Avaya Solution & Interoperability Test Lab

Application Notes for configuring blackchair Spotlight Session Manager Audit V6 with Avaya Aura® System Manager R7.1 and Avaya Aura® Session Manager R7.1 – Issue 1.0

Abstract

These Application Notes describe the configuration steps required to integrate Spotlight Session Manager Audit V6 with Avaya Aura® System Manager R7.1 and Avaya Aura® Session Manager R7.1. Session Manager Audit is capable of identifying changes made to Avaya Aura® System Manager with regard to a set of Session Manager objects.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

©2017 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the configuration steps required to integrate Spotlight Session Manager Audit V6 with Avaya Aura® System Manager R7.1 and Avaya Aura® Session Manager R7.1. Session Manager Audit is capable of identifying changes made to Avaya Aura® System Manager with regard to a set of Session Manager objects.

2. General Test Approach and Test Results

All feature test cases were performed manually. All fields and values in the System Manager logs are copied onto the Spotlight Session Manager Audit database. This database is then used to display changes made.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising APIs and/or standards-based interfaces pertinent to the interoperability of the tested products and their functionalities. DevConnect Compliance Testing is not intended to substitute full product performance or feature testing performed by DevConnect members, nor is it to be construed as an endorsement by Avaya of the suitability or completeness of a DevConnect member's solution.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in these DevConnect Application Notes included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

©2017 Avaya Inc. All Rights Reserved.

2.1. Interoperability Compliance Testing

blackchair Spotlight Session Manager Audit, which will be referred to as Session Manager Audit throughout the remainder of this document, was installed on a virtual server running Microsoft Windows 2008 Server R2 and Microsoft SQL Server 2008 R2. A client PC using the FireFox web browser was used to access the Session Manager Audit.

During compliance testing the following objects were checked in the System Manager logs relating to Session Manager and Routing.

- Session Manager
  - Remote Access
  - Application Sequences
  - Applications
  - Session Manager instances
  - Session Manager terminal group parameters
  - Conference Factory settings
  - Failover groups
  - Hostname resolution IPs
  - Session Manager Service State
  - Dial Pattern assignment
  - Communication Profiles
  - SIP firewall configurations
  - Tracer configuration
- Routing
  - Adaptations
  - Dial Pattern
  - Entity link
  - Domains
  - Regular Expressions
  - Locations
  - Routing policy
  - SIP entity
  - Time Ranges

2.2. Test Results

All test cases passed.

©2017 Avaya Inc. All Rights Reserved.

2.3. Support

For technical support on Spotlight Release Management, contact blackchair as shown below.

- Web: http://www.theblackchair.com/contact-us/
- Tel: +44 845 456 6751
- Email: support@theblackchair.com

3. Reference Configuration

Figure 1 shows the network topology during compliance testing. The Spotlight Session Manager Audit server was placed on the Avaya telephony LAN. A user browsing to the Spotlight Release Management server using a web browser is capable of viewing changes made to the Session manager configuration using packages of objects built from the Spotlight Audit environment.

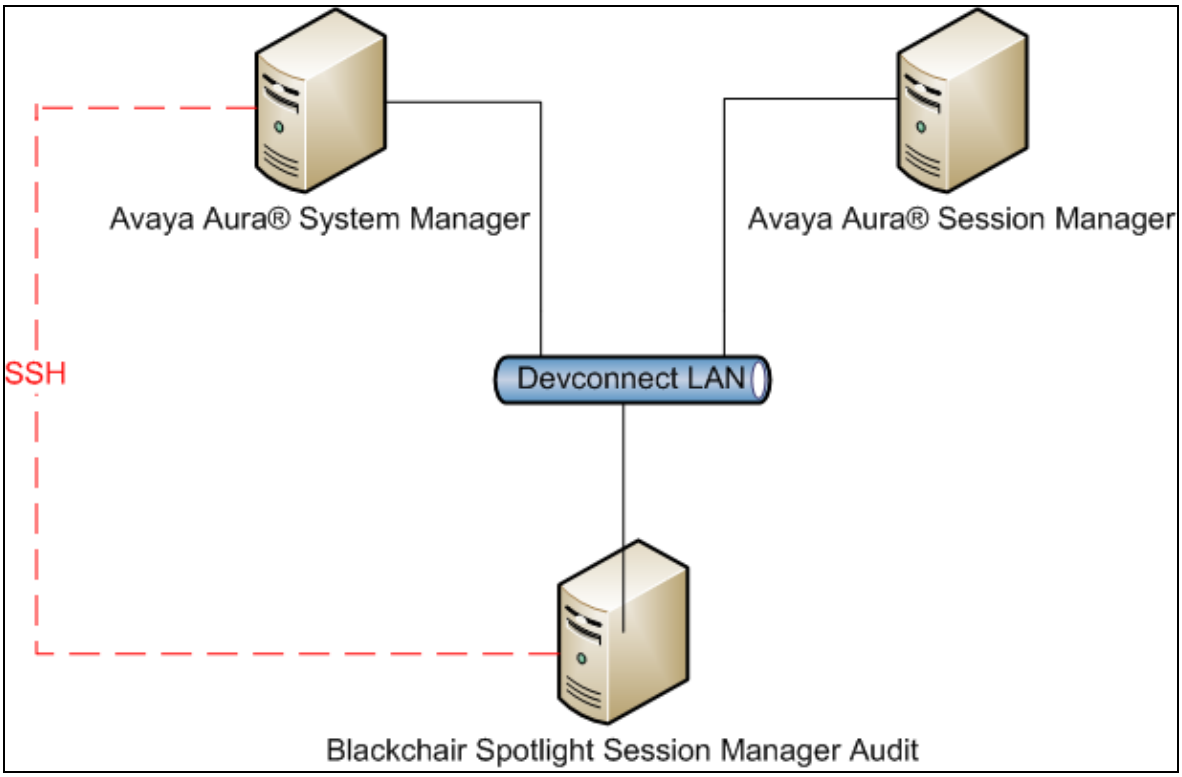


Figure 1: Network solution of blackchair Spotlight Session Mananger Audit V6 and Avaya Aura® System Manager R7.1 with Avaya Aura® Session Manager R7.1

©2017 Avaya Inc. All Rights Reserved.

4. Equipment and Software Validated

The following equipment and software was used for the sample configuration provided.

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	R7.1.0.0 Build No. 7.1.0.0.1125193 Update 7.1.0.0.126816
Avaya Aura® Session Manager running on a virtual server	R7.1.0.0.710028
blackchair Spotlight Session Manager Audit running on a Virtual Server - Windows 2008 R2 O/S - MS SQL 2008 R2	Version 6

©2017 Avaya Inc. All Rights Reserved.

5. Configure Avaya Aura® System Manager

This section describes the steps required to configure System Manager to allow Spotlight Session Manager Audit to extract information from the logs.

An SSH user must be created on System Manager that has permissions to access the following log files and use touch to extract the required information. The creation of a Linux user for this purpose is out with the scope of this document. The default customer user added during implementation has the correct permissions and was used during testing.

a. /var/log/Avaya/mgmt/nrp/nrpaudit.log
b. /var/log/Avaya/mgmt/asm/adminaudit.log

6. Configure blackchair Spotlight Session Manager Audit

This section describes the steps required to configure Spotlight to audit a Session Manager system. It is assumed that Session Manager has been added to an existing Spotlight instance, therefore the process for installing Spotlight framework is not covered here.

First create a Spotlight model database with standard tables. On this database run the following scripts to add tables specific to Session Manager audit:

- VolatileItemTemplates.sql
- TableCreation.sql
- DataDictionaryEntries.sql
- ConfigItemTemplates.sql
- ConfigItems.sql
- ConfigItemVersion.sql
- ASMUpdates
- CreateASMSearchMetaData
- ASM2
- ASM3

Add entries in the slconfig configuration database for the Session Manager environment; details can be found in the guide “blackchair spotlight core audit Avaya deployment guide v060” available from blackchair.

©2017 Avaya Inc. All Rights Reserved.

Now create a data loader service to connect to the System Manager that is used to configure the Session Manager. This is done using the "Create AdditionalLoaderService" tool in the utilities section of the Spotlight installation package. Add to this loader the specific dll, pdb and xml files for the Session Manager audit, supplied by blackchair, and configure the **<RemoteHost>** section in the "ASMPlugin.xml" file as follows:

```
<RemoteHost>
  <Username>uuuuuu</Username>
  <Password>pppppp</Password>
  <RemoteHostIp>n.n.n.n</RemoteHostIp>
  <Environment>Session Manager</Environment>
</RemoteHost>
```

Where

Username = account to ssh to the System Manager server
Password = password for this account
RemoteHostIp = address of the System Manager server
Environment = friendly name for the Session Manager instance; **Session Manager** was used in this testing as the friendly name and is displayed in the Spotlight UI.

Add the appropriate license file to the loader (supplied by blackchair) and start the loader service.

©2017 Avaya Inc. All Rights Reserved.

7. Verification Steps

This section provides the tests that can be performed to verify that blackchair Spotlight Session Manager Audit has successfully connected with the Avaya solution.

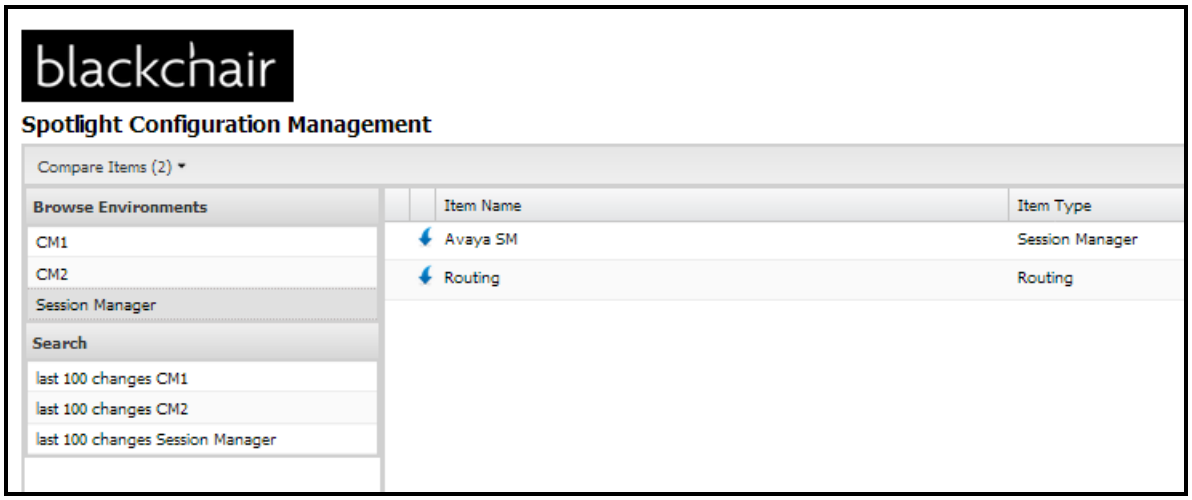
Check the logfile for the loader service, found in the folder specified in the SpotlightLoaderService.exe.config file. The process has completed its connection and initial data download when logfile messages indicate the process is queued, and this can be determined by logfile messages similar to the following:

Load queue item ASMPluginProcessor=queued nn.nnnnnns

Search logfile for the text "exception"; if any instances are found:

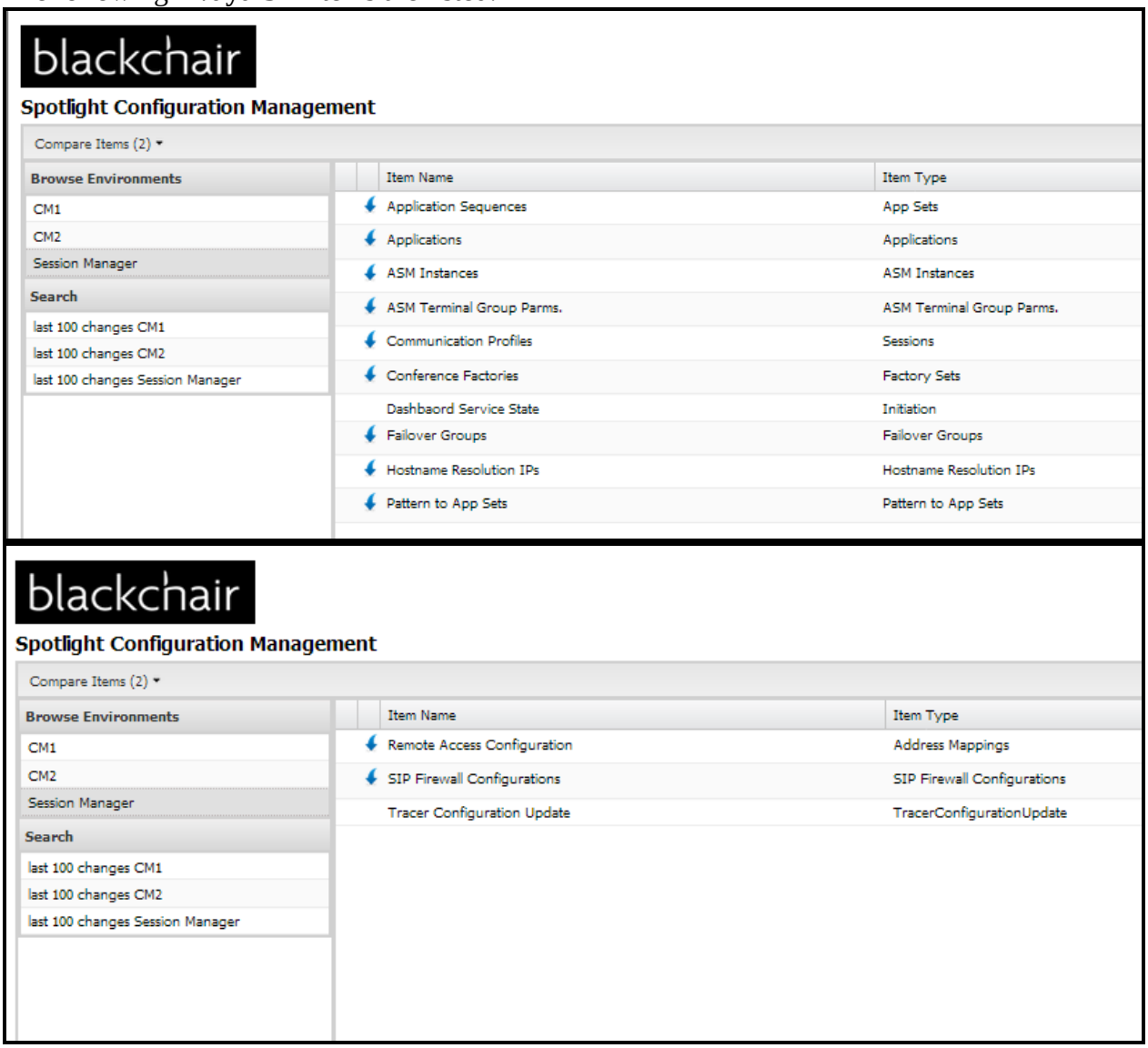
- If a failed connection is indicated to the System Manager check the configuration described in **Section 6**, and check no firewall or network configuration is preventing access to the System Manager from the Spotlight server
- Any other exceptions should be referred to blackchair support using the contact information in **Section 2.3**

The Spotlight UI displays the following structure under the Session Manager environment with the name specified in the **Environment** entry described in **Section 6**. The friendly name is **Session Manager** under **Browse Environments**:



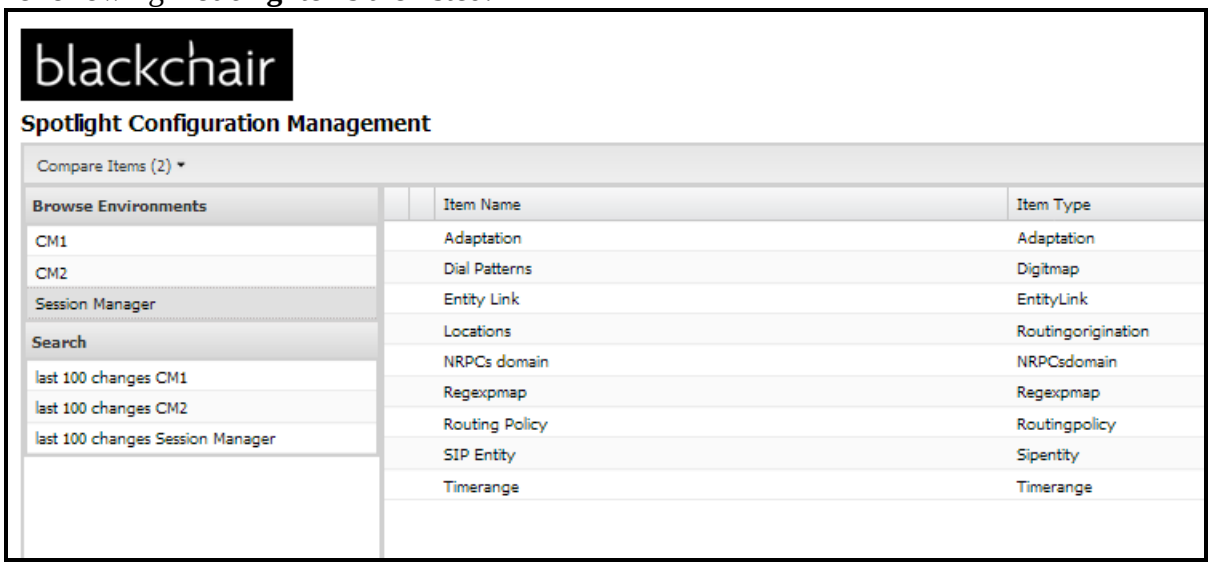
©2017 Avaya Inc. All Rights Reserved.

The following **Avaya SM** items are listed:



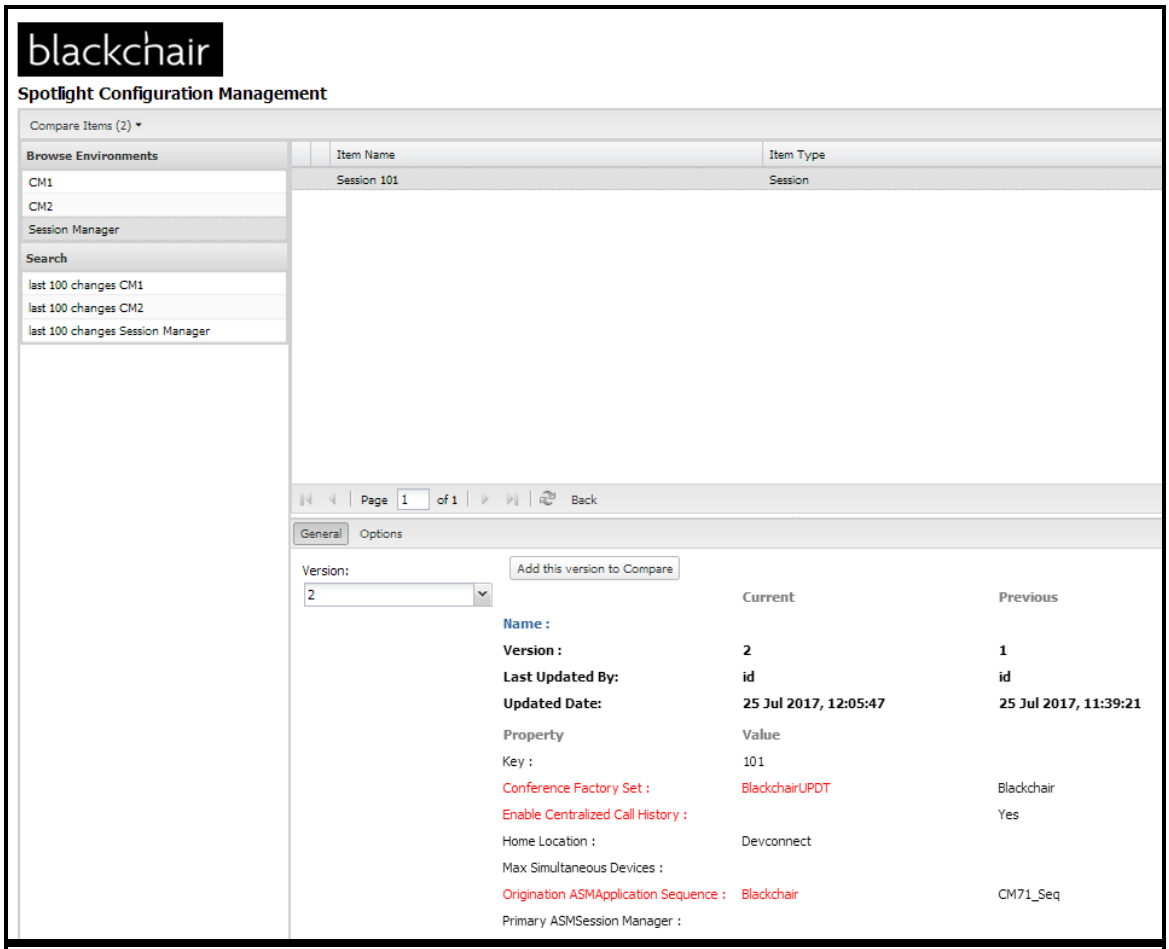
©2017 Avaya Inc. All Rights Reserved.

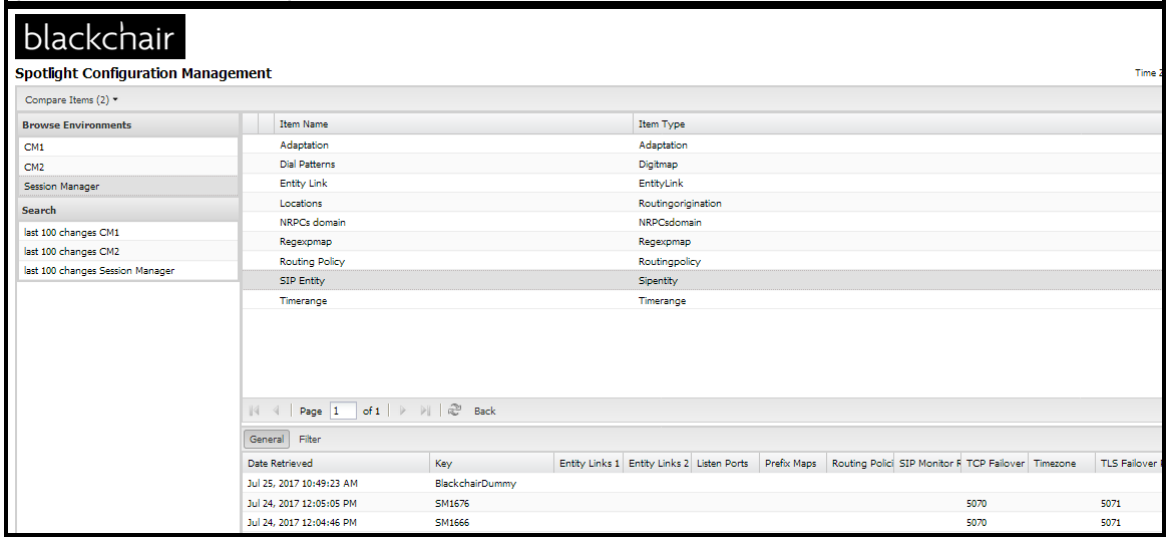
The following **Routing** items are listed:



©2017 Avaya Inc. All Rights Reserved.

Within each item name data is shown corresponding to the Session Manager configuration. The following screen shows an example of **Communication Profile** information found under **Avaya SM**:





©2017 Avaya Inc. All Rights Reserved.

8. Conclusion

These Application Notes describe the configuration steps required for Spotlight Session Manager Audit V6 from blackchair to successfully interoperate with Avaya Aura® System Manager R7.1 with Avaya Aura® Session Manager R7.1. Please refer to **Section 2.2** to see the compliance test results and observations.

9. Additional References

The following documents are available at http://support.avaya.com.

[1] *Implementing Avaya Aura® Session Manager* Document ID 03-603473
[2] *Administering Avaya Aura® Session Manager*, Doc ID 03-603324
[3] *Deploying Avaya Aura® System Manager, Release 7.1, Issue 2*

The following document is available directly from blackchair

[4] *blackchair spotlight core audit Avaya deployment guide v060*

Further product information on blackchair Spotlight can be found at http://www.theblackchair.com

©2017 Avaya Inc. All Rights Reserved.

©2017 Avaya Inc. All Rights Reserved.
Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes 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 these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.

©2017 Avaya Inc. All Rights Reserved.