AVAYA

Avaya Solution & Interoperability Test Lab

Application Notes for solution redundancy of NICE Recording R6.x with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R6.3 - Issue 1.0

Abstract

These Application Notes describe the configuration steps for NICE Recording R6.x to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R6.3 in a 2N dual redundancy configuration.

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.

PG; Reviewed:
SPOC 9/27/2018
Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.
1 of 34
NR_AES63_2NRed

1. Introduction

These Application Notes describe the configuration steps for the solution redundancy of NICE Recording 6.x to interoperate with the Avaya solution consisting of an Avaya Aura® Communication Manager R7.1 and two Avaya Aura® Application Enablement Services R6.3. The Recorder uses Communication Manager's Multiple Registration feature via the Application Enablement Services (AES) Device, Media, and Call Control (DMCC) interface and the Telephony Services API (TSAPI) to capture the audio and call details for call recording on various Communication Manager H.323 and Digital endpoints, listed in **Section 4**.

Note*: Compliance testing was carried out with NICE Recording (NRX) V6.6.2 and the connection to AES uses the NICE Avaya Link Controller V5.4. The NICE Avaya Link Controller is common to the following NICE products; NICE Inform Recorder (NIR), NICE Recording (NRX) and NICE Trading Recorder (NTR). Feature functionality may vary between the different NICE recording products. Additional information can be obtained from NICE technical support as noted in* **Section 2.3**.

The redundancy consists of two NICE servers connected to two AES's in a 2N redundancy configuration (Active/Active), which means that NICE server 1 is only connected to AES server 1 and NICE server 2 connected to AES server 2. There are no high availability options between servers, this is a 2N connection where the NICE to AES connection is duplicated with a second NICE to AES connection. Each or the two NICE servers operates independently making their own duplicate recordings of the calls. For testing purposes, the NICE Recording "All-in-One" deployment was chosen. 2N redundancy is also supported for the semi-distributed and fully distributed deployments.

DMCC works by allowing software vendors to create soft phones, in memory on a recording server, and use them to monitor and record other phones. This is purely a software solution and does not require telephony boards or any wiring beyond a typical network infrastructure. The DMCC API associated with the AES server monitors the digital and VoIP extensions. The application uses the AE Services DMCC service to register itself as a recording device at the target extension. When the target extension joins a call, the application automatically receives the call's aggregated RTP media stream via the recording device and records the call.

NICE Recording is fully integrated into a LAN (Local Area Network) and includes easy-to-use Web based applications (i.e., Nice Application) that works with the Microsoft .NET framework and used to retrieve telephone conversations from a comprehensive long-term calls database. This application registers an extension with Communication Manager and waits for that extension to be dialed. NICE Recording contains tools for audio retrieval, centralized system security authorization, system control, and system status monitoring. Also included is a call parameters database that tightly integrates via CTI link PABXs and ACD's including optional advanced audio archive database management, search tools, a wide variety of Recording-on-Demand capabilities, and comprehensive long-term call database for immediate retrieval.

2. General Test Approach and Test Results

The interoperability compliance testing evaluated the ability of NICE Recording to carry out call recording in a variety of scenarios using DMCC Multi-Registration with AES and Communication Manager. A range of Avaya endpoints were used in the compliance testing all of which are listed in **Section 4**.

The focus of these Application Notes and the compliance testing was on the redundancy capabilities of the NICE servers in a 2N configuration with AES. After each call was placed, recordings on both NICE servers were observed and verified. Various failure scenarios were played out by pulling the LAN cables from each of the NICE servers and the AES's.

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.

For the testing associated with these Application Notes, the interface between Avaya systems and NICE Recording did not include use of any specific encryption features as requested by NICE.

2.1. Interoperability Compliance Testing

The interoperability compliance test included both feature functionality and serviceability testing. The feature functionality testing focused on placing and recording calls in different call scenarios with good quality audio recordings and accurate call records. The tests included:

- **Inbound/Outbound calls** – Test call recording for inbound and outbound calls to the Communication Manager to and from PSTN callers.
- **Hold/Transferred/Conference calls** – Test call recording for calls transferred to and in conference with PSTN callers.
- **Feature calls** - Test call recording for using features such as Call Park and Call Pickup.
- **Calls to Elite Agents** – Test call recording for calls to Communication Manager Agents. These include calls to VDN's and to Hunt Groups.

- **Redundancy testing** - The behavior of NICE Recording under different simulated LAN failure conditions.

Redundancy Testing focuses on the following failover scenarios.

Failure and recovery to each component.
1. Pull LAN cable on AES 1, make test calls and observe recordings on NICE server 1 and NICE server 2.
2. Plug back in LAN cable on AES1, make test calls and observe recordings on NICE server 1 and server 2.
3. Pull LAN cable on AES 2, make test calls and observe recordings on NICE server 1 and server 2.
4. Plug back in LAN cable on AES2, make test calls and observe recordings on NICE server 1 and server 2.
5. Pull LAN cable on NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
6. Plug back in LAN cable on NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
7. Pull LAN cable on NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.
8. Plug back in LAN cable on NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

Failure and recovery to each side.
9. Pull LAN cable on AES 1 and NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
10. Plug back in cable on AES 1 and NICE_Rec1, make test calls and observe recordings on NICE server 1 and server 2.
11. Pull LAN cable on AES 2 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.
12. Plug back in cable on AES 2 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

Total AES failure.
13. Pull LAN cable on AES 1 and AES 2, make test calls and observe recordings on NICE server 1 and server 2. (Only need to test one call here as no recordings expected).
14. Plug back in AES 1 and AES 2, make test calls and observe recordings on NICE server 1 and server 2.

Total NICE failure.
15. Pull LAN cable on NICE_Rec1 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2. (Only need to test one call here as no recordings expected).
16. Plug back in NICE_Rec1 and NICE_Rec2, make test calls and observe recordings on NICE server 1 and server 2.

Communication Manager/Media Gateway failures.
17. Pull and Restore LAN cable on G430 Media Gateway (quickly).
18. Pull and Restore LAN cable on G430 Media Gateway (hang up call when pulled).
19. Pull and Restore LAN cable on Communication Manager.
20. Pull and Restore LAN cable on both Communication Manager and G430 Media Gateway.

2.2. Test Results

All functionality and redundancy test cases were completed successfully. The following issue was noted. **Power failure to Communication Manager**, there was an issue with the recordings of digital sets after a power failure to Communication Manager. The original media stream was present alongside the new media stream being recorded. This only occurred on one of the NICE servers and this was random over a repeat of the same test. A reboot of the NICE server or restarting the services would solve the issue. Both Avaya and NICE are investigating this issue.

2.3. Support

Technical support can be obtained for NICE Recording from the website http://www.nice.com

3. Reference Configuration

The configuration in **Figure 1** was used to compliance test NICE Recording with the Avaya solution using DMCC Multi-Registration to record calls. The NICE server is setup for DMCC Multi-Registration mode and connects to the AES. The setup below is a "2N" redundancy configuration with the NICE to AES connection doubled. Communication Manager then has two "switch connections" to AES.
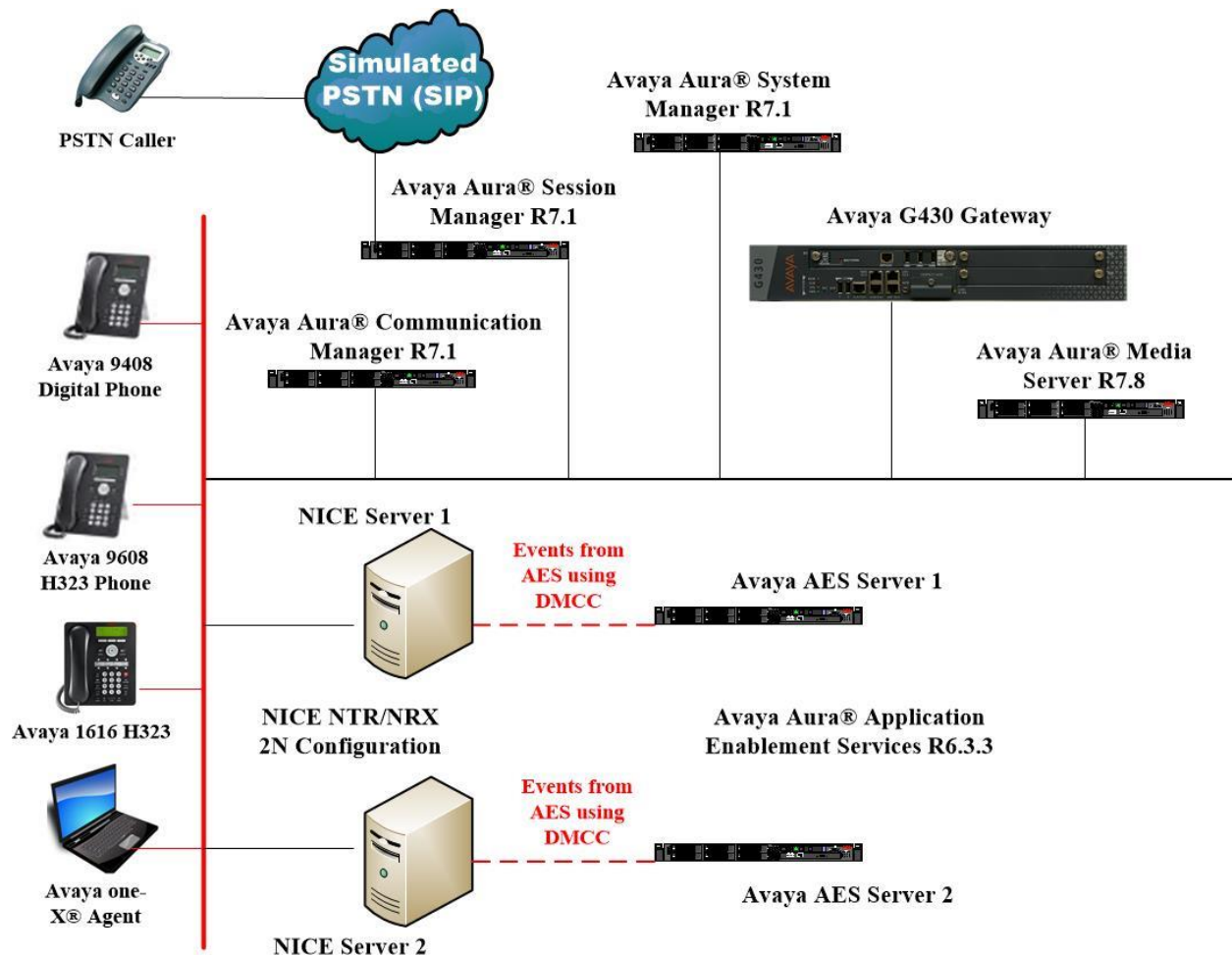
Figure 1: Connection of solution redundancy of NICE Recording R6.x with Avaya Aura® Communication Manager R7.1 and Avaya Aura® Application Enablement Services R6.3 in a 2N redundancy configuration

4. Equipment and Software Validated

The following equipment and software were used for the sample configuration provided:

Equipment/Software	Release/Version
Avaya Aura® System Manager running on a virtual server	System Manager 7.1.3.0 Build No. - 7.1.0.0.1125193 Software Update Revision No: 7.1.3.0.37763 Feature Pack 3
Avaya Aura® Session Manager running on a virtual server	Session Manager R7.1 Build No. – 7.1.3.0.713014
Avaya Aura® Communication Manager running on a virtual server	R7.1.3.0.0 (01.0.532.0-24515)
Avaya Aura® Application Enablement Services running on Virtual Server	R6.3.3 Build No – 6.3.3.9.10-0
Avaya Aura® Media Server running on a virtual server	7.8.0.240
Avaya G430 Gateway	37.42.0 /1
Avaya 9608 H.323 Deskphone	96x1 H.323 R6.6.028
Avaya 1616 H.323 Deskphone	R1_3_11-022417
Avaya one-X® Agent (H.323)	R2.5.50022.0
Avaya 9408 Digital Deskphone	FW Version 2
NICE Recording (NRX) running on a virtual server All-in-one deployment on Windows Server 2012 R2	NICE Recording R6.6.2 UP2 NICE Avaya Integration 80.0.1 NICE Avaya Link Controller V5.4

5. Configure Avaya Aura® Communication Manager

The information provided in this section describes the configuration of Communication Manager relevant to this solution. For all other provisioning information such as initial installation and configuration, please refer to the product documentation in **Section 10**.

The configuration illustrated in this section was performed using Communication Manager System Administration Terminal (SAT).

5.1. Verify System Features

Use the **display system-parameters customer-options** command to verify that Communication Manager has permissions for features illustrated in these Application Notes. On **Page 3**, ensure that **Computer Telephony Adjunct Links?** is set to **y** as shown below.

```
display system-parameters customer-options                    Page   3 of  11
                            OPTIONAL FEATURES

    Abbreviated Dialing Enhanced List? y           Audible Message Waiting? y
        Access Security Gateway (ASG)? n              Authorization Codes? y
        Analog Trunk Incoming Call ID? y                        CAS Branch? n
 A/D Grp/Sys List Dialing Start at 01? y                          CAS Main? n
Answer Supervision by Call Classifier? y                  Change COR by FAC? n
                                  ARS? y  Computer Telephony Adjunct Links? y
                 ARS/AAR Partitioning? y  Cvg Of Calls Redirected Off-net? y
           ARS/AAR Dialing without FAC? y                     DCS (Basic)? y
             ASAI Link Core Capabilities? n              DCS Call Coverage? y
             ASAI Link Plus Capabilities? n              DCS with Rerouting? y
          Async. Transfer Mode (ATM) PNC? n
     Async. Transfer Mode (ATM) Trunking? n   Digital Loss Plan Modification? y
                ATM WAN Spare Processor? n                          DS1 MSP? y
                                 ATMS? y          DS1 Echo Cancellation? y
                   Attendant Vectoring? y
```

5.2. Note procr IP Address for Avaya Aura® Application Enablement Services Connectivity

Display the procr IP address by using the command **display node-names ip** and noting the IP address for the **procr** and AES (**aesredundnacy1** and **aesredundancy2**).

```
display node-names ip                                         Page   1 of   2
                              IP NODE NAMES
     Name              IP Address
SM100             10.10.40.52
aesredundancy1    10.10.40.125
aesredundancy2    10.10.40.127
default           0.0.0.0
g450              10.10.40.15
procr             10.10.40.47
```

5.3. Configure Transport Link for Avaya Aura® Application Enablement Services Connectivity

To administer the transport link to AES use the **change ip-services** command. On **Page 1** add an entry with the following values:

- **Service Type:** Should be set to **AESVCS**.
- **Enabled:** Set to **y**.
- **Local Node:** Set to the node name assigned for the procr in **Section 5.2**
- **Local Port:** Retain the default value of **8765**.

```
change ip-services                                          Page   1 of   4

                              IP SERVICES
  Service     Enabled     Local      Local       Remote      Remote
   Type                   Node       Port        Node        Port
AESVCS          y         procr      8765
```

Go to **Page 4** of the **ip-services** form and enter the following values:

- **AE Services Server:** Name obtained from the AES server, in this case **aesredundnacy1**.
- **Password:** Enter a password to be administered on the AES server.
- **Enabled:** Set to **y**.

Note: The two AES server links will be added on **Page 4,** one for aesredundancy1 and another for aesredundancy2.

Note: The password entered for **Password** field must match the password on the AES server in **Section 6.2**. The **AE Services Server** should match the administered name for the AES server; this is created as part of the AES installation, and can be obtained from the AES server by typing **uname –n** at the Linux command prompt.

```
change ip-services                                          Page   4 of   4
                     AE Services Administration

  Server ID    AE Services        Password         Enabled    Status
                 Server
     1:        aesredundnacy1      ********            y          idle
     2:        aesredundancy2      ********            y          idle
     3:
```

5.4. Configure CTI Link for TSAPI Service

Add a CTI link using the **add cti-link n** command. Enter an available extension number in the **Extension** field. Enter **ADJ-IP** in the **Type** field, and a descriptive name in the **Name** field. Default values may be used in the remaining fields.

Note: Two CTI links were already configured on this Communication Manager and therefore the next available CTI links were 3 and 4.

Note: This step will be repeated for the second AES server by adding CTI link 4.

```
add     cti-link 3                                           Page   1 of   3
                                 CTI LINK
 CTI Link: 1
Extension: 4497
     Type: ADJ-IP
                                                                       COR: 1

     Name: aesredundancy1
```

5.5. Configure H.323 Stations for Multi-Registration

All endpoints that are to be monitored by NICE will need to have IP Softphone set to Y. IP Softphone must be enabled in order for Multi-Registration to work. Type **change station x** where x is the extension number of the station to be monitored also note this extension number for configuration required during the NICE Recorder setup in **Section 7** Note the **Security Code** and ensure that **IP SoftPhone** is set to **y**.

```
change station x                                             Page   1 of   6
                                 STATION


Extension: x                          Lock Messages? n              BCC: 0
     Type: 9608                    Security Code: 1234              TN: 1
     Port: S00101                     Coverage Path 1:              COR: 1
     Name: Extension                  Coverage Path 2:              COS: 1
                                      Hunt-to Station:
STATION OPTIONS
                                      Time of Day Lock Table:
            Loss Group: 19       Personalized Ringing Pattern: 1
                                        Message Lamp Ext: 1591
           Speakerphone: 2-way         Mute Button Enabled? y
       Display Language: english
 Survivable GK Node Name:
         Survivable COR: internal       Media Complex Ext:
   Survivable Trunk Dest? y                   IP SoftPhone? y

                                      IP Video Softphone? n
                      Short/Prefixed Registration Allowed: default
```

6. Configure Avaya Aura® Application Enablement Services

This section provides the procedures for configuring Application Enablement Services. The procedures fall into the following areas:
- Verify Licensing
- Create Switch Connection
- Administer TSAPI Link
- Identify Tlinks
- Enable TSAPI and DMCC Ports
- Enable Control for DMCC
- Create CTI User
- Associate Devices with CTI User

6.1. Verify Licensing

To access the AES Management Console, enter **https://<ip-addr>** as the URL in an Internet browser, where <ip-addr> is the IP address of AES. At the login screen displayed, log in with the appropriate credentials and then select the **Login** button.
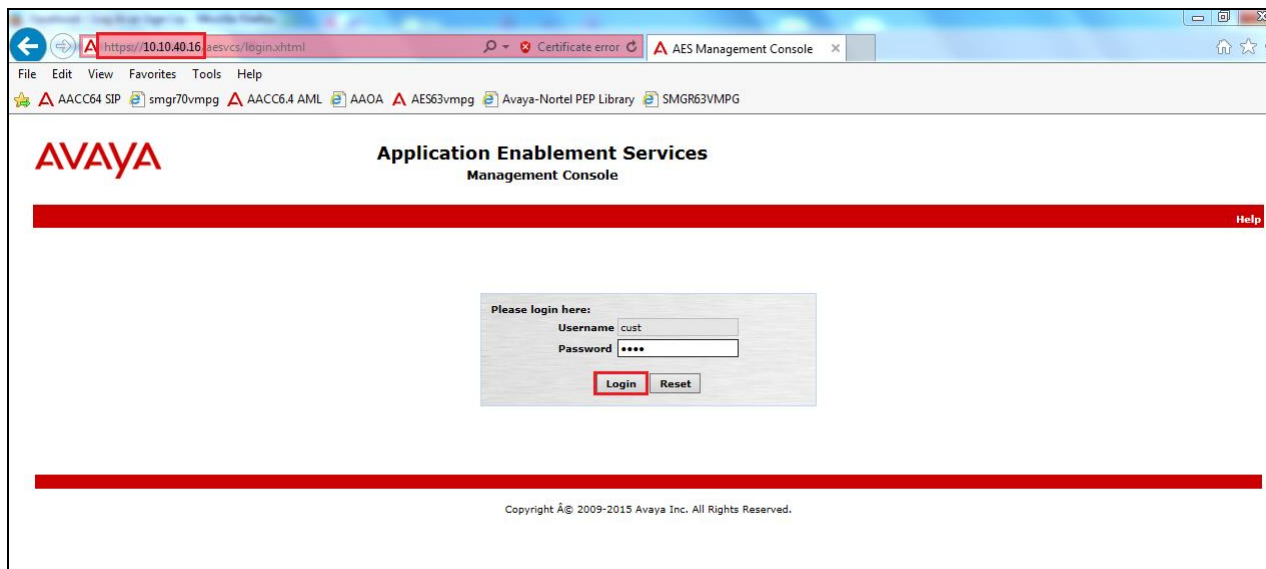
The Application Enablement Services Management Console appears displaying the **Welcome to OAM** screen (not shown). Select **AE Services** and verify that the TSAPI and DMCC Services are licensed by ensuring that **TSAPI Service** and **DMCC Service** are in the list of **Services** and that the **License Mode** is showing **NORMAL MODE**. If not, contact an Avaya support representative to acquire the proper license for your solution.

6.2. Create Switch Connection

From the AES Management Console navigate to **Communication Manager Interface** → **Switch Connections** to set up a switch connection. Enter a name for the Switch Connection to be added and click the **Add Connection** button.

In the resulting screen, enter the **Switch Password**; the Switch Password must be the same as that entered into Communication Manager AE Services Administration screen via the **change ip-services** command, described in **Section 5.3**. Default values may be accepted for the remaining fields. Click **Apply** to save changes.

From the **Switch Connections** screen, select the radio button for the recently added switch connection and select the **Edit PE/CLAN IPs** button (not shown), see screen at the bottom of the previous page. In the resulting screen, enter the IP address of the procr as shown in **Section 5.2** that will be used for the AES connection and select the **Add/Edit Name or IP** button.

6.3. Administer TSAPI link

From the Application Enablement Services Management Console, select **AE Services** → **TSAPI** → **TSAPI Links**. Select **Add Link** button as shown in the screen below.
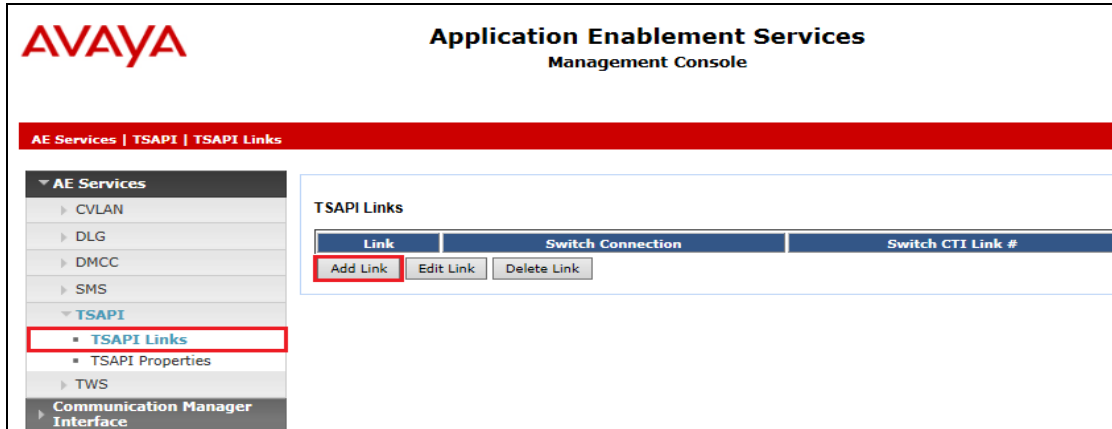
On the **Add TSAPI Links** screen (or the **Edit TSAPI Links** screen to edit a previously configured TSAPI Link as shown below), enter the following values:

- **Link:** Use the drop-down list to select an unused link number.
- **Switch Connection:** Choose the switch connection **cm71vmpg**, which has already been configured in **Section 6.2** from the drop-down list.
- **Switch CTI Link Number:** Corresponding CTI link number configured in **Section 5.4** which is **3**.
- **ASAI Link Version:** This can be set to **5**(This was used for compliance testing but the latest version available can be chosen).
- **Security:** This can be left at the default value of **both**.

Once completed, select **Apply Changes**.

Another screen appears for confirmation of the changes made. Choose **Apply**.
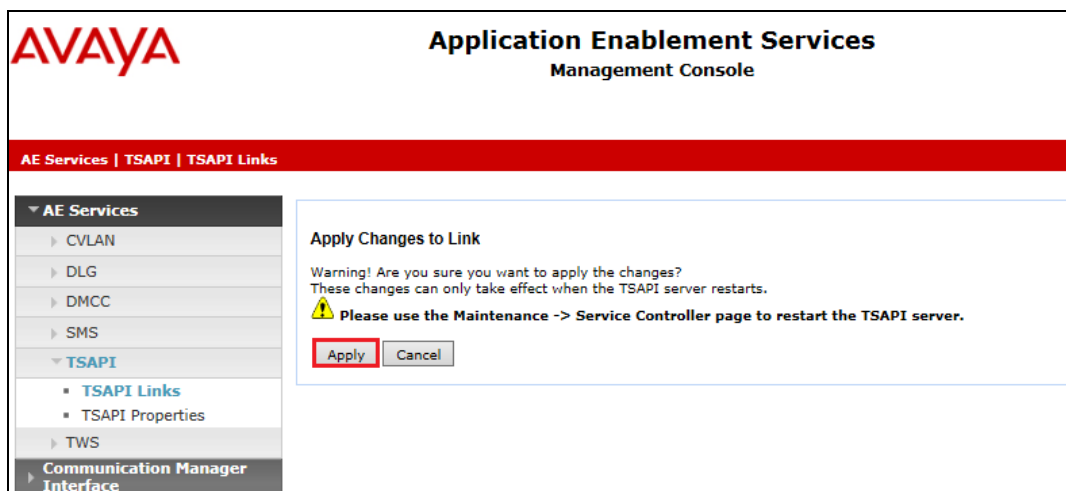
When the TSAPI Link is completed, it should resemble the screen below.
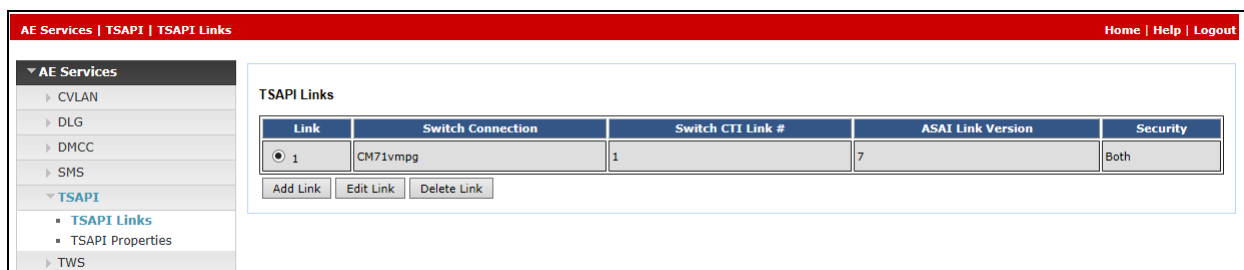
The TSAPI Service must be restarted to effect the changes made in this section. From the Management Console menu, navigate to **Maintenance → Service Controller**. On the Service Controller screen, tick the **TSAPI Service** and select **Restart Service**.
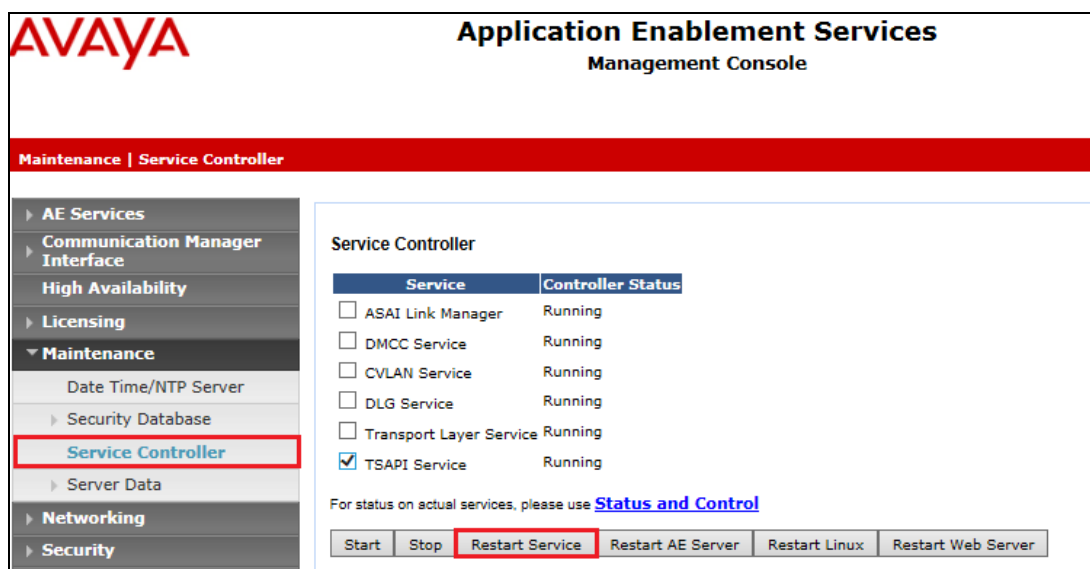
6.4. Identify Tlinks

Navigate to **Security → Security Database → Tlinks**. Verify the value of the **Tlink Name**. This will be needed to configure NICE Recording in **Section 7**.

PG; Reviewed:
SPOC 9/27/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

16 of 34
NR_AES63_2NRed

6.5. Enable TSAPI and DMCC Ports

To ensure that TSAPI ports are enabled, navigate to **Networking → Ports**. Ensure that the TSAPI ports are set to **Enabled** as shown below. Ensure that the **DMCC Server Ports** are also **Enabled** and take note of the **Unencrypted Port 4721** which will be used later in **Section 7**.

6.6. Enable Control for DMCC

To ensure that the NICE servers are capable for logging into the Communication Manager extensions without the need for a station password, control for DMCC must be ticked under **Security Database → Control** as shown below. Ensure that **Enable SDB for DMCC Service** is ticked, the other box may already be ticked as it was in the example below.

PG; Reviewed:
SPOC 9/27/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

18 of 34
NR_AES63_2NRed

6.7. Create CTI User

A User ID and password needs to be configured for NICE Recording to communicate with the Application Enablement Services server. Navigate to the **User Management → User Admin** screen then choose the **Add User** option.

Note: In the example below a user called NICE1 was created for AES1 and NICE2 created for AES2. The same user name 'NICE' could be created on both AES's.

Note: If there was one AES and two NICE recorders these two recorders could use the same User ID and Password again only requiring one user to be setup on the AES for both recorders.
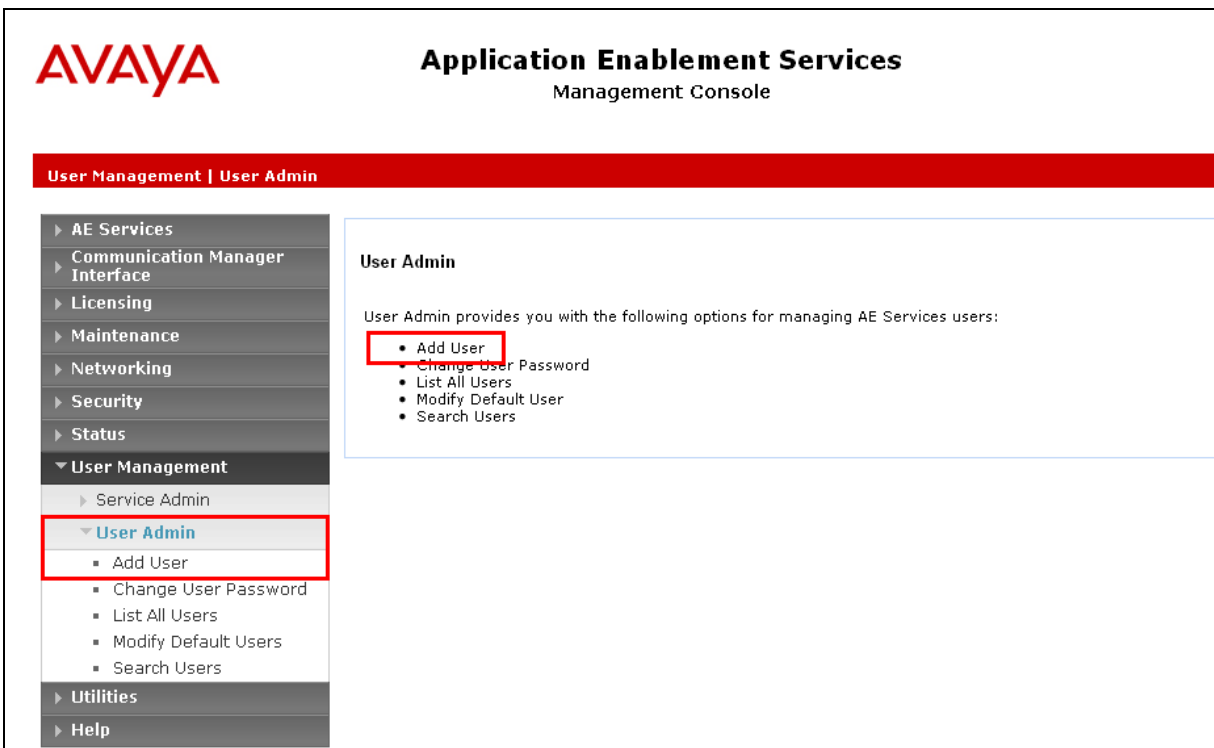
In the **Add User** screen shown below, enter the following values:

- **User Id -** This will be used by NICE Recording setup in **Section 7**.
- **Common Name** and **Surname -** Descriptive names need to be entered.
- **User Password** and **Confirm Password -** This will be used with the NICE Recording setup in **Section 7**.
- **CT User -** Select **Yes** from the drop-down menu.

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

Scroll down and click on **Apply Changes**.

6.8. Associate Devices with CTI User

Navigate to **Security → Security Database → CTI Users → List All Users**. Select the CTI user added in **Section 6.6** and click on **Edit Users**.

In the main window ensure that **Unrestricted Access** is ticked. Once this is done click on **Apply Changes**.

Edit CTI User

User Profile:	User ID	NICE1
	Common Name	NICE1
	Worktop Name	NONE ▾
	Unrestricted Access	☑
Call and Device Control:	Call Origination/Termination and Device Status	None ▾
Call and Device Monitoring:	Device Monitoring	None ▾
	Calls On A Device Monitoring	None ▾
	Call Monitoring	☐
Routing Control:	Allow Routing on Listed Devices	None ▾

Apply Changes | Cancel Changes

Note: The AES Security Database (SDB) provides the ability to control a user's access privileges. The SDB stores information about Computer Telephony (CT) users and the devices they control. The DMCC service, the TSAPI service, and Telephony Web Services use this information for permission checking. Please look to **Section 10** for more information on this.

7. Configure NICE Recording

The installation of NICE Recording is usually carried out by an engineer from NICE and is outside the scope of these Application Notes. For information on the installation of NICE Recording, contact NICE as per the information provided in **Section 2.3**.

The following sections will outline the process involved in connecting NICE Recording to the Avaya Solution. All configuration of NICE Recording for connection with the AES is performed using a web browser connecting to the NICE Recording Application Server. Open a web browser as shown navigate to **http://<NICE ServerIP>/** as shown below and enter the appropriate credentials and log in.

Note: The screenshots show the NICE Trading Recording (NTR) recorder variant. The Web browser functionality is the same for the NICE Inform Recorder & NICE Recording variants.

Note: Some IP addresses may show different as some of these screen shots are simply examples of what should be setup.

Once logged in, click on the **cti integration** tab. Within this tab there are other tabs as shown in the screen below, **cti servers**, **links**, **link groups**, **targets** etc.

PG; Reviewed:
SPOC 9/27/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

23 of 34
NR_AES63_2NRed
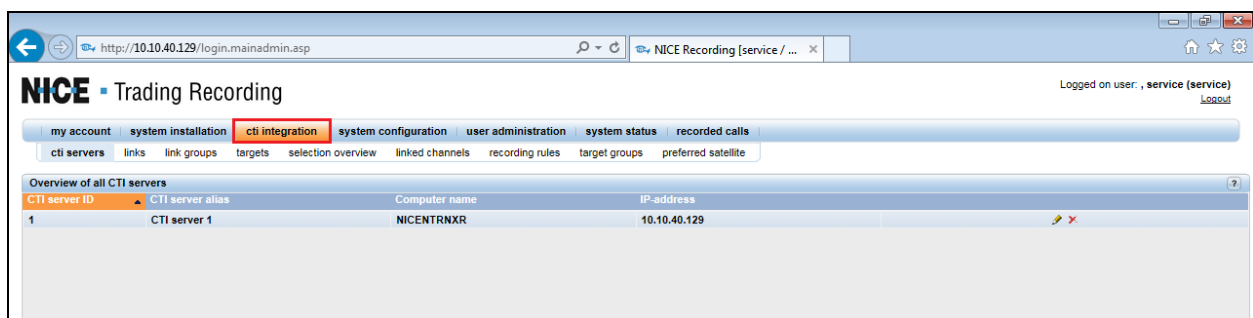
Note: Information on the connection to Avaya is gathered prior to any installation. This information includes the connection to the AES as well as devices to be monitored along with any AES usernames, passwords that need to be used for the connection. During the installation the connections to AES/CM are setup and created and therefore these Application Notes can only show the existing connections that were created during setup.

Clicking on **cti servers** tab will show the CTI server setup during the installation. By clicking on the edit icon highlighted changes can be made to this if deemed necessary.
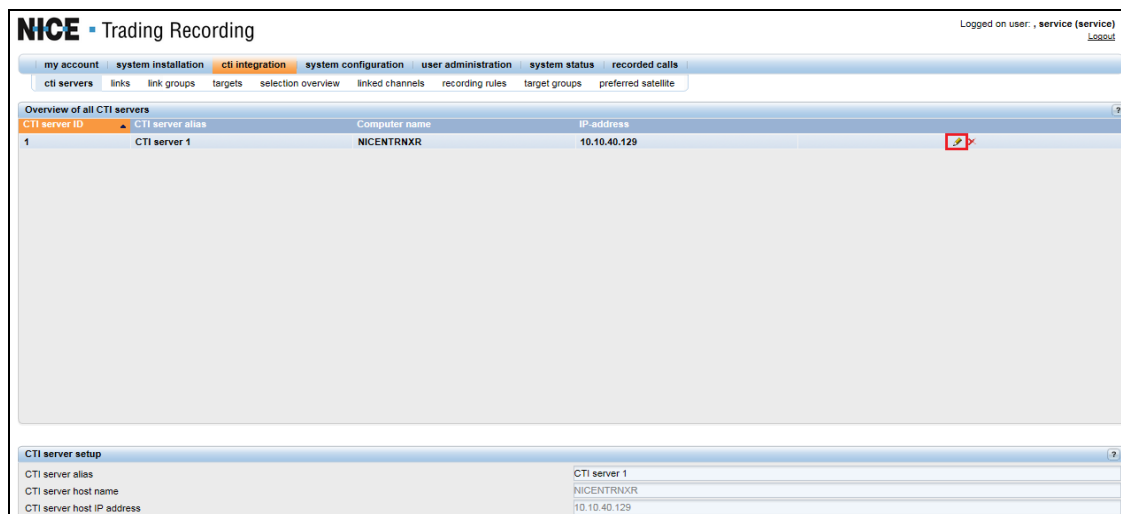
The link to AES is configured during the installation of NICE Recording, however this connection may need to be altered and if so click on the edit icon as shown below.
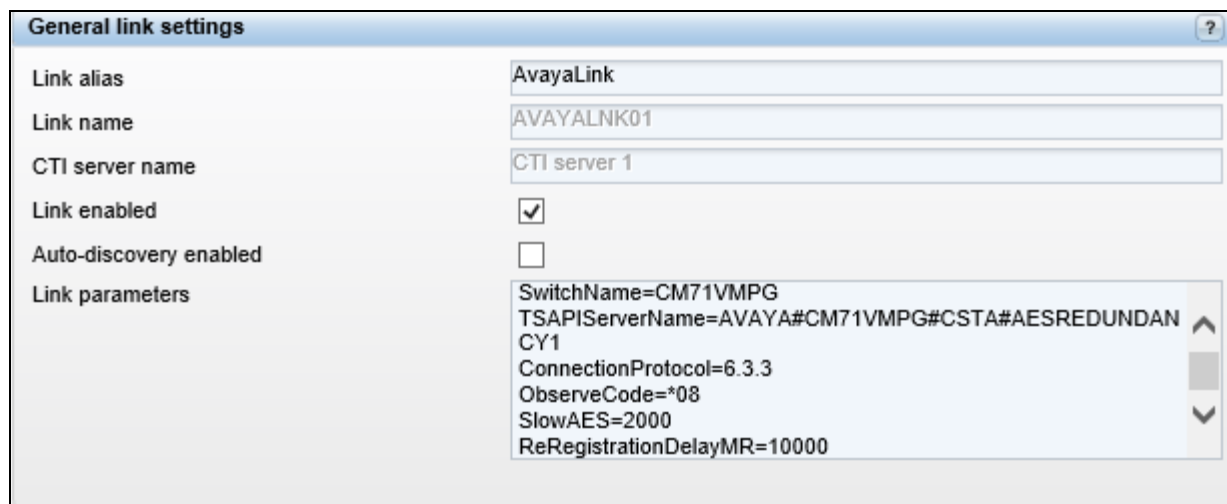
Under the links tab the existing link to AES is shown and can be edited by clicking on the icon opposite the link as highlighted.
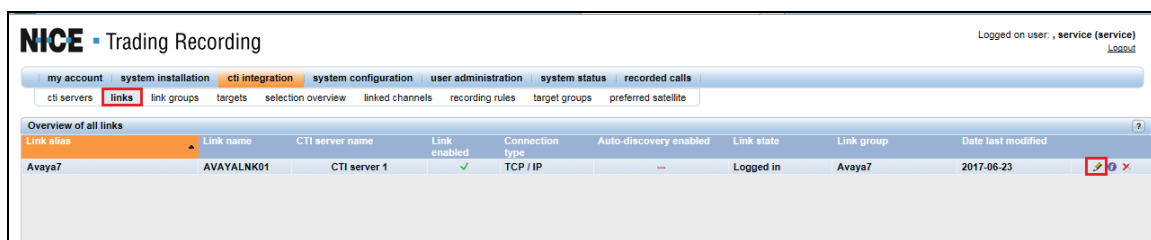
Pressing the edit button above will allow changes to be made to the following.
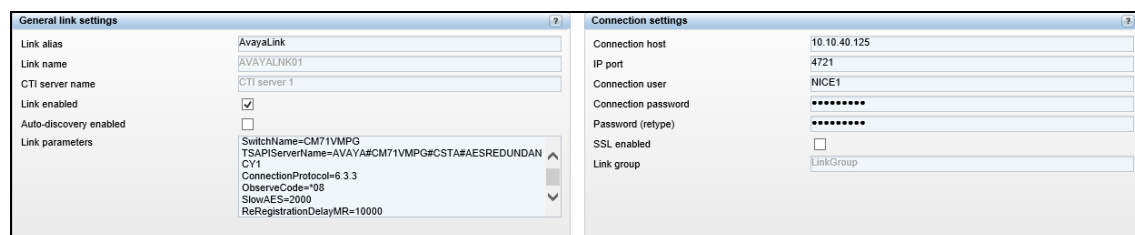
These are the parameters that were used during compliance testing. The information shown here was taken from the AES settings as outlined throughout **Section 6**.
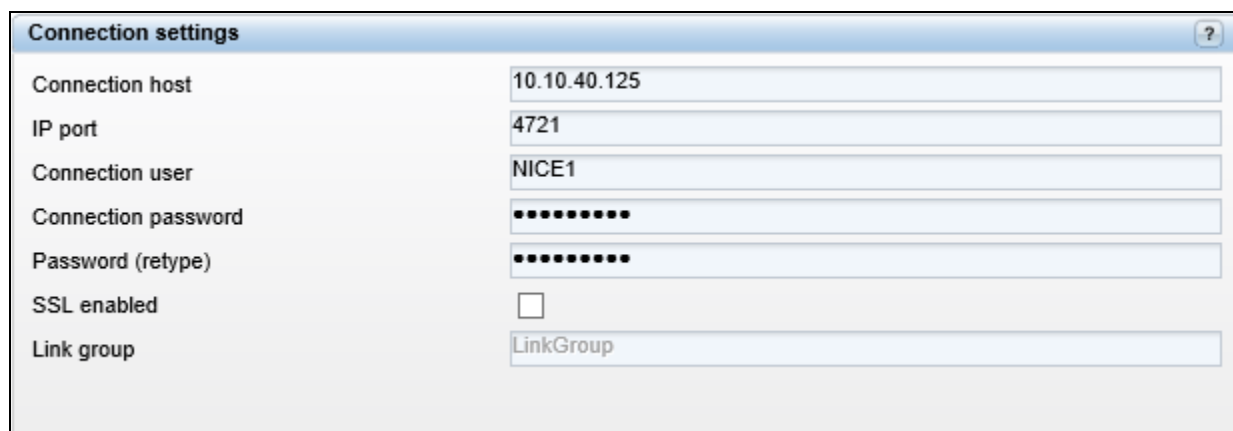
The **Connection host**, **IP port**, the **Connection user** and **password** should not need any editing as these will be added as part of the original installation. In the even that there is a bad connection these fields can be re-entered as shown below.

Note: In the example below a user called NICE1 was created for AES1 and NICE2 created for AES2. The same user name 'NICE' could be created on both AES's.

Note: If there was one AES and two NICE recorders these two recorders could use the same User ID and Password again only requiring one user to be setup on the AES for both recorders.

A link group must be added, and this is done by first clicking on the link groups tab as shown below. Then click on the + icon highlighted, this will open a new window where the link information can be entered and saved by clicking on **OK**. A suitable **Link group name** is given, the **CTI server** that was added during the installation is chosen. The **channel assignment** was **ALL** for compliance testing, the others were left as default as shown below.
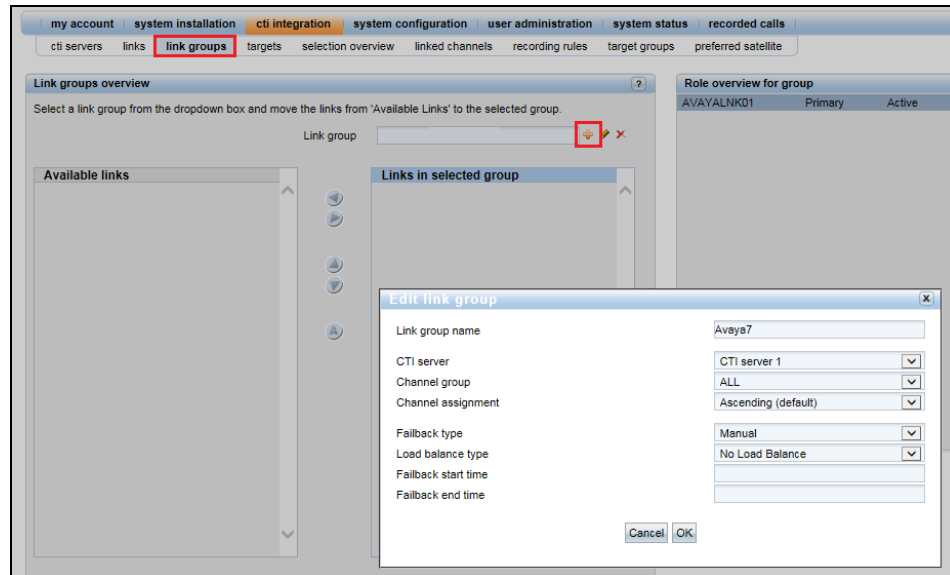
The existing link that was created during installation is now added to the newly created link group.
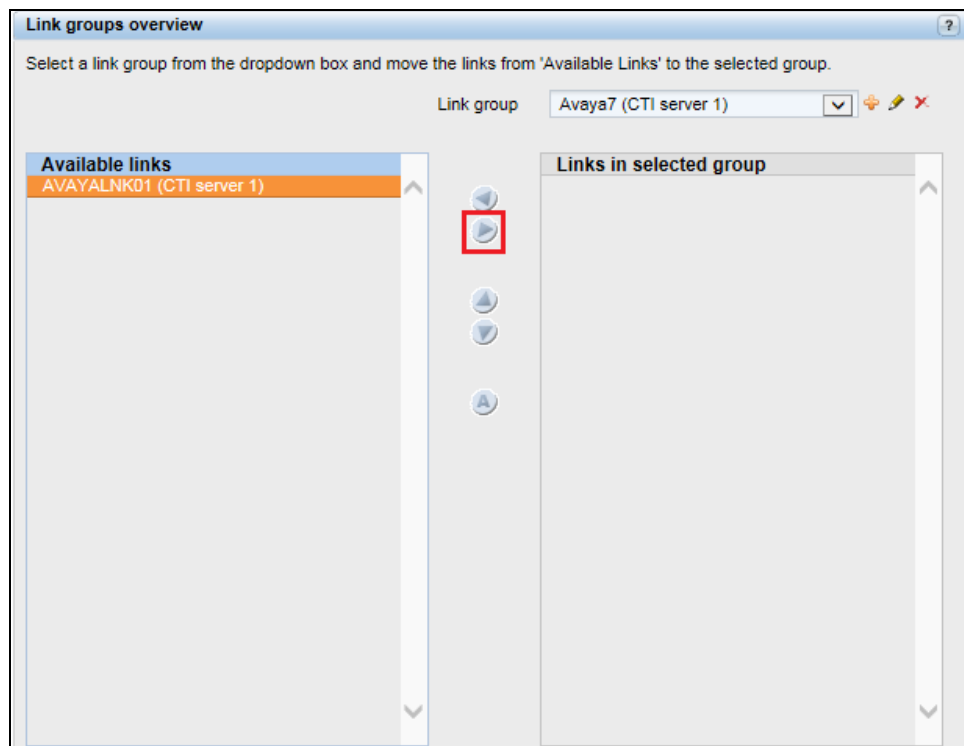
Targets can be added by clicking on the targets tab and clicking on the + icon highlighted below. Targets are Avaya phones that need to be monitored. The screen below shows an existing list of phones that are already being monitored but clicking on the + icon will add a new phone.

Once the + icon is pressed a new window is opened as shown below. Here the information on the new Avaya extension is entered, this new extension being **4002**. Note that the **Target Type** can be chosen from the list of options below. For "Multi-Registration" recording **Extension MR** is selected as shown below.

This newly added target is displayed below.

The selection overview tab provides a list of all the monitored devices as well as any VDN's hunt groups or any other monitored endpoints on Communication Manager.

This concludes the setup of the NICE Application Server for DMCC Multi-Registration recording.

8. Verification Steps

This section provides the steps that can be taken to verify correct configuration of NICE Recording and AES.

8.1. Verify Avaya Aura® Communication Manager CTI Service State

Before checking the connection between NICE Recording and AES, check the connection between Communication Manager and AES to ensure it is functioning correctly. Check the AESVCS link status by using the command **status aesvcs cti-link**. Verify the **Service State** of the CTI link is **established**.

```
status aesvcs cti-link

                    AE SERVICES CTI LINK STATUS

CTI      Version     Mnt     AE Services      Service      Msgs      Msgs
Link                 Busy     Server          State        Sent      Rcvd

1        7           no       aes71vmpg       established   15        15
1        4           no       aes71vmpg       established   105       105
1        5           no       aesredundancy1  established   865       865
1        5           no       aesredundancy2  established   413       413
```

8.2. Verify TSAPI Link

On the AES Management Console, verify the status of the TSAPI link by selecting **Status → Status and Control → TSAPI Service Summary** to display the **TSAPI Link Details** screen. Verify the status of the TSAPI link by checking that the **Status** is **Talking** and the **State** is **Online**.

8.3. Verify DMCC link on AES

Verify the status of the DMCC link by selecting **Status → Status and Control → DMCC Service Summary** to display the **DMCC Service Summary – Session Summary** screen. The screen below shows that the user **NICE** is connected from the IP address **10.10.40.126**, which is the NICE server.

8.4. Verify calls are being recorded

From any of the monitored Avaya endpoints make a series of inbound and outbound calls. Once these calls are completed they should be available for playback through a web browser to the NICE Recording server.

Open a browser session to the NICE server as is shown below. Enter the appropriate credentials and log in.

Click on **recorded calls** at the top of the screen. Select **Submit query** from the bottom of the screen as shown below.

Click on whatever recording is required for play back and this will play back the recording using the sound device on that PC to play back the call.

PG; Reviewed:
SPOC 9/27/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

32 of 34
NR_AES63_2NRed

9. Conclusion

These Application Notes describe the configuration steps required for solution redundancy of NICE Recording R6.x to successfully interoperate with Avaya Aura® Communication Manager R7.1 using Avaya Aura® Application Enablement Services R7.1 in a 2N redundancy configuration to connect to using DMCC Multi-Registration to record calls. All feature functionality and serviceability test cases were completed successfully with some issues and observations noted in **Section 2.2**.

10. Additional References

This section references the Avaya and NICE product documentation that are relevant to these Application Notes.

Product documentation for Avaya products may be found at *http://support.avaya.com*.
   [1] *Administering Avaya Aura® Communication Manager,* Release 7.1.3 Issue 7 May 2018
   [2] *Avaya Aura® Communication Manager Feature Description and Implementation,* Release 7.1.3 Issue 6 May 2018
   [3] *Avaya Aura® Application Enablement Services Administration and Maintenance Guide* Release 6.3 02-300357 June 2014

Product documentation for NICE products may be found at: http://www.nice.com/.
Of particular relevance is the *NICE - Avaya DMCC CTI Integration Manual*.

©2018 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.