the following steps. The CA might only provide an SSL certificate. If this occurs contact your CA and obtain the CA's root certificate. If you still cannot get a root certificate, skip to Step 6.
  - a. From the **Host** drop-down menu, select the name of the host where you want to install the root certificate. The host you select depends on your deployment:
    - If you are installing a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
    - If you are installing certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host.

 **Caution:**

Do not select **localhost**.

- b. Select **Switch To**.
- c. Select **Import**.

The system displays the Trusted Certificate Import page.

- d. In the **Certificate Alias** field, enter the name used when you requested the certificate and add the suffix **Root** to the name.
- e. In the **Certificate PEM** text area, copy and paste the root certificate.
- f. Select **Apply**.

The system displays the following message:

```
Certificate imported successfully
```

- g. Select **Close**.

The system displays the Trusted Certificates page.

6. If you received an intermediate certificate from the CA, perform the following steps. If you received more than one intermediate certificate, repeat these steps. If you did not receive an intermediate certificate, skip to Step 7.
  - a. From the **Host** drop-down menu, select the name of the host where you want to install the intermediate certificate. The host you select depends on your deployment:
    - If you are installing a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
    - If you are installing certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host.

 **Caution:**

Do not select **localhost**.

- b. Select **Switch To**.
- c. Select **Import**.

The system displays the Trusted Certificate Import page.

- d. In the **Certificate Alias** field, enter the name used when you requested the certificate and add the suffix **Intermediate** to the name.
- e. In the **Certificate PEM** text area, copy and paste the intermediate certificate.
- f. Select **Apply**.

The system displays the following message:

```
Certificate imported successfully
```

- g. Select **Close**.

The system displays the Trusted Certificates page.

7. On the **Tasks** tab, select **Security > Administer Server Certificates**.

The system displays the Server Certificates page.

8. If you are replacing an expiring SSL certificate, perform the following steps. Otherwise, skip to Step 9.

- a. From the **Host** drop-down menu, select the name of the host where you want to delete the SSL certificate. The host you select depends on your deployment:
  - If you are deleting a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
  - If you are deleting certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host just before you install the new root certificate.

 **Caution:**

Do not select **localhost**.

- b. Select **Switch To**.
- c. Select the SSL certificate you want to delete.
- d. Select **Delete**.

The system displays a confirmation dialog box.

- e. Select **OK**.

The system displays the Server Certificates page.

9. From the **Host** drop-down menu, select the name of the host where you want to install the SSL, intermediate, and root certificates. The host you select depends on your deployment:

- If you are installing a certificate for an All-in-One, Single, or Dual host deployment, select the host name of the All Functions host.
- If you are installing certificates for a Multi-host deployment, select the Administration host first. Repeat this procedure for each Reporting host and the RTD host.

 **Caution:**

Do not select **localhost**.

10. Select **Switch To**.
11. Select **Import**.  
The system displays the Server Certificate Import page.
12. In the **Certificate Alias** field, enter the name used when the certificate was requested.
13. Leave the **Establish Chain of Trust** option unselected. For more information about this option, see [Establishing the chain of trust](#) on page 168.
14. Select the **Import Certificate for server access** option.
15. In the **Certificate PEM** text area, copy and paste the SSL certificate provided by the CA.
16. Enter a blank line in the text box.
17. Copy and paste the intermediate certificate, if provided by the CA. If the CA provided more than one intermediate certificates, enter a blank line between each intermediate certificate.
18. Enter a blank line in the text box.
19. Copy and paste the root certificate, if provided by the CA. If not provided by the CA, leave blank.
20. Select **Apply**.  
The system displays the following message:

```
Certificate imported successfully
```

21. Select **Close**.  
The system displays the Server Certificates page.
22. Depending on the type of host where you installed the certificate, do one of the following:
  - If you installed a certificate on an All Functions host, enter the following commands:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss
restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```
  - If you installed a certificate on the Administration host, enter:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
```
  - If you installed a certificate on a Reporting host, enter:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss
restart
```
  - If you installed a certificate on the RTD host, enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

- For Multi-host deployment, repeat this procedure for every Reporting host and the RTD host.

---

## Next steps

If you did not select the **Import Certificate for server access** option and need to edit the `server.xml` files, see:

- [Manually adding the certificate name for the OAM certificate](#) on page 168
- [Manually adding the certificate name for the Reporting certificate](#) on page 169
- [Manually adding the certificate name for the RTD certificate](#) on page 170

---

## Establishing the chain of trust

By default, when you import the root and intermediate certificates into the trusted server repository as described in [Installing server certificates](#) on page 163, a chain of trust is automatically established between the root, intermediate, and SSL certificates. You may need to manually establish the chain of trust if the IT department requires this option.

To manually establish the chain of trust while you are importing the SSL certificate, select the **Establish Chain of Trust** option. This option means that all certificates in the chain must exist in the trusted certificate repository. The system rejects the import if any of the certificates in the chain are missing. If you select this option, and the error message displays the message `Chain of trust could not be established`, you must ensure that you imported all certificates of the CA in the chain into the Trusted Certificates repository.

---

## Manually adding the certificate name for the OAM certificate

### About this task

Follow this procedure to manually add the certificate name for the OAM certificate and restart the AdminTomcat container.

### Procedure

- Back up the default OAM Tomcat `server.xml` file.
- Enter the following command to edit the `server.xml` file:  

```
vi $CATALINA_HOME/conf/server.xml
```
- Browse through the file until you find the following block of code:

```
<!-- The OAM default cert -->
  <Connector port="28443" maxHttpHeaderSize="8192"
    maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
```



```

    acceptCount="100" scheme="https" secure="true"
    keystoreFile="/opt/coreservices/avaya/certs/pfxs/CCRAdmin.pfx"
    keystorePass="password" keystoreType="PKCS12"
    clientAuth="false" sslProtocol="TLS">
<!-- end of OAM -->

```

4. Find the `keystoreFile` attribute. Change the name of the `.pfx` file to the name you noted before the upgrade as the Certificate Alias option for the Administration container (typically, the All Functions or Administration host). For example, change the default `CCRAdmin.pfx` filename to `AdminCert.pfx` (the Certificate Alias name plus the `.pfx` suffix).

The following is an example showing the new trusted certificate alias:

```

<!-- The OAM default cert -->
    <Connector port="28443" maxHttpHeaderSize="8192"
        maxThreads="150" minSpareThreads="25" maxSpareThreads="75"
        enableLookups="false" disableUploadTimeout="true"
        acceptCount="100" scheme="https" secure="true"
        keystoreFile="/opt/coreservices/avaya/certs/pfxs/AdminCert.pfx"
        keystorePass="password" keystoreType="PKCS12"
        clientAuth="false" sslProtocol="TLS"
    </!-- end of OAM -->

```

5. Save and close the file.
6. To restart the proper containers, enter the following commands:
 

```

sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart

```

---

## Manually adding the certificate name for the Reporting certificate

### About this task

Follow this procedure to manually add the certificate name for the Reporting certificate and restart the Reporting JBoss container.

### Procedure

1. Back up the default reporting tool Tomcat `$JBASS_HOME/server/ccr3/deploy/jbossweb-tomcat55.sar/server.xml` file.
2. Enter the following command to edit the `server.xml` file:
 

```

vi $JBASS_HOME/server/ccr3/deploy/jbossweb-tomcat55.sar/server.xml

```
3. Browse through the file until you find the following block of code:

```

<!-- SSL/TLS Connector configuration using the admin devl guide keystore
-->
    <Connector port="18443" address="${jboss.bind.address}"
        maxThreads="250" strategy="ms"
maxHttpHeaderSize="8192"
        emptySessionPath="true"

```

```

        scheme="https" secure="true" clientAuth="false"
        keystoreFile="/opt/coreservices/avaya/certs/pfxs/CCRReport.pfx"
        keystoreType="PKCS12"
        keystorePass="password" sslProtocol="TLS" URIEncoding="UTF-8"> /

```

4. Find the `keystoreFile` attribute. Change the name of the `.pfx` file to the name you noted before the upgrade as the Certificate Alias option for the Reporting container (typically, the All Functions or Administration host). For example, change the default `CCRAdmin.pfx` filename to `ReportCert.pfx` (the Certificate Alias name plus the `.pfx` suffix).

The following is an example showing the new trusted certificate alias:

```

<!-- SSL/TLS Connector configuration using the admin devl guide keystore
-->
    <Connector port="18443" address="{jboss.bind.address}"
        maxThreads="250" strategy="ms"
maxHttpHeaderSize="8192"
        emptySessionPath="true"
        scheme="https" secure="true" clientAuth="false"
        keystoreFile="/opt/coreservices/avaya/certs/pfxs/
ReportCert.pfx"
        keystoreType="PKCS12"
        keystorePass="password" sslProtocol="TLS" URIEncoding="UTF-8"> /

```

5. Save and close the file.
6. To restart the proper containers, enter the following commands:
 

```

sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart

```

---

## Manually adding the certificate name for the RTD certificate

### About this task

Follow this procedure to manually add the certificate name for the RTD certificate and restart the RTDTomcat container.

### Procedure

1. Back up the default RTD Tomcat `$CCR_HOME/RTD/tomcat/apache-tomcat-5.5.27/conf/server.xml` file.
2. Enter the following command to edit the `server.xml` file:
 

```

vi $CCR_HOME/RTD/tomcat/apache-tomcat-5.5.27/conf/server.xml

```
3. Browse through the file until you find the following block of code:

```

<Connector port="38443" maxHttpHeaderSize="8192"
    maxThreads="1500" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="/opt/coreservices/avaya/certs/pfxs/

```

```
CCRReport.pfx"
    keystoreType="PKCS12"
    keystorePass="password" />
```

4. Find the `keystoreFile` attribute. Change the name of the `.pfx` file to the name you noted before the upgrade as the Certificate Alias option for the RTD container (typically, the All Functions or Administration host). For example, change the default `CCRAdmin.pfx` filename to `RTDCert.pfx` (the Certificate Alias name plus the `.pfx` suffix).

The following is an example showing the new trusted certificate alias:

```
<Connector port="38443" maxHttpHeaderSize="8192"
    maxThreads="1500" minSpareThreads="25" maxSpareThreads="75"
    enableLookups="false" disableUploadTimeout="true"
    acceptCount="100" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    keystoreFile="/opt/coreservices/avaya/certs/pfxs/
RTDCert.pfx"
    keystoreType="PKCS12"
    keystorePass="password" />
```

5. Save and close the file.
6. To restart the proper containers, enter the following commands:
 

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss restart
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

---

## Individual certificate management procedures

### Listing trusted certificates

#### Procedure

1. On the **Tasks** tab, select **Security > Trusted Certificates**.
  2. On the Trusted Certificates page, select the host for which you want to view the trusted certificates.
  3. Select **Switch To** to display the certificates for the host.  
The Trusted Certificates page lists the trusted certificates. From this page, you can view, add, import, export, and delete server certificates.
-

## Viewing trusted certificates

### Procedure

1. On the **Tasks** tab, select **Security > Trusted Certificates**.
  2. On the Trusted Certificates page, select the host for which you want to view the trusted certificates.
  3. Select **Switch To** to display the certificates for the host.
  4. Select the certificate you want to view.
  5. Select **View**.  
The Trusted Certificate Details page displays the content of the certificate.
  6. Select **Close**.  
The system displays the Trusted Certificates dialog box.
- 

## Importing trusted certificates

### Procedure

1. On the **Tasks** tab, select **Security > Trusted Certificates**.
  2. On the Trusted Certificates page, select the host for which you want to import a trusted certificate.
  3. Select **Switch To**.
  4. When the system displays the certificates for the host, select **Import**.
  5. On the Trusted Certificate Import page, enter a name into the **Certificate Alias** field.
  6. Paste the content of the trusted certificate into the **Certificate PEM** text box.
  7. Select **Apply**.  
The system displays the following message:  

```
Certificate imported successfully
```
  8. Select **Close**.
-

## Exporting trusted certificates

### Procedure

1. On the **Tasks** tab, select **Security > Trusted Certificates**.
  2. On the Trusted Certificates page, select the host for which you want to export a trusted certificate.
  3. Select **Switch To**.
  4. When the system displays the certificates for the host, select the certificate you want to export.
  5. Select **Export**.
  6. On the Trusted Certificate Export page, copy the contents of the **Certificate PEM** text box to a text editor so you can save the certificate to another system.
  7. Select **Close**.
- 

## Deleting trusted certificates

### Procedure

1. On the **Tasks** tab, select **Security > Trusted Certificates**.
  2. On the Trusted Certificates page, select the host for which you want to delete a trusted certificate.
  3. Select **Switch To**.
  4. When the certificates for the host are displayed, select the certificate you want to delete.
  5. Select **Delete**.
  6. When the system displays the confirmation dialog box, select **OK**.  
The system displays the Trusted Certificates dialog box showing that the selected certificate is deleted.
- 

## Creating default server certificate settings

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates > Administer Certificate Defaults**.

2. On the Server Certificate Default Settings page, enter the default certificate settings that you want to apply to all future certificate requests.
  3. Select **Apply**.  
The system displays the Server Certificates page.
- 

## Listing server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.
  2. On the Server Certificates page, select the host for which you want to view the server certificates.
  3. Select **Switch To** to display the certificates for the host.  
The Server Certificates page lists the server certificates. From this page, you can view, add, import, export, and delete server certificates.
- 

## Viewing server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.
  2. On the Server Certificates page, select the host for which you want to view the server certificates.
  3. Select **Switch To** to display the certificates for the host.
  4. Select the certificate you want to view.
  5. Select **View**.  
The Server Certificate Details page displays the content of the certificate.
  6. Select **Close**.  
The system displays the Server Certificates page.
- 

## Adding server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.

2. On the Server Certificates page, select the host for which you want to add a server certificate.
  3. Select **Switch To** to display the certificates for the host.
  4. Select **Add**.
  5. Complete the data fields on the Add Server Certificate page required to create the server certificate.
  6. Select **Apply**.  
The system displays the Server Certificates Request page that shows the Certificate Request PEM.
- 

## Importing server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.
  2. In the Server Certificates page, select the host for which you want to import a server certificate.
  3. Select **Switch To**.
  4. When the certificates for the host are displayed, select **Import**.
  5. In the Server Certificate Import page, enter a name into the **Certificate Alias** field.
  6. Select **Establish Chain of Trust**, if shown.
  7. Paste the content of the server certificate into the **Certificate PEM** text box.
  8. Select **Apply**.  
The system displays the following message:  
`Certificate imported successfully`
  9. Select **Close**.
- 

## Exporting server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.
2. On the Server Certificates page, select the host for which you want to export a server certificate.

3. Select **Switch To**.
  4. When the certificates for the host are displayed, select the certificate you want to export.
  5. Select **Export**.
  6. On the Server Certificate Export page, copy the content of the **Certificate PEM** text box to a text editor so you can save the certificate to another system.
  7. Select **Close**.
- 

## Deleting server certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates**.
  2. On the Server Certificates page, select the host for which you want to delete a server certificate.
  3. Select **Switch To**.
  4. When the certificates for the host are displayed, select the certificate you want to delete.
  5. Select **Delete**.
  6. When the confirmation dialog box displays, select **OK**.  
The system displays the Server Certificates page that shows that the selected certificate was deleted.
- 

## Viewing pending certificates

### Procedure

1. On the **Tasks** tab, select **Security > Administer Server Certificates > View Pending Certificates**.
2. On the Pending Certificate Requests page, select the host for which you want to view the pending certificates.
3. Select **Switch To**.
4. When the pending certificates for the host are displayed, select the certificate you want to enroll or delete.
5. Select **Manual Enroll** or **Delete**.



**\* Note:**

Avaya IQ does not enable the **Auto Enroll** option.

- If you selected **Manual Enroll**, the system displays the Pending Certificates page. To complete the procedure, select **Close**.
- If you selected **Delete**, the system displays a confirmation dialog box. To continue, select **OK**.

The system displays the Pending Certificate Requests page.

## Synchronizing JKS

### Procedure

1. On the **Tasks** tab, select **Security > Synchronize JKS**.
2. On the JKS Synchronization dialog box, do not change the name displayed in the **Host** field.
3. Select the trusted certificate and server certificate you want to synchronize.
4. If you want to remove extra entries that will not be synchronized, select the **Remove Extra** option.
5. Select **Synchronize JKS**.  
The system displays a success or failure message.

## Troubleshooting server certificates

### About this task

If the certificates installed by you are not being recognized by the system, perform the following steps:

### Procedure

1. Depending on the type of host where you installed the certificate, do one of the following:

- If you installed a certificate on an All Functions host, enter the following commands:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
```

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss  
restart
```

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

- If you installed a certificate on the Administration host, enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w AdminTomcat restart
```

- If you installed a certificate on a Reporting host, enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w ReportingJBoss  
restart
```

- If you installed a certificate on the RTD host, enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

2. Clear your browser's cache.
- 

---

## Updating data source releases

### About this task

To upgrade Communication Manager to a new release, you must change the source options to match the new release. For example, if you upgrade Avaya IQ 4.2 to Avaya IQ 5.0 and you upgrade Communication Manager from 4.1 to 5.2 at the same time, you must change the release number administered for that Communication Manager system.

#### Important:

You must coordinate any upgrades between Avaya IQ and data sources. Make sure that you schedule the upgrades during no or low traffic periods so that the data buffers retain the call data during the upgrade. You should upgrade the Avaya IQ system first and then upgrade the source system.

### Procedure

1. On the **Tasks** tab, select **Connection Management > Administer Connections**.
2. Select **Communication Manager**.  
The system displays a list of administered Communication Manager.
3. Select to highlight the system that has been upgraded.
4. Select **Edit**.
5. On the **General** tab, change the **Release** option to match the release of the upgraded Communication Manager system.
6. Select **OK**.  
The system changes the Avaya IQ system to communicate with the upgraded source system.

7. Confirm that data is being transferred from the source system to Avaya IQ, when you upgrade the source.

---

## Adjustment for Daylight Saving Time correction

### About this task

You may need to apply a daylight saving time fix if you operate in countries where daylight changes apply. The procedure is not applicable in countries not located in the daylight savings time zones, such as India and other Asian countries. In countries where daylight changes apply, for example, United Kingdom and United States, scheduled reports in Avaya IQ systems generate at incorrect times after the daylight saving time changes. Administrators can apply the following daylight problem fix, and you can follow this procedure if you upgrade Avaya IQ to a later version.

### Procedure

1. To apply the daylight saving time fix before you install Avaya IQ:
  - a. Log on as root on the All Functions or Administration host.
  - b. Run the following command to edit the ReportingJBoss.xml file:
 

```
vi $CCR_HOME/data/admin/sdl/processcontainer/ReportingJBoss.xml
```
  - c. Verify that the `—ApplyDaylightFix` property is set to `TRUE`. If this property is not present in `ReportingJBoss.xml`, add `—ApplyDaylightFix` property in its string property.
 

For example: `<stringProperty property="arguments" default="-server -XX:CMSInitiatingOccupancyFraction=60 -XX:ParallelGCThreads=2 -XX:GCHeapFreeLimit=20 -XX:GCTimeLimit=80 -XX:+UseThreadPriorities -DApplyDaylightFix=TRUE -Ddss.message_lifetime=60 -Ddss.thread_pool_size=32 -Xmx1500m -XX:MaxPermSize=128m -Dlog4j.configuration=file$CCR_HOME/appserver/jboss-boot.log4j.properties -DLOG_FILE_PREFIX=RPT_ -Dorg.jboss.logging.Log4jService.catchSystemOut=false -Dorg.jboss.logging.Log4jService.catchSystemErr=false" required="false">`
  - d. Save and close the `ReportingJBoss.xml` file.
  - e. Use the following command to edit the `configureSDLData.sh` file:
 

```
vi /opt/coreservices/cs_mgm/bin/linux/configureSDLdata.sh
```
  - f. Remove the comment symbol (`#`) on the following lines:
 

```
#JVMPROPERTIES="$JVMPROPERTIES -Dcoreservice.admin.installdir=$CSBASE/cs_mgmt"
#JVMPROPERTIES="$JVMPROPERTIES -Dproduct.installdir=$CCR_HOME"
```

- g. Save and close the file.
  - h. Run the shell script you just edited:

```
sh /opt/coreservices/cs_mgm/bin/linux/  
configureSDLdata.sh
```
  - i. Start `wdservice` with the following command:

```
service wdinit restart
```
  - j. Add the comment symbol (`#`) to the following lines where they were removed earlier:

```
JVMPROPERTIES="$JVMPROPERTIES -Dcoreservice.admin.installdir=$CSBASE/  
cs_mgmt "  
JVMPROPERTIES="$JVMPROPERTIES -Dproduct.installdir=$CCR_HOME"
```
  - k. Save and close the file.
2. To apply the daylight saving time fix after you install Avaya IQ:
    - a. Open the `/opt/coreservices/watchd/conf` directory.
    - b. Search for the file with the extension `.conf` and the file name with the ReportingJBoss service ID.
    - c. Set `-DApplyDayLightFix=TRUE`.
    - d. Open the `/opt/coreservices/lifecycle/persistence` directory.
    - e. Search for the file name with the ReportingJBoss service ID.
    - f. Set the `-DApplyDaylightFix=TRUE`.
    - g. Run `service wdinit restart` to restart `wdinit` services.

---

## Tuning parameters to prevent overload during pump-up

When Avaya IQ connects to a medium-sized or large-sized Communication Manager system, the high traffic that Avaya IQ receives during pump-up causes the input queue of the Input Translator component to become full. This can cause data loss as well as numerous errors in Data Collection and Data Processing logs with the string `Queue size limit hit`.

### About this task

You can use the Input Translator queue size, which is a tunable parameter, to throttle data processing during pump-up. By default, the value is set to 25,000. If you expect Avaya IQ to receive moderate or high pump-up data, tune this parameter value accordingly. Tune this value incrementally in steps of 25,000. Setting this parameter to a very high initial value, for example, 150,000, can lead to memory-related problems.

#### **Caution:**

To initialize this change, you must restart the Data Collection or Data Processing containers. While the containers restart, data is lost. Perform this procedure during a low traffic or no traffic period.

## Procedure

1. Log on to the Avaya IQ OAM interface.
2. Select **Tasks > Connection Management > Administer Connections**.
3. Select **Communication Manager**.
4. Select the Communication Manager system for which you need to tune the Input Translator value.
5. Select **Edit**.
6. On the **General** tab, look for the **Input Translator Worker Queue Size** parameter.
7. Change the size to a new value.
8. Select **Apply** to save the change.
9. Log on as root to the All Functions host in an All-in-One, Single, or Dual host deployment, or log on as root to the Data Collection host associated with the Communication Manager system in question.
10. Enter the following command to determine the status of the Data Processing or Data Collection containers.

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

The system displays the list of containers. Look for the DataProcessingJBoss container on All-in-One, Single host, or Dual host or the DataCollectionJBoss container on Multi-host. If you have a link to more than one data source, you will see more than one container.

11. Restart the container associated with the Communication Manager system whose Input Translator parameter you changed by entering the following command:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w Container restart
```

where *Container* is either DataCollectionJBoss or DataProcessingJBoss.

---



# Chapter 9: Troubleshooting activities

---

## InputTranslator component becomes full during pumpup

When you connect Avaya IQ to a medium or large cabinet PBX system, Avaya IQ may receive high traffic from the PBX system during pumpup. Because of this high traffic, the InputTranslator component becomes full. This may cause data loss and numerous other errors. The system logs these errors in a log file with the message `Queue size limit hit`.

---

### Proposed solution

#### About this task

The InputTranslator queue size is a customized parameter used to throttle data processing during pumpup. The default value of the queue size is set to 25,000. If you connect Avaya IQ to a medium or large PBX system and expect to receive moderate or high pumpup data, then you must increase the value accordingly. Avaya recommends setting this value incrementally by 25,000. Setting this parameter to a very high value, for example, 150,000 may lead to memory-related problems.

Follow these steps to change the InputTranslator queue size.

#### Procedure

1. Log in as root on the Administration or All Functions host.
2. On the **Tasks** tab, select **Connection Management > Administer Connections**.
3. On the **All Connection Types** dialog box, select **Communication Manager**.
4. On the **Connection Resources** dialog box, select the communication manager for which you want to modify the parameter.
5. Click **Edit**.
6. On the **General** tab, enter a new value in the **Input Translator Worker Queue Size** field.
7. Click **Apply** to save the changes.

**\* Note:**

You must start the Data collection (MH) and Data processing (DH) hosts for the changes to be effective.

---

---

## Cognos fails to start during turnkey installation

Cognos may fail to start during turnkey installation. Due to this failure, report users cannot gain access to the Reporting UI and the APC UI. This network error arises because of a mismatch in the NIC settings of Avaya IQ and the Ethernet switch port.

---

### Proposed solution

#### About this task

On Avaya IQ, set the following values: autoneg to “on”, speed to “100” and duplex to “full”.

#### Procedure

On the console, enter `ethtool -s eth0 speed 100 duplex full autoneg on`.

---

---

### Proposed solution

#### About this task

You can permanently set the NIC settings on Avaya IQ by the following procedure.

#### Procedure

1. On the console, enter `cd /etc/sysconfig/network-scripts`.
  2. Enter `vi ifcfg-eth0`.
  3. In the file, add the following line `ETHTOOL_OPTS="speed 100 duplex full autoneg on`.
- 

#### Next steps

You can monitor the network statistics by running the following command `watch -n1 netstat -i` and watching the RX-ERR and TX-ERR columns.



---

## Report input page does not display any data

This issue arises due to a data pump-up failure for the IQ Input Adapter (IQIA) data source. For example, if you want to select an agent or a queue on the report input page, you may find the fields empty.

---

### Proposed solution

#### About this task

To resolve the problem of report input page with empty data fields:

#### Procedure

1. Verify in OAM whether all containers and Avaya IQ services are running.
  2. To restart the pump-up process, restart the corresponding Avaya Aura® Contact Center DataProcessingJBoss container.
  3. View the `messages_iqiait.log` file to verify whether Avaya IQ is receiving messages. If the data is pumped up successfully, the log file displays the status as `InitializationDone`.
  4. View the `arc.log` file for error messages. You should view the `arc.log` file only if you do not find the message `InitializationDone` in the `messages_iqiait.log` file.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  5. Contact the system administrator or Avaya Services for assistance.
- 

---

## IQIA data source does not display entities

In OAM, the IQIA data source does not display entities, such as agent or queue names. This issue arises due to a data pump-up failure for the IQIA data source.

---

## Proposed solution

### About this task

To resolve the problem of the IQIA data source with empty data fields:

### Procedure

1. Verify in OAM whether all containers and Avaya IQ services are running.
  2. To restart the pump-up process, restart the corresponding Avaya Aura® Contact Center DataProcessingJBoss container.
  3. View the `messages_iqiait.log` file to verify whether Avaya IQ is receiving messages. If the data is pumped up successfully, the log file displays the status as `InitializationDone`.
  4. View the `arc.log` file for error messages. You should view the `arc.log` file only if you do not find the message `InitializationDone` in the `messages_iqiait.log` file.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  5. Contact the system administrator or Avaya Services for assistance.
- 

---

## Report does not display any data

The report does not display any data, or the data displayed in the report does not refresh at stipulated intervals. This issue occurs when the communication between Avaya Aura® Contact Center and IQIA data source is disrupted.

---

## Proposed solution

### About this task

To resolve the problem of data not displayed or refreshed on reports:

### Procedure

1. Verify in OAM whether all the Avaya IQ services are running on all hosts, such as the Data Processing hosts, Reporting hosts, RTD host, and others. You can also verify the services on all hosts using the lifecycle command `sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status`.

Status of PE IQ Input Adapter\_<AACC source name> does not change

2. Verify if the system has logged any error message in the `arc.log` file.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
3. Contact your system administrator or Avaya Services for assistance.

---

## Status of PE IQ Input Adapter\_<AACC source name> does not change

In OAM, the PE IQ Input Adapter\_<AACC source> name always shows the status as *starting*.

In the Lifecycle processes, the PEIQAdapter\_<AACC source name> always shows the status as *starting*.

This issue occurs when the ActiveMQ JMS broker is not available or not started.

---

## Proposed solution

### About this task

To resolve the problem where the PE IQIA\_<AACC source> status does not change:

### Procedure

1. Verify in OAM whether the IQIA source configuration parameter displays the correct ActiveMQ JMS Broker URL. This ActiveMQ JMS Broker URL must correspond to the IQIA Receiver JMS broker and the IQIA Sender JMS broker URLs.
2. Verify whether the ActiveMQ JMS broker is operational on the Avaya Aura® Contact Center machine.

For information on how to verify the operational status of the ActiveMQ JMS broker refer to the topic [Verifying operational status of ARConnector and ActiveMQ JMS broker](#) on page 187.

---

## Verifying operational status of ARConnector and ActiveMQ JMS broker

In Avaya Aura® Contact Center 6.1, the ActiveMQ JMS broker runs on a Windows console and the ARConnector runs as a Windows service.

- To verify the operational status of the ActiveMQ JMS broker on Avaya Aura® Contact Center server, verify whether the ActiveMQ Windows console is running. If the console is not running, restart the ActiveMQ JMS broker Windows console.
- To verify the operational status of the ARConnector on Avaya Aura® Contact Center server, verify whether the ARConnector service is running. If the service is not running, restart the ARConnector service.

In Avaya Aura® Contact Center 6.2, the ActiveMQ JMS broker is an integral part of the ARConnector service. Therefore, when you start the ARConnector service, the ActiveMQ JMS broker becomes operational.

---

## ARConnector initialization fails

---

### Proposed solution

#### About this task

This issue occurs when the SEI Event Service is not running.

#### Procedure

1. Verify whether the `arc.log` file shows the CORBA errors.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  2. If the `arc.log` file shows the CORBA errors, then verify whether the SEI Event Service is running. You can check the status of the `ES_Service` on Avaya Aura® Contact Center server.  
Click **Start > Avaya > Contact Center Common Utilities > System Control and Monitor Utility**.
  3. Verify the `CCMS_SEI_1.log` file for more details.  
You can find the `CCMS_SEI_1.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS\CCMS_SEI_x.log`, which is a default path.
-

---

## Proposed solution

### About this task

This issue is a rare occurrence, and therefore, there may not be a specific reason for the occurrence of this issue.

### Procedure

1. Verify whether the `arc.log` file shows the SEI initialization thread hung message.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  2. If the `arc.log` file shows the SEI error message, then restart the Event Service or restart all CCMS services on the Avaya Aura® Contact Center server.  
Click **Start > Avaya > Contact Center Common Utilities > System Control and Monitor Utility**.
- 

---

## Proposed solution

### About this task

This issue may arise if the ActiveMQ JMS broker of the Avaya Aura® Contact Center ARConnector has not started, or is not available.

### Procedure

1. Verify whether the `arc.log` file shows the...`Connection refused: connect` message.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  2. If the `arc.log` file shows the connection refused error, then verify whether the ARConnector JMS shows the status of the ActiveMQ JMS broker as *operational*.
-

---

## SEILink does not receive heartbeat messages

The SEILink on ARConnector does not receive a heartbeat message from Avaya Aura<sup>®</sup> Contact Center and the IQIA logs linkdown message and raises an alarm. This issue occurs if the SEI Event Service process is not functional on the Avaya Aura<sup>®</sup> Contact Center server.

---

### Proposed solution

#### About this task

To resolve the problem where SEILink does not receive heartbeat messages:

#### Procedure

1. Verify whether the `DataProcessingJBoss_<iqia-source-name>.log` file shows pump-up errors.  
You can find the `DataProcessingJBoss_<iqia-source-name>.log` file on the DP host at `/var/log/Avaya/CCR/ DataProcessingJBoss_<iqia-source-name>DataProcessingJBoss_<iqia-source-name>.log`.
  2. Verify whether the `arc.log` shows `Still alive, sleeping` message at every 10 second interval.  
You can find the `arc.log` file on the Avaya Aura<sup>®</sup> Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  3. Verify whether the SEI event Service is running. You can check the status of the `ES_Service` on Avaya Aura<sup>®</sup> Contact Center server.  
Click **Start > Avaya Contact Center > Common Utilities > System Control and Monitor Utility**.
  4. View the `CCMS_SEI_1.log` file for more details on the status of SEI event service.  
You can find the `CCMS_SEI_1.log` file on the Avaya Aura<sup>®</sup> Contact Center host at `D:\Avaya\Logs\CCMS\CCMS_SEI_x.log`, which is a default path.
  5. Contact the system administrator or Avaya Services for assistance.
-

---

## SEILink logs CORBA errors

The SEILink logs CORBA exceptions and the IQIA logs linkdown message. This issue occurs because of a failure in the Avaya Aura® Contact Center Event Service CORBA connection.

---

### Proposed solution

#### About this task

To resolve the problem where SEILink logs CORBA errors:

#### Procedure

1. Verify whether the `DataProcessingJBoss_<iqia-source-name>.log` file shows pump-up errors.  
You can find the `DataProcessingJBoss_<iqia-source-name>.log` file on the DP host at `/var/log/Avaya/CCR/ DataProcessingJBoss_<iqia-source-name>DataProcessingJBoss_<iqia-source-name>.log`.
  2. Verify whether the `arc.log` file shows CORBA exceptions.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  3. Allow some time for the system to recover automatically.
  4. Contact the system administrator or Avaya Services for assistance.
- 

---

## IQIA does not receive JMS messages

This issue occurs when either the IQIA container process stops or exists on its own.

---

### Proposed solution

#### About this task

To resolve the problem where IQIA does not receive JMS messages:

## Procedure

1. Verify whether the `DataProcessingJBoss_<iqia-source-name>.log` file shows messages that help you identify whether the system is processing any messages.  
You can find the `DataProcessingJBoss_<iqia-source-name>.log` file on the DP host at `/var/log/Avaya/CCR/ DataProcessingJBoss_<iqia-source-name>DataProcessingJBoss_<iqia-source-name>.log`.
  2. Restart the IQIA `DataProcessingJBoss` container on the Avaya IQ server.
- 

---

## IQIA logs linkdown message and raises an alarm

This is a CORBA issue. This issue arises when an incompatible version of ARConnector tries to communicate with the SEI component of Avaya Aura® Contact Center.

---

## Proposed solution

### About this task

To resolve the problem where IQIA logs Linkdown message and raises an alarm:

### Procedure

1. Verify whether the `arc.log` file shows the CORBA error and the `IncompatibleVersion` message.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  2. Verify whether the ARConnector version is compatible with the SEI event service.  
To verify the installed version of ARConnector on Avaya Aura® Contact Center server:
    - a. Click **Start > Control Panel > Add or Remove Programs**.
    - b. Select the ARConnector. The version number is displayed under the **Version** column.
  3. Contact the system administrator or Avaya Services for assistance.
-



---

## **IQIA pump-up request fails**

---

### **Proposed solution**

#### **About this task**

This issue occurs because of a network problem from installing IQIA, ActiveMQ, and ARConnector on more than one machine.

#### **Procedure**

1. Verify whether the `DataProcessingJBoss_<iqia-source-name>.log` file shows pump-up errors.  
You can find the `DataProcessingJBoss_<iqia-source-name>.log` file on the DP host at `/var/log/Avaya/CCR/ DataProcessingJBoss_<iqia-source-name>DataProcessingJBoss_<iqia-source-name>.log`.
  2. Verify that the machines on which IQIA, ActiveMQ, and ARConnector are installed communicate with each other.
- 

---

## **ARConnector stops posting JMS messages**

---

### **Proposed solution**

#### **About this task**

The IQIA stops posting JMS messages and the system logs a `LINKDOWN` message and raises an alarm. This issue occurs if the ARConnector Service is not running.

#### **Procedure**

1. Verify whether the `messages_iqiait.log` file contains the `LINKDOWN` message.  
You can find the `messages_iqiait.log` file on the DP host at `/var/log/Avaya/CCR/DataProcessingJBoss_<iqia-source-name>/messages_iqiait.log`.

2. Restart the ARConnector and monitor the `arc.log` file.  
You can find the `arc.log` file on the Avaya Aura® Contact Center host at `D:\Avaya\Logs\CCMS`, which is a default path.
  3. Contact the system administrator or Avaya Services for assistance.
- 

---

## Proposed solution

### About this task

This issue may occur due to an insufficient memory on the Avaya Aura® Contact Center server.

### Procedure

1. Verify whether you have set the memory as per the Buffering and ActiveMQ sizing guidelines on the server where ARConnector is installed.
  2. Contact the system administrator or Avaya Services for assistance.
- 

---

## Changing the default Avaya Aura® Contact Center ARC, HEP and REP expiration values for spec contact sessions

### About this task

Avaya Aura® Contact Center ARC, Historical Event Processing (HEP) and Real-time Event Processing (REP) use Email, Voice, Document, FAX, SMS, WebChat, Default, and Unidentified as channel types. Based on the channel type, the contact sessions in Avaya Aura® Contact Center ARC, HEP, and REP expire automatically based on default time settings.

Avaya Aura® Contact Center, HEP, and REP verify these expired sessions every 60 minutes. You can change the default expiration value of the contact sessions for individual channels or all channels.

To change the default expiration value of the contact sessions, perform the following steps:

### Procedure

1. For individual channels in Avaya Aura® Contact Center, change the value of each individual channel (`CHANNEL_NAME.SessionExpireMinutes`) in the `<ARConnector-Home>/data/eventmgt/XML/specinfo.properties` file on the Avaya Aura® Contact Center server.

2. For individual channels in HEP or REP, change the value of each individual channel (CHANNEL\_NAME.SessionExpireMinutes) in the SDProperty table of SDS database on the Avaya IQ database server.
3. For changing the value of the audit (default is 60 minutes), change the SessionAuditIntervalMinutes values in the <ARConnector-Home>/config/ar.properties file on the Avaya Aura® Contact Center server and in the SDProperty table of SDS database on the Avaya IQ database server.

**\* Note:**

The expiration values of the channels on Avaya Aura® Contact Center must be smaller than the values of the same channels on HEP or REP. This allows Avaya Aura® Contact Center to clean up the session and send appropriate messages to the downstream. This behavior applies only to L23/L22 and not to L21.

---

### Next steps

Restart Avaya Aura® Contact Center ARC and the Data Processing container after you change the default expiration values.

---

## IQ pump-up request fails

**\* Note:**

Use this procedure on AACC systems to resolve the following problem.

Avaya IQ receives pump-up from the Avaya Aura® Contact Center 6.2 system on administrator-configured items such as queues, skillsets and routing points. However, Avaya IQ fails to receive pump-up for the current agent states, and real time event stream after the pump-up completes and the traffic begins. This problem occurs due to incompatible socket configuration on some servers that prevents the SEILink C++ ORB from being discovered by the Java-side ORB.

---

## Proposed solution

### About this task

On the Avaya Aura® Contact Center system, make changes to the `jacorb.properties` file to change the search algorithm used to find a free socket.

### Procedure

1. Log on to the Avaya Aura® Contact Center server where you have installed Manager Server.

2. Navigate to the `D:\Avaya\Contact Center\Manager Server\ARConnector\config` directory.
3. Open the `jacorb.properties` file in Notepad for editing.
4. Make the following changes under the section `Socket Factories`:
  - a. Enter # at the beginning of the line starting with `jacorb.net.socket_factory=org.jacorb.orb.factory.PortRangeSocketFactory`.
  - b. Delete # from the beginning of the line starting with `jacorb.net.socket_factory=org.jacorb.orb.factory.DefaultSocketFactory`.
  - c. Enter # at the beginning of the lines starting with `jacorb.net.socket_factory.port.min=31051` and `jacorb.net.socket_factory.port.max=31056`.
5. Save file.
6. Exit Notepad.

**\* Note:**

You can see the Avaya IQ system pumping-up the current agent states, and real time event stream automatically if ARC is still re-trying the ORB connection.

---

**Next steps**

If you still do not see the current agent states, and real time event stream on the Avaya IQ system, wait for 5 minutes and restart the ARConnector service.

---

## Deleting buffer storage and index files after making changes in the Data Processing dispatcher persistence configuration

If you make any changes to the Data Processing dispatcher persistence configuration that is present in Data Processing PE, you need to delete buffer storage and index files to ensure that the changes are effective.

---

## Proposed Solution

### Procedure

1. Ensure that there is no buffering. To check the status of the buffering, in the `/opt/Avaya/CCR/data/buffer/xxxx.eventprocessor.dispatcher` directory, run the following command:

```
sh /opt/Avaya/CCR/bin/BufferIndexReader.sh.
```

**\* Note:**

If data buffering occurs, find the root cause of the data buffering and stop the data buffering.

2. After changing the dispatcher persistence properties, stop the Data Processing JBoss container.
  3. From the `/opt/Avaya/CCR/data/buffer/xxxx.eventprocessor.dispatcher` directory, delete all the buffer storage files and the index files. If these files have data, the data will be lost.
  4. Restart the DP container.
-



# Chapter 10: Backing up system and database data

---

## Backup strategies

Backing up your data reduces the risk of losing data due to hardware failures, human errors, application failures, and security breaches, such as hackers or viruses. Maintaining quality backups is economical and minimizes costs for your contact center operation. Your contact center incurs additional costs to recover data if you do not back up data or if the backup is of poor quality. You might experience these costs as system downtime, data loss, or unnecessary financial expense. You must back up your data if your data is crucial to the successful operation of your contact center.

 **Caution:**

If you fail to back up your system and database data, you will lose data in the event of a fully system failure. Even if you back up your data on a regular basis, you may still lose some administrative data between the time of the last backup and when your system fails. If you follow the recommended backup strategies defined in this section, you can minimize the potential data losses and increase chances for a successful recovery.

Take in to consideration the following points when developing your backup strategies:

### **Determine how critical the data is to the business**

- What data do you need to back up?
- What damage or repercussions would occur if you lost data?
- How quickly must the system become operational again after the system becomes inoperative?
- How frequently do you update the data in your database?
- How long can you afford to let the application remain nonfunctional while you recover your database?
- How big is your database?
- What will you use to back up your data? Disk or tape?
- Is it necessary to rotate your backup media?
- How frequently should you backup your data?

## Create a data backup policy

- Use the tools your software vendors provide and support. Follow the recommendations of your software vendors.
  - For software-only deployments: Use Linux tools for the operating system backups and Oracle tools for the database backups. Only IT personnel and database administrators (DBA) must perform these tasks.
  - For turnkey deployments: Use the tools Avaya provides for operating system and database backups. Assign personnel to perform these backups.
- Schedule daily, weekly, or monthly backups on a regular basis.

Create weekly full backups and daily incremental backups as required.
- Determine if you will create backups after all administrative changes.

If you do regular incremental backups, retain all administrative changes in case of a system failure. For a turnkey deployment, if daily Data Collection traffic volume exceeds 500,000, you must increase the frequency of archive log backup.
- Determine how long you will retain a backup.

Ensure that you retain backups for one week, that is, one full backup and six incremental backups. You can purge backups older than 14 days to save space on the system.

## Verify that backups are of good quality

Use a reliable backup system.

## Determining required space for a software-only deployment

For backups, the amount of storage space depends on many factors. Unfortunately, there is no simple formula to determine the amount of required backup space.

When a system is designed, the Implementation Planning Tool (IPT) determines a projected amount of database data based on the number of data sources, retention requirements, and three-year growth. The projections are based on one, two, and three years of database data. The size of storage disks required for a system is engineered based on that projection. Customers must also determine how many years of data to save and how many weeks of backups to save. All of these factors must go into planning the amount of space required for backups.

For a minimum starting point, customers must have enough space to back up the database data projected by the IPT, plus the following system data:

- For the system base backup: 6 GB. This backup is done the first time backup is run, but the file should be backed up on a regular basis.
- For each daily system data backup: 650 MB, or 3.9 GB per week.

Customers must plan for this initial amount of data backup requirements based on the IPT projections and the daily and weekly system backup values. Customers must monitor this closely and allocate enough backup storage space as database storage needs increase over time.



## Determining required space for a turnkey deployment

For backups, the amount of storage space depends on many factors. Unfortunately, there is no simple formula to determine the amount of required backup space.

When your system is designed, the Implementation Planning Tool (IPT) determines the required amount of database storage space based on the number of data sources, retention requirements, optimal performance, and three-year growth. The IPT does not give any year-by-year projections of the database data sizes, so it is difficult to plan for the proper amount of backup storage space. You must also determine how many years of data you want to save and how many weeks of backups you want to save. All of these factors must go into planning your backup space.

At a minimum, you must have enough space to back up the database data, plus the following system data:

- For the system base backup: 6 GB. This backup is done the first time you run backup, but the file should be backed up on a regular basis.
- For each daily system data backup: 650 MB, or 3.9 GB per week.

Plan for an initial amount of data backup requirements based on the daily and weekly system backup values, but also plan for long-term increases in storage needs as you store more data. With a turnkey deployment, you must also consider the following default disk storage sizes when determining your backup space requirements:

- For an All-in-One host deployment, the system is equipped with 1.2 TB of storage space.
- For a Single, Dual, or Multi-host deployment, the system is equipped with 3.2 TB of storage space on each disk array. Each system has at least one disk array, with up to a total of eight disk arrays.

For example, with a Dual host deployment that has two disk arrays, you would potentially need to back up 10 GB for system data and 6.4 TB for database data each week. In reality, your initial backup needs will be much smaller than this example implies, but there is no way to easily project how much backup storage space to plan for. Avaya Provisioning teams often suggest that customers provide 500 GB of backup space as an initial size for backup space. Once an initial value is determined, customers must monitor this closely and allocate enough backup storage space as database storage needs increase over time.

## Store backups in a safe location

For backups on removable media, keep the media secured in your equipment room. For backups on equipment such as a repository, the same requirement applies.

## Backup procedures

For customers that have a software-only deployment, use the procedures in the following sections:

- [Backing up Avaya IQ data in a software-only deployment](#) on page 202
- [Backing up the operating system in a software-only deployment](#) on page 203
- [Backing up The database on a software-only deployment](#) on page 203

For customers that have a turnkey deployment, use the procedures in [Data backups and database maintenance for a turnkey deployment](#) on page 204.

---

## Backing up Avaya IQ data in a software-only deployment

### About this task

Routinely backing up Avaya IQ data is critical to the smooth operation of your contact center. Should one of your application hosts fail, having a backup of the Avaya IQ data helps speed recovery of the system.

#### Important:

You should create a routine backup schedule and follow it for all Avaya IQ application hosts in the deployment other than the database host. For more information about how to back up the database host, see [Backing up the database on a software-only deployment](#) on page 203.

For the procedures to restore the backup files for a recovery, see [Restoring Avaya IQ in a software-only deployment](#) on page 219 and [Recovering and restoring the database host](#) on page 222. You must involve Avaya or Avaya Partner personnel in a recovery procedure of this type.

You must perform a backup of Avaya IQ data:

- After the initial implementation.
- After a major set of administrative changes.
- After you change any third-party configuration data.

At a minimum, you should do a backup no less than once a week. You can administer the backup to run on a scheduled basis, but you must manually copy the data to media on a regular basis. You must determine what type of media you will use for the backup.

Backups of the Avaya IQ data require about 10 GB of temporary free space. Before you begin this procedure, find a directory that has this amount of free space.

### Procedure

1. Log on to your application host as root or a root-level user.
2. Enter the following command to remove the last backup file start a new backup:

```
sh /opt/Avaya/CCR/bin/runBackup.sh -bkploc BackupLocation -force
```

The variable *BackupLocation* is the mount point on the network drive where you want to back up the data. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.
3. Enter the following command to view the status of the backup:

```
tail -f /var/log/Avaya/CCR/backup/iqbackup.log
```

4. Transfer your backup files to a backup media such as a tape repository or disk repository.
5. Store the backup media in a safe location.
6. Repeat this procedure for every application host in your deployment.

---

**Related topics:**

[Backing up the operating system in a software-only deployment](#) on page 203

[Backing up the database in a software-only deployment](#) on page 203

[Backing up custom reports](#) on page 204

---

## Backing up the operating system in a software-only deployment

### About this task

You must routinely back up the OS used with the application and database hosts on a backup media of your choice.

---

## Backing up the database in a software-only deployment

Routinely backing up the database is critical to the smooth operation of your contact center. Should your database host fail, a database backup helps in the speedy recovery of the system. You should create a routine backup schedule and follow this schedule for the database host. The size of your warehouse, the desired duration of performing a backup, and the ease of recovery play a big part when determining your backup strategy.

Avaya have tested RMAN for software-only deployments and therefore you must use RMAN to do Oracle backups. The RMAN backups were also used to successfully restore the database during recovery testing.

By default, Avaya IQ creates historical and real-time database indexes with the NOLOGGING option. This setting may impact database recovery. The following directories include the scripts for creating indexes:

- `/opt/Avaya/CCR/data/db/oracle/scripts/create_historical_index.sql`
- `/opt/Avaya/CCR/data/db/oracle/scripts/create_realtime_indexes.sql`

Your DBA can modify indexes with LOGGING turned on or, if needed, you can drop and recreate indexes with LOGGING turned on.

You can administer the backup to run on a scheduled basis and write the backed up data to media. You must determine what type of media you will use for the backup. A backup of the database can be very large.

To back up the database and restore your database from a backup, follow the documented procedures of your database vendor. For additional steps to restore the database, see [Recovering and restoring the database host](#) on page 222. If you require help when restoring your database, you can contact Avaya or Avaya Partner personnel to help you with database recovery.

---

## Backing up custom reports

Custom reports are backed up during normal backup procedures. However, it is difficult to restore individual custom reports from these backups. To resolve this issue, you can use export tools developed for the High Availability feature to back up custom reports.

To back up custom reports, see “Exporting reports” in *Avaya IQ High Availability and Survivability*.

To restore backed up reports, see [Restoring custom reports](#) on page 225.

---

## Backing up Avaya IQ data in a turnkey deployment

The backup feature for a turnkey deployment works automatically after you enable the feature. You can enable the backup feature at initial installation or at any time after installation. The backup feature automatically backs up the Avaya IQ software and database data and places the backup files in a location of your choice. Select a mounted drive on your network or on a storage array as the location for the backup files. Do not select a removable media tape drive or disc drive. For more information on why backups are so critical to quick recovery in case of failures, see [Backup strategies](#) on page 199 on page 187.

### **Caution:**

When selecting a network drive or storage array for backups, ensure that the backup device has enough free space to store 2 to 3 weeks of backup data. If the backups fail because there is not enough space for the data, this will adversely affect the operation of Avaya IQ. The turnkey database host uses the IBM EXP3000 disk array for data storage. Each EXP3000 has twelve 600 GB storage disks for a total storage of 3.6 TB per disk array. Each pair of disks is a mirrored pair. For data backup, you need as much as 3.6 TB of storage for each disk array in the deployment. You must also monitor your backup logs to ensure that backups complete successfully and delete obsolete backup data from your backup device so that you do not run out of space.

**! Important:**

Avaya IQ turnkey customers must not use or leverage the Oracle tools or applications by any method, direct or indirect. To gain access to the Oracle database, customers must only use the methods, tools, and applications that Avaya provides.

If the backup feature was not enabled at installation, enable your backups using the procedure in [Enabling the backup feature](#) on page 206.

When backups are enabled, the following default backup schedule occurs:

- Saturday, 1:45 a.m.: full database backup on the database host.
- Every day except Saturday, 1:45 a.m.: incremental database backup on the database host.
- Every day, 1:45 a.m.: software backup of the Oracle base software and the software configuration data. Unless you upgrade or patch the base software, subsequent backups will only back up the configuration data. The backup program automatically determines whether the base software has to be backed up.
- Every day, 1:45 a.m.: software backup of the Avaya IQ base software, Oracle base software, and Avaya IQ software configuration data. Unless you upgrade or patch the base software (Avaya IQ or Oracle), subsequent backups will only back up the configuration data. The backup program automatically determines whether the base software has to be backed up.

**! Important:**

The turnkey backup program automatically deletes old backups every two weeks. Therefore, you must occasionally save the backup data to a secure location separate from the default location in case you later need an older set of backups.

You can also run a backup on demand. See [Running an on-demand backup](#) on page 210.

To check the status of your backups, you must view the backup log files on a daily basis. There is one log file for the Avaya IQ software backup and another log file for the database backup. For information about how to check the status of the backups, see the following sections:

- [Confirming a successful system data backup on The Avaya IQ host](#) on page 212
- [Confirming a successful database data backup on The database host](#) on page 213

**\* Note:**

In a turnkey deployment, while running the automatic database backup, the system creates certain files in the backup directory. The number of files created depends upon the number of fact tables in the database. Turnkey has 10 fact tables and therefore you may find 10 files created in the backup directory. The file names are in the following format `MM-DD-YYYY_AVAYAIQ_DB_<file number>`.

For example, you may see the 10 files as follows:

`MM-DD-YYYY_AVAYAIQ_DB_01****_1_1`, `MM-DD-YYYY_AVAYAIQ_DB_02****_2_1`  
through `MM-DD-YYYY_AVAYAIQ_DB_0a****_10_1`.

In addition, a control file `controlfile_*****` is also created in the backup process. While restoring the IQ database, you may require all these files. Therefore, you must back up the entire backup directory before you delete any file.

**Related topics:**

- [Backing up custom reports](#) on page 204
- [About enabling backups](#) on page 206
- [Backup worksheet](#) on page 206
- [Verifying the backup mount point on an application and database host](#) on page 207
- [Setting the NFS mount point for backups](#) on page 208
- [Activating the backup feature](#) on page 209
- [Running an on-demand backup](#) on page 210
- [Confirming a successful system data backup on an application host](#) on page 212
- [Confirming a successful database data backup on the database host](#) on page 213
- [Backing up Avaya IQ data on Windows](#) on page 214

---

## About enabling backups

You must enable backups for the Avaya IQ software and data. To do this, you must have a mountable network drive or storage array to which the Avaya IQ application and database hosts can back up files. This network drive or storage array must be accessible from all hosts in the Avaya IQ deployment.

You must also set the permissions on your remote storage devices to allow the backups to work. For backups from an application host, the permissions should be `root:root`. For backups from the database host, the permissions should be `oracle:oinstall`.

---

## Backup worksheet

Use the following worksheet to plan the settings you want to use for the backups.

| Information                                                                                                                                                                 | Default value | Your value |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------|
| Enable backup<br>You can enable backup during the initial installation. You can change this option later.                                                                   | Yes           |            |
| Backup location<br>You cannot back up directly to a tape or disc device. You must first back up to a network drive and then back up the data to a tape or disc, if desired. | N/A           |            |
| Day of week for full database backup                                                                                                                                        | Saturday      |            |

| Information                                                                                                                                                                                                          | Default value | Your value |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|------------|
| Database backup time<br>You can schedule backups for a slow traffic period. Note: Though the interface shows a value for seconds, you can only set the value to 00.                                                  | 01:45:00      |            |
| Frequency of archive log backups<br>For deployments that have large call volumes, you can back up archive logs twice a day during no or low traffic times. Use the Database Diagnostic tool to schedule the backups. | None assigned |            |

## Verifying the backup mount point on an application and database host

### About this task

You must enable backups for the Avaya IQ software and data on a mountable network drive or storage array. Ensure that you can gain access to this network drive or storage array from all hosts in the Avaya IQ deployment. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

To verify that you enabled the portmap service for the NFS mount point:

### Procedure

1. Log on to the application or database host as root or a root-level user.
2. Enter the following command to check if the portmap service is running:  

```
service portmap status
```

You see the following response:

```
portmap (pid xxxx) is running...
```

Where xxxx is the pid number.
3. If the portmap service is not functional, enter:  

```
service portmap start
```
4. Verify that the proper permissions are set on the NFS mount point server.
5. Repeat this procedure on all hosts.

### Related topics:

[Restoring the software base and system configuration data on an application host](#) on page 254

---

## Setting the NFS mount point for backups

Setting an NFS mount point for backups can be a difficult procedure. If you need assistance, contact Avaya Support personnel.

### Procedure

1. Configure the network drive for NFS mount and log on to the host that the network drive resides. Follow the instructions the host OS vendor provides to make the network drive ready for NFS mount. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

2. Enter:

```
mkdir MountPoint
```

The *MountPoint* variable is a path from the host to the backup location on the network drive or storage array. For example, you can name the mount point / backup.

3. Enter:

```
vi /etc/fstab
```

4. Add a single line at the end of the file using the following syntax:

```
HostName:RemotePath MountPoint nfs  
rw,rsize=32768,wsiz=32768,timeo=14,intr
```

The variables for this command are as follows:

- The *HostName* variable represents the name of the system where the network drive is located or the name of the storage array.
- The *RemotePath* variable is the path on the network drive or storage array to where the files will be backed up. The customer must identify the remote path.
- The *MountPoint* variable must match the directory you created on this host.

5. Write and save the file.

6. Enter:

```
cd /
```

```
mount -a
```

The mount point is linked to the file system on the network drive or storage array.

7. To confirm that you administered the mount point correctly, enter:

```
df -h
```

Repeat this procedure to readminister the mount point correctly.

---



## Next steps

You must create a new directory to back up the database. This directory must not be a part of Avaya IQ software.

1. Log on to the database host as root or as a user with root-level permissions.
2. Open a terminal window.
3. Enter the following command to change the directory to the mount point created:

```
cd MountPoint
```

4. Enter the following command to create a directory where you want to back up the database:

```
mkdir dbbackup
```

---

## Activating the backup feature

### About this task

#### **Warning:**

The database stops and restarts when you enable the backup feature.

### Procedure

1. Log on to the database host as root or a root-level user.
2. Open a terminal window.
3. To activate the database backup, enter:  

```
sh /avaya/bin/config_db_backup.sh
```
4. When prompted, select an option to reconfigure the database backup and perform the following:
  - Enter the location of the backup file system or storage array.
  - Select the start day of the week.
  - Enter the time of day when you want the backups to run.
5. Select **OK**.

#### **Note:**

After you activate the backup feature on the database host, you must verify the cron job for the database backup in the `/etc/cron.d` file. In earlier releases, you were able to view the details of the cron jobs installed using the `crontab -l` command. On the application hosts, you can still use the `crontab -l` command. However, on a turnkey database host, you must verify cron jobs from the `/etc/cron.d` file. Before you edit an existing cron job file, make a copy of the `cron.d` file so that you can revert to the original file if you experience any problems.

6. To activate the Avaya IQ system backup, enter:  

```
sh /avaya/bin/config_iq_backup.sh
```
  7. When prompted, select the option to reconfigure the Avaya IQ backup options. Answer the following questions:
    - Enter the location of the backup file system or storage array.
    - Select the start day of the week.
    - Enter the time of day when you want the backups to run.
  8. Select **OK**.
  9. Enter the following command on the database host to run the database diagnostic tool:  

```
sh /avaya/bin/db_diagnostic_mgr.sh
```

Verify that none of the menu options show an asterisk (\*). If any menu items show an asterisk, you should run the menu options to clear the problem. You can also use this tool to see the backup schedule. For more information about the database diagnostic tool, see [About database monitoring diagnostics](#) on page 35.
  10. Log on to the application host as root or a root-level user.
  11. To activate the Avaya IQ system backup, enter:  

```
sh /avaya/bin/config_iq_backup.sh
```
  12. When prompted, select the option to reconfigure the Avaya IQ backup options. Answer the following questions:
    - Enter the location of the backup file system or storage array.
    - Select the start day of the week.
    - Enter the time of day when you want the backups to run.
  13. Select **OK**.
  14. Repeats Steps 10 through 13 on every application host in the deployment.
- 

---

## Running an on-demand backup

Once you have enabled the backup feature, backups will run on a regular schedule. Should a condition occur where you need to run a backup on demand, use the procedures in this section. You can run a backup of the Avaya IQ system data on the All Functions host and you can run a backup of the system data and database data on the database host.

### Related topics:

[Running an on-demand system backup on an application host](#) on page 211

[Running an on-demand backup of system and database data on the database host](#) on page 211

## Running an on-demand system backup on an application host

### Procedure

1. Log on to your application host as root or a root-level user.
2. Enter the following command to remove the last backup file start a new backup:
 

```
sh /opt/Avaya/CCR/bin/runBackup.sh -bkploc BackupLocation -force
```

The variable *BackupLocation* is the mount point on the network drive where you want to back up the data.
3. Enter the following command to view the status of the backup:
 

```
tail -f /var/log/Avaya/CCR/backup/iqbackup.log
```
4. Transfer your backup files to a backup media such as a tape repository or disk repository.
5. Store the backup media in a safe location.
6. Repeat this procedure for every application host in your deployment.

---

### Related topics:

[Confirming a successful system data backup on an application host](#) on page 212

## Running an on-demand backup of system and database data on the database host

### Procedure

1. Log on to Linux on the database host as root or a root-level user.
2. Enter the following command on the database host to run the database diagnostic tool:
 

```
sh /avaya/bin/db_diagnostic_mgr.sh
```
3. From the main menu, select **f**. Oracle Backup Management.
4. From the next menu, select one of the following options:
 

```
a. RMAN Backups - Database
b. RMAN Backups - Archive logs
```

5. If the system displays the following menu the first time you run a backup after activating backups, select option d. Run a Fix:

```
a. Display Last Execution Results
b. Compare Last Two Execution Results
c. Run Detection
d. Run a Fix
e. View last backup

x. Exit
```

6. From the next menu, select one of the following options:

```
a. Initiate a full database backup
b. Initiate a incremental database backup
c. Initiate an archive log backup
```

7. Answer yes at the confirmation prompt.

8. Enter the following commands to manually back up the DBID and INITORA files:

```
a. cp /avaya/Avaya_IQ/services/env/DBID /<BackupLocation>
b. cp /avaya/Avaya_IQ/services/env/INITORA /<BackupLocation>
```

---

## Next steps

For more information, see [Confirming a successful database data backup on the database host](#) on page 213.

## Related topics:

[Confirming a successful system data backup on an application host](#) on page 212

[Confirming a successful database data backup on the database host](#) on page 213

---

# Confirming a successful system data backup on an application host

## About this task

For every system backup session, the system writes a message to the following log file on the All Functions host and the database host:

```
/var/log/Avaya/CCR/backup/iqbackup.log
```

The system backs up the Avaya IQ base software first and then the Avaya IQ software configuration data. Unless you upgrade or patch the base Avaya IQ or Oracle software, subsequent backups require only a backup of the configuration data. In this scenario, you will only find the second set of messages in the log file.

## Procedure

To confirm a successful backup, verify that the message was written using the following command:

```
more /var/log/Avaya/CCR/backup/iqbackup.log
```

The following is the first set of messages you should see when the backup starts and after it finishes:

```
backup started Timestamp
backup base to /BackupLocation
backup: backup image - /BackupLocation/
iq_base_HostName_092305_20080313.tar.gz
backup base completed Timestamp
```

The following is the second set of messages you should see when the backup starts and after it finishes:

```
backup data to /BackupLocation
backup: backup image - /BackupLocation/
iq_data_HostName_092713_20080313.tar.gz
backup data completed Timestamp
```

---

### Related topics:

[Running an on-demand system backup on an application host](#) on page 211

[Running an on-demand backup of system and database data on the database host](#) on page 211

---

## Confirming a successful database data backup on the database host

### Procedure

1. Enter the following command on the database host to run the database diagnostic tool:

```
sh /avaya/bin/db_diagnostic_mgr.sh
```

2. From the main menu, select **f**. Oracle Backup Management.
3. From the next menu, select one of the following options:

```
a. RMAN Backups - Database
b. RMAN Backups - Archive logs
```

4. From the next menu, select the following option:

```
e. View last backup
```

5. Answer yes at the confirmation prompt.

The following is an example of messages you see when the backup starts and after it finishes. The example does not include all the messages in between the start and finish messages:

```
Timestamp : /opt/Avaya/CCR/bin/db_backup.sh started
Timestamp : BackupType DB backup
. . . . .
. . . . .
Timestamp: /opt/Avaya/CCR/bin/db_backup.sh successfully finished.
```

6. To view a history of database backups, enter the following command:

```
more /avaya/Avaya_IQ/services/log/db_backup.log
```

---

**Related topics:**

[Running an on-demand backup of system and database data on the database host](#) on page 211

---

## Backing up custom reports

Custom reports are backed up during normal backup procedures. However, it is difficult to restore individual custom reports from these backups. To resolve this issue, you can use export tools developed for the High Availability feature to back up custom reports.

To back up custom reports, see “Exporting reports” in *Avaya IQ High Availability and Survivability*.

To restore backed up reports, see [Restoring custom reports](#) on page 225.

---

## Backing up Avaya IQ data on Windows

### Before you begin

- To allow file sharing between the Windows and the Linux machine, ensure that the firewall is OFF or if the firewall is ON, then firewall settings should be configured to allow file sharing.
- For database backup, specify the correct database OS user and group.
- Restart the database host after you have enabled the database backup.
- Mount the file system as cifs. The samba file system has a restriction of 2 GB per file.

### Procedure

1. Log on to the database and the Avaya IQ host as root or a user with root-level privileges.
2. To mount the Avaya IQ Turnkey Linux DVD on the Linux machine, enter:  

```
mount /dev/dvd /mnt
```
3. Copy the following RPMs from the Linux DVD to the database and the Avaya IQ hosts.
  - `libsmbclient-3.0.33-3.28.el5.x86_64.rpm`
  - `samba-common-3.0.33-3.28.el5.x86_64.rpm`

- samba-client-3.0.33-3.28.el5.x86\_64.rpm

- To install a fresh copy of samba RPMs on the database and Avaya IQ hosts, enter:  
rpm ivh <path of RPM> \*.rpm
- To upgrade the existing samba RPMs on the database and Avaya IQ hosts, enter:  
rpm -Uvh <path of RPM> \*.rpm

**\* Note:**

The RPMs should be installed in a sequential order as follows:

- libsmbclient-3.0.33-3.28.el5.x86\_64.rpm
- samba-common-3.0.33-3.28.el5.x86\_64.rpm
- samba-client-3.0.33-3.28.el5.x86\_64.rpm

- Log on to the Windows machine where you want to store the backup from the Linux machine.
- Create a local user on the Windows machine.
- Log out and log in to the Windows system using the local user's credentials.
- Assign the Windows local user with full control of the Windows shared drive.
- Share a local drive on Windows for backing up the Avaya IQ data.
- On the database host, enter the following commands:
  - To create a backup directory enter: `mkdir /backup`
  - To mount the Windows share drive, enter: `mount -t cifs //<Windows Server name/IP address>/<Windows shared directory name> /backup (backup directory created on Linux) -o username=(windows user name) test,uid=oracle,gid=oinstall.`
  - When the system prompts for password, enter the <Windows server password>
  - (Optional) Reboot the database host if the system displays any error message.
- On the Avaya IQ host, enter the following commands:
  - To create a backup directory, enter: `mkdir /backup`
  - To mount the Windows share drive, enter: `mount -t cifs //<Windows Server name/IP address>/<windows shared directory name> /backup (backup directory created on Linux) -o username=test.`
  - When the system prompts for password, enter the <Windows server password>
  - (Optional) Reboot the Avaya IQ host if the system displays any error message.

**\* Note:**

- If you use the Windows machine for permanent backups, the Avaya IQ system on Linux has to survive reboot to mount cifs. Therefore, you must add the following lines to the `/etc/fstab` file on Linux:

```
//windows_server/backup /backup cifs  
rw,user,username=window_user_name,uid=oracle,gid=oinstall,password  
=password 0 0
```

- To verify whether the lines that you have added in step 2 are correct, reboot the host and enter:

```
df -h
```

For more information about backing up the Avaya IQ data, see [Backing up Avaya IQ data in a turnkey deployment](#) in the Maintaining and Troubleshooting guide.

---



# Chapter 11: Restoring system and database data

---

## Reasons for restoring Avaya IQ

The typical reasons for doing a restore include:

- Recovering from disk failures, file system corruptions, or user errors when deleting files
- Recovering from host computer hardware failures when you must replace the old host computer with a new host computer
- Recovering from a failed upgrade to revert to the previous version of Avaya IQ.
- Recovering any of the following directories or files:
  - Avaya IQ directories
  - Critical system directories, such as `/var`, `/opt`, `/etc`, or `/u01`
  - Specific Avaya IQ files

---

## Overview of Avaya IQ data restores

An Avaya IQ data restore:

- Preserves all user information
- Preserves all passwords
- Uses the previous license

If you are restoring to new hardware, the previous license is valid until it expires. Generate the new license with the new MAC address for the new Administration or All Function host's Network Interface Controller (NIC).

- Connects to the same database host
- Applies to Single host, Dual host, or Multi-host deployments

---

## Restored directories and files

The procedures in this section use commands that restore entire contents of the following directories.

| Directory         | Restores                                                              |
|-------------------|-----------------------------------------------------------------------|
| /etc              | System wide configuration files                                       |
| /var/log          | Variable configuration information, log files, and system information |
| /opt/Avaya        | Avaya IQ files                                                        |
| /avaya            | Turnkey-related files                                                 |
| /opt/coreservices | Files that are common across Avaya products                           |
| \$ORACLE_HOME     | Oracle critical files                                                 |

### Related topics:

[Restoring Avaya IQ in a software-only deployment](#) on page 219

[Selectively restoring Avaya IQ files or directories](#) on page 224

---

## Prerequisites for restoring Avaya IQ data

Before beginning any restore procedure, you must fulfill the following prerequisites:

- Obtain recent full backups of the Avaya IQ data and the database data. See *Backing up system and database data* in this document. If you are restoring the system back to the previous version (rollback), you must have access to backups for that previous version of the product. Backups for two different versions must be stored in separate locations so that the data for one version is not confused with the data for another version.

### Caution:

As with any kind of restoration process, the restored system will only be as good as the most recent backups. If it has been a long time since the last full backup, there will be data loss between the time when the restore occurs and the time of the last full backup. There is no process to restore that lost data.

- Obtain an Avaya IQ license file that is valid for the release you want to restore.
- Determine the mount point for NFS backups. You must readminister the mount points after the upgrade.

- Determine the Oracle backup destination. Use the command `cat /avaya/Avaya_IQ/services/env/backup_location` for Avaya IQ 5.1.x and 5.2.x.
- For restores on a software-only system, obtain the CAT installation test outputs to validate the restore.
- For restores on a turnkey system, obtain the firmware and uEFI discs for the release you are restoring.

**⚠ Caution:**

If you have more than one backup saved, ensure that you use the most recent backup. If you restore the files and directories in an older backup version, your system can inadvertently revert to an old configuration.

---

## Restoring Avaya IQ and data for a software-only deployment

---

### RMAN

Recovery Manager (RMAN) is a utility provided by Oracle for backing up, restoring, and recovering Oracle databases. Before you read the procedures in this section, ensure that you have setup and configured RMAN and either know the tools and techniques for using it, or have access to the appropriate Oracle documentation.

---

### Restoring Avaya IQ in a software-only deployment

#### Before you begin

Complete the [prerequisites](#) on page 218.

#### About this task

Use this procedure to restore Avaya IQ under the following conditions:

- When you want to roll back to a previous version of the software.
- When the application host has a disk failure.
- When you replace the application host hardware with new hardware.

This procedure was tested with several server manufacturers and works if your hardware is supported by Red Hat Enterprise Linux 5.4 or later.

## Procedure

1. If an application host being replaced is still operational (that is, the host is being upgraded to a better server), disconnect the host from the network or shut it down to prevent IP address conflicts. The one exception to this rule is when you are replacing an Administration host or an All Functions host; there is no need to disconnect or shut down the host.

2. Install the operating system using the procedures documented by your operating system vendor.  
Verify that the system is fully operational with the same IP address and configuration as before.

3. Copy the tar file you saved during the backup procedure to the new application host.

You can copy the file using scp or removable media, or any storage location of backup files.

4. Enter the following commands to restore the files required for the configuration data:

```
cd /
```

```
tar -xzvf BackupDirectory/iq_base_HostName_TimeStamp.tar.gz
  */CAT/install.out" "*/CAT/dba.out" "*/CAT/hostinfo.out" "*/
  CAT/connection.out" "*/current.conf"
```

where *BackupDirectory* is the location of the backup files, *HostName* is the name of the host, and *TimeStamp* is the time stamp of the most recent backup.

5. Insert the *Avaya IQ Software Only* disc into the disc drive.

6. Enter the following commands to mount the disc drive:

```
mount /dev/cdrom /mnt
```

```
cd /mnt
```

7. Enter the following command to confirm that you will restore the proper version of Avaya IQ:

```
sh Avaya_IQ_Install.bin -version
```

For example, the Avaya IQ 5.1.1 should return the following value:

```
Version: 5.1.1.0.77_8019
```

8. Enter the following command to restore the Avaya IQ data:

```
sh /mnt/restore/runRestore.sh -bkploc BackupDirectory -
  binloc /mnt -license LicenseFileLocation
```

where:

- *BackupDirectory* is the location of the backup files. The backup directory must include both the *iq\_base* and *iq\_data.tar.gz* files.
- *LicenseFileLocation* is the full path to the license file, including the license file name. If you do not have a copy of the original license file, create

a zero-length file named `license.xml` to allow you to complete the restore. Later, you must install a valid license file.

The restore process will take from 15 to 45 minutes.

9. Enter the following commands to delete the contents in the `iks` directory:

```
cd $CCR_HOME/data
rm -rf iks
```

**\* Note:**

You must delete the contents in the `iks` directory to avoid corrupting Avaya IQ data.

10. Reboot the application host.  
From the console, kudzu checks for hardware changes. If there are no further hardware changes, the boot process continues. If there are hardware changes, kudzu prompts for more information.

After the reboot, Avaya IQ services should start and operate normally.

11. Enter the following command to confirm that you have restored the proper version of Avaya IQ:

```
cat /opt/Avaya/CCR/version.txt
```

For example, the Avaya IQ 5.1 should return the following value:

```
Version: 5.1.1.0.77_8019
```

12. Verify that Avaya IQ is operating normally by using the procedure *Confirming a valid installation and configuration* in *Implementing Avaya IQ*.

---

## Next steps

Reapply any patches, service packs or hot fixes that were installed since the original installation of the software.

If you are using NOLOGGING for your database, you must re-index the database after doing a database restore. Use your own scripts, or use the scripts shown in the following location on the application host:

- `/opt/Avaya/CCR/data/db/oracle/scripts/create_historical_index.sql`
- `/opt/Avaya/CCR/data/db/oracle/scripts/create_realtime_indexes.sql`

## Related topics:

[Restored directories and files](#) on page 218

---

## Recovering and restoring the database host

### Before you begin

Complete the [Prerequisites for restoring Avaya IQ data](#) on page 218.

### About this task

Use this procedure when your database host was destroyed and as a consequence, you have lost all your database files, which includes control files, logs, and data files.

### Procedure

1. Verify that the new database host has the same disk layout as the original so that you do not have to rename the files during recovery.
2. Verify that the new disks have enough space to hold all software and data that was on the original database host.
3. Verify that the operating system environment is the same as the original with the same service pack and patch levels.
4. Verify that the new database host has enough memory to support Oracle and the operating system, and that the Oracle memory structures - such as shared pool, DB buffer caches, and so on - are sized identically to the original database instance.
5. Restore the database backup from tape or storage media to disk.  
The preferred location is the flash recovery area. For example, `/u01/app/oracle/flash_recovery_area`.
6. Install Oracle.  
Install the same version of Oracle that was on the damaged database host. Ensure that the version number and patch configurations are identical. You might have to install one or more patch sets and patches.

#### Important:

Do not create a database. Instead, create a listener using the Network Configuration Assistant. Ensure that it has the same name and listening ports as the original listener. You can find relevant listener configuration information in the `listener.ora` file in the tar backup file.

7. After the Oracle installation is complete, create all directories required for data files, logs (online and archived), control files, and backups.  
Ensure that all directory paths match the paths on the original database host.  
For this step, you do not need to know where the database files are located. You can get this information from the backup spfile and control file later in this procedure.

8. Check the contents of the database initialization file for directories containing critical database files.

The database initialization file is in `$ORACLE_HOME/dbs/init<database instance>.ora`.

**! Important:**

These directories must exist to initialize and start the Avaya IQ database.

9. Create the Oracle service.
 

You must create an Oracle service before you create a database. Use the `oradim` utility from a command line to create the service using the following steps:

  - a. Run the Oracle startup script in `/etc/init.d/dbora`.  
Make sure that the script is executable.
  - b. Add the Oracle service.
  - c. Verify that the Oracle service exists and at which run levels.
10. From a backup file or by other means, you must recover and restore the following files:
  - `$ORACLE_HOME/dba/orapwDBName`
  - `$ORACLE_HOME/network/admin/tnsnames.ora`
11. Locate the database ID (DBID) from the control file.
 

The DBID is needed for subsequent steps and is in the control files.
12. Invoke RMAN and connect to the target database.
 

RMAN does not require login credentials because you are making a connection from an OS account that belongs to Oracle. For example, `su - oracle`.

RMAN accepts a connection to the database although the database is yet to be recovered as shown by the error messages in the following example.
13. Using RMAN commands, restore the spfile from the flash recovery area.
14. Using `sqlplus`, create directories for the control file and the archive destination from the spfile.
15. Using RMAN commands, restore the backup control files.
 

In the previous step, the control files were restored as listed in the `CONTROL_FILES` initialization parameter. This step restores the backup control files.
16. Shutdown the instance.
17. Restart the instance in mount mode.
 

A restart is required because the instance must re-read the initialization parameter file for control file locations. At the end of this step, RMAN also has proper configuration parameters that are stored in the control file.
18. Using `sqlplus`, create the location of the redo logs.

19. If you see directories in your output that you did not create earlier, using the SQL output from the previous example, manually create these directories now.
20. Using RMAN, restore all data files used for the Avaya IQ database.
21. Using RMAN commands, recover the Avaya IQ database.  
These commands also reset the logs.
22. Check your restored Avaya IQ environment.

---

## Selectively restoring Avaya IQ files or directories

The Avaya IQ backup scripts generate two compressed tar files:

- A base file that contains backups of `$CSBASE`, `$CCR_HOME`, and `$ORACLE_HOME`, plus some other Oracle-related files. The name of this file is `iq_base_<HostName>_<TimeStamp>.tar.gz`.
- A data file that contains backups of Avaya IQ files and backups of `/home` and `/etc`. The name of this file is `iq_data_<HostName>_<TimeStamp>.tar.gz`.

Use the procedures given in this section to restore files and directories selectively on an application host.

### **Caution:**

When you restore a file or a directory, the version you restore may be older than the version you replaced. This could cause data inconsistencies and Avaya IQ may not function properly.

### **Before you begin**

Complete the [prerequisites](#) on page 218.

### **Procedure**

1. Log on to the application host as root or a root-level user.
2. Copy the tar file you saved during the backup procedure to the application host where you want to restore the files or directories.  
You can copy the file using scp or removable media. Any temporary storage location for the backup files should have sufficient space.
3. To list the files that are contained in the “base” tar file, enter the following command:  

```
tar -tzvf iq_base_<HostName>_<TimeStamp>.tar.gz | more
```
4. Decide which files or directories you want to restore. For example, if you want to restore the `/opt/coreservices/scc/runtime/0789033a29347a880129347a951b001f.dat` file from the “base” tar file, enter the following command to restore that file:



```
tar -xzvf /u01/mnt/iq_base_<HostName>_<TimeStamp>.tar.gz -
C / "/opt/coreservices/scc/runtime/
0789033a29347a880129347a951b001f.dat"
```

5. To restore files from the “data” tar file, you must first extract the files to a temporary location. Enter the following commands to extract and list the files:

```
tar -xzvf /u01/mnt/iq_data_<HostName>_<TimeStamp>.tar.gz -
C /tmp "/etc.tar.gz"
cd /tmp/iq_data/
tar -tzvf etc.tar.gz | more
```

6. If you believe your `/etc/hosts` file has been corrupted, enter the following commands to restore that file:

```
cd /tmp/iq_data/
tar -tzvf etc.tar.gz "/etc/hosts"
```

---

#### Related topics:

[Restored directories and files](#) on page 218

---

## Restoring custom reports

To restore custom reports that you have backed up using the High Availability export tool, see “Importing reports” in *Avaya IQ High Availability and Survivability*.

---

## Restoring data on a turnkey deployment

This section describes how you can restore service or data on a turnkey system when the following occurs:

- The software database becomes corrupted or data has been lost.
- One or more disk drives fail on an application host, database host, or EXP3000 disk array.
- When the application host or database host computer fails and must be replaced.

#### ! Important:

These procedures do not describe how to recover from other hardware failures such as faulty network ports, video ports, and so on. See *Installing and Maintaining Avaya IQ Turnkey Hardware* or contact Avaya support for procedures on how to recover from those types of failures.

## Restore scenarios

This section describes the different restore scenarios that can happen for a turnkey system made up of Avaya S8800 Servers and IBM EXP3000 disk arrays. Since there is an application host and a database host, and there are several disk layouts, the restore scenarios require specific procedures. In a single host deployment, a single computer handles both application and database functions. Use the procedure(s) shown for each scenario. Replacement disks must be new, in a clean condition, and must be the same size as the original disks.

### ! Important:

If you need to restore both the application host and the database host, there is a timing issue for the application host that the database host must be operating normally before the application host can connect to the database host. That is, if you restore the application host before you restore the database host, the restore will fail on the application host.

| Scenario                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Procedure                                                                                                                                                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Data corruption or data loss has occurred                                                                                                                                                                                                                                                                                                                                                                                                                                            | <a href="#">Restoring data after a software failure</a> on page 228                                                                                                                                                                                                                                                                                 |
| Any one of the follow occurs: <ul style="list-style-type: none"> <li>• A single system disk fails on an Avaya S8800 application/database host in a single host deployment</li> <li>• A single system disk fails on an Avaya S8800 application host in a dual host or multi-host deployment</li> <li>• A single system disk fails on an Avaya S8800 database host in a dual host or multi-host deployment</li> <li>• A single data disk fails on an IBM EXP3000 disk array</li> </ul> | <a href="#">Installing replacement disks when a single disk fails</a> on page 231                                                                                                                                                                                                                                                                   |
| One or two mirrored pairs of system disks fail on an Avaya S8800 application/database host in a single host deployment                                                                                                                                                                                                                                                                                                                                                               | Do both of the following procedures, even if there are no failed disks on the EXP3000: <ul style="list-style-type: none"> <li>• <a href="#">Replacing one or more mirrored pairs of system disks on an application/database host in a single host deployment</a> on page 232</li> <li>• <a href="#">Restoring an EXP3000</a> on page 270</li> </ul> |
| One or two mirrored pairs of system disks fail on an Avaya S8800 application host in a dual host or multi-host deployment                                                                                                                                                                                                                                                                                                                                                            | <a href="#">Replacing both system disks on an Avaya IQ application host</a> on page 245                                                                                                                                                                                                                                                             |

| Scenario                                                                                                                                                      | Procedure                                                                                                                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| One or two mirrored pairs of system disks fail on an Avaya S8800 database host in a dual host or multi-host deployment                                        | Do both of the following procedures, even if there are no failed disks on the EXP3000: <ul style="list-style-type: none"> <li>• <a href="#">Replacing both system disks on The database host</a> on page 257</li> <li>• <a href="#">Restoring an EXP3000</a> on page 270</li> </ul> |
| One or more mirrored pairs of data disks fail on the EXP3000 disk array, or an EXP3000 disk array fails completely and the entire disk array must be replaced | <a href="#">Restoring an EXP3000</a> on page 270                                                                                                                                                                                                                                    |
| An Avaya S8800 application host or database host computer fails completely and must be replaced                                                               | <a href="#">Restoring a replacement S8800 host computer</a> on page 276                                                                                                                                                                                                             |
| You want to roll back to the previous version of Avaya IQ                                                                                                     | <a href="#">Restoring back to Avaya IQ 5.1.1</a> on page 280                                                                                                                                                                                                                        |

---

## Gathering recovery information

### Procedure

During system restores, you will need the networking information used during the original installation. There are several ways you can get this information:

- Gather the information from the First Boot worksheets that were completed during the original installation.
- In a multi-host deployment, you can use any of the hosts still operating to recover a subset of the networking information, such as the gateway, DNS, NTP server, and so on.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.

- Contact your IT department to obtain a listing of the IP addresses of the application and database hosts, and the setup of the network configuration.
-

---

## Restoring data after a software failure

Use the procedure in this section to restore database data when events like data corruption or data loss occur.

### Restoring the software base, system configuration data, and database data on a database host

To restore the system configuration data on the database host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in this procedure restore the software base and database data.

#### Before you begin

See the requirements shown in [Prerequisites for restoring Avaya IQ data](#) on page 218.

#### Procedure

1. Inform all of the Avaya IQ users to log off from the administration and reporting interfaces.
2. Log on to the database host as root or a root-level user. On a single host deployment, the database host is the same host as the All Functions host.
3. Mount the backup file system so you can access the backup files.
4. Enter:  

```
cd /
```
5. Enter the following command to restore the files required for the configuration data:  

```
tar -xzf <BackupDirectory>/  
iq_base_<HostName>_<TimeStamp>.tar.gz "*" /CAT/install.out "  
"*/CAT/dba.out" "*/CAT/hostinfo.out" "*/CAT/connection.out "  
"*/current.conf"
```

where *<BackupDirectory>* is the location of the backup files, *<HostName>* is the name of the host, and *<TimeStamp>* is the time stamp of the most recent backup.
6. Depending on your deployment, do one of the following:

- On a single host deployment, skip this step. The `db_restore.sh` script will automatically shut down the Avaya IQ software.
- On a dual host deployment, enter the following command on the All Functions host to shut down the Avaya IQ software:

```
service wdinit stop
```

- On a multi-host deployment, enter the following command on the Administration host and every Reporting host to shut down the Avaya IQ software:

```
service wdinit stop
```

7. Enter the following commands to restore the software base and database data:

```
cd /
sh /avaya/Oracle/db_restore.sh
```

8. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:

```
tail -f /var/log/Avaya/CCR/restore/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last
backup may not get recovered.
```

9. Enter the following commands to re-index the database; this procedure may take some time depending on the amount of traffic on the system:

```
cd /opt/Avaya/CCR/data/db/oracle/scripts
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_realtime_indexes.sql CCRRT
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_historical_index.sql CCR
```

10. Enter the following command to remove the turnkey installation user ID:

```
sh /avaya/bin/harden_security.sh
```

11. When the restore is complete, enter the following command to reboot the database host:

```
reboot
```

12. Log on to the All Functions or Administration host as root or a root-level user.

13. When re-indexing is complete, enter the following command on the database host to restart the Avaya IQ software:

```
service wdinit start
```

14. Depending on your deployment, do one of the following:

- On a single host deployment, enter the following command on the Data Collection hosts to start up the Avaya IQ software:

```
service wdninit start
```

- On a dual host deployment, enter the following command on the All Functions and Data Collection hosts to start up the Avaya IQ software:

```
service wdninit start
```

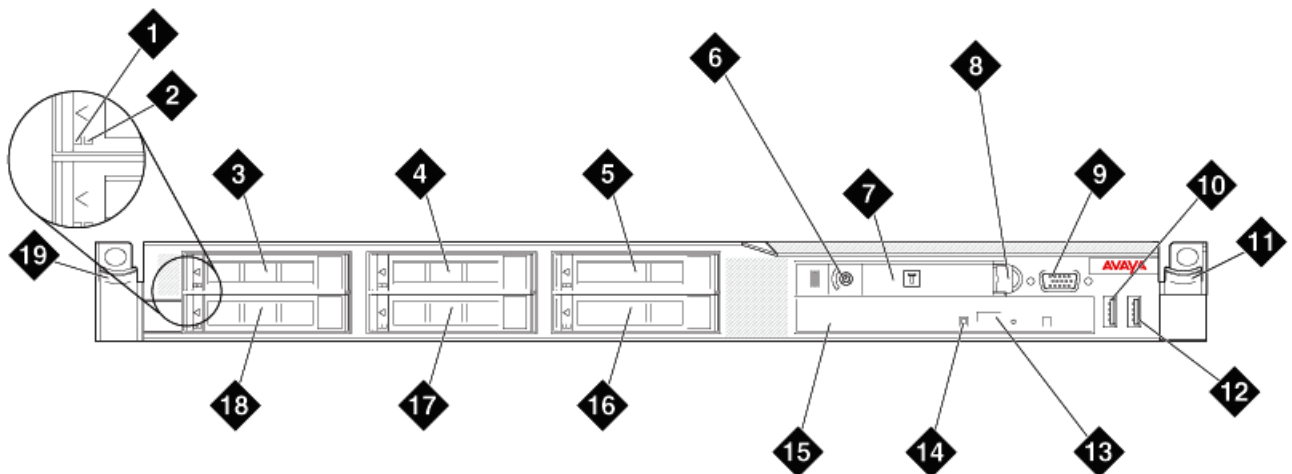
- On a multi-host deployment, enter the following command on every Data Collection, Data Processing, Reporting, and RTD hosts to start up the Avaya IQ software:

```
service wdninit start
```

## Disk layouts on Avaya S8800 and IBM EXP3000 turnkey systems

Before you can restore a turnkey system, you must understand how the disks are laid out on the turnkey system. The disks on a turnkey system are laid out as follows.

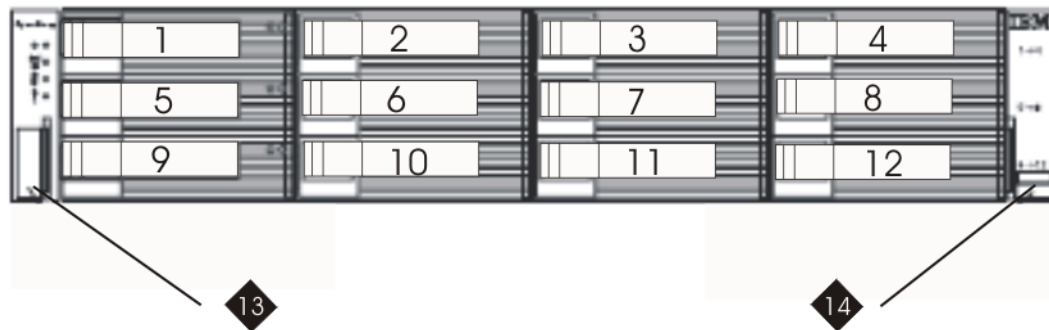
The Avaya S8800 Server used as an application host or database host has two pairs of system disks. The system disks are numbered 0 through 3. See the following diagram for the disk drive layout.



hw881fn LAO 092209

|          |                                            |
|----------|--------------------------------------------|
| 3 and 18 | Disk drives 0 and 1 (mirrored pair 1)      |
| 4 and 17 | Disk drives 2 and 3 (mirrored pair 2)      |
| 5 and 16 | Disk bays 4 and 5 (not used with Avaya IQ) |

The IBM EXP3000 disk array database storage has six pairs of storage disks. These data disks are numbered 1 through 12. See the following diagram for the disk drive layout.



|                 |                 |
|-----------------|-----------------|
| Disks 1 and 2   | Mirrored pair 1 |
| Disks 3 and 4   | Mirrored pair 2 |
| Disks 5 and 6   | Mirrored pair 3 |
| Disks 7 and 8   | Mirrored pair 4 |
| Disks 9 and 10  | Mirrored pair 5 |
| Disks 11 and 12 | Mirrored pair 6 |

## Installing replacement disks when single disks in a mirrored pair fails

### About this task

When only one disk in a pair of system or data disks fails, you can remove and replace the one failed disk without any special recovery procedures. When the single disk is replaced, the operating system automatically synchronizes the replacement disk with the mirrored disk that is operating properly.

If multiple single disks fail, you can still replace each single disk one at a time, again without any special recovery procedures.

### Procedure

1. Do not turn the system off.  
This procedure can be done with the system operating.
2. Identify the faulty disk drive(s). Faulty disk drives can be identified by the amber flashing LEDs. If the disk drive is operating normally, the LED is green.
3. Remove the faulty disk drive.

**⚠ Caution:**

Since the disk drives are very close together, make sure that you are removing the disk that is faulty, and not the disk that is operating normally. Should you accidentally remove the non-faulty disk from a disk pair, you must treat this repair as if a pair of mirrored disks failed. Depending on whether the accident occurred on an application host, database host, or an EXP3000, see the procedures in the following sections:

- [Replacing one or more mirrored pairs of system disks on an application host in a dual host or multi-host deployment](#) on page 245
  - [Replacing one or more mirrored pairs of system disks on the database host in a dual host or multi-host deployment](#) on page 257
  - [Restoring an EXP3000](#) on page 270
4. Insert the replacement disk drive.  
The system automatically synchronizes the replacement disk.
  5. Repeat this procedure for any other single disks that have failed.

---

## Replacing one or more mirrored pairs of system disks on an application/database host in a single host deployment

Should one or more mirrored pairs of system disks fail on an application/database host in a single host deployment, you must do the following procedures shown in this section:

- Rebuild the system disks on the host
- Install the OS, Oracle, and Avaya IQ, and run Linux First Boot on the host
- Install the Oracle software on the database host
- Install the Oracle client software on the application hosts
- Set the backup mount point on the host
- Restore the software base, system configuration data, and database data on the database host
- Update the RTD properties file

## Rebuilding the system disks on an application or database host

### Before you begin

For detailed disk replacement procedures on an application or database host, see *Installing and Maintaining Avaya IQ Turnkey Hardware*.

Obtain the *S8800 Avaya IQ 5.2 Firmware Updates* and *S8800 Avaya IQ 5.2 uEFI Setting Tools* discs.



Obtain a USB keyboard, USB mouse, and VGA monitor to connect to the front panel of the host being updated.

## Procedure

1. Log on to each application host in the deployment as root or a root-level user.
2. Enter the following command to shut down the host:  

```
shutdown now
```
3. Turn off the power on the host.
4. Insert one or more pairs of replacement system disks.
5. Turn on the power to the host.
6. Insert the *S8800 Avaya IQ 5.2 Firmware Updates* disc into the disc drive.
7. Enter the following command to reboot the application host:

```
reboot
```

You will see the following types of messages:

- Shutdown messages
- System initializing messages
- IBM System X messages
- Controller messages
- Running inventory

8. When the following message is displayed, enter 1 after the prompt:  

```
Enter the item number to Updates| ("q" to quit ToolsCenter):
```
9. When the following message is displayed, enter *y* after the prompt:  

```
Do you want to start it now? Y(yes)/N(no)/Q(quit)
```

You will see the following types of messages:

- Extracting...
- Executing...
- Initializing, Please Wait...
- Messages displaying which firmware will be updated.

10. Either wait 60 seconds for the update to start, or press *A* to start the update immediately.  
 The updates begin to load. It will take from 30 to 40 minutes on each host. When the updates are finished, a list of the updates is displayed.
11. Enter *Q* to quit the update program.
12. Enter *Yes* and *q* again.

The host reboots and automatically changes the factory firmware settings to the proper Avaya IQ firmware settings.

13. While the system is rebooting, remove the disc from the disc drive and insert the *S8800 Avaya IQ 5.2 uEFI Setting Tools* disc into the disc drive.  
After the system reboots, the factory uEFI settings are changed to the Avaya IQ uEFI settings.
  14. When the update is finished, press Enter to continue.  
The disc is automatically ejected.
  15. After the disc ejects, remove the disc and press Enter to continue.  
The system reboots.
  16. Insert the *S8800 IQ 5.2 MR10/MR10M RAID Tools* disc into the application host disc drive.
  17. Enter the following command to reboot the host:  

```
reboot
```

On boot up, the RAID utility performs an inventory of storage devices attached to the database host. A menu appears showing two options:

    - Host
    - EXP3000
  18. Select option 1, Host.  
The RAID tools automatically configures the system disks with RAID 10.
  19. Remove the disc from the database host disc drive.
  20. Review the output displayed on the console to verify that no errors appear or are reported.  
A menu will prompt you to exit the program.
- 

## Installing the OS, Oracle, and Avaya IQ, and running First Boot on an application or database host

### Procedure

1. Insert the *Avaya IQ 5.2 Linux* disc into the disc drive.
2. Enter the following command to reboot the host:  

```
reboot
```

The host reboots. A Red Hat banner page displays the instructions for running the kickstart program.
3. Enter `ks`.

Several messages are displayed. The console screen will turn blue for a while, then more messages are displayed. This process takes about 45 minutes.

4. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Linux* disc, and replace it with the *Avaya IQ 5.2 Oracle* disc.  
The system starts up automatically and the Oracle database software is copied from the disc to the host. After about 45 minutes, a message requesting a reboot is displayed.
5. Remove the disc after the system ejects the disc.
6. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Oracle* disc, and replace it with the *Avaya IQ 5.2 Software* disc.  
The system starts up automatically and the Avaya IQ software is copied from the disc to the host. After about 15 minutes, a message requesting a reboot is displayed.
7. Remove the disc after the system ejects the disc.
8. Press `Enter` to reboot.
9. Monitor the messages.  
All messages except for `smartd` and `NFS statd` must show `OK`.  
The system displays the Welcome page
10. Click **Forward**.  
The system displays the License Agreement page.
11. Accept the license agreement.
12. Click **Forward**.  
The system displays the Keyboard page.
13. Select the appropriate keyboard language for the system. The default is U.S. English.  
You must use a USB keyboard.
14. Click **Forward**.  
The system displays the Root Password page to set the root password for the system.
15. Set the root password (must be six characters).  
**!** **Important:**  
You can use the root ID and password to log on to the server with root permissions. Root permissions have the highest and least restrictive privileges. Any knowledge of this password must be controlled and shared with only the customer and provisioning personnel.
16. Click **Forward**.  
The system displays the Network Setup page.
17. Click **Change Network Configuration....**

**\* Note:**

When administering the networking options, it is possible that the networking dialog box can disappear from the display and the Change Network Configuration... dialog box can be active. If this happens, press **Alt+Tab** to switch the networking dialog box to the front of the display.

18. Click the **Devices** tab.

19. Select the **eth0** check box. Ensure that the **Eth0** line is highlighted.

**! Important:**

Do not disable USB0 since it is used by the Integrated Manager Module (IMM).

20. Click **Edit**.

**\* Note:**

Use the information collected on the *First Boot installation worksheet for networking* to complete the following steps.

21. Click the **General** tab.

Perform the following tasks:

- Select the **Activate device when computer starts** check box.
- Click **Statically set IP addresses**.
- Enter the IP address, subnet mask, and default gateway address for the host.

22. Click **OK**.

23. Click the **DNS** tab.

Provide the following information:

- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the fully qualified domain name (FQDN), for example, *HostName.DomainName.com*.
- **Primary, Secondary, and Tertiary DNS server IP address:** Indicates the primary, secondary, and tertiary server addresses. You must enter the primary DNS server IP address and, if applicable, the secondary and tertiary DNS server IP addresses.
- **DNS search path:** Indicates the DNS search path, which is your DNS domain name. For example, *DomainName.com*.

24. Click the **Hosts** tab.

25. Click **New**.

26. Provide the following information:

- **Address:** Indicates the IP address of the host.
- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the fully qualified domain name (FQDN), for example, *HostName.DomainName.com*.
- **Alias:** Indicates the short version of the fully qualified domain name of the host. For example, if the fully qualified domain name is *IQone.company.com*, then the alias is *IQone*.

27. Click **OK**.
28. Click **New**.
29. Click **OK**.  
The system saves the network configuration.
30. Click the **Devices** tab.
31. Select the **eth0** check box.
32. Click **Activate**.
33. Click **Yes**.
34. Click **OK**.
35. Ensure that the system status shows `eth0` as `active`.
36. Choose **File > Save**.  
The system saves the network configuration information.
37. Click **OK** when the system prompts to confirm the changes.
38. Choose **File > Quit**.  
The network setup shows `eth0` has a `static` boot protocol.
39. Click **Forward**.  
The system displays the Firewall page.
40. Select the security level.  
Avaya requires that you select **wwwhttp**, **wwwhttps**, and **ssh** as trusted services.
41. Click **Forward**.
42. Click **Yes** to accept the security level settings.
43. Ensure that **SELinux - Disabled** is selected.
44. Click **Forward**.  
The system displays the Time Zone page.
45. Click **Yes**.

The system confirms the settings and restarts the system after the First Boot process is complete.

46. Select the appropriate time zone.

47. Click **Forward**.

The system displays the Date and Time page.

48. Select the appropriate date and time.

49. Click the **Network Time Protocol** tab.

50. Select **Enable Network Time Protocol**.

51. Delete all the default NTP servers in the NTP server list.

52. Click **Add**.

53. Enter the IP address or the fully qualified server name of the NTP server for the network.

54. Click **Forward**.

The system checks for the NTP server connection.

 **Caution:**

Do not continue if the NTP server connection check is unsuccessful. An NTP server is required for Avaya IQ installation. The Avaya IQ installation fails if an NTP server is not available. Find the correct NTP server information and repeat steps 43 through 59, or configure your NTP server so that it is working properly.

55. If prompted, click **Configure** to set up your monitor.

Select the options that best fit the monitor hardware.

56. Click **Forward**.

The system displays the Set Up Software Updates page.

57. Click **Forward**.

The system displays a warning message about adding users. Ignore this message and continue with the installation.

58. Click **Continue**.

59. Click **Forward**.

The system displays the Sound Card page.

60. Click **Forward**.

The system displays the Additional CDs page.

61. Click **Finish**.

62. Click **OK** on the reboot dialog.

---

## Installing the Oracle software on the database host

### Procedure

1. Log on to the database host as root. For a single host deployment, this is the same host as the application host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:
 

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language               | Locale      |
|------------------------|-------------|
| Simplified Chinese     | zh_CN.UTF-8 |
| English US             | en_US.UTF-8 |
| French                 | fr_FR.UTF-8 |
| German                 | de_DE.UTF-8 |
| Italian                | it_IT.UTF-8 |
| Japanese               | ja_JP.UTF-8 |
| Korean                 | ko_KR.UTF-8 |
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where `<locale>` is a variable from the table:
 

```
LANG=<locale>; export LANG
```
  - d. Save and close the file.
  - e. Enter:
 

```
echo $LANG
```

Verify that the desired language variable is displayed.
4. Enter the following commands to install the database software and create the database:
 

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Recover DBHostIPAddress  
DBHostName &
```

where *DBHostIPAddress* is the IP address for the database host and *DBHostName* is the hostname (FQDN) of the database host.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

---

## Installing the Oracle client software on the application hosts

The Oracle client software must be installed on the Administration and Reporting hosts in a multi-host deployment, and on the All Functions host in a single or dual host deployment.

### Procedure

1. Log on to the Administration or All Functions host as root. In a single host deployment, the All Functions host is the same as the Database host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language           | Locale      |
|--------------------|-------------|
| Simplified Chinese | zh_CN.UTF-8 |
| English US         | en_US.UTF-8 |
| French             | fr_FR.UTF-8 |



| Language               | Locale      |
|------------------------|-------------|
| German                 | de_DE.UTF-8 |
| Italian                | it_IT.UTF-8 |
| Japanese               | ja_JP.UTF-8 |
| Korean                 | ko_KR.UTF-8 |
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where <locale> is a variable from the table:

```
LANG=<locale>; export LANG
```

- d. Save and close the file.

- e. Enter:

```
echo $LANG
```

Verify that the desired language variable is displayed.

4. Enter the following commands to install the database client software:

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Client DBHostIPAddress  
DBHostName&
```

where *DBHostIPAddress* is the IP address of the database host and *DBHostName* is the host name (FQDN) of the database host.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

6. Repeat this procedure on all Reporting hosts.

## Verifying the backup mount point on an application and database host

### About this task

You must enable backups for the Avaya IQ software and data on a mountable network drive or storage array. Ensure that you can gain access to this network drive or storage array from all hosts in the Avaya IQ deployment. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

To verify that you enabled the portmap service for the NFS mount point:

### Procedure

1. Log on to the application or database host as root or a root-level user.
2. Enter the following command to check if the portmap service is running:

```
service portmap status
```

You see the following response:

```
portmap (pid xxxx) is running...
```

Where xxxx is the pid number.

3. If the portmap service is not functional, enter:  

```
service portmap start
```
4. Verify that the proper permissions are set on the NFS mount point server.
5. Repeat this procedure on all hosts.

---

### Related topics:

[Restoring the software base and system configuration data on an application host](#) on page 254

## Restoring the software base, system configuration data, and database data on a database host

To restore the system configuration data on the database host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in this procedure restore the software base and database data.

## Before you begin

See the requirements shown in [Prerequisites for restoring Avaya IQ data](#) on page 218.

## Procedure

1. Inform all of the Avaya IQ users to log off from the administration and reporting interfaces.
2. Log on to the database host as root or a root-level user. On a single host deployment, the database host is the same host as the All Functions host.
3. Mount the backup file system so you can access the backup files.
4. Enter:
 

```
cd /
```
5. Enter the following command to restore the files required for the configuration data:
 

```
tar -xzvf <BackupDirectory>/
iq_base_<HostName>_<TimeStamp>.tar.gz */CAT/install.out "
*/CAT/dba.out" */CAT/hostinfo.out" */CAT/connection.out "
*/current.conf"
```

where *<BackupDirectory>* is the location of the backup files, *<HostName>* is the name of the host, and *<TimeStamp>* is the time stamp of the most recent backup.
6. Depending on your deployment, do one of the following:
  - On a single host deployment, skip this step. The `db_restore.sh` script will automatically shut down the Avaya IQ software.
  - On a dual host deployment, enter the following command on the All Functions host to shut down the Avaya IQ software:
 

```
service wdninit stop
```
  - On a multi-host deployment, enter the following command on the Administration host and every Reporting host to shut down the Avaya IQ software:
 

```
service wdninit stop
```
7. Enter the following commands to restore the software base and database data:
 

```
cd /
sh /avaya/Oracle/db_restore.sh
```
8. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:
 

```
tail -f /var/log/Avaya/CCR/restore/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last
backup may not get recovered.
```

9. Enter the following commands to re-index the database; this procedure may take some time depending on the amount of traffic on the system:

```
cd /opt/Avaya/CCR/data/db/oracle/scripts
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_realtime_indexes.sql CCRRT
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_historical_index.sql CCR
```

10. Enter the following command to remove the turnkey installation user ID:  

```
sh /avaya/bin/harden_security.sh
```
11. When the restore is complete, enter the following command to reboot the database host:  

```
reboot
```
12. Log on to the All Functions or Administration host as root or a root-level user.
13. When re-indexing is complete, enter the following command on the database host to restart the Avaya IQ software:  

```
service wdinit start
```
14. Depending on your deployment, do one of the following:

- On a single host deployment, enter the following command on the Data Collection hosts to start up the Avaya IQ software:

```
service wdinit start
```

- On a dual host deployment, enter the following command on the All Functions and Data Collection hosts to start up the Avaya IQ software:

```
service wdinit start
```

- On a multi-host deployment, enter the following command on every Data Collection, Data Processing, Reporting, and RTD hosts to start up the Avaya IQ software:

```
service wdinit start
```

---

## Updating the RTD properties file

After a restore, the RTD properties file may not be configured properly with the IP address of the All Functions or Administration host. Use this procedure to update the RTD properties file

### Procedure

1. Enter:

```
cd /opt/Avaya/CCR/RTD/tomcat/apache-tomcat-5.5.27/webapps/
RTD/conf/
```

2. Create a backup copy of the RTD properties file using the following command:

```
cp rtd.properties rtd.properties.orig
```

3. Open the RTD properties file for editing:

```
vi rtd.properties
```

4. Replace the string `ADMINHOST_IPADDRESS` with the IP address of the All Functions or Administration host.

5. Save and close the file:

```
:wq!
```

6. Copy the Admin Tomcat crossdomain.xml file using the following command:

```
cp /opt/coreservices/tomcat-5.5.27/webapps/ROOT/
crossdomain.xml /opt/Avaya/CCR/RTD/tomcat/apache-
tomcat-5.5.27/webapps/ROOT
```

7. Restart RTD using the following command:

```
/opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

---

## Next steps

Continue with the following procedures:

- If you replaced a pair of disks on the database host, follow the procedures in [Restoring an EXP3000](#) on page 270. If you only replaced a pair of disks in an application host, you do not have to restore the EXP3000.
- Reapply any patches, service packs, or hot fixes that were installed since the original installation of the software.
- [Confirming a successful restore](#) on page 276

---

## Replacing one or more mirrored pairs of system disks on an application host in a dual host or multi-host deployment

Should one or more mirrored pairs of system disks fail on an application host in a dual host or multi-host deployment, you must do the following procedures shown in this section:

- Rebuild the system disks on the application host
- Install the OS, Oracle, and Avaya IQ, and run Linux First Boot on the application host
- Install the Oracle client software on the application host
- Set the backup mount point on the host

- Restore the software base and system configuration data on the application host
- Update the RTD properties file

## Rebuilding the system disks on an application or database host

### Before you begin

For detailed disk replacement procedures on an application or database host, see *Installing and Maintaining Avaya IQ Turnkey Hardware*.

Obtain the *S8800 Avaya IQ 5.2 Firmware Updates* and *S8800 Avaya IQ 5.2 uEFI Setting Tools* discs.

Obtain a USB keyboard, USB mouse, and VGA monitor to connect to the front panel of the host being updated.

### Procedure

1. Log on to each application host in the deployment as root or a root-level user.
2. Enter the following command to shut down the host:  

```
shutdown now
```
3. Turn off the power on the host.
4. Insert one or more pairs of replacement system disks.
5. Turn on the power to the host.
6. Insert the *S8800 Avaya IQ 5.2 Firmware Updates* disc into the disc drive.
7. Enter the following command to reboot the application host:  

```
reboot
```

You will see the following types of messages:

- Shutdown messages
- System initializing messages
- IBM System X messages
- Controller messages
- Running inventory

8. When the following message is displayed, enter `1` after the prompt:  

```
Enter the item number to Updates| ("q" to quit ToolsCenter):
```
9. When the following message is displayed, enter `y` after the prompt:  

```
Do you want to start it now? Y(yes)/N(no)/Q(quit)
```

You will see the following types of messages:

- Extracting...

- Executing...
  - Initializing, Please Wait...
  - Messages displaying which firmware will be updated.
10. Either wait 60 seconds for the update to start, or press **A** to start the update immediately.  
The updates begin to load. It will take from 30 to 40 minutes on each host. When the updates are finished, a list of the updates is displayed.
  11. Enter **Q** to quit the update program.
  12. Enter **Yes** and **q** again.  
The host reboots and automatically changes the factory firmware settings to the proper Avaya IQ firmware settings.
  13. While the system is rebooting, remove the disc from the disc drive and insert the *S8800 Avaya IQ 5.2 uEFI Setting Tools* disc into the disc drive.  
After the system reboots, the factory uEFI settings are changed to the Avaya IQ uEFI settings.
  14. When the update is finished, press **Enter** to continue.  
The disc is automatically ejected.
  15. After the disc ejects, remove the disc and press **Enter** to continue.  
The system reboots.
  16. Insert the *S8800 IQ 5.2 MR10/MR10M RAID Tools* disc into the application host disc drive.
  17. Enter the following command to reboot the host:  

```
reboot
```

  
On boot up, the RAID utility performs an inventory of storage devices attached to the database host. A menu appears showing two options:
    - Host
    - EXP3000
  18. Select option 1, **Host**.  
The RAID tools automatically configures the system disks with RAID 10.
  19. Remove the disc from the database host disc drive.
  20. Review the output displayed on the console to verify that no errors appear or are reported.  
A menu will prompt you to exit the program.
-

## Installing the OS, Oracle, and Avaya IQ, and running First Boot on an application or database host

### Procedure

1. Insert the *Avaya IQ 5.2 Linux* disc into the disc drive.
2. Enter the following command to reboot the host:  
`reboot`  
The host reboots. A Red Hat banner page displays the instructions for running the kickstart program.
3. Enter `ks`.  
Several messages are displayed. The console screen will turn blue for a while, then more messages are displayed. This process takes about 45 minutes.
4. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Linux* disc, and replace it with the *Avaya IQ 5.2 Oracle* disc.  
The system starts up automatically and the Oracle database software is copied from the disc to the host. After about 45 minutes, a message requesting a reboot is displayed.
5. Remove the disc after the system ejects the disc.
6. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Oracle* disc, and replace it with the *Avaya IQ 5.2 Software* disc.  
The system starts up automatically and the Avaya IQ software is copied from the disc to the host. After about 15 minutes, a message requesting a reboot is displayed.
7. Remove the disc after the system ejects the disc.
8. Press `Enter` to reboot.
9. Monitor the messages.  
All messages except for `smartd` and `NFS statd` must show `OK`.  
The system displays the Welcome page
10. Click **Forward**.  
The system displays the License Agreement page.
11. Accept the license agreement.
12. Click **Forward**.  
The system displays the Keyboard page.
13. Select the appropriate keyboard language for the system. The default is U.S. English.  
You must use a USB keyboard.



14. Click **Forward**.

The system displays the Root Password page to set the root password for the system.

## 15. Set the root password (must be six characters).

**!** **Important:**

You can use the root ID and password to log on to the server with root permissions. Root permissions have the highest and least restrictive privileges. Any knowledge of this password must be controlled and shared with only the customer and provisioning personnel.

16. Click **Forward**.

The system displays the Network Setup page.

17. Click **Change Network Configuration...****\*** **Note:**

When administering the networking options, it is possible that the networking dialog box can disappear from the display and the Change Network Configuration... dialog box can be active. If this happens, press **Alt+Tab** to switch the networking dialog box to the front of the display.

18. Click the **Devices** tab.19. Select the **eth0** check box. Ensure that the **Eth0** line is highlighted.**!** **Important:**

Do not disable USB0 since it is used by the Integrated Manager Module (IMM).

20. Click **Edit**.**\*** **Note:**

Use the information collected on the *First Boot installation worksheet for networking* to complete the following steps.

21. Click the **General** tab.

Perform the following tasks:

- Select the **Activate device when computer starts** check box.
- Click **Statically set IP addresses**.
- Enter the IP address, subnet mask, and default gateway address for the host.

22. Click **OK**.23. Click the **DNS** tab.

Provide the following information:

- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the

fully qualified domain name (FQDN), for example,  
*HostName.DomainName.com*.

- **Primary, Secondary, and Tertiary DNS server IP address:** Indicates the primary, secondary, and tertiary server addresses. You must enter the primary DNS server IP address and, if applicable, the secondary and tertiary DNS server IP addresses.
- **DNS search path:** Indicates the DNS search path, which is your DNS domain name. For example, *DomainName.com*.

24. Click the **Hosts** tab.

25. Click **New**.

26. Provide the following information:

- **Address:** Indicates the IP address of the host.
- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the fully qualified domain name (FQDN), for example,  
*HostName.DomainName.com*.
- **Alias:** Indicates the short version of the fully qualified domain name of the host. For example, if the fully qualified domain name is *IQone.company.com*, then the alias is *IQone*.

27. Click **OK**.

28. Click **New**.

29. Click **OK**.

The system saves the network configuration.

30. Click the **Devices** tab.

31. Select the **eth0** check box.

32. Click **Activate**.

33. Click **Yes**.

34. Click **OK**.

35. Ensure that the system status shows `eth0` as `active`.

36. Choose **File > Save**.

The system saves the network configuration information.

37. Click **OK** when the system prompts to confirm the changes.

38. Choose **File > Quit**.

The network setup shows `eth0` has a `static` boot protocol.

39. Click **Forward**.  
The system displays the Firewall page.
40. Select the security level.  
Avaya requires that you select **wwwhttp**, **wwwhttps**, and **ssh** as trusted services.
41. Click **Forward**.
42. Click **Yes** to accept the security level settings.
43. Ensure that **SELinux - Disabled** is selected.
44. Click **Forward**.  
The system displays the Time Zone page.
45. Click **Yes**.  
The system confirms the settings and restarts the system after the First Boot process is complete.
46. Select the appropriate time zone.
47. Click **Forward**.  
The system displays the Date and Time page.
48. Select the appropriate date and time.
49. Click the **Network Time Protocol** tab.
50. Select **Enable Network Time Protocol**.
51. Delete all the default NTP servers in the NTP server list.
52. Click **Add**.
53. Enter the IP address or the fully qualified server name of the NTP server for the network.
54. Click **Forward**.  
The system checks for the NTP server connection.  
  
**⚠ Caution:**  
Do not continue if the NTP server connection check is unsuccessful. An NTP server is required for Avaya IQ installation. The Avaya IQ installation fails if an NTP server is not available. Find the correct NTP server information and repeat steps 43 through 59, or configure your NTP server so that it is working properly.
55. If prompted, click **Configure** to set up your monitor.  
Select the options that best fit the monitor hardware.
56. Click **Forward**.  
The system displays the Set Up Software Updates page.
57. Click **Forward**.

The system displays a warning message about adding users. Ignore this message and continue with the installation.

58. Click **Continue**.
  59. Click **Forward**.  
The system displays the Sound Card page.
  60. Click **Forward**.  
The system displays the Additional CDs page.
  61. Click **Finish**.
  62. Click **OK** on the reboot dialog.
- 

## Installing the Oracle client software on the application hosts

The Oracle client software must be installed on the Administration and Reporting hosts in a multi-host deployment, and on the All Functions host in a single or dual host deployment.

### Procedure

1. Log on to the Administration or All Functions host as root. In a single host deployment, the All Functions host is the same as the Database host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:  

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language           | Locale      |
|--------------------|-------------|
| Simplified Chinese | zh_CN.UTF-8 |
| English US         | en_US.UTF-8 |
| French             | fr_FR.UTF-8 |
| German             | de_DE.UTF-8 |
| Italian            | it_IT.UTF-8 |
| Japanese           | ja_JP.UTF-8 |
| Korean             | ko_KR.UTF-8 |

| Language               | Locale      |
|------------------------|-------------|
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where <locale> is a variable from the table:

```
LANG=<locale>; export LANG
```

- d. Save and close the file.

- e. Enter:

```
echo $LANG
```

Verify that the desired language variable is displayed.

4. Enter the following commands to install the database client software:

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Client DBHostIPAddress  
DBHostName&
```

where *DBHostIPAddress* is the IP address of the database host and *DBHostName* is the host name (FQDN) of the database host.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

6. Repeat this procedure on all Reporting hosts.

## Verifying the backup mount point on an application and database host

### About this task

You must enable backups for the Avaya IQ software and data on a mountable network drive or storage array. Ensure that you can gain access to this network drive or storage array from all hosts in the Avaya IQ deployment. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

To verify that you enabled the portmap service for the NFS mount point:

## Procedure

1. Log on to the application or database host as root or a root-level user.
2. Enter the following command to check if the portmap service is running:  

```
service portmap status
```

You see the following response:

```
portmap (pid xxxx) is running...
```

Where xxxx is the pid number.
3. If the portmap service is not functional, enter:  

```
service portmap start
```
4. Verify that the proper permissions are set on the NFS mount point server.
5. Repeat this procedure on all hosts.

---

### Related topics:

[Restoring the software base and system configuration data on an application host](#) on page 254

## Restoring the software base and system configuration data on an application host

To restore the system configuration data on an S8800 application host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in the procedure restore the software base.

### Before you begin

During the replacement of a failed Administration or All Functions host, the MAC address of the server will change. When this happens, you must also obtain and install a new license file for the deployment.

### About this task

#### Important:

Remember to perform this restore on all application hosts in the deployment.

## Procedure

1. Inform all of the Avaya IQ users to log off from the administration and reporting interfaces.
2. Log on to the application host as root or a root-level user.
3. Mount the backup file system so you can access the backup files.
4. Enter:
 

```
cd /
```
5. Enter the following command to restore the files required for the configuration data:
 

```
tar -xzvf BackupDirectory/iq_base_HostName_TimeStamp.tar.gz
  */CAT/install.out" "*/CAT/dba.out" "*/CAT/hostinfo.out" "*/
  CAT/connection.out" "*/current.conf"
```

where *BackupDirectory* is the location of the backup files, *HostName* is the name of the host, and *TimeStamp* is the time stamp of the most recent backup.
6. Insert the *Avaya IQ Software Only* disc into the disc drive.
7. Enter the following commands to mount the disc drive:
 

```
mount /dev/cdrom /mnt
cd /mnt
```
8. Enter the following command to confirm that you will restore the proper version of Avaya IQ:
 

```
sh Avaya_IQ_Install.bin -version
```

For example, the Avaya IQ 5.2 should return a value similar to the following:

```
Version: 5.2.0.0.xxx_yyyy
```
9. Enter the following command to restore the Avaya IQ data:
 

```
sh /mnt/restore/runRestore.sh -bkploc BackupDirectory -
  binloc /mnt -license LicenseFileLocation
```

where:

  - *BackupDirectory* is the location of the backup files. The backup directory must include both the *iq\_base* and *iq\_data.tar.gz* files.
  - *LicenseFileLocation* is the full path to the license file, including the license file name. If you do not have a copy of the original license file, create a zero-length file named *license.xml* to allow you to complete the restore. Later, you must install a valid license file.

The restore process will take from 15 to 45 minutes.
10. Enter `cd $CCR_HOME/data`
11. Enter `rm -rf iks` to delete the contents in the *iks* directory.

**\* Note:**

You must delete the contents in the `iks` directory to avoid corrupting Avaya IQ data.

12. When the restore is complete, enter the following command to restart the Avaya IQ software:

```
service wdninit start
```

---

**Related topics:**

[Verifying the backup mount point on an application and database host](#) on page 207

## Updating the RTD properties file

After a restore, the RTD properties file may not be configured properly with the IP address of the All Functions or Administration host. Use this procedure to update the RTD properties file

### Procedure

1. Enter:

```
cd /opt/Avaya/CCR/RTD/tomcat/apache-tomcat-5.5.27/webapps/  
RTD/conf/
```

2. Create a backup copy of the RTD properties file using the following command:

```
cp rtd.properties rtd.properties.orig
```

3. Open the RTD properties file for editing:

```
vi rtd.properties
```

4. Replace the string `ADMINHOST_IPADDRESS` with the IP address of the All Functions or Administration host.

5. Save and close the file:

```
:wq!
```

6. Copy the Admin Tomcat `crossdomain.xml` file using the following command:

```
cp /opt/coreservices/tomcat-5.5.27/webapps/ROOT/  
crossdomain.xml /opt/Avaya/CCR/RTD/tomcat/apache-  
tomcat-5.5.27/webapps/ROOT
```

7. Restart RTD using the following command:

```
/opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

---

### Next steps

Continue with the following procedures:



- If you replaced a pair of disks on the database host, follow the procedures in [Restoring an EXP3000](#) on page 270. If you only replaced a pair of disks in an application host, you do not have to restore the EXP3000.
- Reapply any patches, service packs, or hot fixes that were installed since the original installation of the software.
- [Confirming a successful restore](#) on page 276

---

## Replacing one or more mirrored pairs of system disks on the database host in a dual host or multi-host deployment

Should one or more mirrored pairs of system disks fail on the database host in a dual host or multi-host deployment, you must do the following procedures shown in this section:

- Rebuild the system disks on the database host
- Install the OS, Oracle, and Avaya IQ, and run Linux First Boot on the database host
- Install the Oracle software on the database host
- Install the Oracle client software on the application hosts
- Set the backup mount point on the host
- Restore the software base, system configuration data, and database data on the database host
- Update the RTD properties file

## Rebuilding the system disks on an application or database host

### Before you begin

For detailed disk replacement procedures on an application or database host, see *Installing and Maintaining Avaya IQ Turnkey Hardware*.

Obtain the *S8800 Avaya IQ 5.2 Firmware Updates* and *S8800 Avaya IQ 5.2 uEFI Setting Tools* discs.

Obtain a USB keyboard, USB mouse, and VGA monitor to connect to the front panel of the host being updated.

### Procedure

1. Log on to each application host in the deployment as root or a root-level user.
2. Enter the following command to shut down the host:  
`shutdown now`
3. Turn off the power on the host.
4. Insert one or more pairs of replacement system disks.

5. Turn on the power to the host.
6. Insert the *S8800 Avaya IQ 5.2 Firmware Updates* disc into the disc drive.
7. Enter the following command to reboot the application host:  
`reboot`  
You will see the following types of messages:
  - Shutdown messages
  - System initializing messages
  - IBM System X messages
  - Controller messages
  - Running inventory
8. When the following message is displayed, enter `1` after the prompt:  
`Enter the item number to Updates| ("q" to quit ToolsCenter):`
9. When the following message is displayed, enter `y` after the prompt:  
`Do you want to start it now? Y(yes)/N(no)/Q(quit)`  
You will see the following types of messages:
  - Extracting...
  - Executing...
  - Initializing, Please Wait...
  - Messages displaying which firmware will be updated.
10. Either wait 60 seconds for the update to start, or press `A` to start the update immediately.  
The updates begin to load. It will take from 30 to 40 minutes on each host. When the updates are finished, a list of the updates is displayed.
11. Enter `Q` to quit the update program.
12. Enter `Yes` and `q` again.  
The host reboots and automatically changes the factory firmware settings to the proper Avaya IQ firmware settings.
13. While the system is rebooting, remove the disc from the disc drive and insert the *S8800 Avaya IQ 5.2 uEFI Setting Tools* disc into the disc drive.  
After the system reboots, the factory uEFI settings are changed to the Avaya IQ uEFI settings.
14. When the update is finished, press `Enter` to continue.  
The disc is automatically ejected.
15. After the disc ejects, remove the disc and press `Enter` to continue.  
The system reboots.

16. Insert the *S8800 IQ 5.2 MR10/MR10M RAID Tools* disc into the application host disc drive.
  17. Enter the following command to reboot the host:
 

```
reboot
```

On boot up, the RAID utility performs an inventory of storage devices attached to the database host. A menu appears showing two options:

    - Host
    - EXP3000
  18. Select option 1, Host.  
The RAID tools automatically configures the system disks with RAID 10.
  19. Remove the disc from the database host disc drive.
  20. Review the output displayed on the console to verify that no errors appear or are reported.  
A menu will prompt you to exit the program.
- 

## Installing the OS, Oracle, and Avaya IQ, and running First Boot on an application or database host

### Procedure

1. Insert the *Avaya IQ 5.2 Linux* disc into the disc drive.
2. Enter the following command to reboot the host:
 

```
reboot
```

The host reboots. A Red Hat banner page displays the instructions for running the kickstart program.
3. Enter *ks*.  
Several messages are displayed. The console screen will turn blue for a while, then more messages are displayed. This process takes about 45 minutes.
4. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Linux* disc, and replace it with the *Avaya IQ 5.2 Oracle* disc.  
The system starts up automatically and the Oracle database software is copied from the disc to the host. After about 45 minutes, a message requesting a reboot is displayed.
5. Remove the disc after the system ejects the disc.
6. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.2 Oracle* disc, and replace it with the *Avaya IQ 5.2 Software* disc.

The system starts up automatically and the Avaya IQ software is copied from the disc to the host. After about 15 minutes, a message requesting a reboot is displayed.

7. Remove the disc after the system ejects the disc.
8. Press `Enter` to reboot.
9. Monitor the messages.  
All messages except for `smartd` and `NFS statd` must show `OK`.  
The system displays the Welcome page
10. Click **Forward**.  
The system displays the License Agreement page.
11. Accept the license agreement.
12. Click **Forward**.  
The system displays the Keyboard page.
13. Select the appropriate keyboard language for the system. The default is U.S. English.  
You must use a USB keyboard.
14. Click **Forward**.  
The system displays the Root Password page to set the root password for the system.
15. Set the root password (must be six characters).  
**! Important:**  
You can use the root ID and password to log on to the server with root permissions. Root permissions have the highest and least restrictive privileges. Any knowledge of this password must be controlled and shared with only the customer and provisioning personnel.
16. Click **Forward**.  
The system displays the Network Setup page.
17. Click **Change Network Configuration....**  
**\* Note:**  
When administering the networking options, it is possible that the networking dialog box can disappear from the display and the Change Network Configuration... dialog box can be active. If this happens, press `Alt+Tab` to switch the networking dialog box to the front of the display.
18. Click the **Devices** tab.
19. Select the **eth0** check box. Ensure that the **Eth0** line is highlighted.  
**! Important:**  
Do not disable `USB0` since it is used by the Integrated Manager Module (IMM).

20. Click **Edit**.

**\* Note:**

Use the information collected on the *First Boot installation worksheet for networking* to complete the following steps.

21. Click the **General** tab.

Perform the following tasks:

- Select the **Activate device when computer starts** check box.
- Click **Statically set IP addresses**.
- Enter the IP address, subnet mask, and default gateway address for the host.

22. Click **OK**.

23. Click the **DNS** tab.

Provide the following information:

- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the fully qualified domain name (FQDN), for example, *HostName.DomainName.com*.
- **Primary, Secondary, and Tertiary DNS server IP address:** Indicates the primary, secondary, and tertiary server addresses. You must enter the primary DNS server IP address and, if applicable, the secondary and tertiary DNS server IP addresses.
- **DNS search path:** Indicates the DNS search path, which is your DNS domain name. For example, *DomainName.com*.

24. Click the **Hosts** tab.

25. Click **New**.

26. Provide the following information:

- **Address:** Indicates the IP address of the host.
- **Hostname:** For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces. Use the fully qualified domain name (FQDN), for example, *HostName.DomainName.com*.
- **Alias:** Indicates the short version of the fully qualified domain name of the host. For example, if the fully qualified domain name is *IQone.company.com*, then the alias is *IQone*.

27. Click **OK**.
28. Click **New**.
29. Click **OK**.  
The system saves the network configuration.
30. Click the **Devices** tab.
31. Select the **eth0** check box.
32. Click **Activate**.
33. Click **Yes**.
34. Click **OK**.
35. Ensure that the system status shows `eth0` as `active`.
36. Choose **File > Save**.  
The system saves the network configuration information.
37. Click **OK** when the system prompts to confirm the changes.
38. Choose **File > Quit**.  
The network setup shows `eth0` has a `static` boot protocol.
39. Click **Forward**.  
The system displays the Firewall page.
40. Select the security level.  
Avaya requires that you select **wwwhttp**, **wwwhttps**, and **ssh** as trusted services.
41. Click **Forward**.
42. Click **Yes** to accept the security level settings.
43. Ensure that **SELinux - Disabled** is selected.
44. Click **Forward**.  
The system displays the Time Zone page.
45. Click **Yes**.  
The system confirms the settings and restarts the system after the First Boot process is complete.
46. Select the appropriate time zone.
47. Click **Forward**.  
The system displays the Date and Time page.
48. Select the appropriate date and time.
49. Click the **Network Time Protocol** tab.
50. Select **Enable Network Time Protocol**.

51. Delete all the default NTP servers in the NTP server list.
  52. Click **Add**.
  53. Enter the IP address or the fully qualified server name of the NTP server for the network.
  54. Click **Forward**.  
The system checks for the NTP server connection.
- ⚠ Caution:**  
Do not continue if the NTP server connection check is unsuccessful. An NTP server is required for Avaya IQ installation. The Avaya IQ installation fails if an NTP server is not available. Find the correct NTP server information and repeat steps 43 through 59, or configure your NTP server so that it is working properly.
55. If prompted, click **Configure** to set up your monitor.  
Select the options that best fit the monitor hardware.
  56. Click **Forward**.  
The system displays the Set Up Software Updates page.
  57. Click **Forward**.  
The system displays a warning message about adding users. Ignore this message and continue with the installation.
  58. Click **Continue**.
  59. Click **Forward**.  
The system displays the Sound Card page.
  60. Click **Forward**.  
The system displays the Additional CDs page.
  61. Click **Finish**.
  62. Click **OK** on the reboot dialog.
- 

## Installing the Oracle software on the database host

### Procedure

1. Log on to the database host as root. For a single host deployment, this is the same host as the application host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.

3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:

- a. Enter:

```
vi /etc/profile
```

- b. Select the desired *locale* from the list of supported languages:

| Language               | Locale      |
|------------------------|-------------|
| Simplified Chinese     | zh_CN.UTF-8 |
| English US             | en_US.UTF-8 |
| French                 | fr_FR.UTF-8 |
| German                 | de_DE.UTF-8 |
| Italian                | it_IT.UTF-8 |
| Japanese               | ja_JP.UTF-8 |
| Korean                 | ko_KR.UTF-8 |
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where <locale> is a variable from the table:

```
LANG=<locale>; export LANG
```

- d. Save and close the file.

- e. Enter:

```
echo $LANG
```

Verify that the desired language variable is displayed.

4. Enter the following commands to install the database software and create the database:

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Recover DBHostIPAddress  
DBHostName &
```

where *DBHostIPAddress* is the IP address for the database host and *DBHostName* is the hostname (FQDN) of the database host.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.



This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

## Installing the Oracle client software on the application hosts

The Oracle client software must be installed on the Administration and Reporting hosts in a multi-host deployment, and on the All Functions host in a single or dual host deployment.

### Procedure

1. Log on to the Administration or All Functions host as root. In a single host deployment, the All Functions host is the same as the Database host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:
 

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language               | Locale      |
|------------------------|-------------|
| Simplified Chinese     | zh_CN.UTF-8 |
| English US             | en_US.UTF-8 |
| French                 | fr_FR.UTF-8 |
| German                 | de_DE.UTF-8 |
| Italian                | it_IT.UTF-8 |
| Japanese               | ja_JP.UTF-8 |
| Korean                 | ko_KR.UTF-8 |
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where <locale> is a variable from the table:

```
LANG=<locale>; export LANG
```

- d. Save and close the file.

- e. Enter:

```
echo $LANG
```

Verify that the desired language variable is displayed.

4. Enter the following commands to install the database client software:

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Client DBHostIPAddress  
DBHostName&
```

where *DBHostIPAddress* is the IP address of the database host and *DBHostName* is the host name (FQDN) of the database host.

**\* Note:**

For proper Domain Name System (DNS) resolution with Java and Red Hat Linux, host names must follow specific naming requirements. Use only alphanumeric characters for the name. Do not use special characters, such as hyphens, underscores, or slashes, and do not use spaces.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

6. Repeat this procedure on all Reporting hosts.

---

## Verifying the backup mount point on an application and database host

### About this task

You must enable backups for the Avaya IQ software and data on a mountable network drive or storage array. Ensure that you can gain access to this network drive or storage array from all hosts in the Avaya IQ deployment. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

To verify that you enabled the portmap service for the NFS mount point:

### Procedure

1. Log on to the application or database host as root or a root-level user.
2. Enter the following command to check if the portmap service is running:

```
service portmap status
```

You see the following response:

```
portmap (pid xxxx) is running...
```

Where xxxx is the pid number.

3. If the portmap service is not functional, enter:

```
service portmap start
```

4. Verify that the proper permissions are set on the NFS mount point server.
5. Repeat this procedure on all hosts.

---

#### Related topics:

[Restoring the software base and system configuration data on an application host](#) on page 254

## Restoring the software base, system configuration data, and database data on a database host

To restore the system configuration data on the database host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in this procedure restore the software base and database data.

### Before you begin

See the requirements shown in [Prerequisites for restoring Avaya IQ data](#) on page 218.

### Procedure

1. Inform all of the Avaya IQ users to log off from the administration and reporting interfaces.
2. Log on to the database host as root or a root-level user. On a single host deployment, the database host is the same host as the All Functions host.
3. Mount the backup file system so you can access the backup files.
4. Enter:
 

```
cd /
```

5. Enter the following command to restore the files required for the configuration data:

```
tar -xzf <BackupDirectory>/  
iq_base_<HostName>_<TimeStamp>.tar.gz "*" /CAT/install.out "  
"/CAT/dba.out" "*" /CAT/hostinfo.out" "*" /CAT/connection.out "  
"/current.conf"
```

where *<BackupDirectory>* is the location of the backup files, *<HostName>* is the name of the host, and *<TimeStamp>* is the time stamp of the most recent backup.

6. Depending on your deployment, do one of the following:

- On a single host deployment, skip this step. The `db_restore.sh` script will automatically shut down the Avaya IQ software.
- On a dual host deployment, enter the following command on the All Functions host to shut down the Avaya IQ software:

```
service wdninit stop
```

- On a multi-host deployment, enter the following command on the Administration host and every Reporting host to shut down the Avaya IQ software:

```
service wdninit stop
```

7. Enter the following commands to restore the software base and database data:

```
cd /  
sh /avaya/Oracle/db_restore.sh
```

8. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:

```
tail -f /var/log/Avaya/CCR/restore/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last  
backup may not get recovered.
```

9. Enter the following commands to re-index the database; this procedure may take some time depending on the amount of traffic on the system:

```
cd /opt/Avaya/CCR/data/db/oracle/scripts  
sh /opt/Avaya/CCR/bin/run_sql.sh -m  
create_realtime_indexes.sql CCRRT  
sh /opt/Avaya/CCR/bin/run_sql.sh -m  
create_historical_index.sql CCR
```

10. Enter the following command to remove the turnkey installation user ID:

```
sh /avaya/bin/harden_security.sh
```

11. When the restore is complete, enter the following command to reboot the database host:
 

```
reboot
```
12. Log on to the All Functions or Administration host as root or a root-level user.
13. When re-indexing is complete, enter the following command on the database host to restart the Avaya IQ software:
 

```
service wdinit start
```
14. Depending on your deployment, do one of the following:
  - On a single host deployment, enter the following command on the Data Collection hosts to start up the Avaya IQ software:
 

```
service wdinit start
```
  - On a dual host deployment, enter the following command on the All Functions and Data Collection hosts to start up the Avaya IQ software:
 

```
service wdinit start
```
  - On a multi-host deployment, enter the following command on every Data Collection, Data Processing, Reporting, and RTD hosts to start up the Avaya IQ software:
 

```
service wdinit start
```

---

## Updating the RTD properties file

After a restore, the RTD properties file may not be configured properly with the IP address of the All Functions or Administration host. Use this procedure to update the RTD properties file

### Procedure

1. Enter:
 

```
cd /opt/Avaya/CCR/RTD/tomcat/apache-tomcat-5.5.27/webapps/RTD/conf/
```
2. Create a backup copy of the RTD properties file using the following command:
 

```
cp rtd.properties rtd.properties.orig
```
3. Open the RTD properties file for editing:
 

```
vi rtd.properties
```
4. Replace the string `ADMINHOST_IPADDRESS` with the IP address of the All Functions or Administration host.
5. Save and close the file:
 

```
:wq!
```

6. Copy the Admin Tomcat crossdomain.xml file using the following command:

```
cp /opt/coreservices/tomcat-5.5.27/webapps/ROOT/crossdomain.xml /opt/Avaya/CCR/RTD/tomcat/apache-tomcat-5.5.27/webapps/ROOT
```

7. Restart RTD using the following command:

```
/opt/Avaya/CCR/bin/pecon.sh -v -w RTDTomcat restart
```

---

## Next steps

Continue with the following procedures:

- If you replaced a pair of disks on the database host, follow the procedures in [Restoring an EXP3000](#) on page 270. If you only replaced a pair of disks in an application host, you do not have to restore the EXP3000.
- Reapply any patches, service packs, or hot fixes that were installed since the original installation of the software.
- [Confirming a successful restore](#) on page 276

---

## Restoring disk arrays

### Restoring an EXP3000

Use this procedure to restore an EXP3000 disk array in a turnkey deployment when any of the following conditions occur:

- A pair of mirrored disks fail on an EXP3000 disk array.
- The MR10m controller card on the database host fails and has to be replaced.

#### Before you begin

Replace the defective disk drives or the MR10m controller card before doing this procedure. See *Installing and Maintaining Avaya IQ Turnkey Hardware* for details on how to replace these components.

Contact Avaya support for the turnkey Oracle password, if not known.

#### Procedure

1. Log on to the every application host in the deployment as root or a root-level user.
2. Enter the following command to stop Avaya IQ:  

```
service wdinit stop
```
3. Log on to the database host as root or a root-level user.
4. Enter the following command and log on as an Oracle user:

```
su - oracle
```

5. When prompted, enter the Oracle user password.
6. Enter the following commands to stop the Oracle database:
 

```
sqlplus / as sysdba
shutdown abort
quit
```
7. Enter the following command to exit from the Oracle logon:
 

```
exit
```
8. Enter the following commands to unmount and remove the /u02 file system from /etc/fstab:
 

```
cd /root
umount /u02
vi /etc/fstab
:/u02/d
:wq
```
9. Enter the following commands to Linux logical volume and volume group:
 

```
lvremove /dev/vg0/lvol0
vgremove vg0
```
10. Enter the following commands to determine the Linux physical volumes:
 

```
pvscan
```

The output will be similar to the following example:

```
PV /dev/sda1   VG vg0   lvm2 [407.91 GB / 0   free]
PV /dev/sdb1   VG vg0   lvm2 [407.91 GB / 0   free]
PV /dev/sdc1   VG vg0   lvm2 [407.91 GB / 0   free]
PV /dev/sdd1   VG vg0   lvm2 [407.91 GB / 0   free]
Total: 4 [1.59 TB] / in use: 4 [1.59 TB] / in no VG: 0 [0   ]
```
11. Enter the following commands to remove the Linux physical volumes:
 

```
pvremove <VolumeDrive1> <VolumeDrive2> <VolumeDriveX>
```

where *<VolumeDrive>* represents each of the Linux volumes shown from the `pvscan` command. For example, based on the output shown, the command would be:

```
pvremove /dev/sda1 /dev/sdb1 /dev/sdc1 /dev/sdd1
```
12. Enter the following command to remove the lock files created when the disks were partitioned and the file system was created:
 

```
rm -f /root/.lvm_parts /root/.config_db_lvm_disks
```
13. Insert the *S8800 IQ 5.2 MR10/MR10M RAID Tools* disc into the database host disc drive.
14. Enter the following command to reboot the database host:

reboot

On boot up, the RAID utility performs an inventory of storage devices attached to the database host. A menu appears showing two options:

- Host
- EXP3000

15. Select option 2, EXP3000. At the same time, power-up each EXP3000 disk array in the series, starting with the one connected to the database host. The RAID tools automatically configure every disk array attached to the database host with two virtual drives per disk array and configures the disk array with RAID 10.
16. Review the output displayed on the console to verify that no errors appear or are reported. A menu will prompt you to exit the program.
17. Remove the disc from the database host disc drive.
18. Enter the following command to reboot the database host to ensure that all disk arrays on S8800 Server and the EXP3000 disk array(s) are synchronized.

reboot

19. To verify that the RAID 10 was successfully configured, do any of the following checks:
  - On boot up of the database host, you should see that both RAID controllers are listed, MR10i and MR10m, each with virtual drives. There will be one virtual drive for the MR10i and two virtual drives for each EXP3000 disk array in your deployment.
  - On the POST screen, the LSIMegaRAID display will appear. It can be reviewed by using `Ctrl+H` to access the LSI megaRAID WebBios user interface. Knowledge of the LSI tools is recommended before doing this procedure.
  - Run the command `sfdisk -l`. There will be one virtual drive for the MR10i and two virtual drives for each EXP3000 disk array in your deployment. There will be no disk partitions created at this time for the EXP3000 disk arrays. EXP3000 disk partitions will be automatically created as part of the Oracle installation. The following is an example for two disk arrays:

```
Disk /dev/sda: 109053 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting
from 0
```

| Device    | Boot | Start | End | #cyls | #blocks | Id | System |
|-----------|------|-------|-----|-------|---------|----|--------|
| /dev/sda1 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sda2 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sda3 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sda4 |      | 0     | -   | 0     | 0       | 0  | Empty  |

```
Disk /dev/sdb: 109053 cylinders, 255 heads, 63 sectors/track
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting
from 0
```

| Device    | Boot | Start | End | #cyls | #blocks | Id | System |
|-----------|------|-------|-----|-------|---------|----|--------|
| /dev/sdb1 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdb2 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdb3 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdb4 |      | 0     | -   | 0     | 0       | 0  | Empty  |



```

/dev/sdb1      0      -      0      0      0      Empty
/dev/sdb2      0      -      0      0      0      Empty
/dev/sdb3      0      -      0      0      0      Empty
/dev/sdb4      0      -      0      0      0      Empty

```

Disk /dev/sdc: 109053 cylinders, 255 heads, 63 sectors/track  
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

| Device    | Boot | Start | End | #cyls | #blocks | Id | System |
|-----------|------|-------|-----|-------|---------|----|--------|
| /dev/sdc1 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdc2 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdc3 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdc4 |      | 0     | -   | 0     | 0       | 0  | Empty  |

Disk /dev/sdd: 109053 cylinders, 255 heads, 63 sectors/track  
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

| Device    | Boot | Start | End | #cyls | #blocks | Id | System |
|-----------|------|-------|-----|-------|---------|----|--------|
| /dev/sdd1 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdd2 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdd3 |      | 0     | -   | 0     | 0       | 0  | Empty  |
| /dev/sdd4 |      | 0     | -   | 0     | 0       | 0  | Empty  |

Disk /dev/sde: 35500 cylinders, 255 heads, 63 sectors/track  
Units = cylinders of 8225280 bytes, blocks of 1024 bytes, counting from 0

| Device    | Boot | Start  | End   | #cyls  | #blocks    | Id | System               |
|-----------|------|--------|-------|--------|------------|----|----------------------|
| /dev/sde1 | *    | 0+     | 130   | 131-   | 1052226    | 83 | Linux                |
| /dev/sde2 |      | 131    | 7963  | 7833   | 62918572+  | 83 | Linux                |
| /dev/sde3 |      | 7964   | 12140 | 4177   | 33551752+  | 82 | Linux swap / Solaris |
| /dev/sde4 |      | 12141  | 35499 | 23359  | 187631167+ | 5  | Extended             |
| /dev/sde5 |      | 12141+ | 16056 | 3916-  | 31455238+  | 83 | Linux                |
| /dev/sde6 |      | 16057+ | 17361 | 1305-  | 10482381   | 83 | Linux                |
| /dev/sde7 |      | 17362+ | 18666 | 1305-  | 10482381   | 83 | Linux                |
| /dev/sde8 |      | 18667+ | 35499 | 16833- | 135211041  | 83 | Linux                |

20. Enter the following command to partition the disks in the disk array(s):

```
sh /avaya/Oracle/lvm_parts.sh
```

21. Enter the following command to remake the Linux logical volumes and create or remount the /u02 file system:

```
sh /avaya/Oracle/config_db_lvm_disks.sh
```

22. Enter the following commands to mount the /u02 file system:

```
mount
```

The output will be similar to the following example:

```

/dev/sde7 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
/dev/sde8 on /u01 type ext3 (rw)
/dev/sde6 on /tmp type ext3 (rw)
/dev/sde5 on /var type ext3 (rw)
/dev/sde2 on /opt type ext3 (rw)
/dev/sde1 on /boot type ext3 (rw)
tmpfs on /dev/shm type tmpfs (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)

```

```
nfsd on /proc/fs/nfsd type nfsd (rw)
/dev/mapper/vg0-lvol0 on /u02 type ext3 (rw)
```

Verify that the last line shown in the output is displayed:

```
/dev/mapper/vg0-lvol0 on /u02 type ext3 (rw)
```

23. Continue by restoring the database data as shown in the following section.

---

## Restoring the software base, system configuration data, and database data on a database host

To restore the system configuration data on the database host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in this procedure restore the software base and database data.

### Before you begin

See the requirements shown in [Prerequisites for restoring Avaya IQ data](#) on page 218.

### Procedure

1. Inform all of the Avaya IQ users to log off from the administration and reporting interfaces.
2. Log on to the database host as root or a root-level user. On a single host deployment, the database host is the same host as the All Functions host.
3. Mount the backup file system so you can access the backup files.
4. Enter:

```
cd /
```
5. Enter the following command to restore the files required for the configuration data:

```
tar -xzvf <BackupDirectory>/
iq_base_<HostName>_<TimeStamp>.tar.gz "*" /CAT/install.out "
"/CAT/dba.out" "*" /CAT/hostinfo.out" "*" /CAT/connection.out "
"/current.conf"
```

where *<BackupDirectory>* is the location of the backup files, *<HostName>* is the name of the host, and *<TimeStamp>* is the time stamp of the most recent backup.
6. Depending on your deployment, do one of the following:

- On a single host deployment, skip this step. The `db_restore.sh` script will automatically shut down the Avaya IQ software.
- On a dual host deployment, enter the following command on the All Functions host to shut down the Avaya IQ software:

```
service wdinit stop
```

- On a multi-host deployment, enter the following command on the Administration host and every Reporting host to shut down the Avaya IQ software:

```
service wdinit stop
```

7. Enter the following commands to restore the software base and database data:

```
cd /
sh /avaya/Oracle/db_restore.sh
```

8. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:

```
tail -f /var/log/Avaya/CCR/restore/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last
backup may not get recovered.
```

9. Enter the following commands to re-index the database; this procedure may take some time depending on the amount of traffic on the system:

```
cd /opt/Avaya/CCR/data/db/oracle/scripts
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_realtime_indexes.sql CCRRT
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_historical_index.sql CCR
```

10. Enter the following command to remove the turnkey installation user ID:

```
sh /avaya/bin/harden_security.sh
```

11. When the restore is complete, enter the following command to reboot the database host:

```
reboot
```

12. Log on to the All Functions or Administration host as root or a root-level user.

13. When re-indexing is complete, enter the following command on the database host to restart the Avaya IQ software:

```
service wdinit start
```

14. Depending on your deployment, do one of the following:

- On a single host deployment, enter the following command on the Data Collection hosts to start up the Avaya IQ software:

```
service wdinit start
```

- On a dual host deployment, enter the following command on the All Functions and Data Collection hosts to start up the Avaya IQ software:

```
service wdinit start
```

- On a multi-host deployment, enter the following command on every Data Collection, Data Processing, Reporting, and RTD hosts to start up the Avaya IQ software:

```
service wdinit start
```

---

## Restoring a replacement S8800 host computer

After you have rebuilt an Avaya S8800 application host or database host based on the procedures shown in *Installing and Maintaining Avaya IQ Turnkey Hardware*, you must restore the software and data on the host. The procedures required for this restore depends on whether the host is an application host or database host:

- For an application host, follow the procedures in [Replacing one or more mirrored pairs of system disks on an application host in a dual host or multi-host deployment](#) on page 245
- For a database host, follow the procedures in [Replacing one or more mirrored pairs of system disks on the database host in a dual host or multi-host deployment](#) on page 257

**! Important:**

During the replacement of a failed Administration or All Functions host, the MAC address of the server will change. When this happens, you must also obtain and install a new license file for the deployment.

---

## Confirming a successful restore

### Procedure

1. Log on to the application host.
2. Enter the following commands to confirm that the Tomcat process has started:

```
ps -ef | grep -i tomcat
```

```
more /opt/coreservices/tomcat5/logs/catalina.out | grep "Got Reply"
```

The first command confirms that Tomcat has started. The second message confirms that the Got Reply message has occurred.

3. Enter the following command to confirm that Oracle is displayed as a process:

```
ps -ef | grep ora
```

The display looks similar to the following:

```
ccr      30838 30630  0 09:53 ?          00:00:27 /opt/Avaya/CCR/jrel.5.0_07/
bin/java -Xmx512M -Dorg.apache.activemq.UseDedicatedTaskRunner=true -
Dderby.system.home=../data -Dderby.storage.fileSyncTransactionLog=true -
Djavax.net.ssl.keyStore=/opt/coreservices/avaya/certs/jks/ccrjms.jks -
Djavax.net.ssl.keyStorePasswordFile=/opt/coreservices/avaya/certs/jks/
ccrjms.pwd -Djavax.net.ssl.trustStore=/opt/coreservices/avaya/certs/jks/
trustedcerts.jks -Dcom.sun.management.jmxremote -classpath /opt/
coreservices/activemq-4.0.1/bin/run.jar:/opt/Avaya/CCR/jars/admin/ccr-
admin.jar:/opt/coreservices/activemq-4.0.1/lib/optional/
log4j-1.2.15.jar:/opt/coreservices/activemq-4.0.1/conf -Dactivemq.home=/
opt/coreservices/activemq-4.0.1
com.avaya.ccr.admin.messaging.ActiveMQServerWrapper
```

4. Enter:

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w all status
```

The list of services are displayed similar to what is shown in the following example. Different host types display different numbers of services. The left-justified services are the containers and the indented services are the individual processing elements. Verify that all of the containers are started, including the data processing containers for all associated sources.

List of services :

```
0789d60629cf676e0129cf6777150003 : MessageBrokerService : STARTED
0789d60629cf676c0129cf7f46d700ab : ReportingApplicationService : STARTED
0789d60629cf676c0129cf7f46e900af : ReportingWebServer : STARTED
0789d60629cf676c0129cf7f470100b3 : RTDTomcat : STARTED
0789d60629cf676e0129cf67772c0008 : AdminTomcat : STARTED
    0789d60629cf676e0129cf677773000b : PEOAM_key : STARTED
    0789d60629cf676e0129cf6777890018 : PESDAS_key : STARTED
    0789d60629cf676e0129cf67778d001b : PEHostLogServer : STARTED
    0789d60629cf676e0129cf67779c001f : PENetworkLogServer_key : STARTED
    0789d60629cf676e0129cf6777a10023 : PEHostLogRetrieverServer : STARTED
    0789d60629cf676e0129cf6777a60027 : PENetworkLogRetrieverServer_key :
STARTED
    0789d60629cf676e0129cf6777ab002b : PEAlarmServer_key : STARTED
    0789d60629cf676e0129cf6777b0002f : PEAlarmConfigServer_key : STARTED
    0789d60629cf676e0129cf6777b50033 : PEAlarmRetrieverServer_key : STARTED
    0789d60629cf676e0129cf6777ba0037 : PEAuthorizationServiceKey : STARTED
0789d60629cf676c0129cf7f44e10050 : AdminJBoss : STARTED
    0789d60629cf676c0129cf7f44ec0053 : PEKeyAuthority : STARTED
    0789d60629cf676c0129cf7f44fa0057 : PEIRS : STARTED
    0789d60629cf676c0129cf7f4505005c : PEHDREntityMonitor : STARTED
    0789d60629cf676c0129cf7f45180068 : PERDREntityMonitor : STARTED
    0789d60629cf676c0129cf7f452b0075 : PEHDAPREntityMonitor : STARTED
    0789d60629cf676c0129cf7f453f0082 : PERDAPREntityMonitor : STARTED
    0789d60629cf676c0129cf7f4551008f : PELoadDateKey : STOPPED
    0789d60629cf676c0129cf7f45580092 : PEAggregation : STARTED
    0789d60629cf676c0129cf7f455f0096 : PEAdminRecorder : STARTED
    0789d60629cf676c0129cf7f456b009d : PESchedulerUtility_key : STARTED
    0789d60629cf676c0129cf7f457100a0 : PEETL : STARTED
0789d60629cf676c0129cf7f457700a3 : ReportingJBoss : STARTED
    0789d60629cf676c0129cf7f46c800a7 : PERealTimeReportService : STARTED
```

```
0789d60629cf767c0129cf8bb5b30a28 : DataProcessingJBoss_CM : STARTED
0789d60629cf767c0129cf8bb5c00a2c : PECMAdapter_CM : STARTED
0789d60629cf767c0129cf8bb5c90a33 : PEEventProcessor_CM : STARTED
0789d60629cf767c0129cf8bb6000a56 : PERecorder_CM : STARTED
```

**\* Note:**

If this command fails, wait for some time for the software to load completely or for the system to restart, and run the command again.

5. If after 10 to 15 minutes any of the containers are not started, enter:  

```
sh /opt/Avaya/CCR/bin/pecon.sh -v -w Container restart
```

Where *Container* is the name of the container you need to restart. Repeat this step for every container that has not started.
6. On the **Enterprise** tab, select **Sites > HostSite > HostName**, where *HostSite* is the name of the site and *HostName* is the name of the host.
7. Verify that all subsystems and processes have started.  
The icons for each item will be green. If any subsystems and processes are not green, refresh the browser window until all subsystems and processes are green.
8. On the **Enterprise** tab, select **Sites > Resources > All Resources > SourceName**, where *SourceName* is the name of Communication Manager systems associated with the deployment.
9. Verify that the list of agents, queues, and routing points have been synchronized (uploaded) from all Communication Manager systems.  
The more resources each source has, the longer it will take for synchronization. If you do not see groups being populated with data, refresh the display on the **Enterprise** tab and in the resource dialog. You may see the agents, queues, and routing points first synchronize without names, but the name information will synchronize eventually.
10. At the All Functions, Data Collection, or Data Processing hosts, enter 

```
cd /var/log/Avaya/CCR.
```
11. Enter:  

```
ls | more
```

Look for directories named `DataProcessingJBoss_<SOURCENAME>`. There will be a `DataProcessingJBoss_<SOURCENAME>` directory for every Communication Manager, Proactive Contact, or Voice Portal data source connected to the system.
12. Enter:  

```
cd DataProcessingJBoss_<SOURCENAME>
```
13. Enter:  

```
tail -f hex_dump_all.log
```

You should see a continuous stream of messages being written to this log file. These are messages going between the data source and the Avaya IQ system. The following is an example of these messages:

```
# ---- AVAIL20 (2007-03-22 10:58:54,517) ----
36 d0 00 31 88 ec 0c 77 1a aa 1a 0f 00 00 00 00 00 00
# ---- IDLE20 (2007-03-22 10:58:54,517) ----
36 d7 00 31 88 ed 0a a0 7c 4e 26 01 f7 46 02 61 55
# ---- AVAIL20 (2007-03-22 10:58:54,517) ----
36 d0 00 31 88 ee 0b 55 aa 37 0f bd 00 00 00 00 00 00
# ---- AUX20 (2007-03-22 10:58:54,518) ----
36 d3 00 31 88 ef 05 55 aa 37 00 00
```

If messages are transferring from the data source and all subsystems, processes, and containers are started, you can presume that data from the data sources is being written into the database for report processing.

If messages are not being sent between the systems, there is a problem with the link. Do the following procedures in the order shown, rechecking the Data Processing log file after each procedure:

- a. Stop and start the `DataProcessingJBoss` container as described in Step 7.
  - b. Check the log file for output.
14. Repeat Steps 15 and 16 for every source system associated with the host.
  15. Log on to the database host.
  16. Log on to the reporting interface.
  17. Verify that you can run reports for every data source using the default reporting groups of each data source.  
See *Avaya IQ Standard Reports* for procedures to run reports. Since the system was just installed, the data in the reports will be minimal. You only want to verify that the reports are running and that the reports have data.
  18. Run the following historical reports:
    - Agent Performance by Queue – Summary (totals)
    - Agent Performance by Routing Point – Summary (totals)
    - Work Group Performance by Queue Group – Summary
  19. Run the following real-time reports:
    - Agent Performance
    - Queue Performance
    - Routing Point Performance
  20. On the host hardware, open the light path diagnostic panel. The panel displays the firmware number, which should show **2.6**.
  21. Enable backups on both the application host and the database host as shown in [Backing up Avaya IQ data in a turnkey deployment](#) on page 204.

22. Execute an on-demand backup as shown in [Running an on-demand backup](#) on page 210.

---

## Restoring back to Avaya IQ 5.1.1

If you have to restore the system back to the previous Avaya IQ release, 5.1.1, you must do the following procedures shown in this section:

### **Caution:**

When restoring back to a previous version of Avaya IQ, there will be data loss because of going from a newer database schema to an older database schema.

- Install the OS, Oracle, and Avaya IQ, and run Linux First Boot on the All Functions host; repeat this procedure on the database host
- Install the Oracle software on the database host
- Install the Oracle client software on the All Functions host
- Set the backup mount point on the host
- Restore database data on the database host
- Restore software base and system configuration data on the application hosts and database host

After you have completed the restore, do the following additional procedures:

- Reapply any patches, service packs, or hot fixes that were installed since the original installation of the software.
- Do the steps shown in [Confirming a successful restore](#) on page 276.

## Installing the OS, Oracle, and Avaya IQ, and running First Boot on a host

### **Before you begin**

#### **About this task**

Obtain access to backups of the 5.1.x hosts. If the backups cannot be obtained, you cannot restore the system back to release 5.1.1.

Do backups on the 5.2.x system before restoring the system back to 5.1.1.

Obtain configuration data for the turnkey system, such as IP addresses.

#### **Procedure**

1. Log on to the All Functions host as root or a root-level user.
2. Insert the *Avaya IQ 5.1.1 Linux* disc into the disc drive.



3. Enter the following command to reboot the host:  

```
reboot
```

The host reboots.
4. Enter `ks`.  
Several messages are displayed. The console screen will turn blue for a while, then more messages are displayed. This process takes about 45 minutes.
5. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.1.1 Linux* disc, and replace it with the *Avaya IQ 5.1.1 Oracle* disc.  
The system starts up automatically and the Oracle database software is copied from the disc to the host. After about 45 minutes, a message requesting a reboot is displayed.
6. Remove the disc after the system ejects the disc.
7. When the system prompts you to insert a disc, open the disc drive, remove the *Avaya IQ 5.1.1 Oracle* disc, and replace it with the *Avaya IQ 5.1.1 Software* disc.  
The system starts up automatically and the Avaya IQ software is copied from the disc to the host. After about 15 minutes, a message requesting a reboot is displayed.
8. Remove the disc after the system ejects the disc.
9. Press `Enter` to reboot.
10. Monitor the messages.  
All messages except for `smartd` and `NFS statd` must show `OK`.  
The system displays the Welcome page
11. Click **Forward**.  
The system displays the License Agreement page.
12. Accept the license agreement.
13. Click **Forward**.  
The system displays the Keyboard page.
14. Select **U.S. English** as the keyboard language for the system.  
You must use a USB keyboard.
15. Click **Forward**.  
The system displays the Root Password page.
16. Set the root password (must be six characters).  
**!** **Important:**  
You can use the root ID and password to log on to the server with root permissions. Root permissions have the highest and least restrictive privileges. Any knowledge of this password must be controlled and shared with only the customer and provisioning personnel.

17. Click **Forward**.

The system displays the Network Setup page.

18. Click **Change Network Configuration...**

**\* Note:**

When administering the networking options, it is possible that the networking dialog box can disappear from the display and the Change Network Configuration... dialog box can be active. If this happens, press **Alt+Tab** to switch the networking dialog box to the front of the display.

19. Click the **Devices** tab.
20. Select the **eth0** check box.

**! Important:**

Do not disable USB0 since it is used by the Integrated Manager Module (IMM).

21. Click **Edit**.

**\* Note:**

Use the information collected on the *First Boot installation worksheet for networking* to complete the following steps.

22. Click the **General** tab.

Perform the following tasks:

- Select the **Activate device when computer starts** check box.
- Click **Statically set IP addresses**.
- Enter the IP address, subnet mask, and default gateway address for the host.

23. Click **OK**.

24. Click the **DNS** tab.

Provide the following information:

- **Hostname:** Avaya requires you to use the fully qualified domain name for the server. For example, `HostName.DomainName.com`.
- **Primary, Secondary, and Tertiary DNS server IP address:** Indicates the primary, secondary, and tertiary server addresses. You must enter the primary DNS server IP address and, if applicable, the secondary and tertiary DNS server IP addresses.
- **DNS search path:** Indicates the DNS search path, which is your DNS domain name. For example, `DomainName.com`.

25. Click the **Hosts** tab.

26. Click **New**.

27. Provide the following information:

- **Address:** Indicates the IP address of the host.
- **Hostname:** Indicates the fully qualified domain name of the host.
- **Alias:** Indicates the short version of the fully qualified domain name of the host. For example, if the fully qualified domain name is `IQone.company.com`, then the alias is `IQone`.

28. Click **OK**.
29. Click **New**.
30. Click **OK**.  
The system saves the network configuration.
31. Click the **Devices** tab.
32. Select the **eth0** check box.
33. Click **Activate**.
34. Click **Yes**.
35. Click **OK**.
36. Ensure that the system status shows `eth0` as `active`.
37. Choose **File > Save**.  
The system saves the network configuration information.
38. Click **OK** when the system prompts to confirm the changes.
39. Choose **File > Quit**.  
The network setup shows `eth0` has a `static` boot protocol.
40. Click **Forward**.  
The system displays the Firewall page.
41. Select the security level.  
Avaya requires that you select **www**, **http**, **https**, and **ssh** as trusted services.
42. Click **Forward**.
43. Click **Yes** to accept the security level settings.
44. Ensure that **SELinux - Disabled** is selected.
45. Click **Forward**.  
The system displays the Time Zone page.
46. Click **Yes**.  
The system confirms the settings and restarts the system after the First Boot process is complete.
47. Select the appropriate time zone.
48. Click **Forward**.

The system displays the Date and Time page.

49. Select the appropriate date and time.
50. Click the **Network Time Protocol** tab.
51. Select **Enable Network Time Protocol**.
52. Delete all the default NTP servers in the NTP server list.
53. Click **Add**.
54. Enter the IP address or the fully qualified server name of the NTP server for the network.
55. Click **Forward**.  
The system checks for the NTP server connection.

 **Caution:**

Do not continue if the NTP server connection check is unsuccessful. An NTP server is required for Avaya IQ installation. The Avaya IQ installation fails if an NTP server is not available. Find the correct NTP server information and repeat steps 43 through 59, or configure your NTP server so that it is working properly.

56. If prompted, click **Configure** to set up your monitor.  
Select the options that best fit the monitor hardware.
57. Click **Forward**.  
The system displays the Set Up Software Updates page.
58. Click **Forward**.  
The system displays a warning message about adding users. Ignore this message and continue with the installation.
59. Click **Continue**.
60. Click **Forward**.  
The system displays the Sound Card page.
61. Click **Forward**.  
The system displays the Additional CDs page.
62. Click **Finish**.
63. Click **OK** on the reboot dialog.
64. Repeat this procedure on any other application hosts, and the database host.

## Installing the Oracle software on the database host

### Procedure

1. Log on to the database host as root. For a single host deployment, this is the same host as the application host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:
 

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language               | Locale      |
|------------------------|-------------|
| Simplified Chinese     | zh_CN.UTF-8 |
| English US             | en_US.UTF-8 |
| French                 | fr_FR.UTF-8 |
| German                 | de_DE.UTF-8 |
| Italian                | it_IT.UTF-8 |
| Japanese               | ja_JP.UTF-8 |
| Korean                 | ko_KR.UTF-8 |
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where `<locale>` is a variable from the table:
 

```
LANG=<locale>; export LANG
```
  - d. Save and close the file.
  - e. Enter:
 

```
echo $LANG
```

Verify that the desired language variable is displayed.
4. Enter the following commands to install the database software and create the database:
 

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Recover DBHostIPAddress  
DBHostName &
```

where *DBHostIPAddress* is the IP address of the database host and *DBHostName* is the hostname (FQDN) of the database host.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/install_logs/install_oracle.out
```

Look for any error messages and the successful completion message.

---

## Installing the Oracle client software on the application hosts

The Oracle client software must be installed on the Administration and Reporting hosts in a multi-host deployment, and on the All Functions host in a single or dual host deployment.

### Procedure

1. Log on to the Administration or All Functions host as root. In a single host deployment, the All Functions host is the same as the Database host.
2. If you need to adjust the format of the date and time being displayed for your locale, use the `date +FORMAT` command to change the format. The default format is US English.
3. If you require language support other than the default of US English, continue with the sub-steps below; if you do not need to change the supported languages, skip to Step 4:
  - a. Enter:

```
vi /etc/profile
```
  - b. Select the desired *locale* from the list of supported languages:

| Language           | Locale      |
|--------------------|-------------|
| Simplified Chinese | zh_CN.UTF-8 |
| English US         | en_US.UTF-8 |
| French             | fr_FR.UTF-8 |
| German             | de_DE.UTF-8 |
| Italian            | it_IT.UTF-8 |
| Japanese           | ja_JP.UTF-8 |
| Korean             | ko_KR.UTF-8 |

| Language               | Locale      |
|------------------------|-------------|
| Brazilian Portuguese   | pt_BR.UTF-8 |
| Russian                | ru_RU.UTF-8 |
| Latin American Spanish | es_CO.UTF-8 |

- c. Add the following line to the end of the file where <locale> is a variable from the table:

```
LANG=<locale>; export LANG
```

- d. Save and close the file.

- e. Enter:

```
echo $LANG
```

Verify that the desired language variable is displayed.

4. Enter the following commands to install the database software and create the database:

```
cd /
```

```
sh /avaya/Oracle/install_oracle.sh Client OracleUserPassword  
DBPassword DBHostIPAddress&
```

where *OracleUserPassword* is the password for the Oracle user you assigned, *DBPassword* is the password for the database, and *DBHostIPAddress* is an optional parameter that defines the IP address of the database host.

This command must be entered on a single line. Make sure you end the command with “&” so it can run in the background and you can view the log file.

5. Enter the following command to view the log file:

```
tail -f /avaya/log/ServerName_oracle_install.out
```

Look for any error messages and the successful completion message.

6. Repeat this procedure on all Reporting hosts.

## Verifying the backup mount point on an application and database host

### About this task

You must enable backups for the Avaya IQ software and data on a mountable network drive or storage array. Ensure that you can gain access to this network drive or storage array from all hosts in the Avaya IQ deployment. When setting up NFS mount points, the root and oracle user IDs must have permission to write to the NFS mount point.

To verify that you enabled the portmap service for the NFS mount point:

### Procedure

1. Log on to the application or database host as root or a root-level user.

2. Enter the following command to check if the portmap service is running:

```
service portmap status
```

You see the following response:

```
portmap (pid xxxx) is running...
```

Where xxxx is the pid number.

3. If the portmap service is not functional, enter:  

```
service portmap start
```
4. Verify that the proper permissions are set on the NFS mount point server.
5. Repeat this procedure on all hosts.

---

**Related topics:**

[Restoring the software base and system configuration data on an application host](#) on page 254

## Restoring the software base and database data on a database host

This procedure restores the software base and database data.

### Before you begin

#### About this task

See the requirements shown in [Prerequisites for restoring Avaya IQ data](#) on page 218.

#### Procedure

1. Log on to the database host as root or a root-level user. On a single host deployment, the database host is the same host as the All Functions host.
2. To convert the Oracle scripts from DOS to Unix format, enter:  

```
dos2unix /avaya/Oracle/*.sh
```
3. To create the backup directory, enter the following commands:  

```
mkdir /var/log/Avaya/CCR/backup
```
4. To set permissions for the backup directory, enter  

```
chmod 666 /var/log/Avaya  
chmod 666 /var/log/Avaya/CCR  
chmod 666 /var/log/Avaya/CCR/backup
```
5. Mount the backup file system so you can access the database backup files.
6. Verify that the AvayaIQ directory, the database backup directory, and the subdirectories in the database backup directories folder have the ownership set to oracle and group set to oinstall.



Use `chmod` to update permissions for Oracle and use `chgroup` to set the group properties.

7. Enter the following commands to restore the software base and database data:

```
cd /
sh /avaya/Oracle/db_restore.sh
```

To run this command, you must know the location of the Oracle backup destination. Do not attempt this restore without knowing the location.

8. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:

```
tail -f /var/log/Avaya/CCR/backup/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last
backup may not get recovered.
```

## Restoring the software base and system configuration data on an application host

To restore the system configuration data on an S8800 application host, you must restore the following files from the “base” backup tar file:

- /opt/Avaya/CCR/util/CAT/install.out
- /opt/Avaya/CCR/util/CAT/dba.out
- /opt/Avaya/CCR/util/CAT/hostinfo.out
- /opt/Avaya/CCR/util/CAT/connection.out
- /opt/Avaya/CCR/current.conf

The other steps in the procedure restore the software base.

### About this task

**! Important:**

Remember to perform this restore on all application hosts in the deployment.

### Procedure

1. Log on to the application host as root or a root-level user.
2. Mount the backup file system so you can access the backup files.
3. Enter:
 

```
cd /
```

4. Enter the following command to restore the files required for the configuration data:

```
tar -xzf <BackupDirectory>/  
iq_base_<HostName>_<TimeStamp>.tar.gz "*" /CAT/install.out "  
"/CAT/dba.out" "*" /CAT/hostinfo.out" "*" /CAT/connection.out "  
"/current.conf"
```

where *<BackupDirectory>* is the location of the backup files, *<HostName>* is the name of the host, and *<TimeStamp>* is the time stamp of the most recent backup.

5. Insert the *Avaya IQ 5.1 Software Only* disc into the disc drive.

6. Enter the following commands to mount the disc drive:

```
mount /dev/cdrom /mnt  
cd /mnt
```

7. Enter the following command to confirm that you will restore the proper version of Avaya IQ:

```
sh Avaya_IQ_Install.bin -version
```

For example, the Avaya IQ 5.1.1 should return a value similar to the following:

```
Version: 5.1.x.x.xxx_yyyy
```

8. Enter the following command to restore the Avaya IQ data:

```
sh /mnt/restore/runRestore.sh -bkploc BackupDirectory -  
binloc /mnt -license LicenseFileLocation
```

where:

- *BackupDirectory* is the location of the backup files. The backup directory must include both the *iq\_base* and *iq\_data.tar.gz* files.
- *LicenseFileLocation* is the full path to the license file, including the license file name. If you do not have a copy of the original license file, create a zero-length file named *license.xml* to allow you to complete the restore. Later, you must install a valid license file.

The restore process will take from 15 to 45 minutes.

9. Enter `cd $CCR_HOME/data`

10. Enter `rm -rf iks` to delete the contents in the *iks* directory.

**\* Note:**

You must delete the contents in the *iks* directory to avoid corrupting Avaya IQ data.

11. To convert the Oracle scripts from DOS to Unix format, enter:

```
dos2unix /avaya/Oracle/*.sh
```

12. Enter the following commands to re-index the database; this procedure may take some time depending on the amount of traffic on the system:

```
cd /opt/Avaya/CCR/data/db/oracle/scripts
```

```
sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_realtime_indexes.sql CCRRT

sh /opt/Avaya/CCR/bin/run_sql.sh -m
create_historical_index.sql CCR
```

13. Enter the following commands to restore the software base and database data:

```
cd /

sh /avaya/Oracle/db_restore.sh
```

To run this command, you must know the location of the Oracle backup destination. Do not attempt this restore without knowing the location.

14. During the restore, status messages will be displayed on the console; note any error messages. You can also inspect the log file using the following command:

```
tail -f /var/log/Avaya/CCR/backup/db_restore.log
```

**\* Note:**

You can ignore the following message:

```
Warning: missing redo logs. Some transactions after last
backup may not get recovered.
```

15. Repeat this procedure on all application hosts.

## Selectively restoring Avaya IQ files or directories

The Avaya IQ backup scripts generate two compressed tar files:

- A base file that contains backups of `$CSBASE`, `$CCR_HOME`, and `$ORACLE_HOME`, plus some other Oracle-related files. The name of this file is `iq_base_<HostName>_<TimeStamp>.tar.gz`.
- A data file that contains backups of Avaya IQ files and backups of `/home` and `/etc`. The name of this file is `iq_data_<HostName>_<TimeStamp>.tar.gz`.

Use the procedures given in this section to restore files and directories selectively on an application host.

**⚠ Caution:**

When you restore a file or a directory, the version you restore may be older than the version you replaced. This could cause data inconsistencies and Avaya IQ may not function properly.

### Before you begin

Complete the [prerequisites](#) on page 218.

## Procedure

1. Log on to the application host as root or a root-level user.
2. Copy the tar file you saved during the backup procedure to the application host where you want to restore the files or directories.  
You can copy the file using scp or removable media. Any temporary storage location for the backup files should have sufficient space.

3. To list the files that are contained in the “base” tar file, enter the following command:  

```
tar -tzvf iq_base_<HostName>_<TimeStamp>.tar.gz | more
```

4. Decide which files or directories you want to restore. For example, if you want to restore the `/opt/coreservices/scc/runtime/0789033a29347a880129347a951b001f.dat` file from the “base” tar file, enter the following command to restore that file:

```
tar -xzvf /u01/mnt/iq_base_<HostName>_<TimeStamp>.tar.gz -C / "/opt/coreservices/scc/runtime/0789033a29347a880129347a951b001f.dat"
```

5. To restore files from the “data” tar file, you must first extract the files to a temporary location. Enter the following commands to extract and list the files:

```
tar -xzvf /u01/mnt/iq_data_<HostName>_<TimeStamp>.tar.gz -C /tmp "/etc.tar.gz"
```

```
cd /tmp/iq_data/
```

```
tar -tzvf etc.tar.gz | more
```

6. If you believe your `/etc/hosts` file has been corrupted, enter the following commands to restore that file:

```
cd /tmp/iq_data/
```

```
tar -tzvf etc.tar.gz "/etc/hosts"
```

---

### Related topics:

[Restored directories and files](#) on page 218

---

## Restoring custom reports

To restore custom reports that you have backed up using the High Availability export tool, see “Importing reports” in *Avaya IQ High Availability and Survivability*.

## Index

---

### Special Characters

\*\_console.log .....[53](#)

---

### A

acquiring a license file .....[110](#)  
ActiveMQ .....[17](#)  
activemq.log .....[53](#)  
adding .....[174](#)  
    certificates .....[174](#)  
adjusting daylight saving error .....[179](#)  
ADMIN .....[53](#)  
Admin JBoss container .....[17](#), [68–72](#)  
ADMIN.log .....[53](#)  
administer certificates .....[157](#), [158](#)  
Administration Data Store .....[23](#)  
Administration host .....[63](#)  
Administration Recorder .....[21](#), [23](#)  
administrative data .....[79](#)  
administrative functions, backups .....[48](#)  
agents, queues, routing points missing names .....[71](#)  
Alarm Config Service PE .....[65](#)  
Alarm Retriever Service PE .....[65](#)  
Alarm Viewer does not function .....[65](#)  
alarms .....[94](#)  
alarms are not logged .....[65](#)  
All Functions host .....[62](#)  
application host ....[211](#), [234](#), [240](#), [248](#), [252](#), [254](#), [259](#), [265](#),  
    [280](#),                      [286](#),                      [289](#)  
    installing the Oracle software .....[240](#), [252](#), [265](#), [286](#)  
    installing the OS and running First Boot ....[234](#), [248](#),  
        [259](#),                      [280](#)  
    restoring software base and system configuration  
        data .....[254](#), [289](#)  
    running an on-demand backup .....[211](#)  
application or database host .....[232](#), [246](#), [257](#)  
    rebuilding the system disks .....[232](#), [246](#), [257](#)  
archive log management .....[41](#)  
ARConnector initialization fails .....[188](#), [189](#)  
ARConnector Initialization fails .....[189](#)  
ARConnector JMS messages .....[193](#), [194](#)  
ARConnectors status .....[187](#)  
    ActiveMQ JMS broker status .....[187](#)  
association .....[135](#)  
associations .....[141](#)

    resolving error conditions when modifying or  
        removing associations .....[141](#)  
Avaya IQ application troubleshooting .....[11](#)  
Avaya IQ does not start .....[67](#)  
Avaya IQ Performance Center .....[144](#)  
    managing external application links .....[144](#)  
avaya.debug.log .....[90](#)  
avaya.hostlogserver.log .....[53](#)  
avaya.networklogserver.log .....[53](#)

---

### B

backing up Avaya IQ data .....[202](#)  
    on a software-only deployment .....[202](#)  
backing up certificates .....[159](#)  
backing up the database .....[203](#)  
    on a software-only deployment .....[203](#)  
backing up the OS .....[203](#)  
    in a software-only deployment .....[203](#)  
backup .....[209](#), [214](#)  
    activating the backup feature .....[209](#)  
    on Windows .....[214](#)  
backup mount point .....[207](#), [242](#), [253](#), [266](#), [287](#)  
    verifying on the host .....[207](#), [242](#), [253](#), [266](#), [287](#)  
backup strategies .....[199](#)  
backups .....[204](#), [206](#), [210–214](#)  
    about enabling backups .....[206](#)  
    confirming a successful database data backup on  
        the database host .....[213](#)  
    confirming a successful system data backup on the  
        Avaya IQ host .....[212](#)  
    custom reports .....[204](#), [214](#)  
    running an on-demand backup .....[210](#)  
    running an on-demand backup of system and  
        database data on the database host ....[211](#)  
    running an on-demand system backup on an  
        application host .....[211](#)  
    worksheet .....[206](#)

---

### C

call event data lost .....[67](#)  
ccrDataSource.log .....[53](#)  
ccrFocus.log .....[53](#)  
ccrReports.log .....[53](#)  
centralized logging missing .....[66](#)  
certificate signing requests .....[160](#)

|                                                                       |                                   |                                                    |                                |
|-----------------------------------------------------------------------|-----------------------------------|----------------------------------------------------|--------------------------------|
| certificates .....                                                    | <a href="#">157, 158, 171–176</a> | configuration information errors .....             | <a href="#">67</a>             |
| adding .....                                                          | <a href="#">174</a>               | confirming a successful restore .....              | <a href="#">276</a>            |
| creating default server certificate settings .....                    | <a href="#">173</a>               | considerations .....                               | <a href="#">134</a>            |
| deleting .....                                                        | <a href="#">176</a>               | for updating associations between sources and      |                                |
| deleting trusted certificates .....                                   | <a href="#">173</a>               | hosts .....                                        | <a href="#">134</a>            |
| exporting .....                                                       | <a href="#">175</a>               | contact data .....                                 | <a href="#">79</a>             |
| exporting trusted certificates .....                                  | <a href="#">173</a>               | container .....                                    | <a href="#">61, 72, 77</a>     |
| importing .....                                                       | <a href="#">175</a>               | descriptions .....                                 | <a href="#">72</a>             |
| importing trusted certificates .....                                  | <a href="#">172</a>               | editing .....                                      | <a href="#">77</a>             |
| listing .....                                                         | <a href="#">174</a>               | Container View icons .....                         | <a href="#">73</a>             |
| listing trusted certificates .....                                    | <a href="#">171</a>               | Container View page .....                          | <a href="#">77</a>             |
| viewing .....                                                         | <a href="#">174</a>               | containers and PEs .....                           | <a href="#">74</a>             |
| viewing pending .....                                                 | <a href="#">176</a>               | how they are grouped .....                         | <a href="#">74</a>             |
| viewing trusted certificates .....                                    | <a href="#">172</a>               | coreservices logs .....                            | <a href="#">53</a>             |
| chain of trust .....                                                  | <a href="#">168</a>               | correcting daylight saving time error .....        | <a href="#">179</a>            |
| change default values .....                                           | <a href="#">194</a>               | CS Foundation subsystem .....                      | <a href="#">75</a>             |
| changing .....                                                        | <a href="#">150–152</a>           | CS Tomcat Basic .....                              | <a href="#">17, 66, 72</a>     |
| database user names or passwords .....                                | <a href="#">150</a>               | CS Tomcat container .....                          | <a href="#">17, 65–68, 72</a>  |
| SDS password on Avaya IQ .....                                        | <a href="#">151</a>               | custom conditions .....                            | <a href="#">51</a>             |
| user name or password on Avaya IQ .....                               | <a href="#">152</a>               |                                                    |                                |
| Changing .....                                                        | <a href="#">95</a>                |                                                    |                                |
| password .....                                                        | <a href="#">95</a>                | <b>D</b>                                           |                                |
| administration user in Tomcat .....                                   | <a href="#">95</a>                | data backups and database maintenance for turnkey  |                                |
| Changing host name and IP address .....                               | <a href="#">118</a>               | deployments .....                                  | <a href="#">204</a>            |
| admonishments .....                                                   | <a href="#">118</a>               | Data Collection host .....                         | <a href="#">64</a>             |
| changing host names and IP addresses .....                            | <a href="#">118, 119</a>          | Data Collection JBoss container .....              | <a href="#">17, 67, 68, 72</a> |
| prerequisites .....                                                   | <a href="#">119</a>               | Data Collection subsystem .....                    | <a href="#">75</a>             |
| Changing host names and IP addresses .....                            | <a href="#">118, 131</a>          | Data Export PE .....                               | <a href="#">70</a>             |
| considerations .....                                                  | <a href="#">118</a>               | data flow .....                                    | <a href="#">18, 20</a>         |
| troubleshooting .....                                                 | <a href="#">131</a>               | dual hosts .....                                   | <a href="#">18</a>             |
| Changing host names or IP addresses <a href="#">120, 124–126, 128</a> |                                   | historical .....                                   | <a href="#">20</a>             |
| centralized process .....                                             | <a href="#">120, 124, 125</a>     | multiple hosts .....                               | <a href="#">18</a>             |
| verifying successful change .....                                     | <a href="#">124</a>               | real-time .....                                    | <a href="#">20</a>             |
| verifying successful rollback .....                                   | <a href="#">125</a>               | single host .....                                  | <a href="#">18</a>             |
| manual process .....                                                  | <a href="#">126, 128</a>          | data flow stopped .....                            | <a href="#">69</a>             |
| generating control files .....                                        | <a href="#">126</a>               | data flow through system stops .....               | <a href="#">69</a>             |
| checking reports .....                                                | <a href="#">89</a>                | data flows .....                                   | <a href="#">17</a>             |
| clearing alarms, cannot .....                                         | <a href="#">65</a>                | data is lost .....                                 | <a href="#">67</a>             |
| click through .....                                                   | <a href="#">144</a>               | data missing from summary historical reports ..... | <a href="#">68</a>             |
| CM Message Parser .....                                               | <a href="#">21, 23</a>            | data not displayed .....                           | <a href="#">186</a>            |
| CMAAdapter .....                                                      | <a href="#">21, 23</a>            | data processing fails .....                        | <a href="#">69</a>             |
| CMIT .....                                                            | <a href="#">21, 23</a>            | Data Processing host .....                         | <a href="#">63</a>             |
| cognos fails during installation .....                                | <a href="#">184</a>               | Data Processing JBoss container .....              | <a href="#">17, 67, 68, 72</a> |
| cognos fails to start .....                                           | <a href="#">184</a>               | Data Processing subsystem .....                    | <a href="#">75</a>             |
| Communication Manager and Proactive Contact .....                     | <a href="#">81</a>                | data removal .....                                 | <a href="#">155</a>            |
| Communication Manager Input Translator (CMIT) <a href="#">21, 23</a>  |                                   | data restore .....                                 | <a href="#">228</a>            |
| Communication Manager source associations .....                       | <a href="#">138</a>               | data restores, overview .....                      | <a href="#">217</a>            |
| moving .....                                                          | <a href="#">138</a>               | data source releases, updating .....               | <a href="#">178</a>            |
| concepts .....                                                        | <a href="#">61</a>                | data source troubleshooting .....                  | <a href="#">13</a>             |
| troubleshooting .....                                                 | <a href="#">61</a>                | data, ensuring it is getting processed .....       | <a href="#">89</a>             |
| configCognos.log .....                                                | <a href="#">53</a>                | database backup .....                              | <a href="#">48</a>             |
|                                                                       |                                   | database diagnostic tool .....                     | <a href="#">36, 37</a>         |

|                                                                           |                                                  |
|---------------------------------------------------------------------------|--------------------------------------------------|
| database host                                                             | 211, 228, 239, 243, 257, 263, 267, 274, 285, 288 |
| installing the Oracle software                                            | 239, 263, 285                                    |
| replacing both system disks                                               | 257                                              |
| restoring the software base and database data                             | 288                                              |
| restoring the software base, system configuration data, and database data | 228, 243, 267, 274                               |
| running an on-demand backup of system and database data                   | 211                                              |
| database interfaces                                                       | 47                                               |
| database management                                                       | 154                                              |
| database monitoring diagnostics                                           | 35                                               |
| database schema check                                                     | 157                                              |
| database server resource conditions                                       | 44                                               |
| database server stability                                                 | 35                                               |
| database troubleshooting                                                  | 12                                               |
| database user and password maintenance                                    | 150                                              |
| DataCollectionJBoss_"SOURCENAME"                                          | 53                                               |
| DataCollectionJBoss.log                                                   | 53                                               |
| dataexport.log                                                            | 53                                               |
| DataProcessingJBoss_"SOURCENAME"                                          | 53                                               |
| DataProcessingJBoss.log                                                   | 53                                               |
| date and time zone                                                        | 149                                              |
| using the command                                                         | 149                                              |
| Date and time zone command options                                        | 148                                              |
| date, time, and NTP status, verifying                                     | 150                                              |
| dbsetup/dbsetup.log                                                       | 53                                               |
| Delete buffer storage and index files                                     | 196                                              |
| Data Processing configuration                                             | 196                                              |
| deleting                                                                  | 173, 176                                         |
| server certificates                                                       | 176                                              |
| trusted certificates                                                      | 173                                              |
| Deleting buffer storage and index files                                   | 197                                              |
| deleting Communication Manager source                                     | 139                                              |
| differences between software-only and turnkey                             | 93                                               |
| disk layouts on turnkey system                                            | 230                                              |
| dual host data flow                                                       | 18                                               |

## E

|                                           |     |
|-------------------------------------------|-----|
| e-mail server maintenance                 | 114 |
| Edit Container page                       | 77  |
| editing containers                        | 77  |
| editing properties                        | 114 |
| enabling report usage information         | 57  |
| ensuring that data is getting processed   | 89  |
| error adjustment for daylight saving time | 179 |
| error messages in reports                 | 69  |
| evens and administration data flow        | 19  |
| EXP3000 recovery                          | 270 |
| exporting server certificates             | 175 |
| exporting trusted certificates            | 173 |

|                                                   |    |
|---------------------------------------------------|----|
| external applications cannot access Avaya IQ data | 70 |
|---------------------------------------------------|----|

## G

|                                |     |
|--------------------------------|-----|
| gathering recovery information | 227 |
|--------------------------------|-----|

## H

|                                              |                             |
|----------------------------------------------|-----------------------------|
| hardware troubleshooting                     | 11                          |
| HDAPR                                        | 23                          |
| HDR                                          | 23                          |
| HEP                                          | 21                          |
| hex_dump_all.log                             | 21, 23, 53, 90              |
| historical administration data not recorded  | 68                          |
| Historical Data Consolidation subsystem      | 75                          |
| historical data flow                         | 20                          |
| historical data lost                         | 67                          |
| Historical Data Store                        | 21, 23                      |
| historical user permission data not recorded | 68                          |
| host                                         | 61, 207, 242, 253, 266, 287 |
| verifying backup mount point                 | 207, 242, 253, 266, 287     |
| host administration parameter                | 117                         |
| Host View icons                              | 73                          |
| Host View page                               | 74                          |
| HOT                                          | 21                          |
| how containers and PEs are grouped           | 74                          |

## I

|                                            |                                             |
|--------------------------------------------|---------------------------------------------|
| importing server certificates              | 175                                         |
| importing trusted certificates             | 172                                         |
| initial synchronization fails              | 69                                          |
| input translator                           | 180                                         |
| InputTranslator component                  | 183                                         |
| InSite Knowledge Management                | 14                                          |
| installing                                 | 111, 231, 239, 240, 252, 263, 265, 285, 286 |
| license file                               | 111                                         |
| Oracle software on the application host    | 240, 252, 265, 286                          |
| Oracle software on the database host       | 239, 263, 285                               |
| replacement disks when a single disk fails | 231                                         |
| installing certificates                    | 163                                         |
| installing the OS and running First Boot   | 234, 248, 259, 280                          |
| on the application host                    | 234, 248, 259, 280                          |
| Installing trusted server Certificates     | 132                                         |
| IQ                                         | 195                                         |
| pump-up request fails                      | 195                                         |
| pumpup request fails                       | 195                                         |
| IQIA                                       | 191–193                                     |
| JMS messages                               | 191                                         |

|                             |                                         |
|-----------------------------|-----------------------------------------|
| linkdown message .....      | <a href="#">192</a>                     |
| pump-up request fails ..... | <a href="#">193</a>                     |
| IQIA data source .....      | <a href="#">185</a>                     |
| entities .....              | <a href="#">185</a>                     |
| IRS JBoss container .....   | <a href="#">69</a> , <a href="#">72</a> |

## K

|                                |                    |
|--------------------------------|--------------------|
| key management .....           | <a href="#">27</a> |
| Key Management subsystem ..... | <a href="#">75</a> |
| Knowledge Management .....     | <a href="#">14</a> |

## L

|                                      |                                                                 |
|--------------------------------------|-----------------------------------------------------------------|
| lcm.log .....                        | <a href="#">53</a>                                              |
| licensing .....                      | <a href="#">106</a> , <a href="#">110</a> – <a href="#">113</a> |
| acquiring a license file .....       | <a href="#">110</a>                                             |
| checking license status .....        | <a href="#">112</a>                                             |
| installing a license file .....      | <a href="#">111</a>                                             |
| replacing a license file .....       | <a href="#">113</a>                                             |
| Lifecycle .....                      | <a href="#">53</a>                                              |
| lifecycle manager .....              | <a href="#">61</a>                                              |
| Lifecycle Manager .....              | <a href="#">17</a>                                              |
| Lifecycle watchdog, see watchd ..... | <a href="#">30</a>                                              |
| listing .....                        | <a href="#">174</a>                                             |
| server certificates .....            | <a href="#">174</a>                                             |
| listing trusted certificates .....   | <a href="#">171</a>                                             |
| log files .....                      | <a href="#">53</a> , <a href="#">59</a>                         |
| descriptions .....                   | <a href="#">53</a>                                              |
| sending to support .....             | <a href="#">59</a>                                              |
| viewing .....                        | <a href="#">53</a>                                              |
| log messages .....                   | <a href="#">53</a>                                              |
| enabling .....                       | <a href="#">53</a>                                              |
| log messages not reported .....      | <a href="#">66</a>                                              |
| logs .....                           | <a href="#">94</a>                                              |
| lost call event data .....           | <a href="#">67</a>                                              |

## M

|                                        |                                                                                   |
|----------------------------------------|-----------------------------------------------------------------------------------|
| managing database stability .....      | <a href="#">35</a>                                                                |
| Message Broker Service container ..... | <a href="#">69</a> , <a href="#">72</a>                                           |
| Message Parser .....                   | <a href="#">21</a> , <a href="#">23</a>                                           |
| messages_cmit.log .....                | <a href="#">21</a> , <a href="#">23</a> , <a href="#">53</a>                      |
| messages_cmmsgs.log .....              | <a href="#">21</a> , <a href="#">23</a> , <a href="#">53</a>                      |
| messages_hdapr.log .....               | <a href="#">23</a> , <a href="#">53</a>                                           |
| messages_hdr.log .....                 | <a href="#">23</a> , <a href="#">53</a>                                           |
| messages_hep.log .....                 | <a href="#">21</a> , <a href="#">53</a>                                           |
| messages_hot.log .....                 | <a href="#">21</a> , <a href="#">53</a>                                           |
| messages_pcit.log .....                | <a href="#">21</a> , <a href="#">23</a> , <a href="#">53</a> , <a href="#">91</a> |
| messages_pcmmsgs.log .....             | <a href="#">21</a> , <a href="#">23</a> , <a href="#">53</a> , <a href="#">91</a> |
| messages_rdapr.log .....               | <a href="#">23</a> , <a href="#">53</a>                                           |

|                                                                                        |                                         |
|----------------------------------------------------------------------------------------|-----------------------------------------|
| messages_rdr.log .....                                                                 | <a href="#">23</a> , <a href="#">53</a> |
| messages_rep.log .....                                                                 | <a href="#">21</a> , <a href="#">53</a> |
| messages_rot.log .....                                                                 | <a href="#">21</a> , <a href="#">53</a> |
| Messaging subsystem .....                                                              | <a href="#">75</a>                      |
| metadata sanity check .....                                                            | <a href="#">157</a>                     |
| missing data in reports .....                                                          | <a href="#">69</a>                      |
| modifying .....                                                                        | <a href="#">134</a>                     |
| parameters of an existing Communication Manager<br>source association .....            | <a href="#">134</a>                     |
| monitoring the system .....                                                            | <a href="#">94</a>                      |
| moving .....                                                                           | <a href="#">135</a>                     |
| association of a Communication Manager source<br>from one host to another host .....   | <a href="#">135</a>                     |
| moving association of a Communication Manager source<br>from one host to another ..... | <a href="#">135</a>                     |
| MSGBROKER .....                                                                        | <a href="#">53</a>                      |
| MSGBROKER.log .....                                                                    | <a href="#">53</a>                      |
| multiple hosts data flow .....                                                         | <a href="#">18</a>                      |

## N

|                                            |                     |
|--------------------------------------------|---------------------|
| names data .....                           | <a href="#">79</a>  |
| network troubleshooting .....              | <a href="#">13</a>  |
| networklogserver.log .....                 | <a href="#">66</a>  |
| NFS mount point for backups, setting ..... | <a href="#">208</a> |

## O

|                                                                     |                                                                                                                                                         |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|
| OAM connection names and corresponding database<br>user names ..... | <a href="#">154</a>                                                                                                                                     |
| OAM interface, cannot log into .....                                | <a href="#">66</a>                                                                                                                                      |
| operational state data .....                                        | <a href="#">79</a>                                                                                                                                      |
| oracle alert log management .....                                   | <a href="#">46</a>                                                                                                                                      |
| oracle backup management .....                                      | <a href="#">47</a>                                                                                                                                      |
| Oracle RMAN .....                                                   | <a href="#">219</a>                                                                                                                                     |
| Oracle software .....                                               | <a href="#">239</a> , <a href="#">240</a> , <a href="#">252</a> , <a href="#">263</a> , <a href="#">265</a> , <a href="#">285</a> , <a href="#">286</a> |
| installing on the application host ..                               | <a href="#">240</a> , <a href="#">252</a> , <a href="#">265</a> , <a href="#">286</a>                                                                   |
| installing on the database host .....                               | <a href="#">239</a> , <a href="#">263</a> , <a href="#">285</a>                                                                                         |
| oracle tablespace condition .....                                   | <a href="#">38</a>                                                                                                                                      |
| outbound call event data lost .....                                 | <a href="#">68</a>                                                                                                                                      |
| overview of Avaya IQ data restores .....                            | <a href="#">217</a>                                                                                                                                     |

## P

|                                              |                                           |
|----------------------------------------------|-------------------------------------------|
| passwords .....                              | <a href="#">151</a> , <a href="#">152</a> |
| changing a user name or password on Avaya IQ | <a href="#">152</a>                       |
| changing the SDS password on Avaya IQ .....  | <a href="#">151</a>                       |
| PC Message Parser .....                      | <a href="#">21</a> , <a href="#">23</a>   |
| PCAdapter .....                              | <a href="#">21</a> , <a href="#">23</a>   |
| PCIT .....                                   | <a href="#">21</a> , <a href="#">23</a>   |
| PE .....                                     | <a href="#">77</a>                        |



|                                                   |                                         |                                                        |                                                                 |
|---------------------------------------------------|-----------------------------------------|--------------------------------------------------------|-----------------------------------------------------------------|
| detailed data .....                               | <a href="#">77</a>                      | pump-up command syntax .....                           | <a href="#">32</a>                                              |
| PE Admin Recorder .....                           | <a href="#">71</a>                      | pump-up, see synchronization .....                     | <a href="#">79</a>                                              |
| PE Aggregation .....                              | <a href="#">68</a>                      | pumpup .....                                           | <a href="#">31</a> , <a href="#">180</a>                        |
| PE Alarm Config Server .....                      | <a href="#">65</a>                      | overview .....                                         | <a href="#">31</a>                                              |
| PE Alarm Retriever Server .....                   | <a href="#">65</a>                      | pumpup monitoring tool .....                           | <a href="#">31</a>                                              |
| PE Alarm Server .....                             | <a href="#">65</a>                      |                                                        |                                                                 |
| PE Alarm Service .....                            | <a href="#">65</a>                      |                                                        |                                                                 |
| PE and subsystem descriptions .....               | <a href="#">75</a>                      | <b>Q</b>                                               |                                                                 |
| PE Authorization Service .....                    | <a href="#">65</a>                      | queue size limit hit .....                             | <a href="#">180</a>                                             |
| PE CM Adapter .....                               | <a href="#">67</a> , <a href="#">82</a> |                                                        |                                                                 |
| PE Event Processor .....                          | <a href="#">67</a>                      |                                                        |                                                                 |
| PE HDAPR Entity Monitor .....                     | <a href="#">68</a>                      | <b>R</b>                                               |                                                                 |
| PE HDR Entity Monitor .....                       | <a href="#">68</a>                      | RBAC .....                                             | <a href="#">23</a>                                              |
| PE Host Log Retriever Server .....                | <a href="#">66</a>                      | RDAPR .....                                            | <a href="#">23</a>                                              |
| PE Host Log Server .....                          | <a href="#">66</a>                      | RDR .....                                              | <a href="#">23</a>                                              |
| PE IQIA AACC source status .....                  | <a href="#">187</a>                     | real time administration data not recorded .....       | <a href="#">70</a>                                              |
| PE IRS .....                                      | <a href="#">69</a>                      | Real Time Data Consolidation subsystem .....           | <a href="#">75</a>                                              |
| PE Key Authority .....                            | <a href="#">69</a>                      | Real Time Data Store .....                             | <a href="#">21</a> , <a href="#">23</a>                         |
| PE Load Date .....                                | <a href="#">69</a>                      | Real Time Report Execution subsystem .....             | <a href="#">75</a>                                              |
| PE Message Broker .....                           | <a href="#">69</a>                      | real time user permission data not recorded .....      | <a href="#">70</a>                                              |
| PE Network Log Retriever Server .....             | <a href="#">66</a>                      | real-time data flow .....                              | <a href="#">20</a>                                              |
| PE Network Log Server .....                       | <a href="#">66</a>                      | Realtime Dashboard .....                               | <a href="#">75</a>                                              |
| PE Network Log Service .....                      | <a href="#">66</a>                      | Realtime Dashboard Tomcat .....                        | <a href="#">72</a>                                              |
| PE OAM .....                                      | <a href="#">66</a>                      | reasons for restoring Avaya IQ .....                   | <a href="#">217</a>                                             |
| PE PDS Adapter .....                              | <a href="#">68</a> , <a href="#">82</a> | rebooting hosts .....                                  | <a href="#">99</a>                                              |
| PE RDAPR Entity Monitor .....                     | <a href="#">70</a>                      | reboots .....                                          | <a href="#">96</a>                                              |
| PE RDR Entity Monitor .....                       | <a href="#">70</a>                      | rebuilding system disks .....                          | <a href="#">232</a> , <a href="#">246</a> , <a href="#">257</a> |
| PE Real Time Report Service .....                 | <a href="#">70</a>                      | on the application or database host ...                | <a href="#">232</a> , <a href="#">246</a> , <a href="#">257</a> |
| PE Recorder .....                                 | <a href="#">67</a>                      | recovering and restoring the database host .....       | <a href="#">222</a>                                             |
| PE Reporting Application .....                    | <a href="#">71</a>                      | Recovery Manager .....                                 | <a href="#">219</a>                                             |
| PE Reporting Web .....                            | <a href="#">71</a>                      | redo log management .....                              | <a href="#">44</a>                                              |
| PE Scheduler .....                                | <a href="#">71</a>                      | reinitialize user service .....                        | <a href="#">157</a>                                             |
| PE SDAS .....                                     | <a href="#">67</a>                      | removing .....                                         | <a href="#">138</a>                                             |
| performance metrics .....                         | <a href="#">50</a>                      | Communication Manager source associations .            | <a href="#">138</a>                                             |
| Ping Host field descriptions .....                | <a href="#">77</a>                      | removing data .....                                    | <a href="#">155</a> , <a href="#">156</a>                       |
| Ping Host page .....                              | <a href="#">77</a>                      | from a single fact table .....                         | <a href="#">156</a>                                             |
| ping test .....                                   | <a href="#">29</a>                      | from all fact tables .....                             | <a href="#">155</a>                                             |
| power-cycling a dual host deployment .....        | <a href="#">104</a>                     | removing obsolete users .....                          | <a href="#">156</a>                                             |
| power-cycling a multi-host deployment .....       | <a href="#">105</a>                     | RCL tables .....                                       | <a href="#">156</a>                                             |
| power-cycling a single host deployment .....      | <a href="#">103</a>                     | REP .....                                              | <a href="#">21</a>                                              |
| power-cycling an All-in-One host deployment ..... | <a href="#">103</a>                     | replacement disks, installing when a single disk fails | <a href="#">231</a>                                             |
| power-cycling hosts .....                         | <a href="#">103</a>                     | replacing both system disks on an Avaya IQ application |                                                                 |
| powering .....                                    | <a href="#">96</a>                      | host .....                                             | <a href="#">232</a> , <a href="#">245</a>                       |
| prerequisites for restoring Avaya IQ data .....   | <a href="#">218</a>                     | replacing both system disks on that database host .    | <a href="#">257</a>                                             |
| Proactive Contact Input Translator (PCIT) .....   | <a href="#">21</a> , <a href="#">23</a> | report input page .....                                | <a href="#">185</a> , <a href="#">186</a>                       |
| Proactive Contact maintenance .....               | <a href="#">143</a>                     | data not displayed .....                               | <a href="#">185</a>                                             |
| processing element .....                          | <a href="#">61</a>                      | Report Management subsystem .....                      | <a href="#">75</a>                                              |
| Processing Element Status Information page .....  | <a href="#">77</a>                      | Reporting Application Service container .....          | <a href="#">17</a> , <a href="#">71</a> , <a href="#">72</a>    |
| pu_admin_full.hex .....                           | <a href="#">53</a> , <a href="#">90</a> | reporting host .....                                   | <a href="#">116</a>                                             |
| pu_admin_name.hex .....                           | <a href="#">53</a> , <a href="#">90</a> | changing the reporting host used for aggregation       | <a href="#">116</a>                                             |
| pu_oper.hex .....                                 | <a href="#">53</a> , <a href="#">90</a> | Reporting hosts .....                                  | <a href="#">64</a>                                              |

|                                                                                                     |                                            |                                                  |                          |
|-----------------------------------------------------------------------------------------------------|--------------------------------------------|--------------------------------------------------|--------------------------|
| Reporting JBoss container .....                                                                     | <a href="#">17, 70, 72</a>                 | routine system restart .....                     | <a href="#">99</a>       |
| reporting user interface disabled .....                                                             | <a href="#">70</a>                         | RTD hosts .....                                  | <a href="#">64</a>       |
| reporting Web page inaccessible .....                                                               | <a href="#">70</a>                         | RTD report usage monitoring .....                | <a href="#">58</a>       |
| Reporting Web Service container .....                                                               | <a href="#">17, 71, 72</a>                 | disabling .....                                  | <a href="#">58</a>       |
| Reporting_Execution .....                                                                           | <a href="#">53</a>                         | RTD/* .....                                      | <a href="#">53</a>       |
| Reporting_Execution.log .....                                                                       | <a href="#">53</a>                         | run pump-up .....                                | <a href="#">33</a>       |
| REPORTING_RECORDERS .....                                                                           | <a href="#">53</a>                         | run pump-up in the background .....              | <a href="#">34</a>       |
| Reporting_UI .....                                                                                  | <a href="#">53</a>                         | running a ping test .....                        | <a href="#">29</a>       |
| Reporting_UI.log .....                                                                              | <a href="#">53</a>                         |                                                  |                          |
| reports contain erroneous or missing data .....                                                     | <a href="#">69</a>                         | <b>S</b>                                         |                          |
| reports do not run .....                                                                            | <a href="#">71</a>                         | SaN .....                                        | <a href="#">23</a>       |
| reports, checking .....                                                                             | <a href="#">89</a>                         | scheduled jobs do not run .....                  | <a href="#">71</a>       |
| resolving error conditions when modifying or removing<br>associations .....                         | <a href="#">141</a>                        | security/avaya.security.log .....                | <a href="#">53</a>       |
| restarting .....                                                                                    | <a href="#">30</a>                         | SEILink .....                                    | <a href="#">190, 191</a> |
| Avaya IQ .....                                                                                      | <a href="#">30</a>                         | heartbeat messages .....                         | <a href="#">190</a>      |
| restarting a dual host deployment .....                                                             | <a href="#">100</a>                        | CORBA errors .....                               | <a href="#">191</a>      |
| restarting a single host deployment .....                                                           | <a href="#">100</a>                        | SEILink heartbeat messages .....                 | <a href="#">190</a>      |
| restarting an All-in-One host deployment .....                                                      | <a href="#">100</a>                        | Service Locator .....                            | <a href="#">17</a>       |
| restarting application hosts .....                                                                  | <a href="#">98</a>                         | setting NFS mount point for backups .....        | <a href="#">208</a>      |
| restarting the database host .....                                                                  | <a href="#">98</a>                         | single host data flow .....                      | <a href="#">18</a>       |
| restarts .....                                                                                      | <a href="#">96</a>                         | SNMP events are not propagated .....             | <a href="#">65</a>       |
| restore .....                                                                                       | <a href="#">276</a>                        | software updates .....                           | <a href="#">113</a>      |
| confirming successful restore .....                                                                 | <a href="#">276</a>                        | software-only deployment .....                   | <a href="#">202, 203</a> |
| restore scenarios .....                                                                             | <a href="#">226</a>                        | about backing up the database .....              | <a href="#">203</a>      |
| restored directories and files .....                                                                | <a href="#">218</a>                        | backing up Avaya IQ data .....                   | <a href="#">202</a>      |
| restoring .....                                                                                     | <a href="#">225, 292</a>                   | backing up the operating system .....            | <a href="#">203</a>      |
| custom reports .....                                                                                | <a href="#">225, 292</a>                   | standard real-time report usage monitoring ..... | <a href="#">58, 59</a>   |
| restoring Avaya IQ data .....                                                                       | <a href="#">218</a>                        | disabling .....                                  | <a href="#">59</a>       |
| prerequisites .....                                                                                 | <a href="#">218</a>                        | enabling .....                                   | <a href="#">58</a>       |
| restoring Avaya IQ files or directories .....                                                       | <a href="#">224, 291</a>                   | Starting Avaya IQ services .....                 | <a href="#">132</a>      |
| restoring Avaya IQ in a software-only deployment .....                                              | <a href="#">219</a>                        | stopping the pump-up .....                       | <a href="#">34</a>       |
| restoring Avaya IQ, reasons .....                                                                   | <a href="#">217</a>                        | submitting CSRs .....                            | <a href="#">162</a>      |
| restoring back to 5.1.1 .....                                                                       | <a href="#">280</a>                        | subsystem .....                                  | <a href="#">61</a>       |
| restoring data on a turnkey deployment .....                                                        | <a href="#">225</a>                        | subsystem and PE descriptions .....              | <a href="#">75</a>       |
| restoring the software base and database data on<br>database host .....                             | <a href="#">288</a>                        | summary historical reports missing data .....    | <a href="#">68</a>       |
| restoring the software base and system configuration<br>data on the application host .....          | <a href="#">254, 289</a>                   | support, sending log files to .....              | <a href="#">59</a>       |
| restoring the software base, system configuration data,<br>and database data on database host ..... | <a href="#">228, 243,<br/>267,<br/>274</a> | synchronization .....                            | <a href="#">79</a>       |
| RFTB .....                                                                                          | <a href="#">79, 80</a>                     | Synchronization and Notification (SaN) .....     | <a href="#">23</a>       |
| RLTB .....                                                                                          | <a href="#">80</a>                         | synchronization data flow .....                  | <a href="#">82</a>       |
| RMAN .....                                                                                          | <a href="#">219</a>                        | phase 1 .....                                    | <a href="#">82</a>       |
| Role Based Access Control .....                                                                     | <a href="#">23</a>                         | synchronization data flows .....                 | <a href="#">83–87</a>    |
| Rollback host name or IP address changes .....                                                      | <a href="#">124, 130</a>                   | phase 2 .....                                    | <a href="#">83</a>       |
| centralized process .....                                                                           | <a href="#">124</a>                        | phase 3 .....                                    | <a href="#">84</a>       |
| manual process .....                                                                                | <a href="#">130</a>                        | phase 4 .....                                    | <a href="#">85</a>       |
| rollback to 5.1.1 .....                                                                             | <a href="#">280</a>                        | phase 5 .....                                    | <a href="#">86</a>       |
| ROT .....                                                                                           | <a href="#">21</a>                         | phase 6 .....                                    | <a href="#">87</a>       |
|                                                                                                     |                                            | synchronization verification .....               | <a href="#">88</a>       |
|                                                                                                     |                                            | synchronizing JKS .....                          | <a href="#">177</a>      |
|                                                                                                     |                                            | System Management subsystem .....                | <a href="#">75</a>       |
|                                                                                                     |                                            | system monitoring .....                          | <a href="#">94</a>       |
|                                                                                                     |                                            | system restart .....                             | <a href="#">99</a>       |

|                                             |                         |                                                     |                                         |
|---------------------------------------------|-------------------------|-----------------------------------------------------|-----------------------------------------|
| system status, verifying .....              | <a href="#">29</a>      | updating associations between sources and hosts . . | <a href="#">134</a>                     |
| <hr/>                                       |                         | considerations for customers .....                  | <a href="#">134</a>                     |
| <b>T</b>                                    |                         | users .....                                         | <a href="#">94</a>                      |
| terms .....                                 | <a href="#">61</a>      | cleaning up user accounts .....                     | <a href="#">94</a>                      |
| troubleshooting .....                       | <a href="#">61</a>      | using database diagnostic tool .....                | <a href="#">37</a>                      |
| time zone data .....                        | <a href="#">147</a>     | <hr/>                                               |                                         |
| Tomcat .....                                | <a href="#">168–170</a> | <b>V</b>                                            |                                         |
| changes for trusted certificates .....      | <a href="#">170</a>     | vendor software troubleshooting .....               | <a href="#">14</a>                      |
| traffic_data.hex .....                      | <a href="#">53, 90</a>  | verifying .....                                     | <a href="#">150</a>                     |
| troubleshooting .....                       | <a href="#">91</a>      | date, time, and NTP status .....                    | <a href="#">150</a>                     |
| ETL application .....                       | <a href="#">91</a>      | verifying backup mount point .....                  | <a href="#">207, 242, 253, 266, 287</a> |
| troubleshooting certificates .....          | <a href="#">177</a>     | on application host .....                           | <a href="#">207, 242, 253, 266, 287</a> |
| troubleshooting concepts .....              | <a href="#">61</a>      | verifying system status .....                       | <a href="#">29</a>                      |
| troubleshooting pump-up .....               | <a href="#">180</a>     | viewing .....                                       | <a href="#">172, 174, 176</a>           |
| troubleshooting terms .....                 | <a href="#">61</a>      | certificates .....                                  | <a href="#">174</a>                     |
| turnkey deployments .....                   | <a href="#">204</a>     | pending certificates .....                          | <a href="#">176</a>                     |
| data backups and database maintenance ..... | <a href="#">204</a>     | trusted certificates .....                          | <a href="#">172</a>                     |
| turnkey systems .....                       | <a href="#">230</a>     | <hr/>                                               |                                         |
| disk layouts .....                          | <a href="#">230</a>     | <b>W</b>                                            |                                         |
| <hr/>                                       |                         | watchd .....                                        | <a href="#">30, 53</a>                  |
| <b>U</b>                                    |                         | watchd.conf file .....                              | <a href="#">17</a>                      |
| updates .....                               | <a href="#">113</a>     | wdinit start .....                                  | <a href="#">30</a>                      |
| updating .....                              | <a href="#">178</a>     | wdinit stop .....                                   | <a href="#">30</a>                      |
| data source releases .....                  | <a href="#">178</a>     | wdlog and wdlog_p .....                             | <a href="#">53</a>                      |

