Avaya Aura® Session Manager Call Detail Recording Interface

Abstract

The purpose of this document is to provide the technical interface details necessary to design and build a product which is capable of successfully collecting and managing the CDR data files produced by the new Avaya Aura® Session Manager.

TABLE OF CONTENTS

TABLE OF TABLES

1. INTRODUCTION

This document is intended to provide the technical details necessary to successfully design and build a product which is capable of retrieving and managing the CDR data files produced by the new Avaya Aura® Session Manager.

Topics covered in this document include:

- A description of the Avaya Aura® Session Manager CDR interface architecture
- The required security provisions
- The CDR data file naming convention and structure used by Avaya Aura® Session Manager CDR
- The supported data transport protocols
- A description of the provisions employed to delete the CDR data files
- An example scenario describing the provisions, procedures and concerns associated with the Avaya Aura® Session Manager CDR

Note to the Reader: Unless specifically specified otherwise, throughout the remainder of this document the terms “server” and/or “Session Manager” are intended to refer to the Avaya Aura® Session Manager.

1.1 INTENDED AUDIENCE

The intended audience for this document is the community of companies and organizations that design, build, market and support Session Manager CDR adjunct systems.

1.2 TERMINOLOGY AND ACRONYMS

Table 1 provides a summary of some of the acronyms and terminology used in this document.

Table 1 - Terminology and Acronyms

TERM	MEANING
CDR	Call Detail Record or Call Detail Recording
CM	Avaya Aura® Communication Manager
MA-UUI	No message-associated user-to-user signaling
SFTP	Secure File Transfer Protocol or SSH File Transfer Protocol
SM	Avaya Aura® Session Manager

2. INTERFACE ARCHITECTURE HIGHLIGHTS

2.1 SESSION MANAGER CDR

The architecture of this feature centers on saving CDR records on the server’s local hard drive rather than transmitting CDR call files over an IP connection to the CDR adjunct.

When the Session Manager CDR feature is properly administered on a server, the Session Manager will save its CDR records on its local server’s hard drive. Periodically the CDR adjunct must then log on to each of the Session Manager’s servers and retrieve whatever CDR data files are available.

The CDR adjunct logs into the server via a special login and password that the server administrator has created especially for this purpose. The special login account is a member of the “CDR_User” group. For security reasons the special login used by the CDR adjunct is only given access to the directory where the CDR records are stored.

The CDR format utilized in the first release of Session Manager is a format compatible with existing CDR adjuncts connecting to the Avaya Aura® Communication Manager servers implementing the "Survivable CDR" feature utilizing the Communication Manager "Unformatted" record format, release CM 4.0 and higher.

2.2 CDR RECORD FORMAT

CDR data files produced by Session Manager contain two types of data records:

- date records
- call detail records

All data contained in the CDR data files is stored in standard ASCII characters.

Date Record

The date record is a timestamp in the CDR data file indicating to the CDR processing application that every call record that follows in the file is referred to the new date. The date record is used to synchronize the CDR adjunct's time and date processing with the starting time and date of the information in the CDR data file. Multiple date records can be put in a single CDR data file, even if no date change occurred. Normally, the SM CDR system outputs date information to the CDR data file:

- once a day at midnight
- when the date or time is manually changed on the server
- when a new CDR data file is created

To avoid inconsistencies between the date record and the call records following it, it is a common practice of the server to generate, regardless of the schedule at which CDR files are to be created, a new CDR data file just before midnight with all of the completed calls at that time. Note, in the table below, that the call records contain the time the call ended and the duration; therefore the remaining calls ending after midnight will be reported in the next CDR file, which will be using a date record with the new date. Date records are 13 characters long. The format of the Date record is as follows:

Table 2 – Date Record Format

Position	Description
1-2	Hour (leading 0s added if needed)
3	Colon (":")
4-5	Minute (leading 0s added if needed)
6	Blank
7-8	Month (leading 0s added if needed)
9	Slash ("/")
10-11	Day (leading 0s added if needed)
12	Carriage Return
13	Line Feed

For example, a CDR date record can be:

```
21:32 04/16<CR><LF>
```

Call Detail Record

Originally in SM CDR each call detail record contained 106 characters. The format was as follows:

Table 3 – Call Detail Record Data Format prior to SM 6.1

Position	Description
1-2	Time of day - hours
3-4	Time of day - minutes
5	Duration - hours
6-7	Duration - minutes
8	Duration – tenths of minutes
9	Condition Code
10-17	Space
18-32	Dialed number
33-42	Calling number
43-48	Space
49-55	Terminating SIP Entity
56-57	Space
58-64	Originating SIP Entity
65-73	Space
74	Feature Flag
75-92	Space
93	Bearer Capability Class
94	MA-UUI
95	Resource Flag
96-104	Space
105	Carriage Return
106	Line Feed

Beginning with SM 6.1 each call detail record contained 108 characters. The format is as follows:

Table 3a – Call Detail Record Data Format beginning in SM 6.1

SM CDR Format	
SM Position	**SM Description**
1-2	Time of day-hours
3-4	Time of day-minutes
5	Duration-hours
6-7	Duration-minutes
8	Duration-tenths of minutes
9	Condition code
10-17	Space
18-32	Dialed number
33-42	Calling number
43-48	Space
49-55	Terminating SIP Entity
56-57	Space
58-64	Originating SIP Entity
65-73	Space
74	Feature flag
75-92	Space
93	BCC
94	MA-UUI

SM CDR Format	
95	Resource flag
96-104	Space
105-106	Bandwidth
107	Carriage return
108	Line feed

Fields Description:

Time of day (4 digits): the time (two digit hours, two digit minutes) at which the call ended.

Duration (4 digits): the duration of the call, which the system records in hours (0 to 9), minutes (00 to 59), and tenth of minutes (0 to 9). The system rounds the duration of the call down in 6-seconds increments. For example, the system records the duration of a 5-second call as 0000.

This field will report a 9999 if the call was in progress when a time change was made on the system and the call duration can no longer be determined, and will report a 9599 for calls having a long duration (greater than 10 hours –see condition code 4 below).

Bandwidth (2 digits with a maximum value of '99') indicates the highest bandwidth used by the call, rounded to the nearest multiple of 64k (64,000), for example:

- 0 means < 32Kbps
- 1 means 64Kbps (± 32Kbps)
- 2 means 128Kbps (± 32Kbps)
- 16 means 1024Kbps (± 32Kbps) – this covers 1Mbps (1,000,000bps)
- 31 means 1984Kbps (± 32Kbps) – this covers 2Mbps (2,000,000bps)
- 32 means 2048Kbps (± 32 Kbps)
- 94 means 6016Kbps (± 32 Kbps) – this covers 6Mbps (6,000,000bps)
- 96 means 6144Kbps (± 32 Kbps)
- 99 means 6304Kbps or greater

Single-digit values are recorded with a leading blank (' 3' and not '03').

Condition Code (1 alphanumeric character): indicates the type of call that the call record describes, as listed below. For example, condition code 9 indicates a tandem call. The two condition codes shown in the following table are only condition codes used in the first release of Session Manager. Several other condition codes, still defined as one alphanumeric character, will be added in the following releases and will identify additional condition characteristics of the completed call.

Table 4 – Condition Codes

Code	Description
4	Identifies a call of extremely long duration (a call that lasts for 10 or more hours). When a call exceeds 10 hours, the system creates a call record with this condition code and duration of 9 hours, 59 minutes and 1-9 tenths of a minute. The system creates a similar call record with this condition code after each succeeding 10 hour period. When the call terminates, the system creates a final call record with the appropriate condition code identifying the type of call.
9	Identifies a tandem call. This is the normal condition code for calls that complete normally through SM. This condition code also is used for an incoming call

A	Identifies an outgoing call from a SIP phone

Note 1: The condition code of "A" was added beginning in SM 5.2 when the capability was added to SM to handle "URE to SRE/non-URE" and from "SRE to URE" calls.

Note 2: It is recommended that when the administrator is setting up the trunks in CM that will talk to SM, they turn off CDR on the "change signaling group" **CM SAT** screen for the IMS trunks. Otherwise, the **CM CDR** will capture 2 or more call records for each call. This occurs because of SM's Application Sequencing. These extra trunk records make processing the CM CDR records extremely difficult. (Today there is no automated method to easily merge CM and SM CDR records.)

Dialed Number (15 digits): the fifteen most significant digits of the numeric user portion of the request URI.

Calling Number (10 digits): the ten right-most significant digits of the numeric user portion identifying the calling number, taken from the P-Asserted-Identity: header (if not available, from the Contact:header and, if not available, from the From: header).

Terminating SIP Entity (7 alphanumeric characters): the last seven characters of the outbound SIP Entity administered on the SM server.

Originating SIP Entity (7 alphanumeric characters): the last seven characters of the inbound SIP Entity.

Feature Flag (1 numeric digit): set to "4" in the first SM release, and identifies a voice call with network answer supervision.

Bearer Capability Class (1 alphanumeric character): set to "M" in the first SM release, indicating multimedia call.

MA-UUI (1 numeric digit): set to the digit "0" in the first SM release, and indicating no message-associated user-to-user signaling.

Resource Flag (1 numeric digit): set to the digit "0" in the first SM release, and indicating a circuit-switched call, no conversion device used. Beginning in SM 6.1, the Resource Flag is be set to "4" whenever a call has had a video session during its lifetime.

Space (0x20), Carriage Return (0x0d), Line Feed (0x0a): the corresponding ASCII characters

The Session Manager CDR feature supports SFTP for the secure transfer of CDR data files, and the CDR adjunct must use the same protocol to access and retrieve the CDR data files from the servers.

3. MINIMUM REQUIREMENTS

The following minimum requirements must be met in order to support the Session Manager CDR functionality described in this Interface Document:

- The SM server must be running the first or a subsequent release of Session Manager.
- There must be IP connectivity between the CDR adjunct and the target server at least from time to time to allow remote collection of the CDR data files.

Please note that this document contains no minimum hardware or software specifications describing the revision or performance levels required for the CDR adjunct system. The specification of the adjunct's minimum requirements is left to the CDR adjunct vendor.

4. SECURITY PROVISIONS

If there are firewalls implemented anywhere between the CDR adjunct and the various Session Manager servers it may be necessary to "punch" pinholes in those firewalls to allow communications between the CDR adjunct and the servers. Please work with the network administrators to implement these pinholes if needed.

5. CDR DATA FILE NAMING AND STRUCTURE

The CDR data files generated by the Session Manager CDR feature are stored in a special directory[a] on the server which is created for the sole purpose of storing this information. Anytime the CDR adjunct logs into the server it will be provided direct access to this directory.

The CDR files stored in the mentioned special directory are those CDR data files that the server has completed and closed and that are now ready for the CDR adjunct to collect, process and subsequently delete from the server. Members of the CDR_User group are assigned the rights necessary to read and subsequently delete the CDR data files.

The file naming convention that is used for the CDR data files is as shown below:

tssssss-ssss-YYMMDD-hh_mm

Where:

The file name is fixed at 25 alphanumeric characters, including dashes "-" and underscore "_".

"t" is populated with the character "S" in the first SM release.

"ssssss-ssss" is an alphanumeric string of six characters, followed by a dash "-", and followed by an alphanumeric string of four characters, for a total of eleven characters. This string uniquely identifies the Session Manager server through its IPv4 IP address, in hexadecimal.

"YY" is a two digit number representing the year when the file was created.

"MM" is a two digit number representing the month when the file was created.

"DD" is the two digit number representing the day of the month when the file was created.

"hh" is the two digit number representing the hour of the day when the file was created. (24 hour clock server time)

"mm" is the two digit number representing the number of minutes after the hour when the file was created.

[a] The full path of this special directory is "/var/home/ftp/CDR" but it should be noted that the CDR adjunct's login is limited such that it can only access the files contained in this directory.

For example, for a CDR file created January 29, 2009 at 3:24 PM from a SM at IP address 142.9.147.59, the data file will be named

S008e09-933b-090129-15_24

Note: the CDR data files naming convention used by the Session Manager is compatible with the CDR data files naming convention used by the Avaya Aura® Communication Manager supporting the "CM Survivable CDR" functionality.

6. DATA TRANSPORT PROTOCOLS

Moving the CDR data files from the SM server to the CDR adjunct is accomplished by the CDR adjunct remotely logging on to the Session Manager server and using the SFTP[b] protocol to transfer the CDR data.

Client versions of the above protocol are available for Unix, Linux, Windows and Macintosh based computer platforms. Please see the footnote associated with SFTP for a partial list of available implementations of the protocol.

7. CDR DATA FILE DELETION PROVISIONS

There are two "normal" provisions for removing CDR data files from the server. These methods, listed in order of preference, are:

- Once the CDR adjunct has successfully retrieved a data file from the server and verified that it contains valid data, it is recommended that the adjunct delete it from the server using the provisions of SFTP.

- Anytime the SM server detects that the CDR data files stored on its local hard drive are older than 5 days, the server will automatically remove the identified CDR data file and records this activity in a log file named *cleanup.log*, available in the same directory of the CDR data files.

In addition to the above "normal" methods of removing the CDR data files, it is also possible for an onsite or remote switch administrator/technician (with proper logon permissions) to delete unwanted CDR data files via the appropriate BASH commands. Please note that, in order to perform this activity, the administrator/technician must either have root privileges or must be a member of the CDR_User group.

8. OPERATIONAL PROVISIONS, PROCEDURES AND CONCERNS

This section provides an example of a typical CDR data file retrieval session as well as suggestions and cautions concerning the setup and operation of the Session Manager CDR functionality.

8.1 CDR DATA FILE RETRIEVAL EXAMPLE

The following figure provides a screen capture of a typical manual CDR data file retrieval session from a single server named "MyServer.MyDomain.com". All user inputs are shown as **bold** and highlighted text. All other text is shown as normal text.

[b] "SSH File Transfer Protocol" Internet-Draft available from http://www.ietf.org/internet-drafts/draft-ietf-secsh-filexfer-12.txt. A partial list of available SFTP clients that could be considered for this application is available from http://en.wikipedia.org/wiki/List_of_SFTP_clients

```
C:\WINNT>sftp CDR@MySessionManager.MyDomain.com
Connecting to MySessionManager.MyDomain.com...
This system is restricted solely to authorized users for legitimate
business purposes only. The actual or attempted unauthorized access,
use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and
or criminal and civil penalties under state, federal, or other applicable
domestic and foreign laws.

The use of this system may be monitored and recorded for administrative
and security reasons.  Anyone accessing this system expressly consents
to such monitoring and recording, and is advised that if it reveals
possible evidence of criminal activity, the evidence of such activity
may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the
protection of information assets.
Password: XXXXXX
sftp>
sftp> mget S*
Fetching /S008709-9332-090416-08_26 to S008709-9332-090416-08_26
Fetching /S008709-9332-090416-08_36 to S008709-9332-090416-08_36
Fetching /S008709-9332-090416-08_46 to S008709-9332-090416-08_46
Fetching /S008709-9332-090416-08_56 to S008709-9332-090416-08_56
Fetching /S008709-9332-090416-09_06 to S008709-9332-090416-09_06
Fetching /S008709-9332-090416-09_16 to S008709-9332-090416-09_16
Fetching /S008709-9332-090416-09_26 to S008709-9332-090416-09_26
Fetching /S008709-9332-090416-09_36 to S008709-9332-090416-09_36
Fetching /S008709-9332-090416-21_41 to S008709-9332-090416-21_41
sftp>
sftp> lls –al
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-08_26
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-08_36
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-08_46
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-08_56
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-09_06
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-09_16
-rwxr-----   1 Test   445213 Apr 20 11:18 S008709-9332-090416-09_26
-rwxr-----   1 Test    85873 Apr 20 11:18 S008709-9332-090416-09_36
-rwxr-----   1 Test      331 Apr 20 11:18 S008709-9332-090416-21_41
sftp>
sftp>
sftp> rm S008709-9332-090416-08_26
Removing /S008709-9332-090416-08_26
sftp> rm S008709-9332-090416-08_36
Removing /S008709-9332-090416-08_36
sftp> rm S008709-9332-090416-08_46
Removing /S008709-9332-090416-08_46
sftp> rm S008709-9332-090416-08_56
Removing /S008709-9332-090416-08_56
sftp> rm S008709-9332-090416-09_06
Removing /S008709-9332-090416-08_06
sftp> rm S008709-9332-090416-09_16
Removing /S008709-9332-090416-08_16
sftp> rm S008709-9332-090416-09_26
Removing /S008709-9332-090416-09_26
sftp> rm S008709-9332-090416-09_36
Removing /S008709-9332-090416-09_36
sftp> rm S008709-9332-090416-21_41
Removing /S008709-9332-090416-21_41
```

```
sftp>
sftp> bye

C:\WINNT>
```

Figure 1 - Typical SFTP CDR Data File Retrieval Session

The scenario depicted above consists of the following steps:

1. The user does a "cd" to the directory where the CDR data files are to be transferred.

2. The user begins the session by entering the command line:
   "sftp CDR@MySessionManager.MyDomain.com"

   which launches the SFTP program and passes it the Session Manager server name ("MySessionManager.MyDomain.com" in this example) and the user id ("CDR" in this example).

3. The server then responds with its standard login message. At the end of the login message, the server prompts the user for the password. The user then responds with the password.

4. The user is automatically placed in the CDR data files directory on the SM server.

5. Next a "**`mget S*`**" command is executed to copy all files that exist on the server with file names that begin with a capital "S" to the local directory. The server responds by copying the files that have file names that begin with a capital "S" to the local directory.

6. Next the user does a listing of the *local* directory by entering "**lls –al"** or equivalent command to see which files actually were transferred.

7. Now the user removes each of the transferred files **one at a time** from the server that have just been retrieved. This is done by entering "**rm"** followed by the individual file name.

   NOTE: the files are removed individually just in case a new CDR data file has been added to the directory between the time the files are transferred and the time they are deleted. If a new file had been added during this time period and the "rm *" command were used, the new file would be deleted without having been transferred to the CDR adjunct. Any CDR records that were contained in the "new" file would be lost forever.

Caution: It is recommended that the CDR adjunct perform some type of file verification function to provide some assurance that the file has been accurately received by the adjunct before deleting it from the server. This check could be as simple as comparing the relative file size of the received file with the size of the file on the server to make sure that they are the same size before deleting the file on the server.

The adjunct provider may elect to design the adjunct to retrieve a group of files on one polling pass and then process those files to assure that they are in the correct format and contain valid data. If no errors were detected, the adjunct would then remove the previously retrieved files on the next polling pass. If errors were detected in a file, the adjunct could re-retrieve the errant file before removing it from the server.

8. Finally the adjunct signs off of the server by entering the command "**bye**".

8.2 SWITCH INFORMATION NEEDED TO ADMINISTER THE CDR ADJUNCT

The following information will need to be obtained from the Switch Administrator in order to configure the CDR adjunct and/or retrieve the SM CDR data files:

- The user name and password that have been administered on the SM for use by the CDR adjunct
- A list of the fully qualified domain names or IP addresses for all of the SM servers that the adjunct is to collect CDR data files from.

8.3 FRIENDLY REMINDERS AND SUGGESTIONS

The following are suggestions of things that should be considered when designing and installing the CDR adjunct to support the Session Manager CDR functionality:

- The SM administrator must create a special login and password that is to be provided to the CDR adjunct administrator so the adjunct can retrieve the CDR data files. The administrator should verify that this login and password works on each SM server where CDR is to be collected from by the adjunct.

- The CDR Adjunct must query every SM server in the system (that has been administered to use the CDR feature) in order to ensure that all CDR data files are collected. These queries must be completed in a regular and timely manner to ensure that no CDR data files are deleted by the server before they are collected.

- It may be possible to automate the gathering of the CDR records from the various Session Manager servers using Expect[c] or some other scripting language.

- Please see the current Session Manager Customer documentation for instructions on how to administer the CDR feature on the server. These documents can be found on the support.avaya.com website.
- Session Manager CDR utilizes a compatible CDR format that is available on Avaya Aura® Communication Manager 4.0 and higher platforms with conventional CDR. The compatible format is the "Unformatted" format for "CM Survivable CDR".

8.4 PRECAUTIONARY INFORMATION

Warning: It is critical that all servers in the system which have been administered to support CDR be periodically queried for available CDR data files. Whenever CDR files are identified during the aforementioned query process, they need to be retrieved in a timely manner so they are not lost.

[c] Expect is a tcl based tool for automating and scripting interactive applications such as SFTP, SCP and telnet. The Expect home page is located at http://expect.nist.gov/. Sources for versions of Expect for Unix, Linux and Windows and possibly other operating systems are identified on the NIST web site.

Avaya Aura and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in this Interface Document is subject to change without notice. The configurations, technical data, and recommendations provided in this Interface Document are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in this Interface Document.