Quick Install for Avaya Aura® Device Services

Release 7.1
Issue 1
July 2017

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

Link disclaimer

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

Warranty

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

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

Hosted Service

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

Licenses THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, https://support.avaya.com/LICENSEINFO, UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO

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

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

License types

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

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), 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). You 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").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at https://support.avaya.com/LicenseInfo/ under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

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

Virtualization

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

Third Party Components

"**Third Party Components**" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https://support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM

Service Provider

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

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE

WWW.SIPRO.COM/CONTACT.HTML. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

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

Preventing Toll Fraud

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

Avaya Toll Fraud intervention

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

Security Vulnerabilities

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

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

Trademarks

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

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

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

Contact Avaya Support

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

Contents

Chapter 1. Assumptions for installing Avaya Aura® Device Services

- LDAP is configured with users for authentication.
- System Manager is installed and configured.
- One or multiple Session Manager instances are installed and configured.
- Avaya Aura® Device Services OVA is deployed on same or different host than the one with Session Manager, but within a small latency.
- Avaya Aura® Device Services instance is added to System Manager inventory.
- Session Manager is paired with Avaya Aura® Device Services node.

Chapter 2. Avaya Aura® Device Services Pre-deployment

Adding Data Center

1. Log in to System Manager Web Console.
2. Go to Elements -> Session Manager.

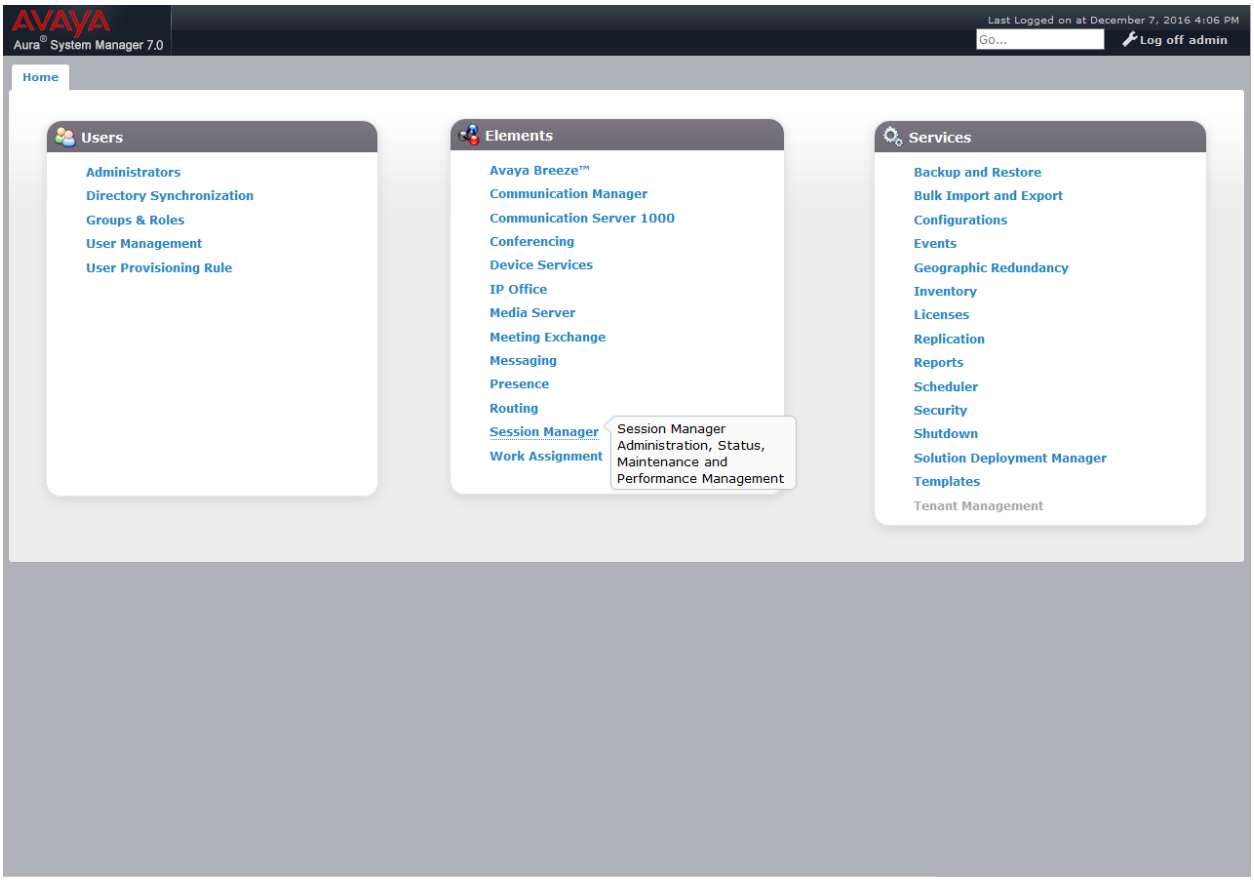


Figure 1: System Manager Web Console

3. In the left navigation pane, click **System Status** tab.

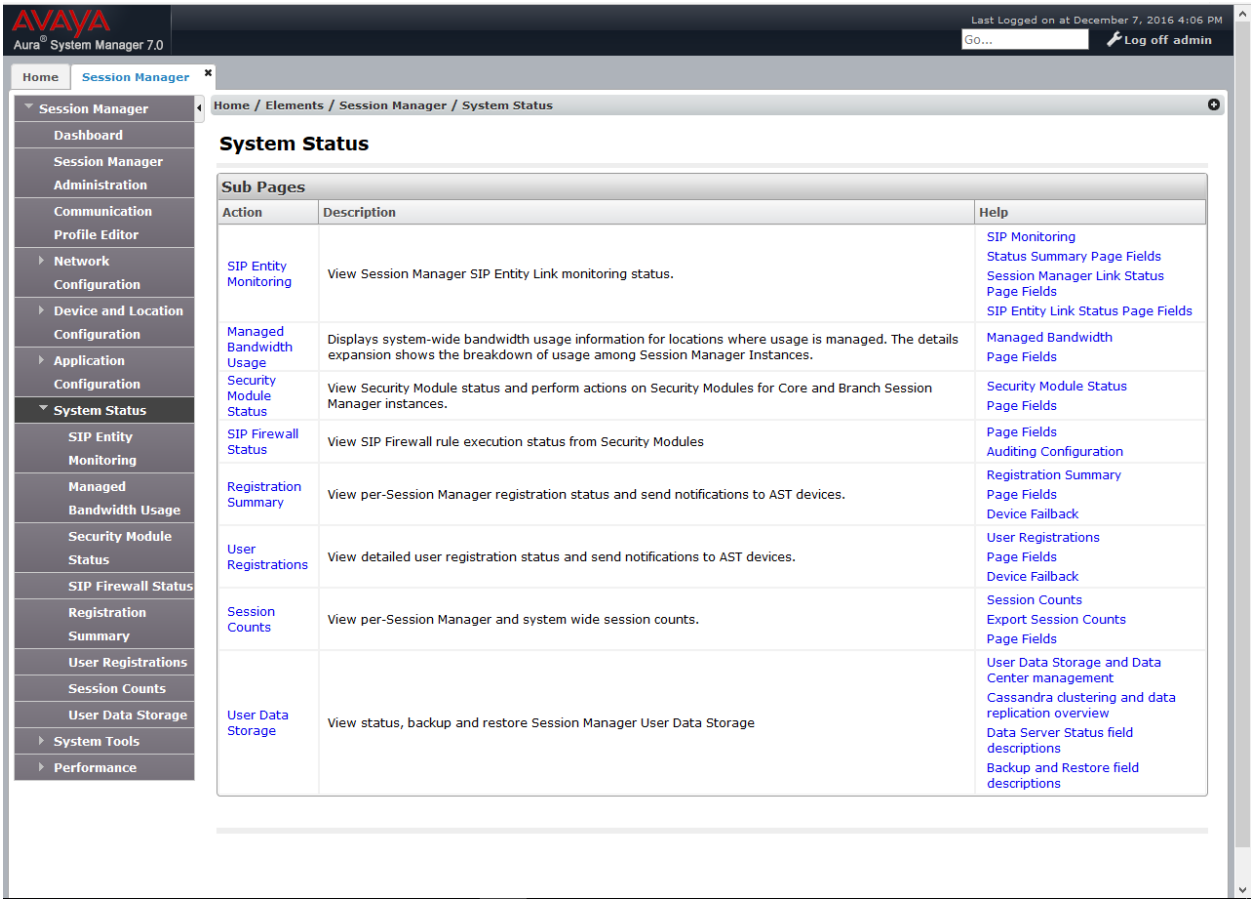


Figure 2: System Status

4. In the **System Status** menu, in **User Data Storage**, click the **Data Center** tab, and then click **New**. The system displays the **Edit Data Center** page.

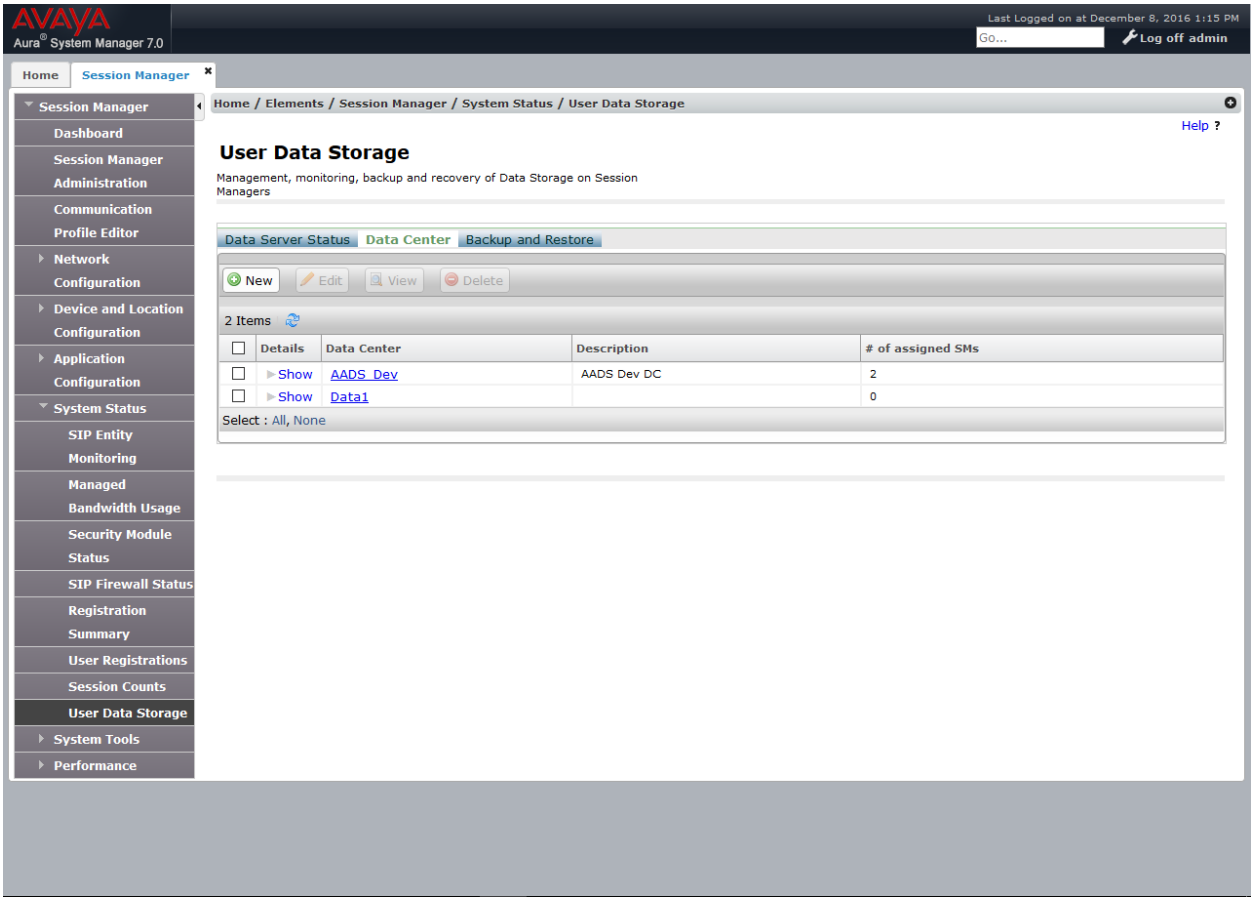


Figure 3: User Data Storage

5. In the **Name** field, type the name of the data center. In the **Description** field type the description about the data center. Click **Commit**.

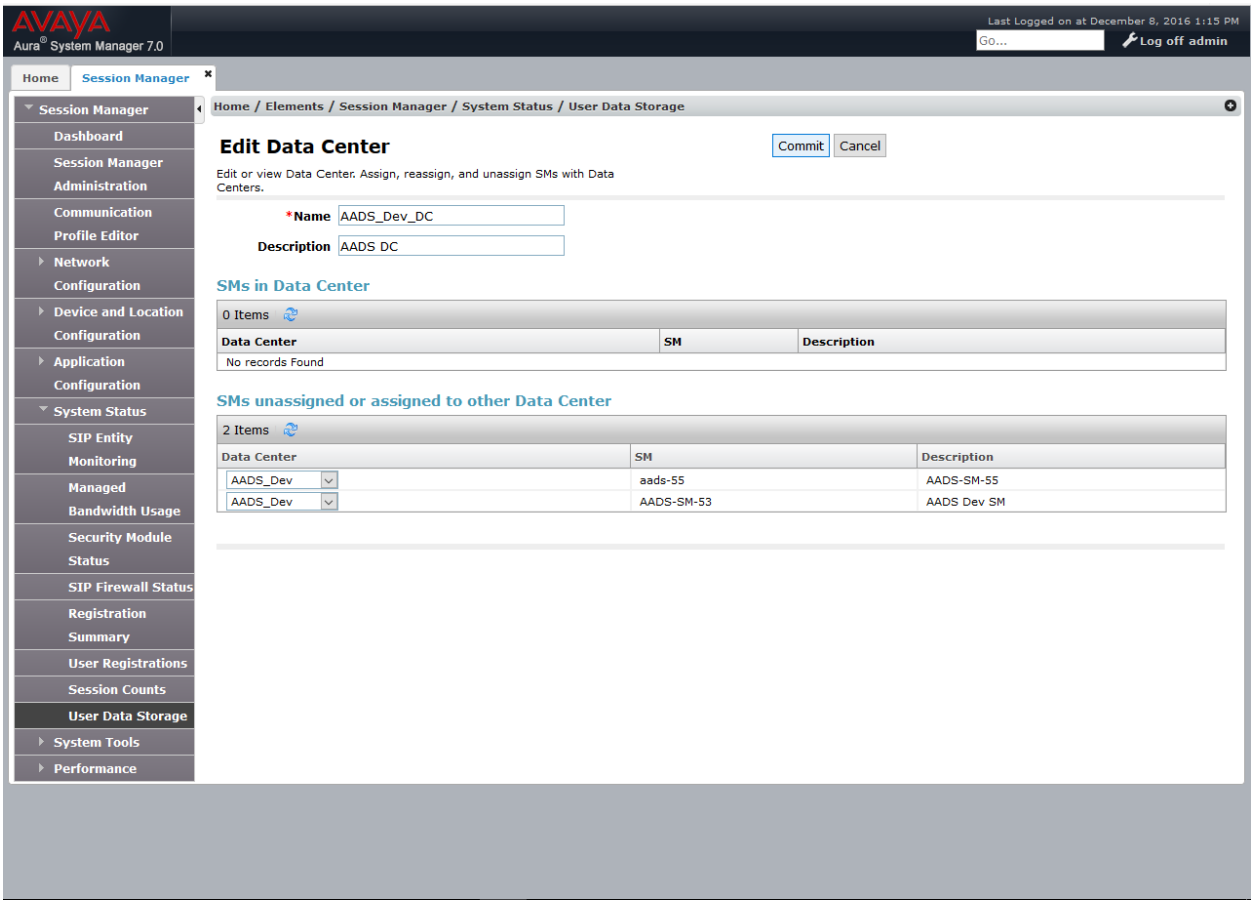


Figure 4: Edit Data Center

You can see the new Data Center added.

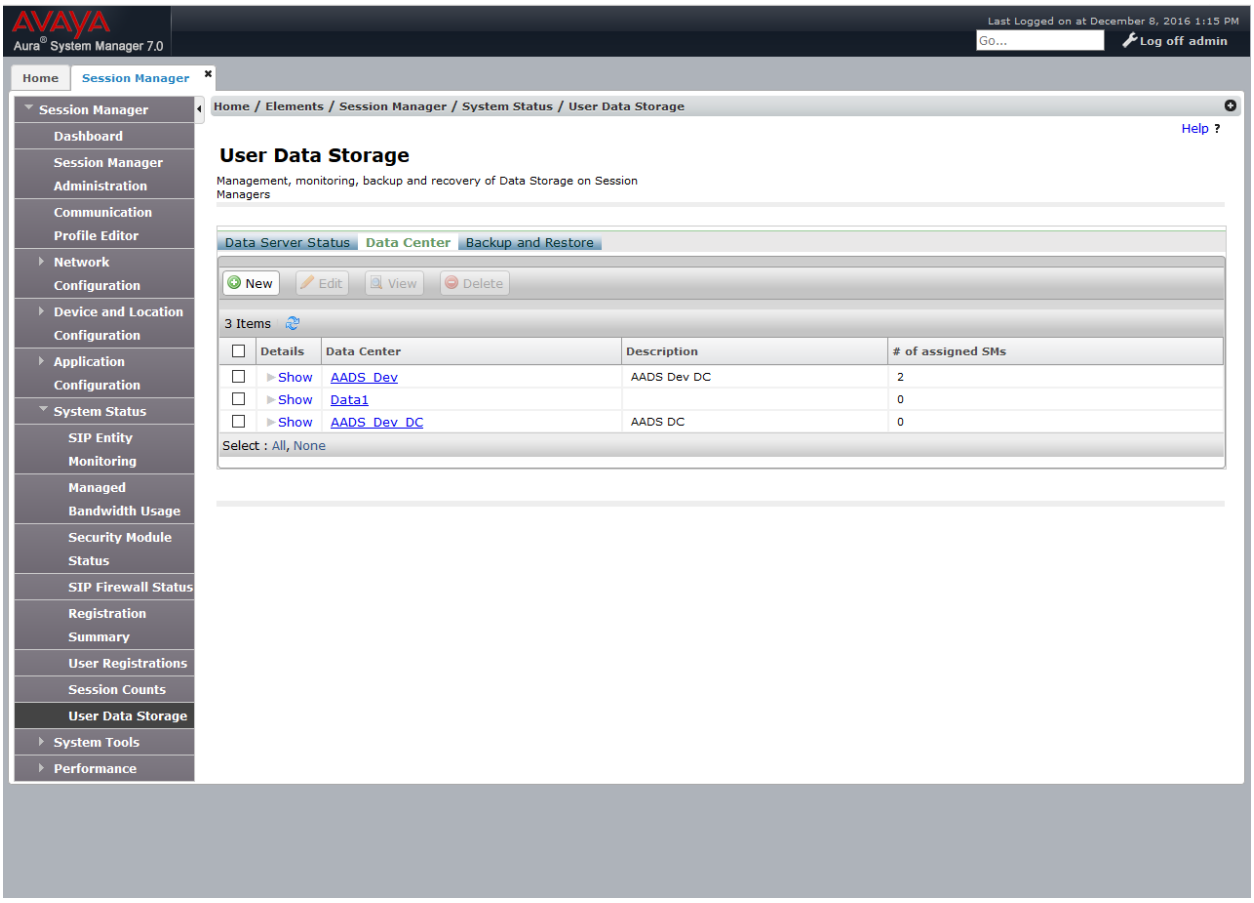


Figure 5: User Data Storage

Assigning Session Manager to Data Center

1. Go to Session Manager -> Session Manager Administration.
2. Click the **Session Manager Instances** tab. Select a Session Manager instance and click **Edit**. The system displays the **Edit Session Manager** page.

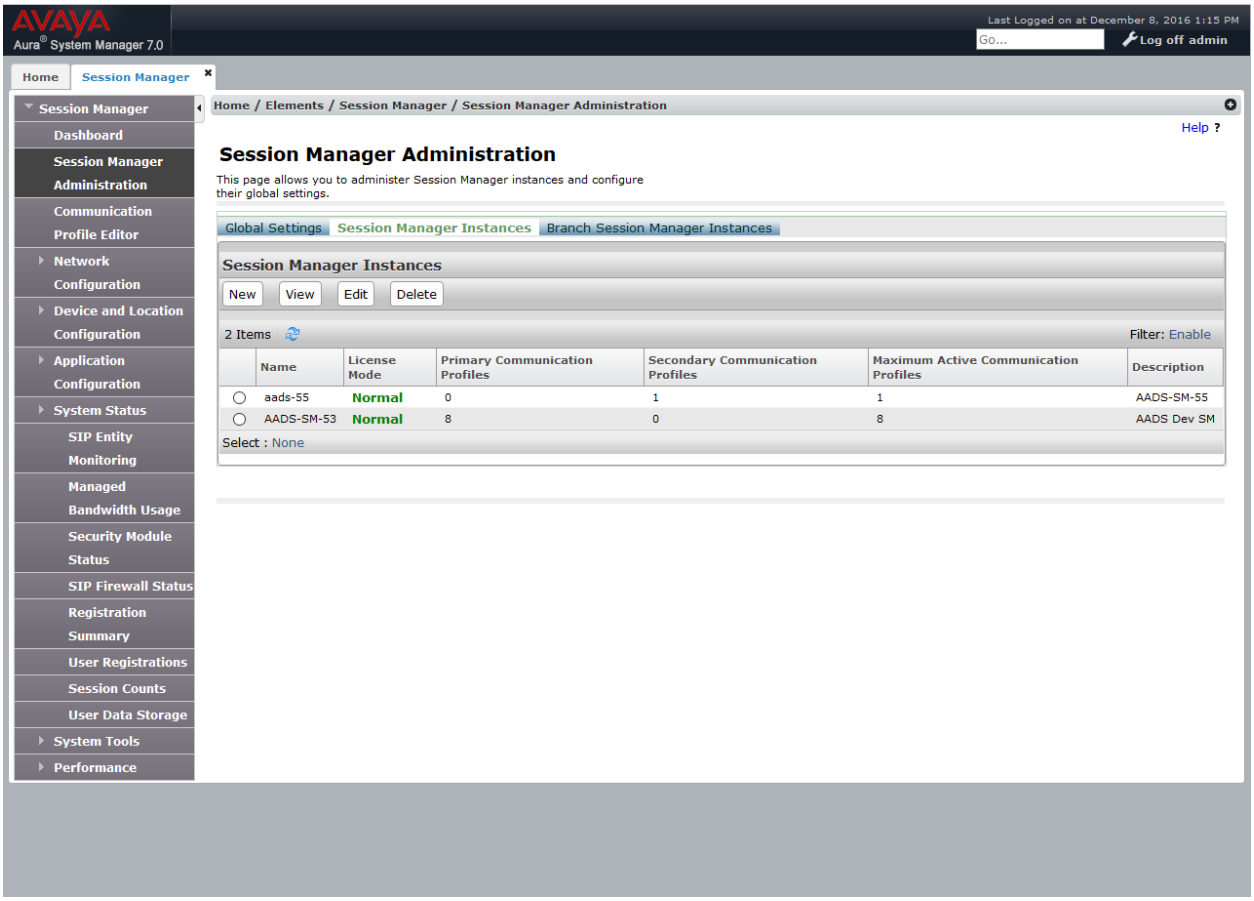


Figure 6: Session Manager Administration

3. To assign Session Manager to data center, under the **General** section, from the **Data Center** drop-down list select the data center name that was created. Click **Commit**. This will assign Session Manager to data center.

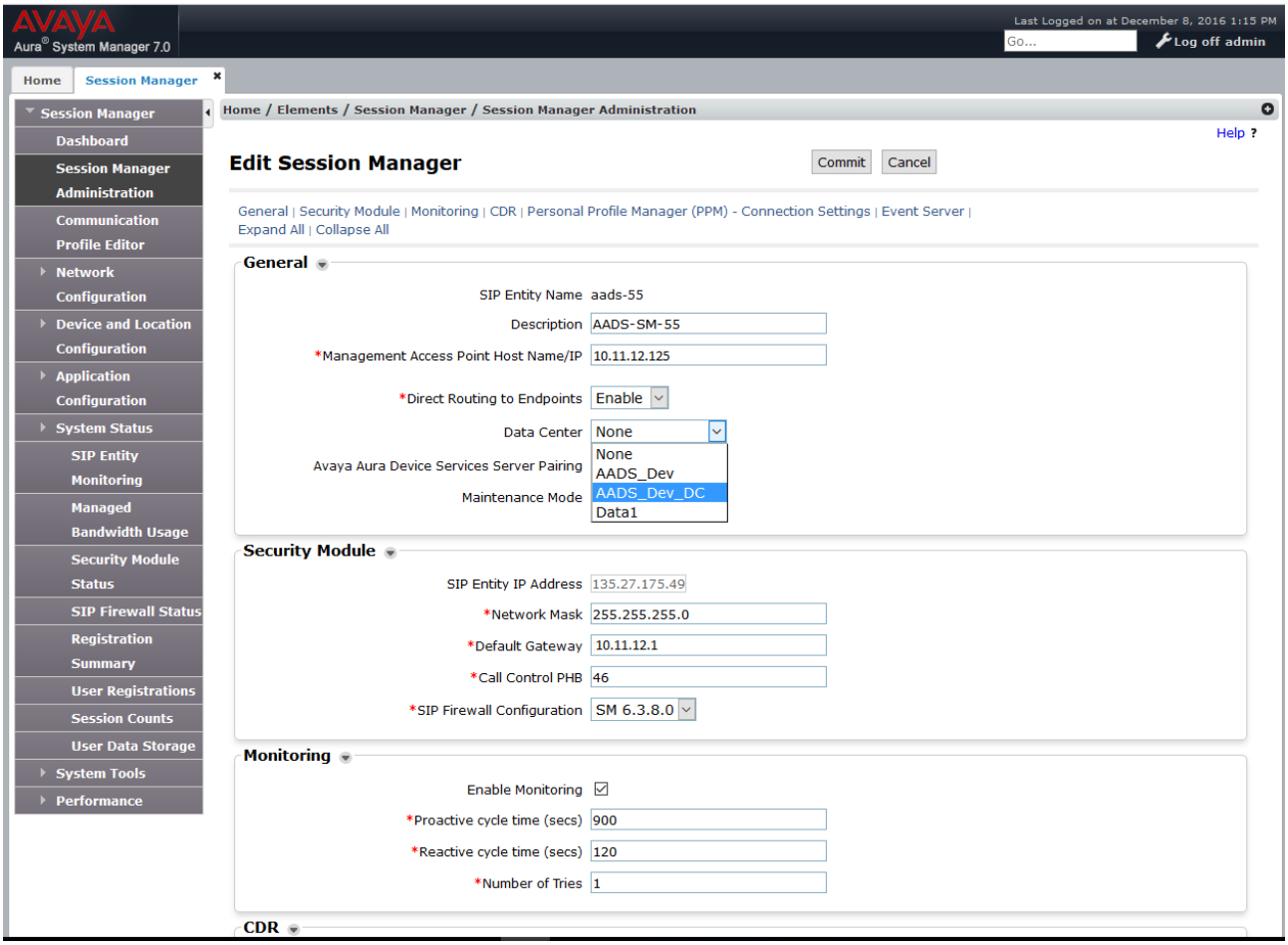


Figure 7: Edit Session Manager

Chapter 3. Avaya Aura® Device Services Deployment

OVA deployment through vSphere Client

1. Open the vSphere client and click **File** -> **Deploy OVF Template**.

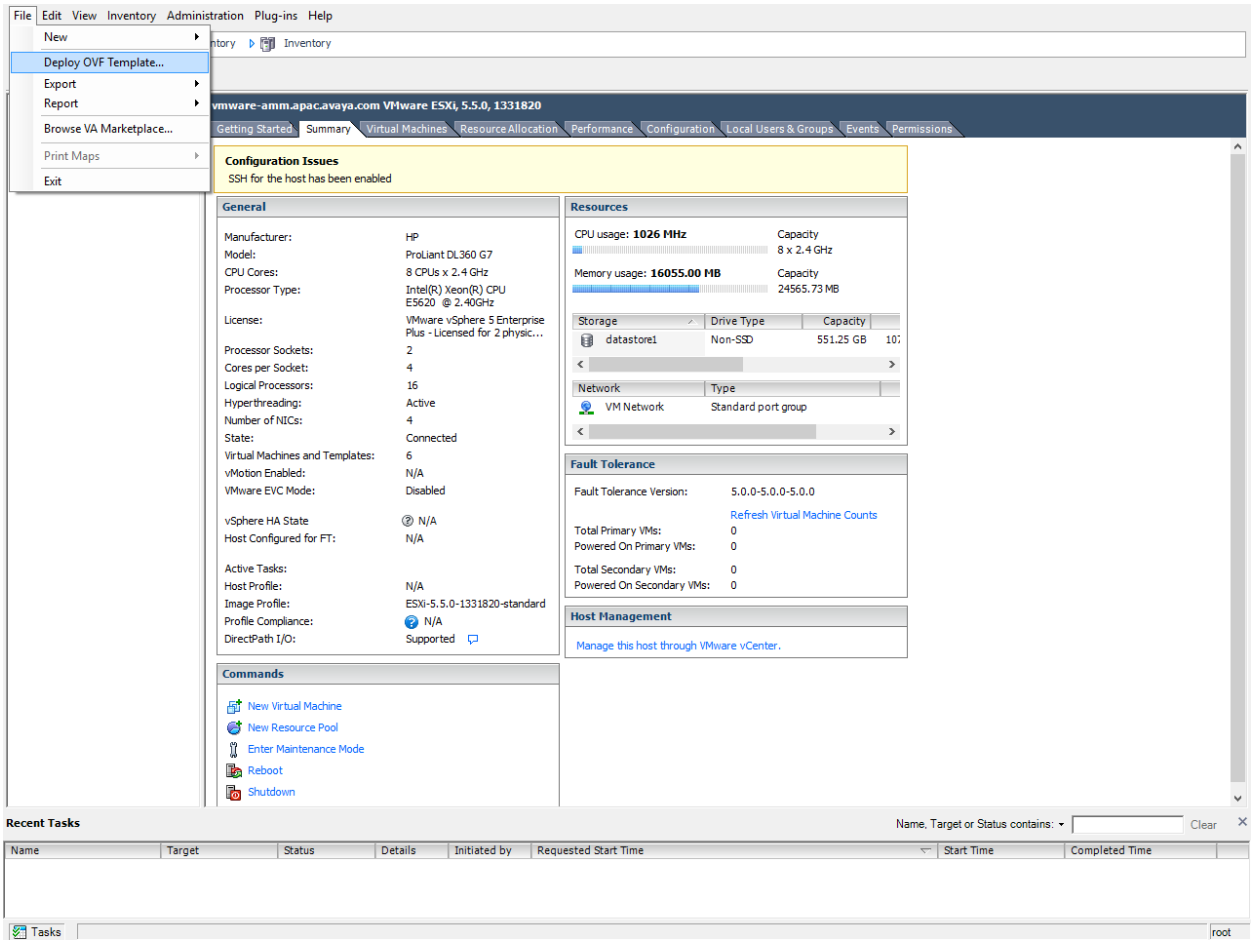


Figure 8: Deploy OVF Template

2. In the Deploy OVF Template window, type the URL in the **Deploy from a file or URL** field. Click **Next**.

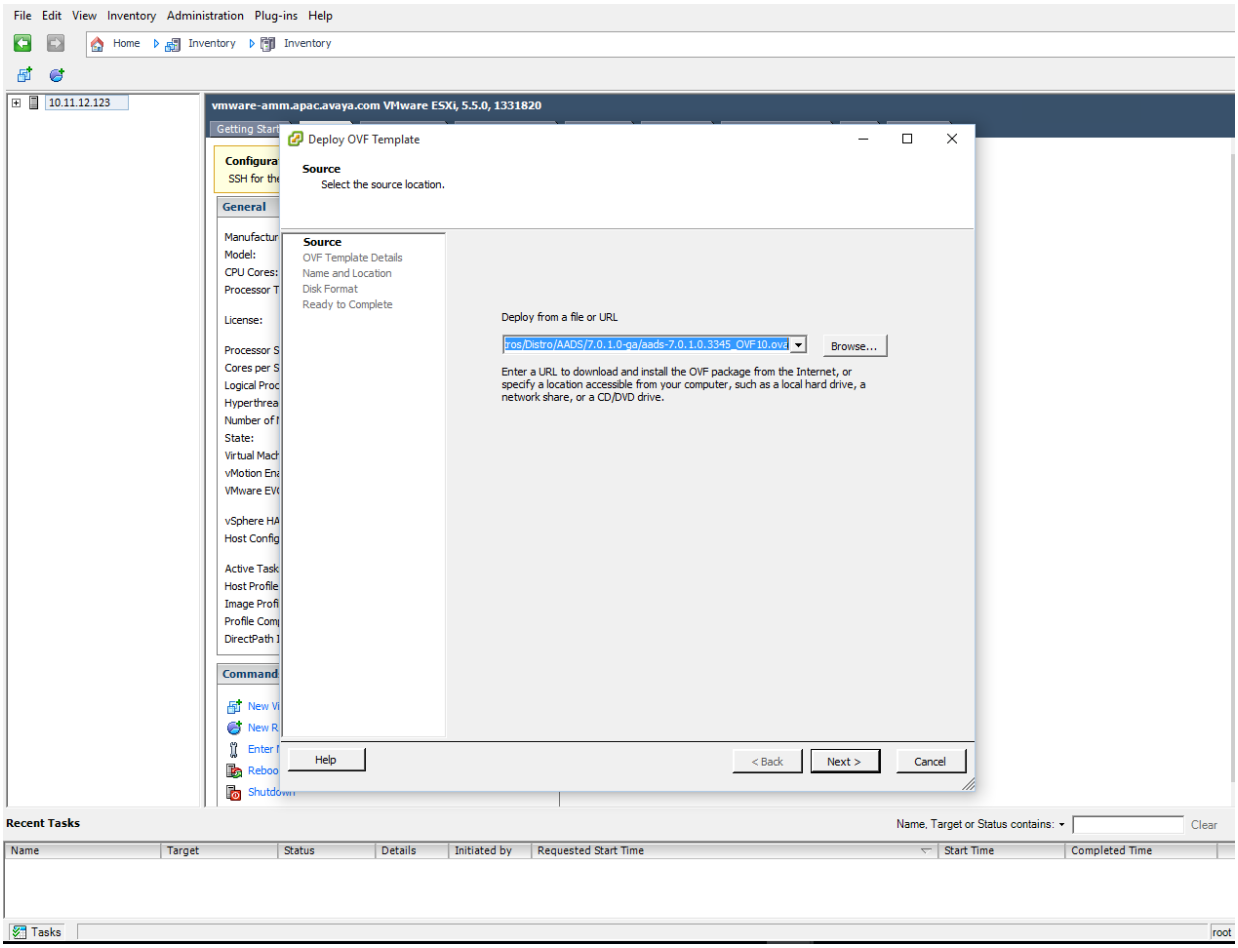


Figure 9: Deploy OVF Template Source

3. In the OVF Template Details window, verify the details of the Avaya Aura® Device Services OVF template and click **Next**. The system displays End User License Agreement window.

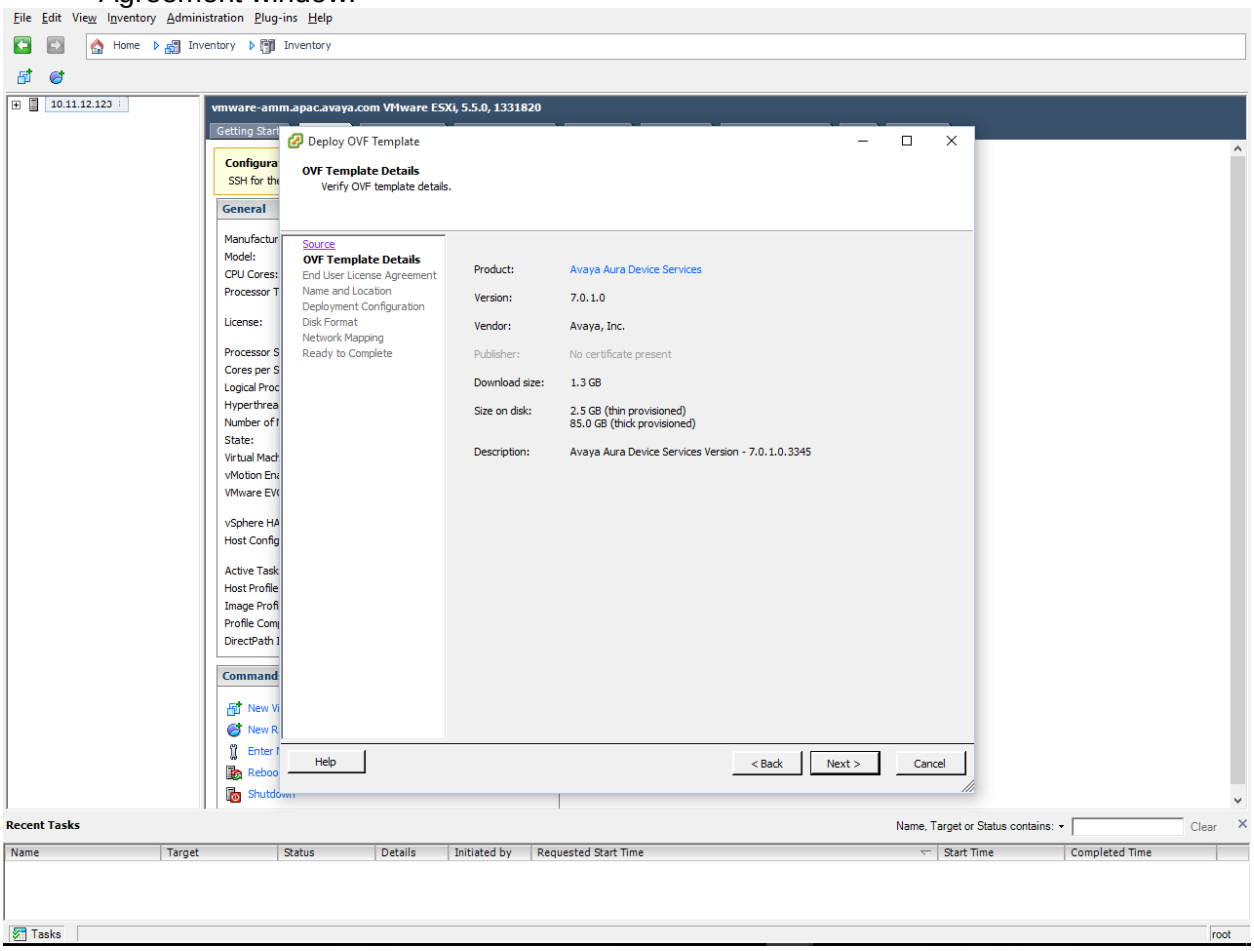


Figure 10: OVF Template Details

4. Read the license agreement and click **Accept**. Click **Next**. The system displays the Name and Location window.

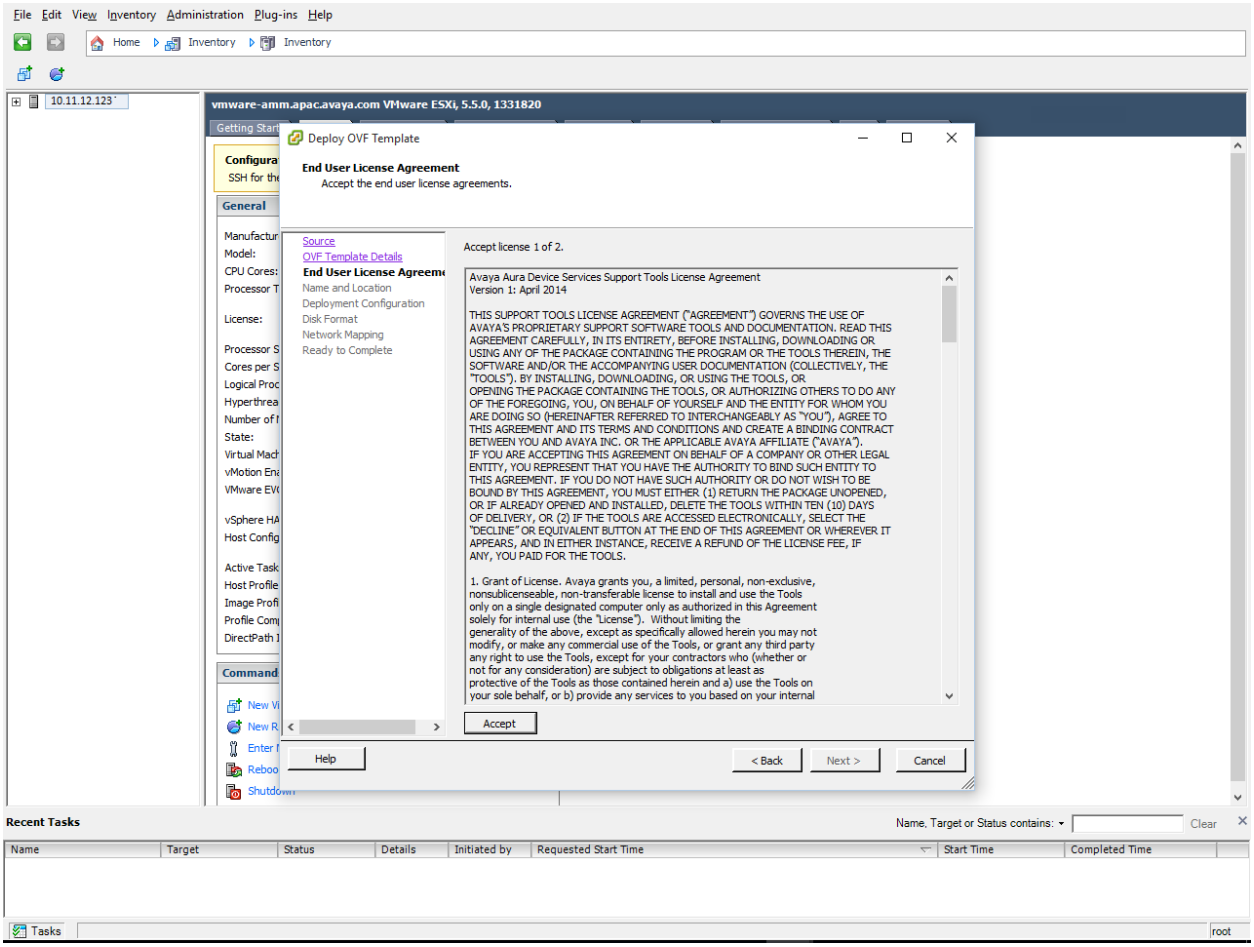


Figure 11: End User License Agreement

5. In the **Name** field, type the name of the new OVA and click **Next**. The system displays the **Deployment Configuration** window.

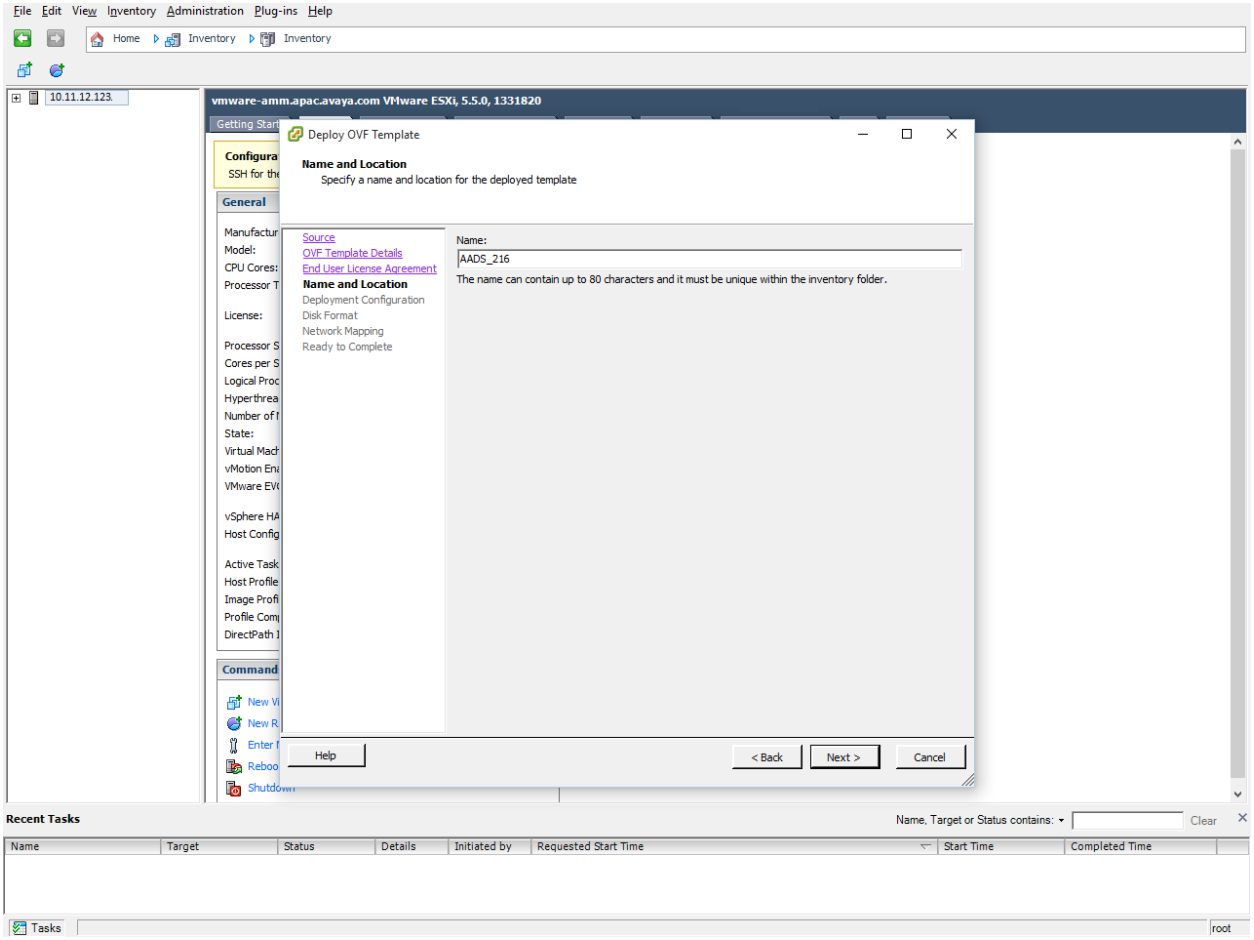


Figure 12: Name and Location

6. In the **Configuration** field, click on the Avaya Aura® Device Services profile that matches your requirement, and click **Next**.

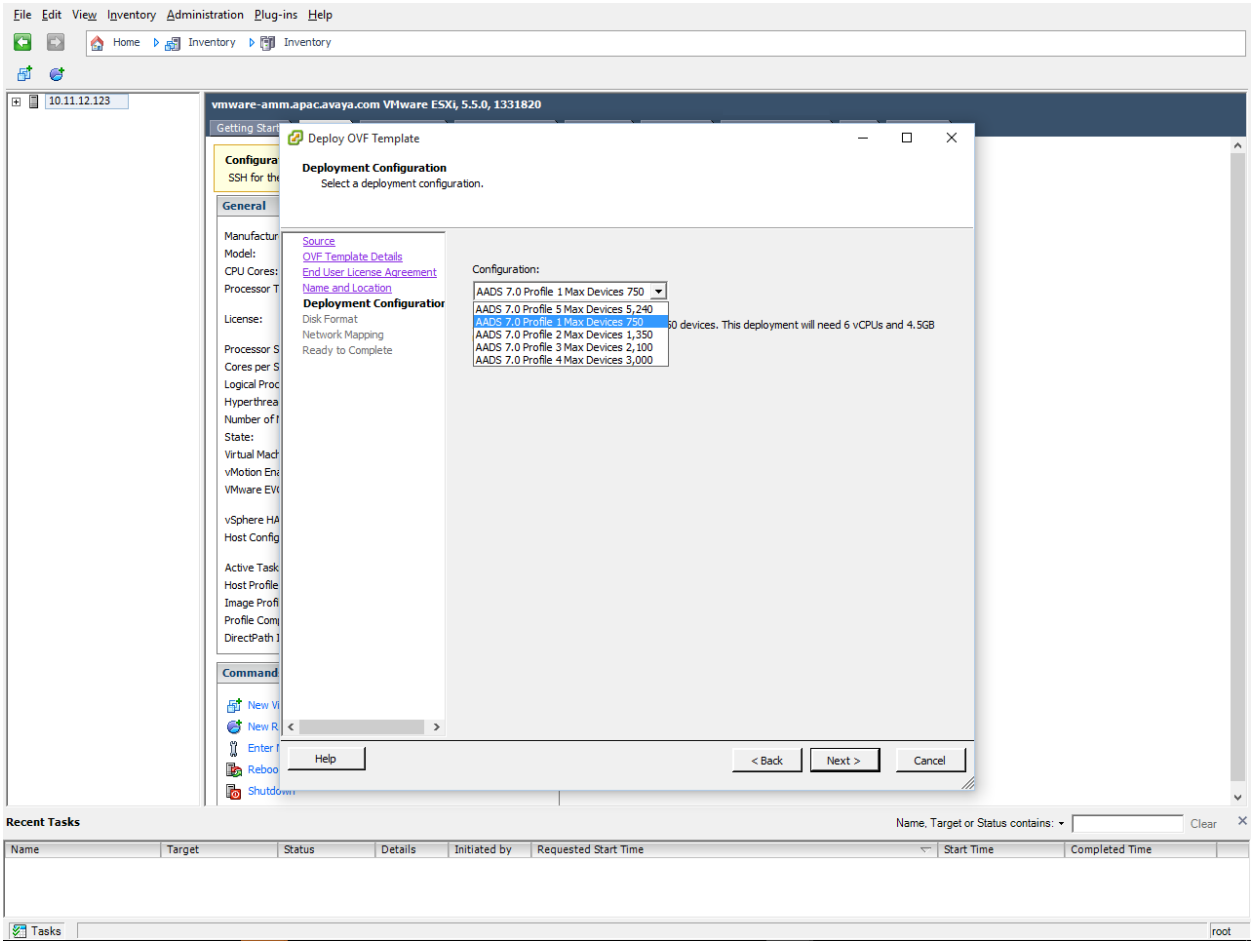


Figure 13: Deployment Configuration

7. In the Disk Format window, select the desired disk format and click **Next**.

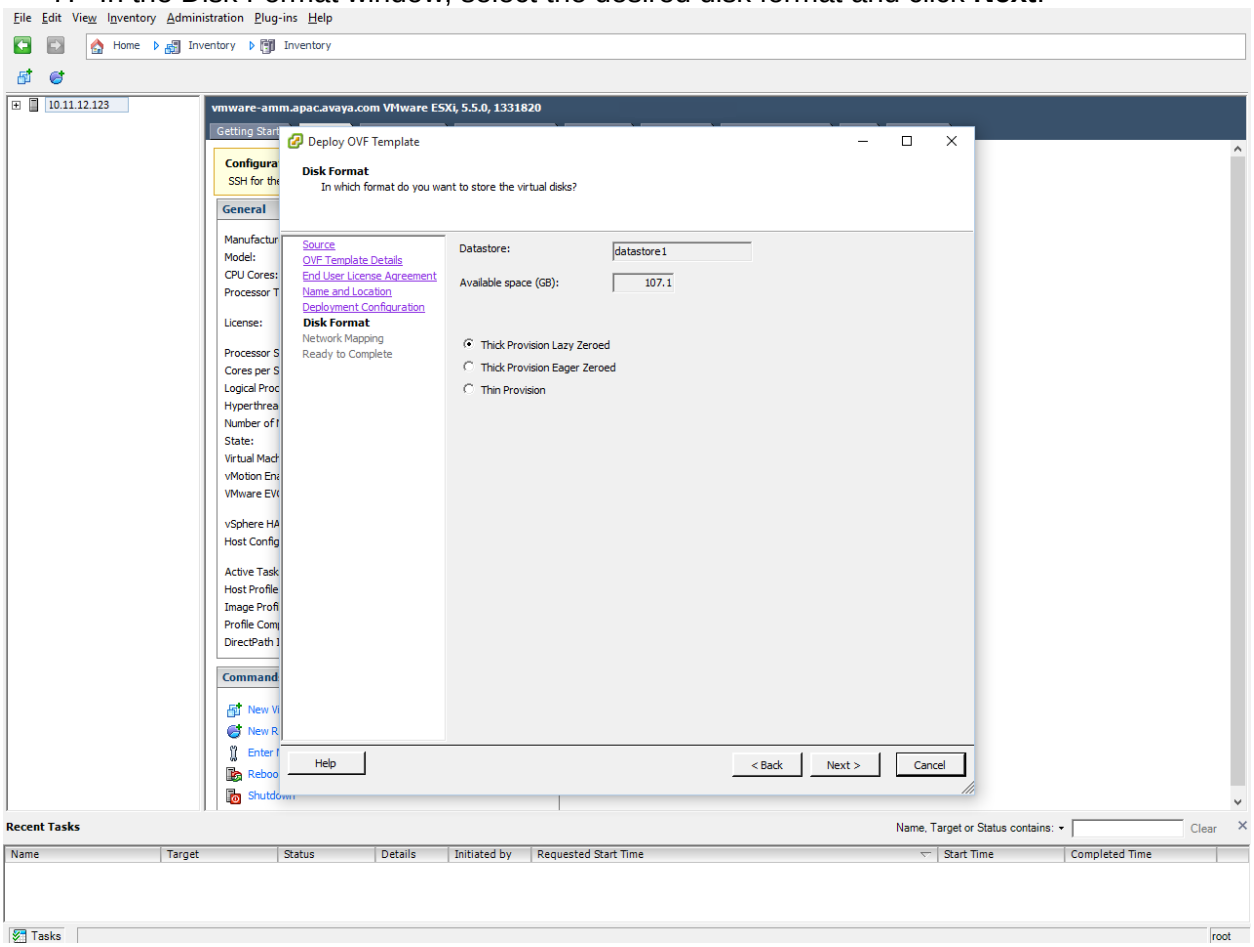


Figure 14: Disk Format

8. In the Network Mapping window, ensure that the correct network available for that virtual machine is selected, and click **Next**. The system displays **Ready to Complete** window.

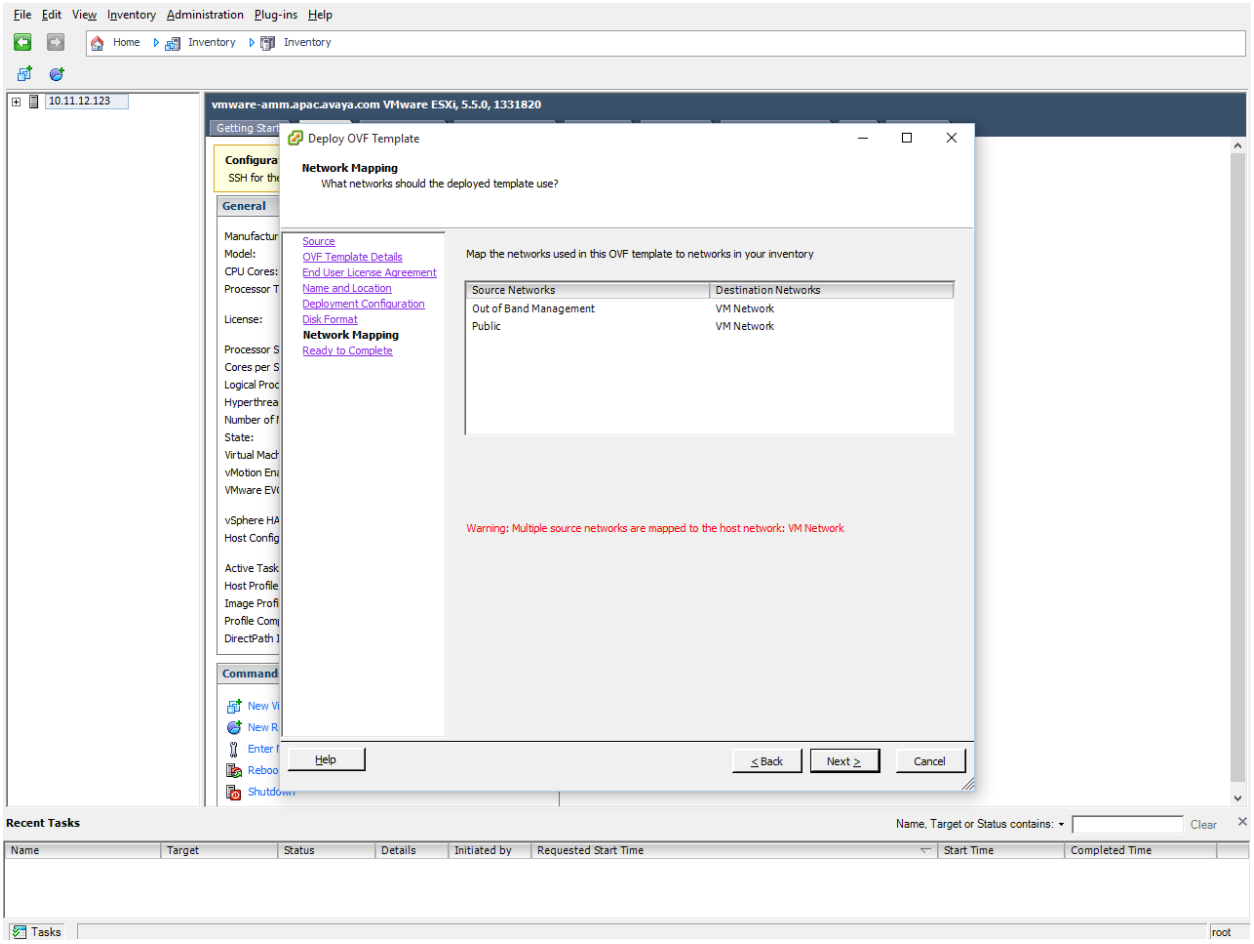


Figure 15: Network Mapping

9. **(Optional)** Click the **Power on after deployment** checkbox to start the Avaya Aura® Device Services automatically after deployment. Verify the deployment settings and click **Finish**.

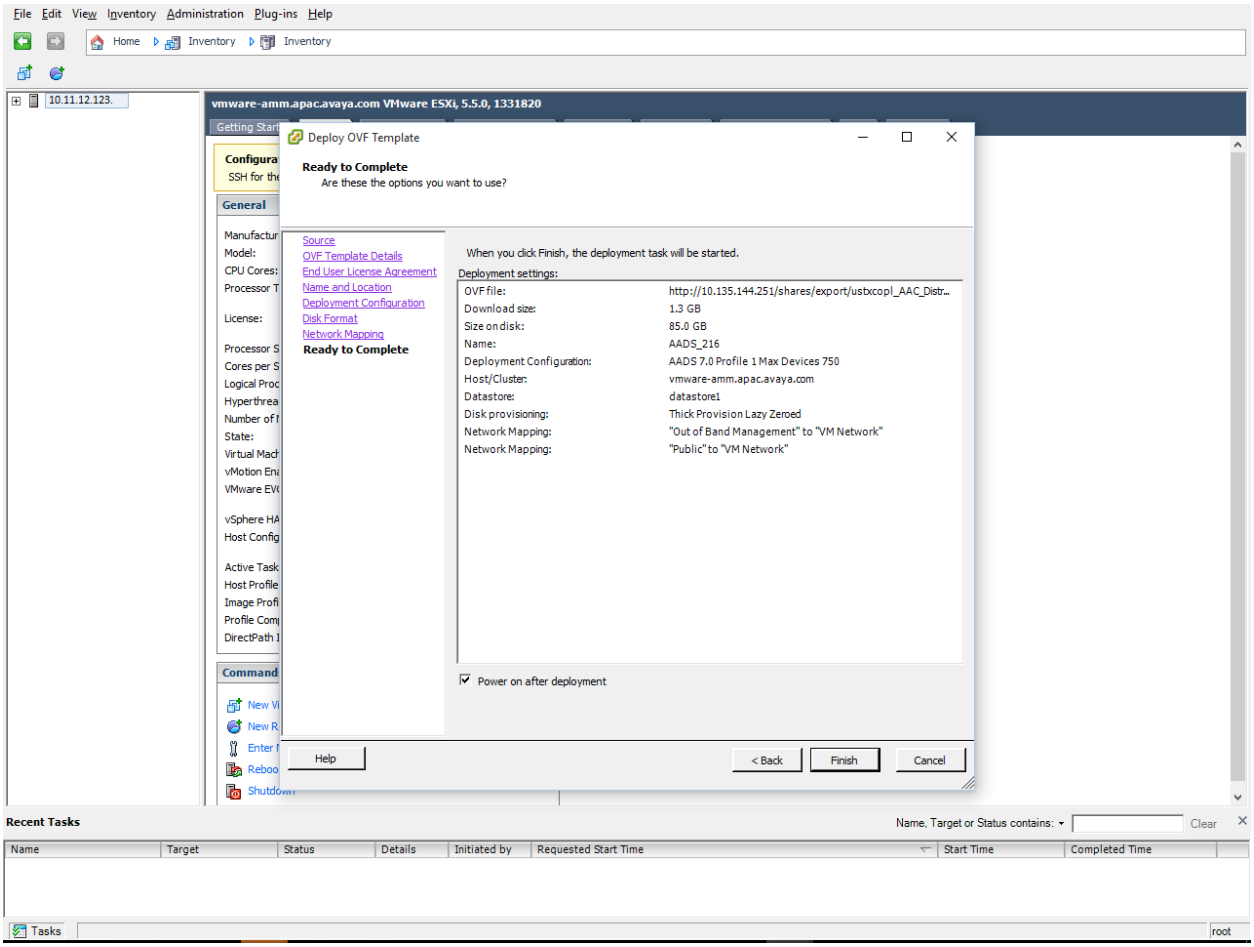


Figure 16: Ready to Complete

10. After you click **Finish**, the system displays the progress of the tasks in the Deploying AADS window.

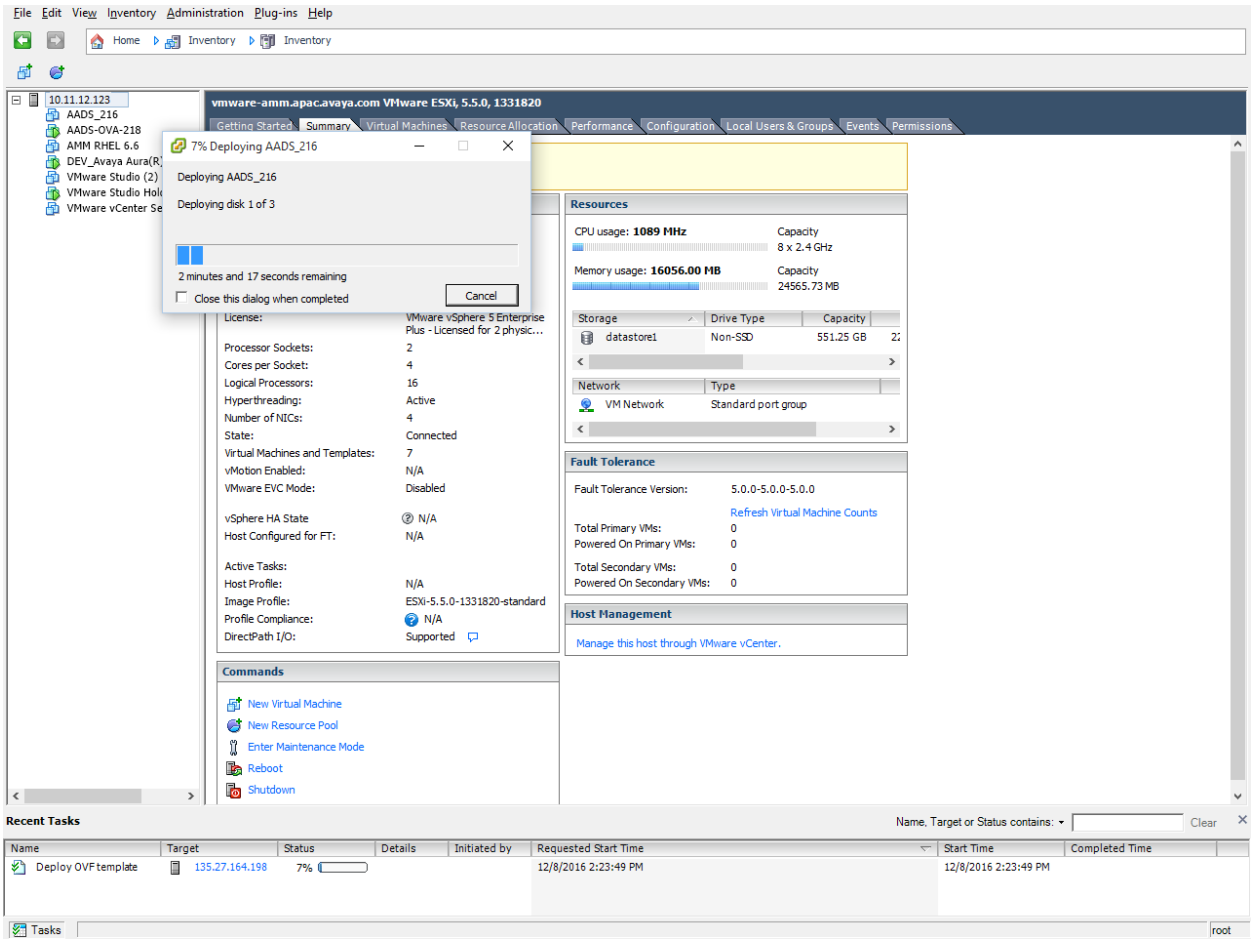


Figure 17: Deploying of AADS

11. After the deployment is complete, system displays **Deployment Completed Successfully** box.
12. In the Deployment Completed Successfully window, click the **Close** button.

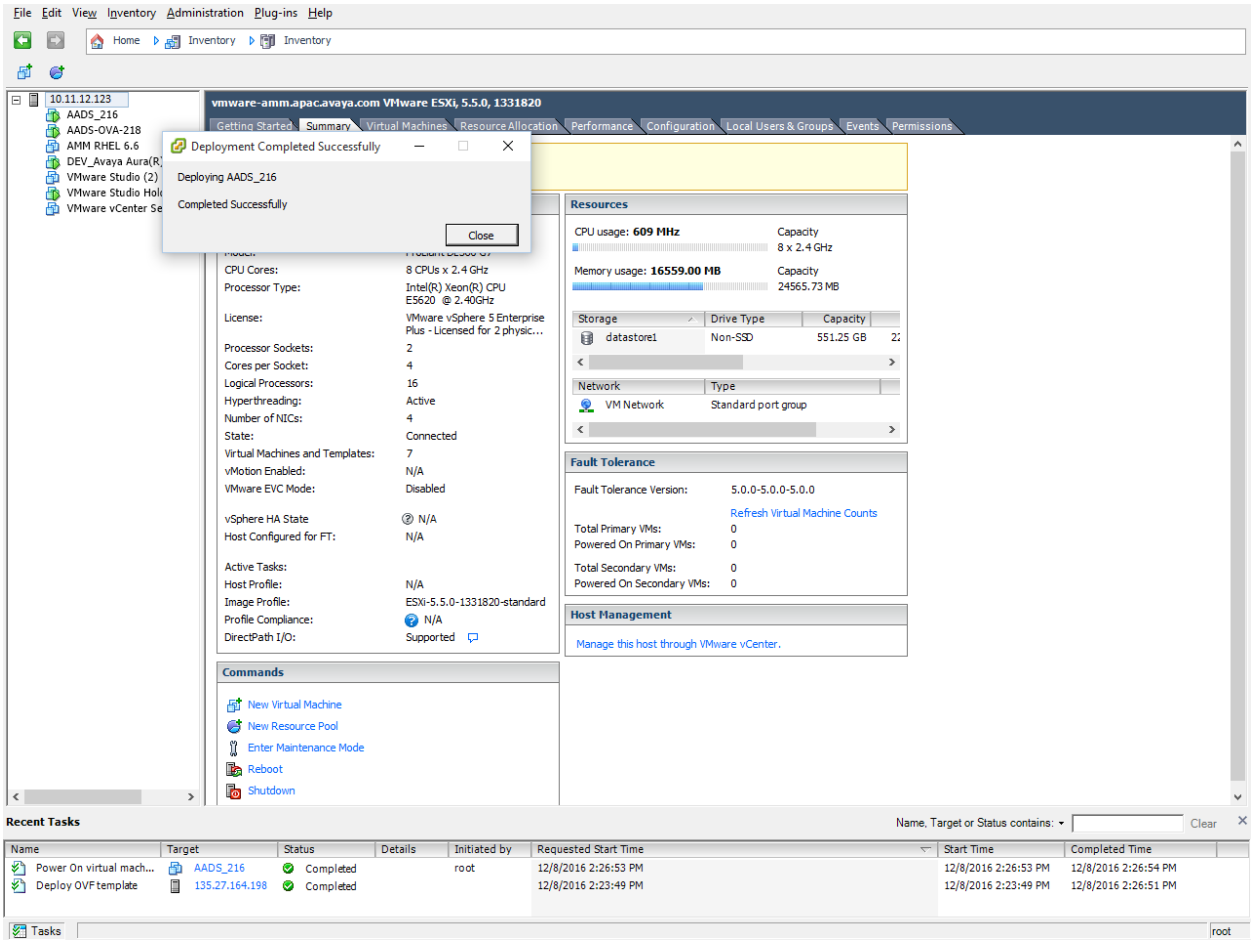


Figure 18: Deployment Completed Successfully

13. Power on VM and go to the console tab. Accept the End User License Agreement (EULA).

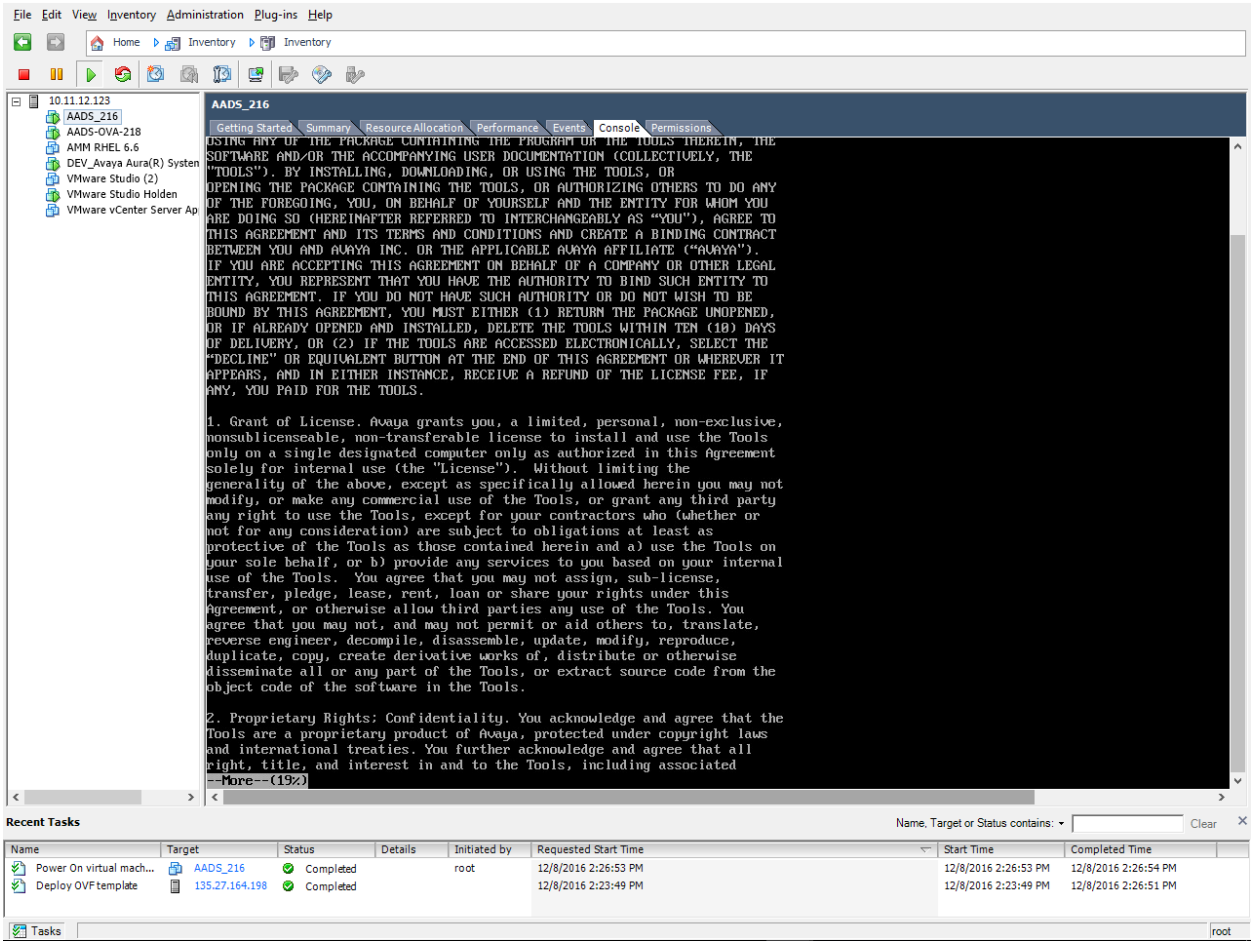


Figure 19: Power on the VM

14. Read the End User License Agreement and type **yes** to accept the End User License Agreement.

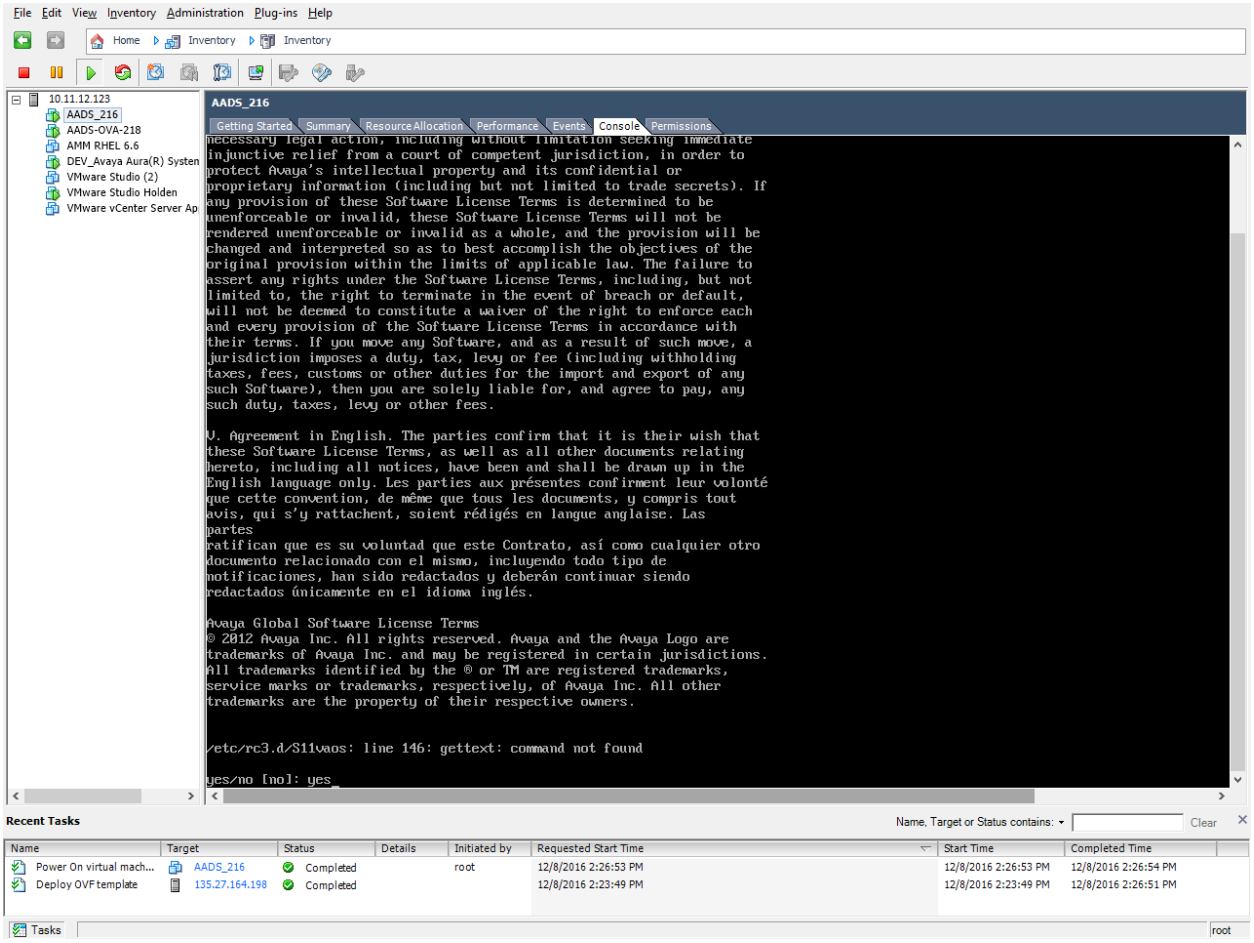


Figure 19: Accept the EULA

15. After the EULA is accepted, the system displays below screen. Type ‘y’ to **Provide user input configuration**.

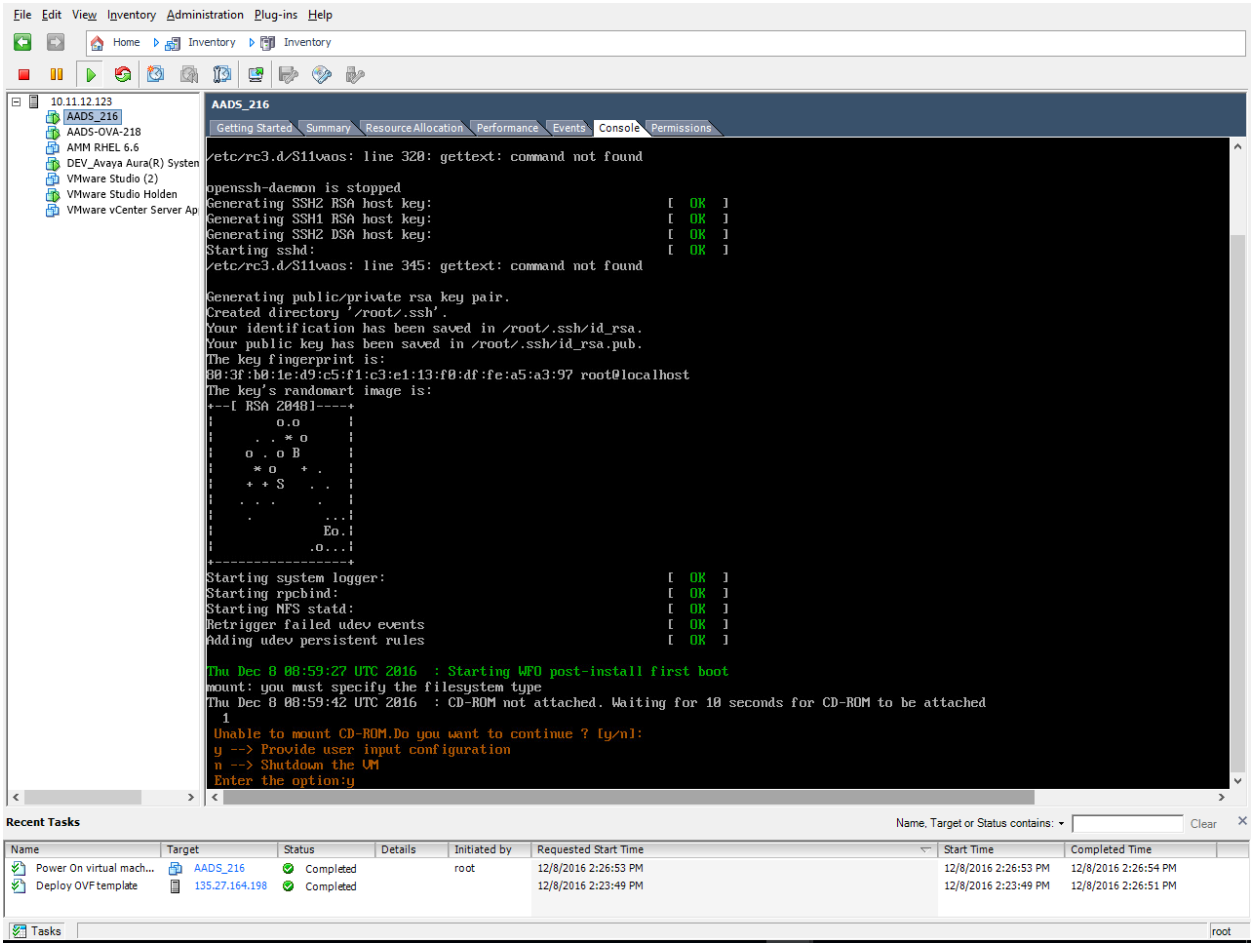


Figure 20: User Input Configuration

16. Enter the **Network settings** parameter for the new VM.

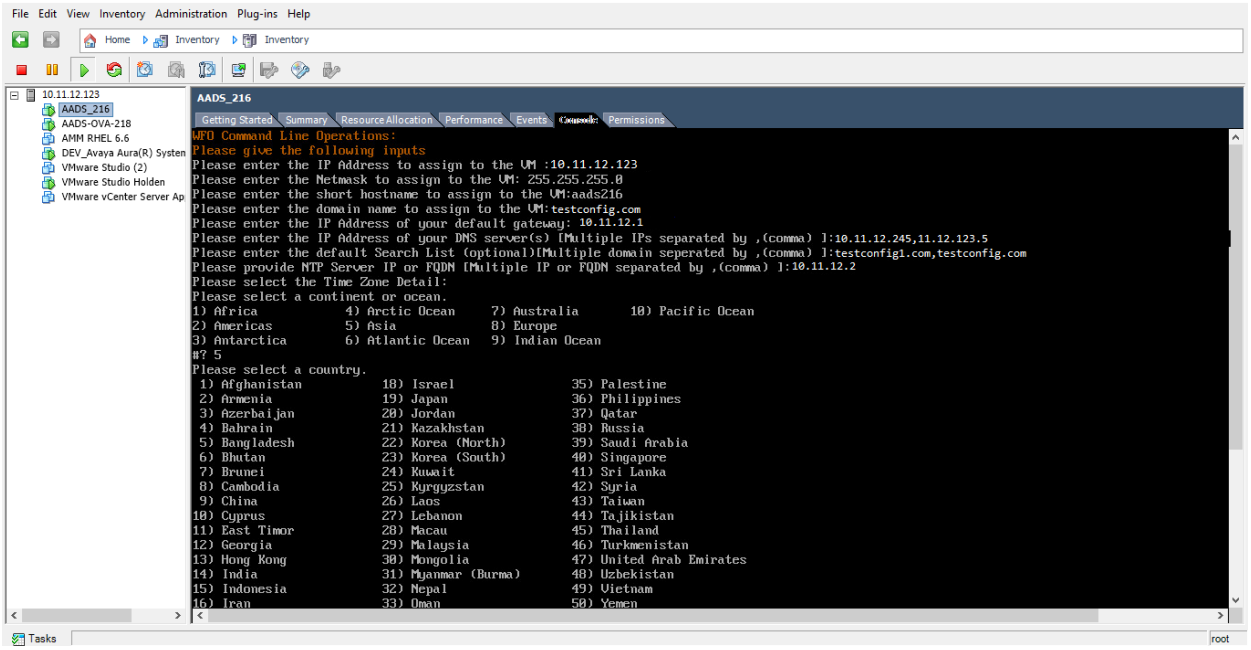


Figure 21: Network Settings for new VM

17. Type the group name for the admin account and press **Enter.**

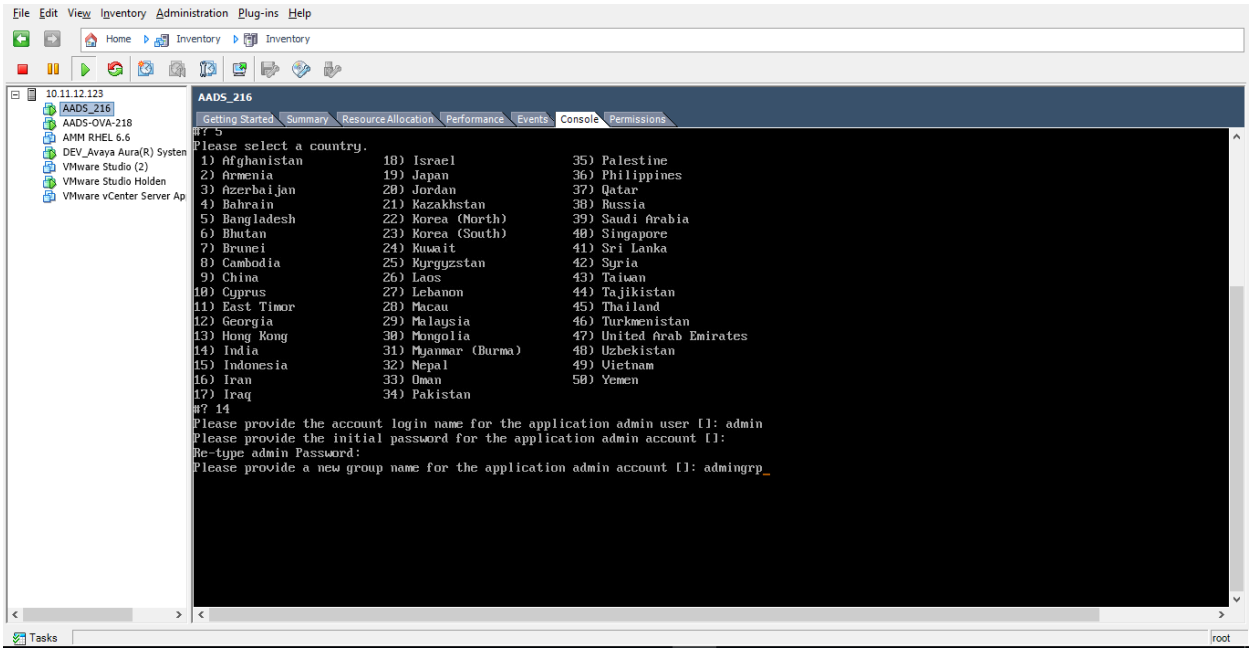


Figure 22: Group name for the admin account

18. Verify the Network Setting parameters. To continue, type “y” and press **Enter**.

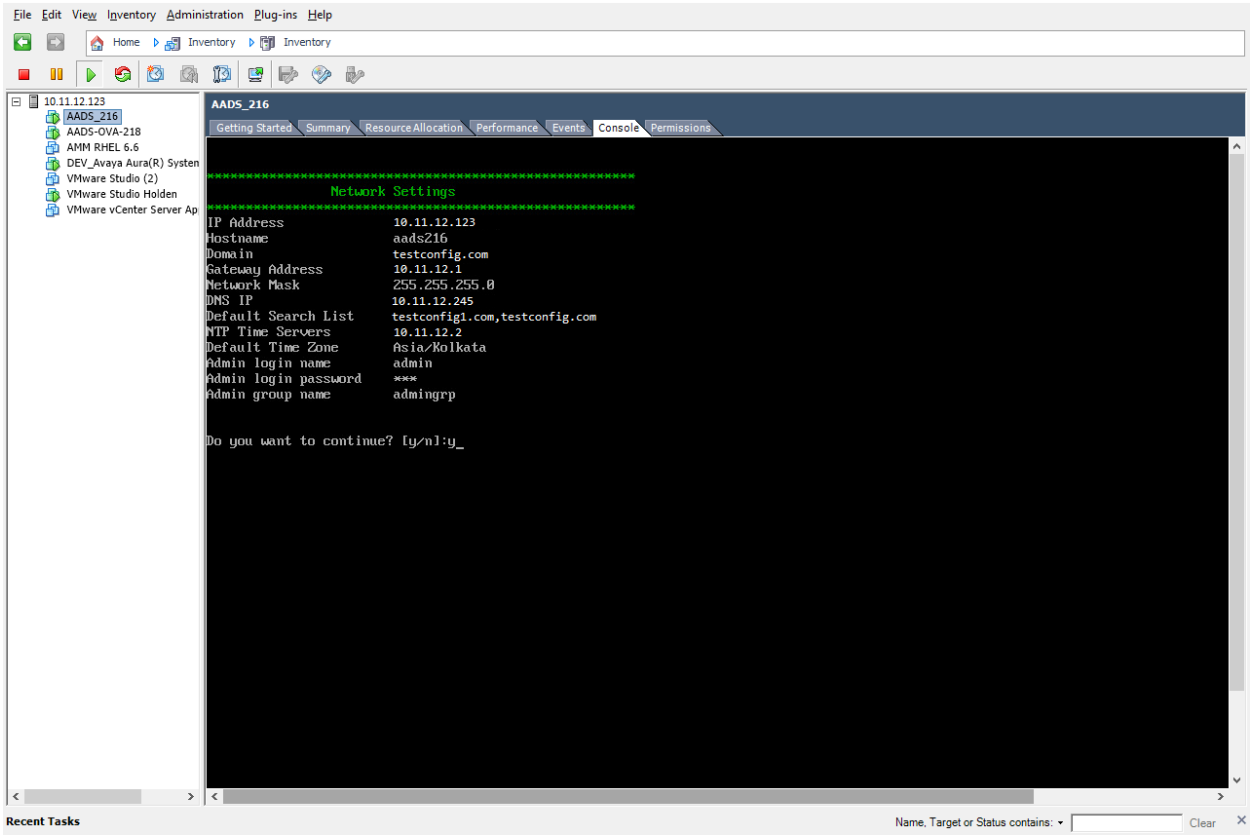


Figure 23: Network Settings

19. After all the steps are successfully completed, the system displays a login prompt for the deployed **Avaya Aura® Device Services** VM.

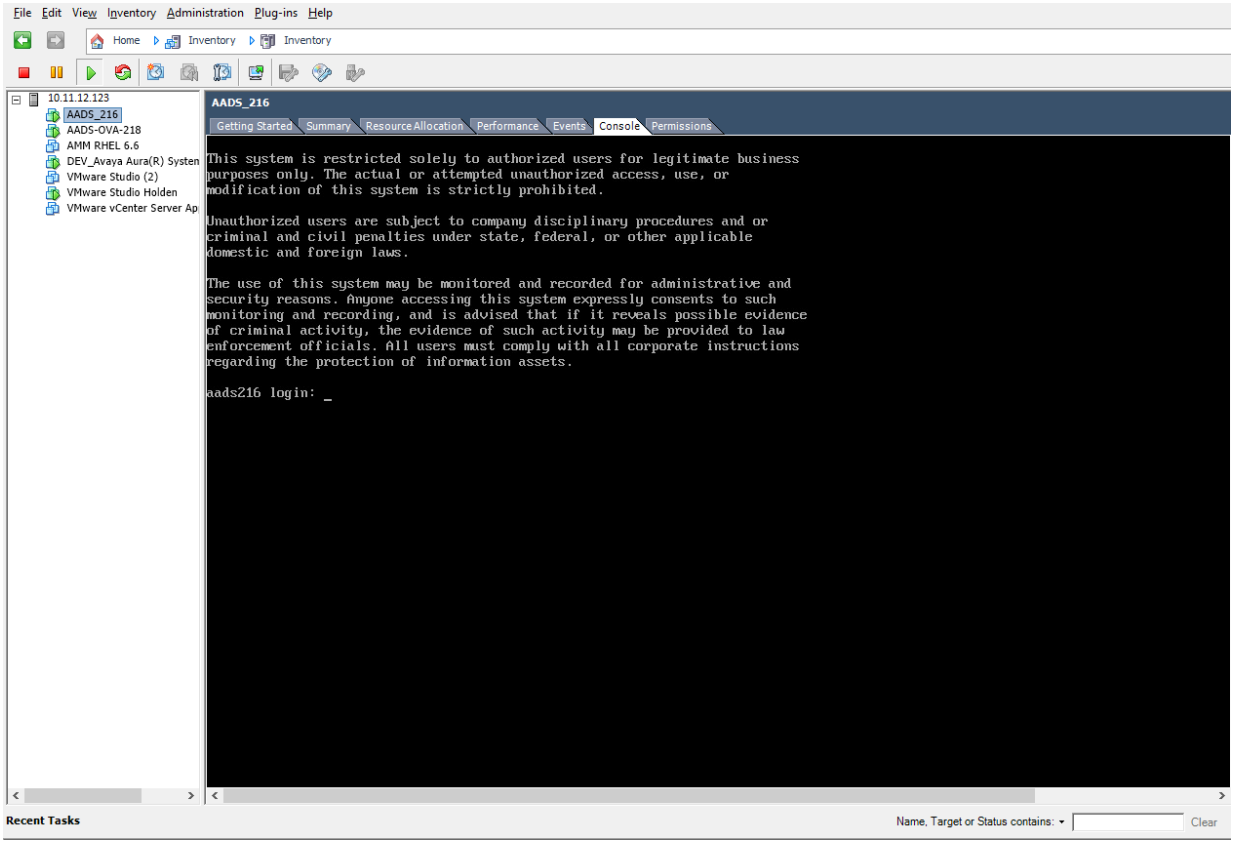


Figure 24: Avaya Aura® Device Services VM login

Chapter 4. Avaya Aura® Device Services Post-deployment

Adding an Avaya Aura® Device Services instance to System Manager Inventory

1. On the System Manager Web console, click **Services** -> **Inventory**.

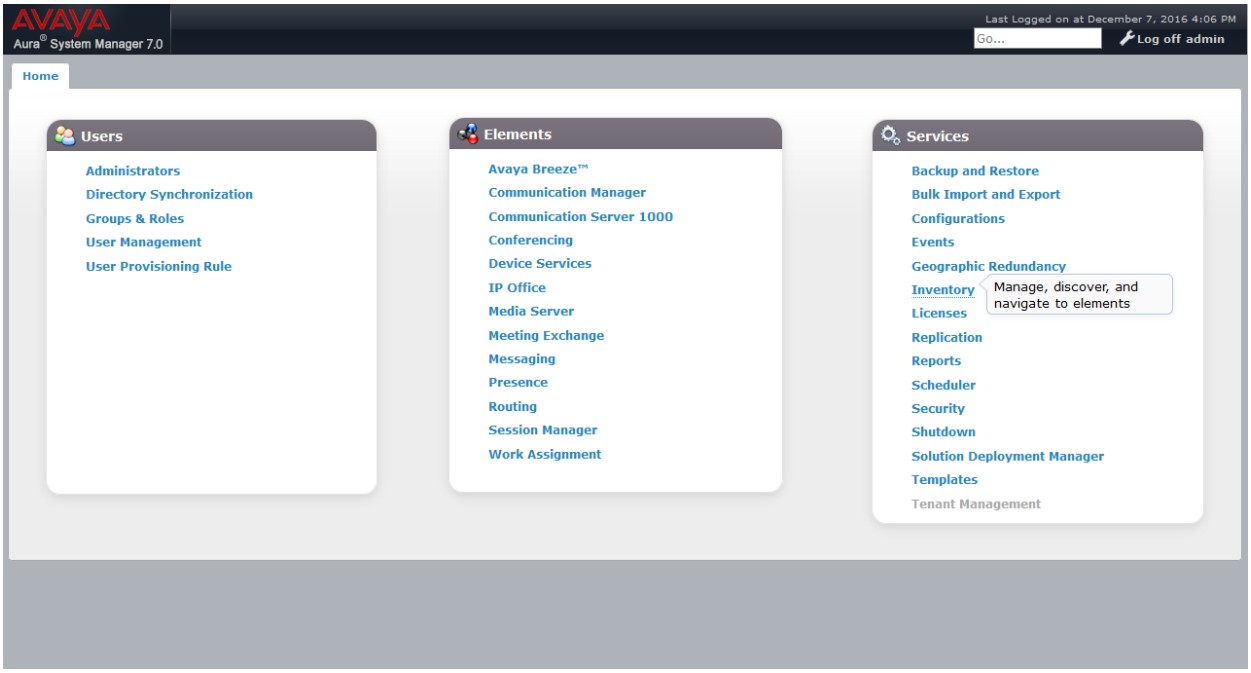


Figure 25: Inventory

2. In the left navigation pane, click **Manage Elements**. On the Manage Elements page, click **New**. The system displays the New Elements page.

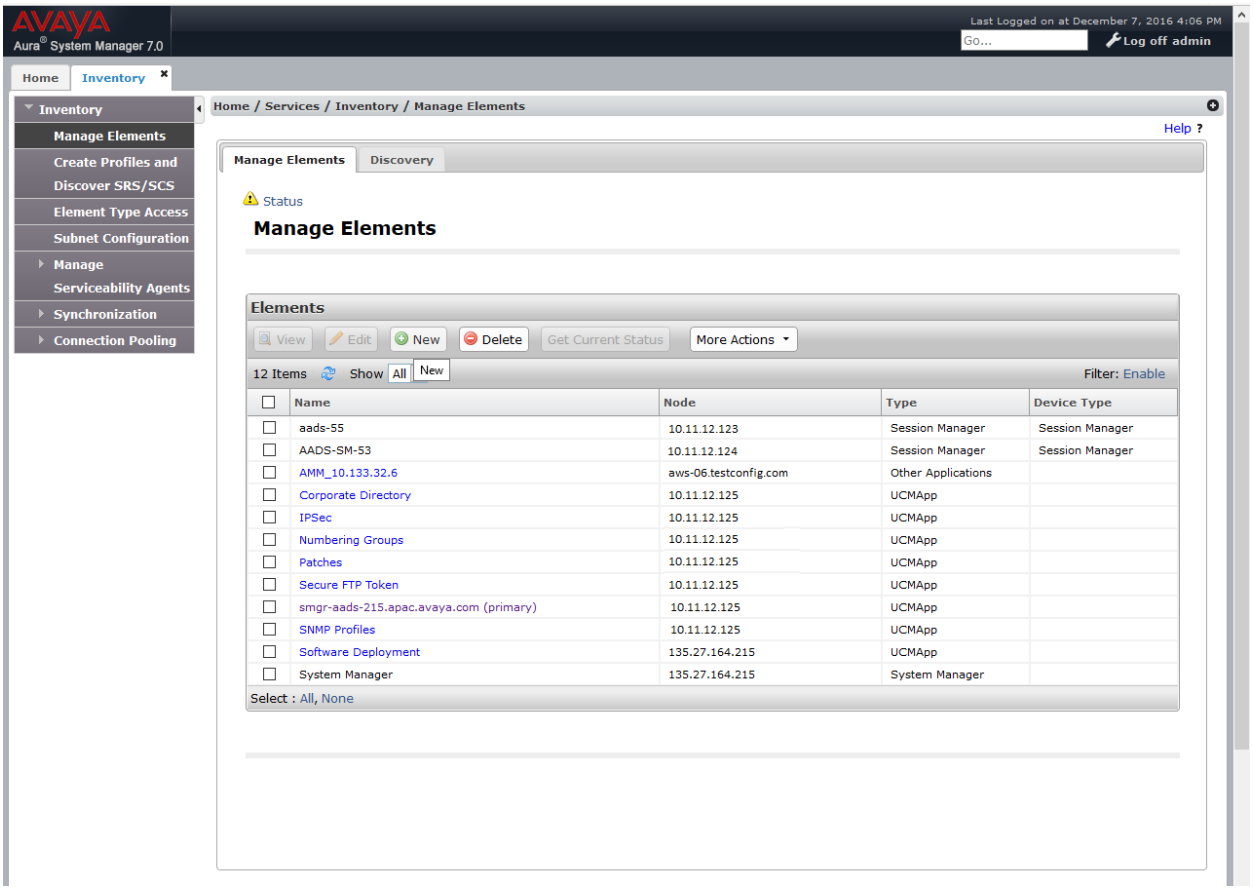


Figure 26: Manage Elements

3. In the **General** section, from the **Type** field select **Avaya Aura Device Services**. The system refreshes the page and displays a **New Avaya Aura Device Services** page.

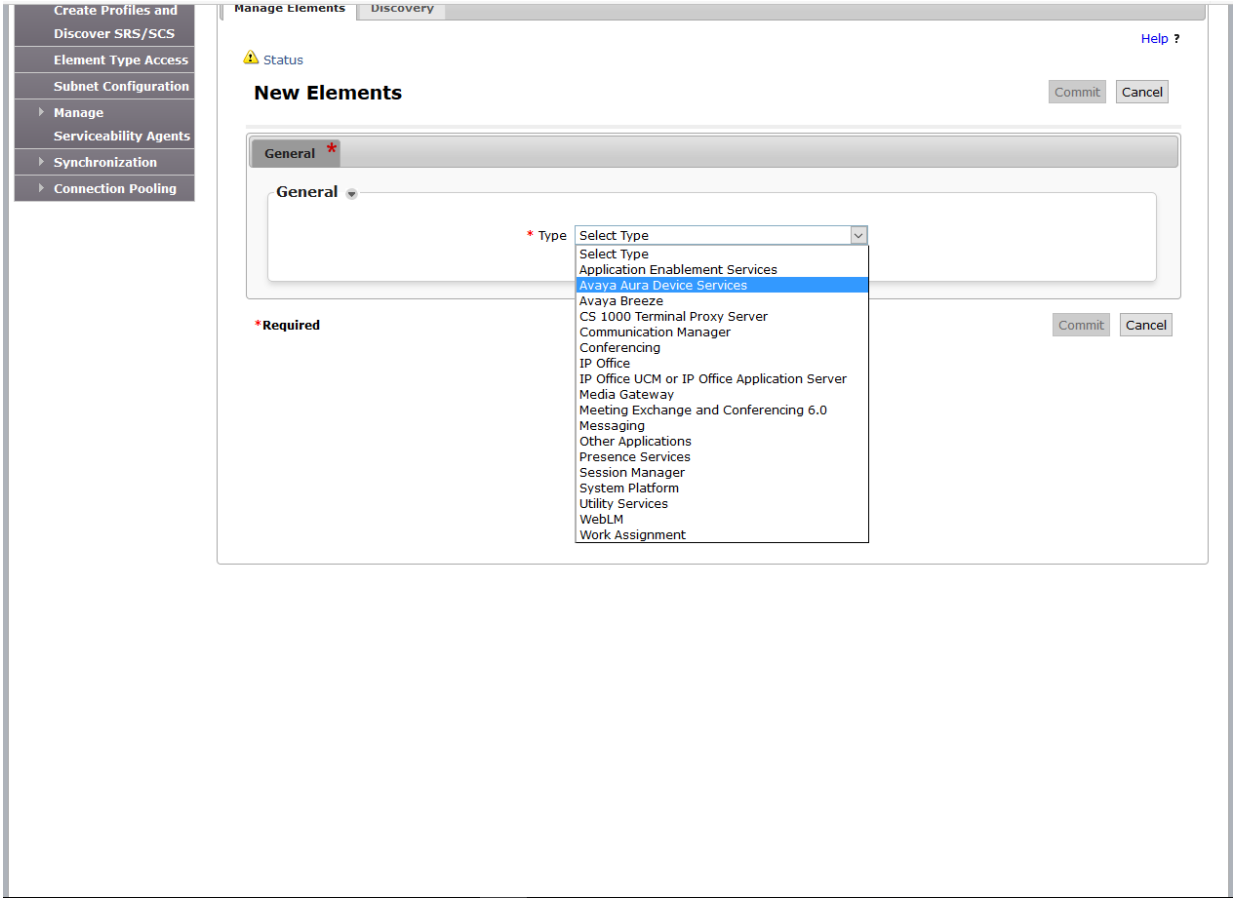


Figure 27: Select type

4. On the **General** tab, perform the following:

a. In the **Name** field, type the Name of the Avaya Aura® Device Services server

b. In the **Node** field, type the IP of the Avaya Aura® Device Services server.

c. In the **Description** field, type the description of the Avaya Aura® Device Services servers.

d. Go to the **Attributes** tab.

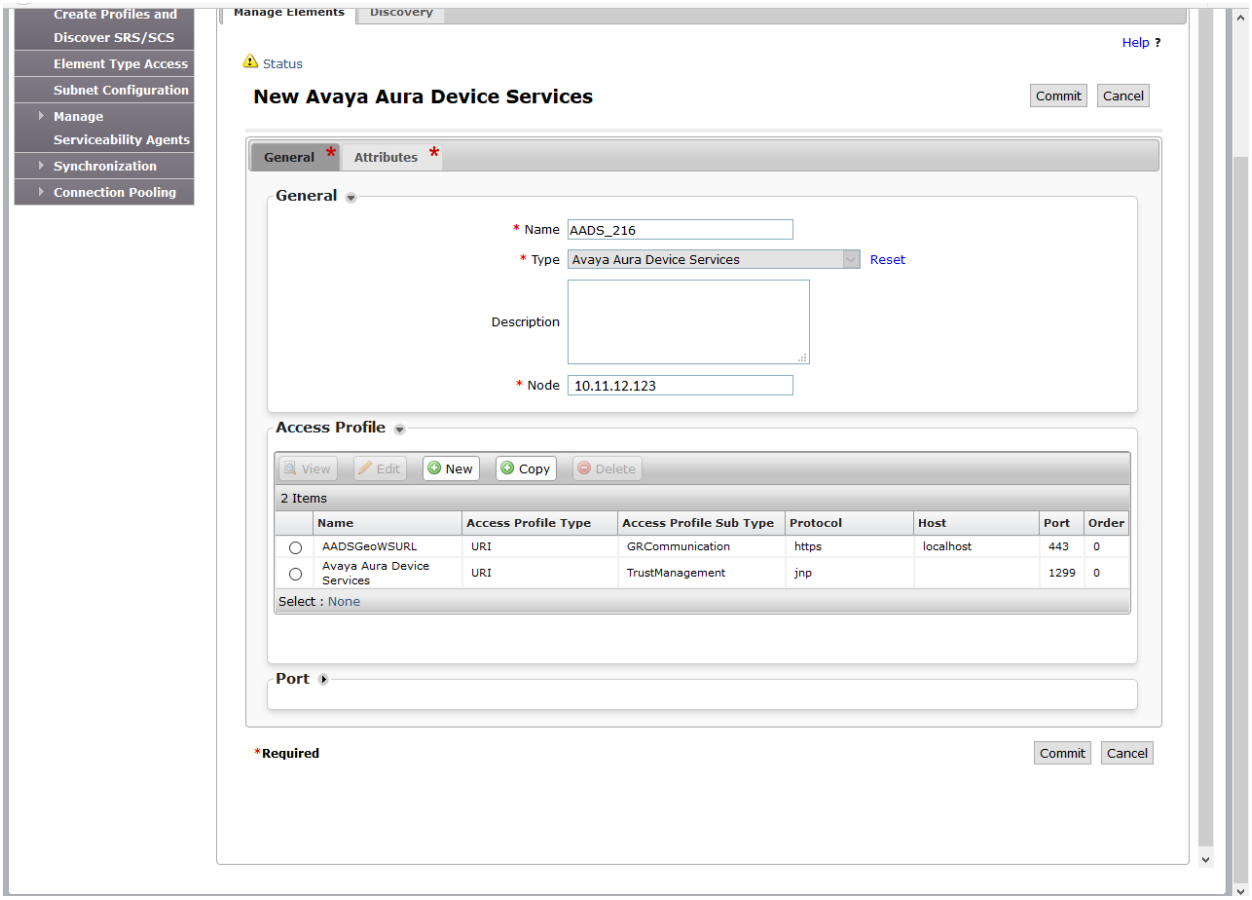


Figure 28: New Avaya Aura® Device Services

5. On the **Attributes** tab, perform the following:

a. In the **Login** field, type the admin login name to access the Avaya Aura® Device Services server This is the admin user provided during AADS OVA deployment.
b. In the **Password** field, type the admin password to access the Avaya Aura® Device Services server This is the password provided during AADS OVA deployment.
c. In the **Confirm Password** field, retype the admin password to access the Avaya Aura® Device Services server.
d. In the **Version** field, type the Avaya Aura® Device Services base version (7).
e. In the **Location** field, type the location of Avaya Aura® Device Services server. This is an optional field.
f. Go back to the **General** tab.

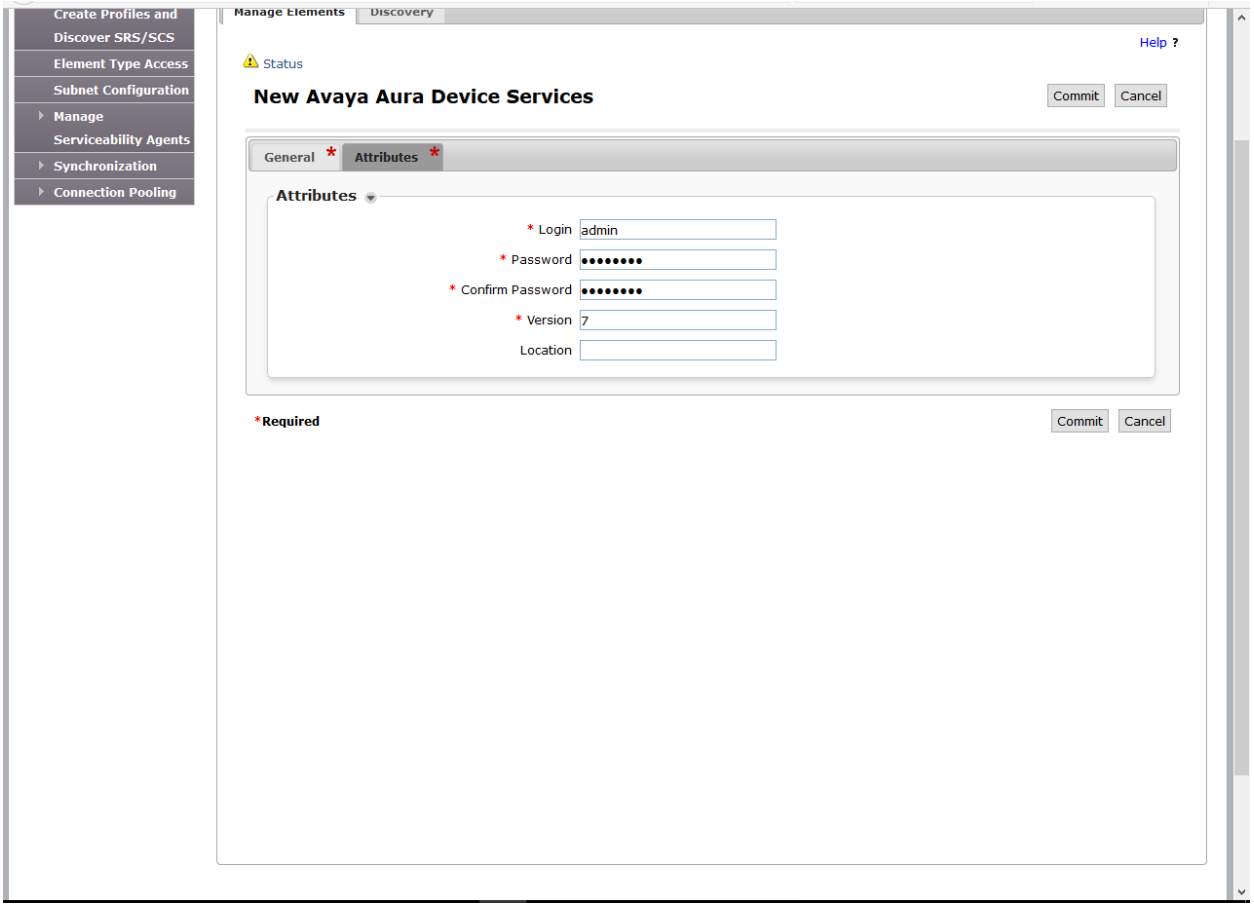


Figure 29: New Avaya Aura® Device Services

6. Select the **TrustManagement** access profile, and click **Edit**.

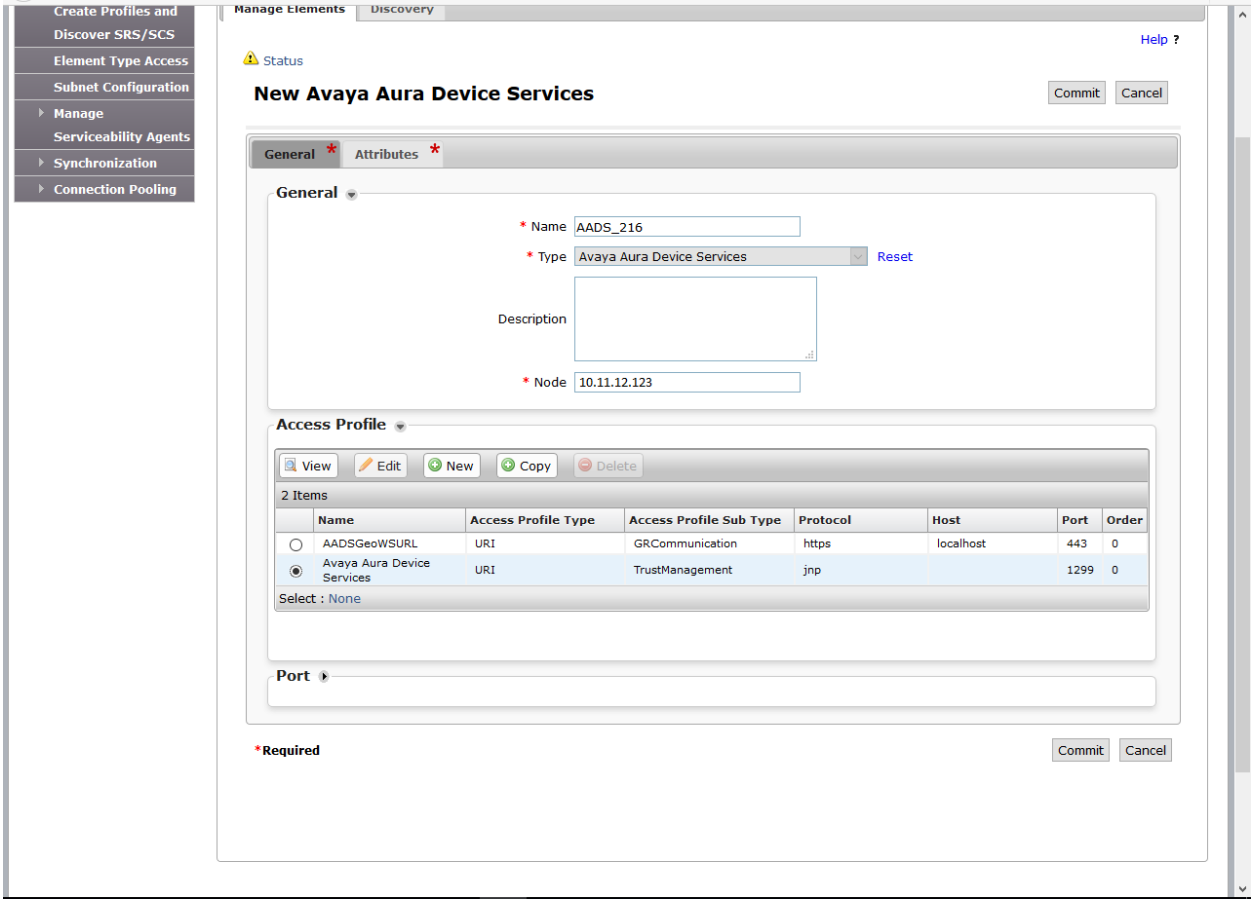


Figure 30: TrustManagement access profile

7. Leave the **Container type** field blank.
8. In the **Host** field, type the hostname of the Avaya Aura® Device Services server. Click **Save**.

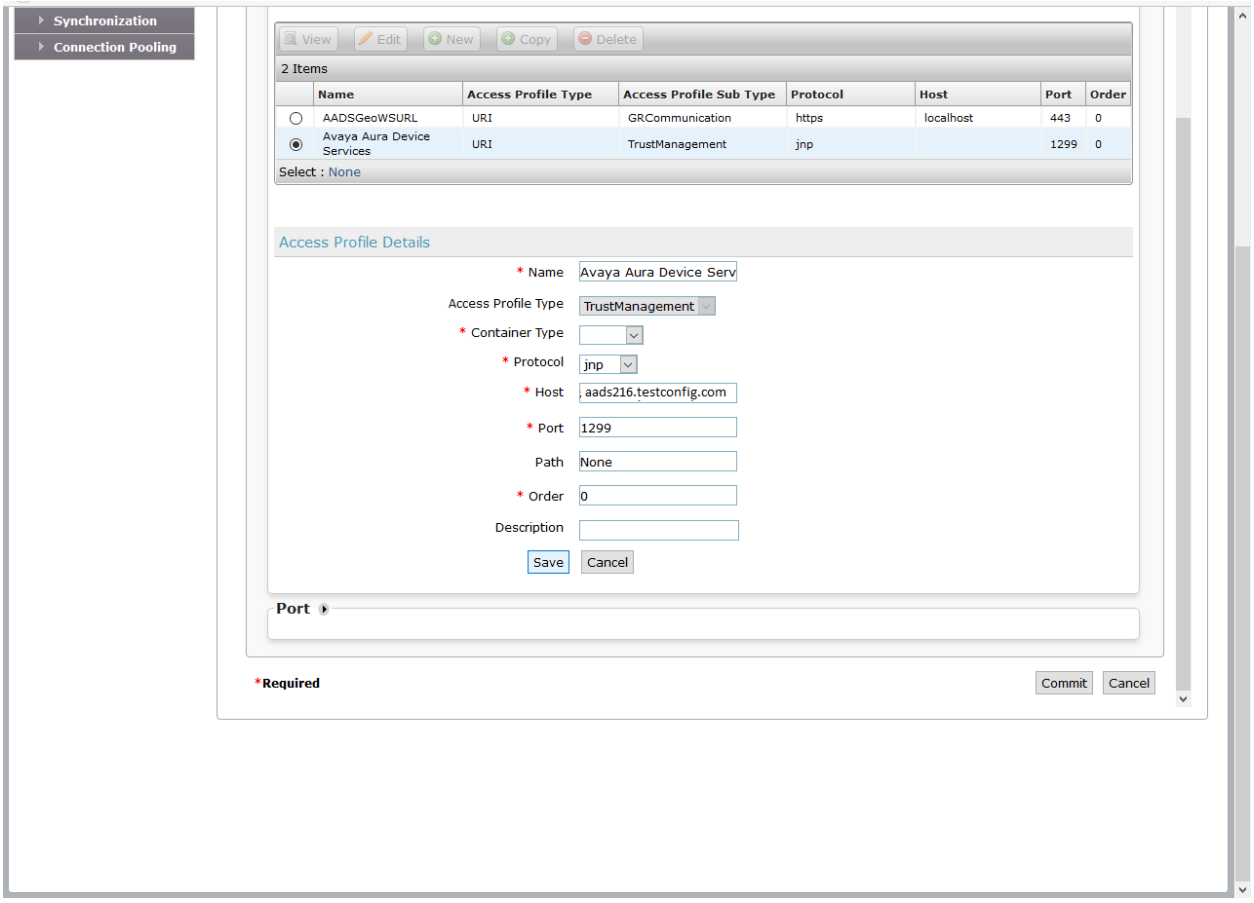


Figure 31: Access Profile Details

9. To enable SSO login, you must add an access profile of type EMURL. To add an EMURL access profile, on the **General** tab, in the Access Profile section, perform the following:

a. Click **New.**
b. In the **Access Profile Type** field, click **EMURL.**
c. In the **Host** field, type the Avaya Aura® Device Services server **FQDN**.
d. In the **Port** field, type **8445**.
e. In the **Path** field, type **/admin**.

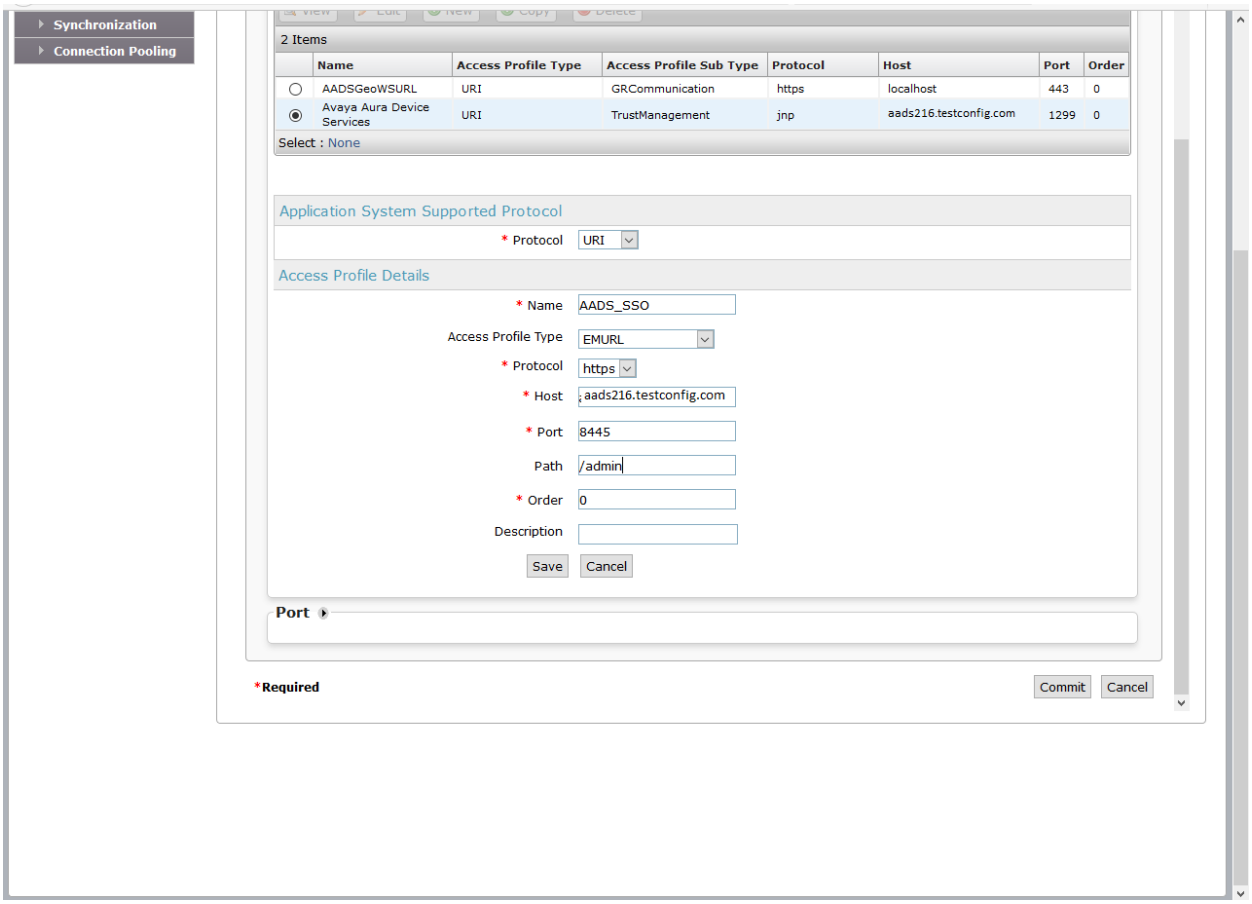


Figure 32: Access Profile Details

10. Click **Commit.**

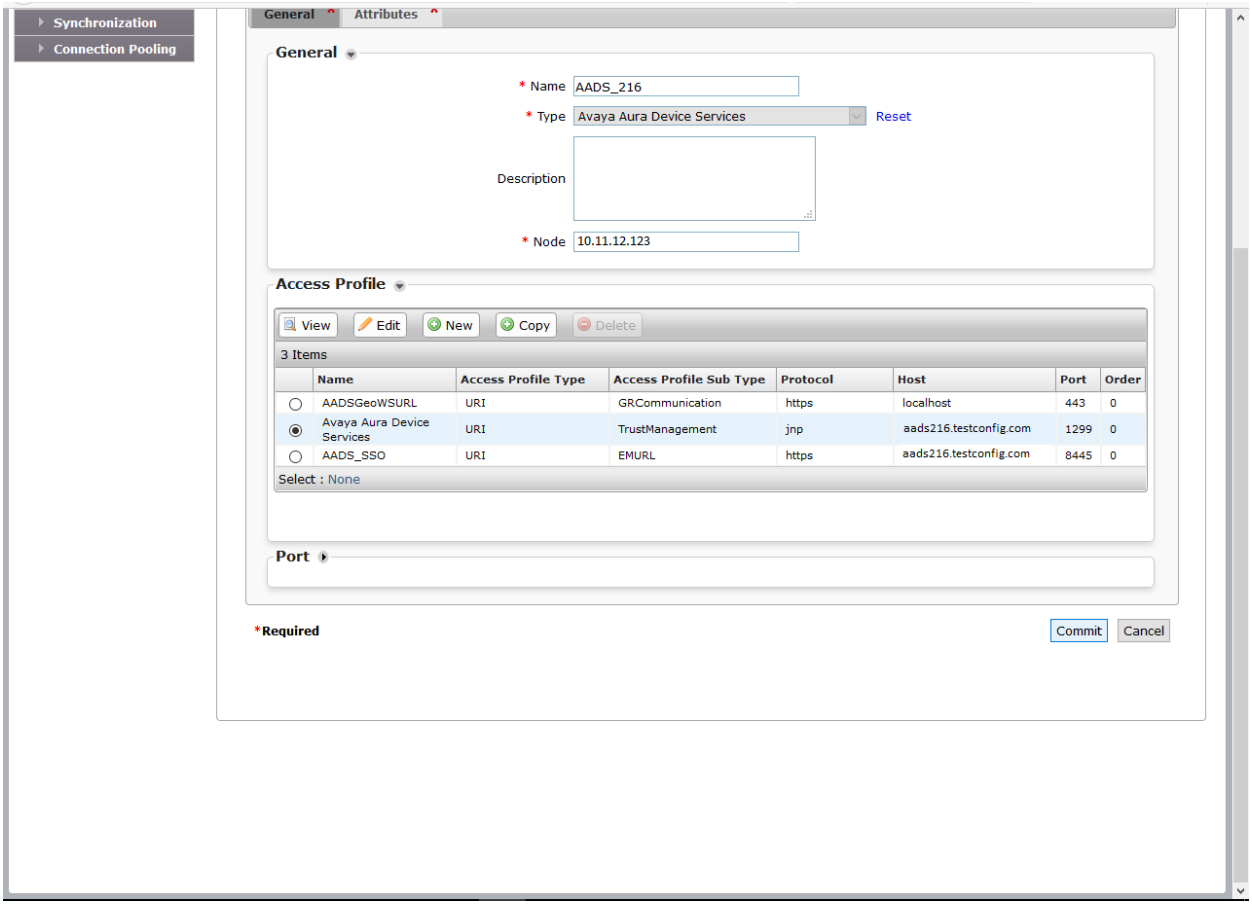


Figure 33: Access Profile Details

11. The **Avaya Aura Device Services** instance is added to **System Manager** Inventory.

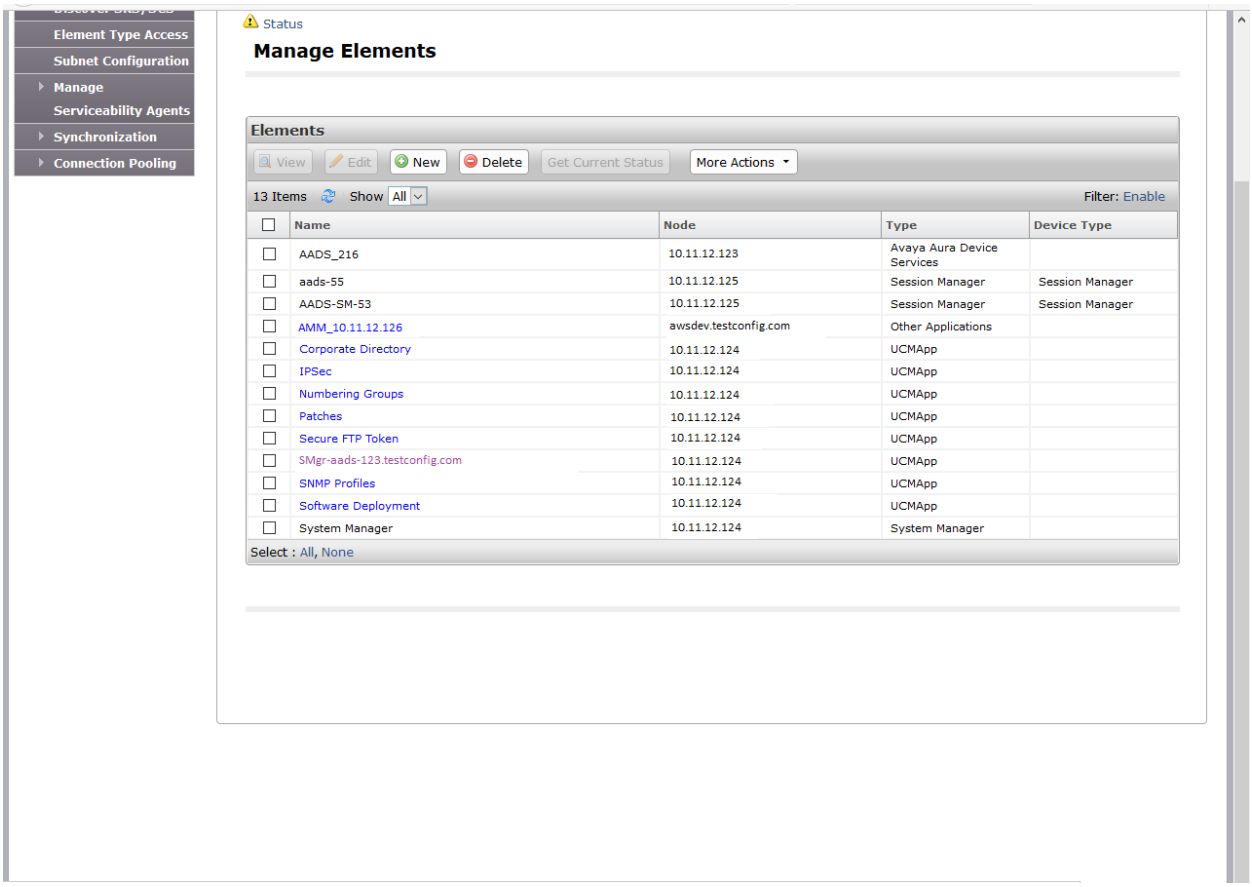


Figure 34: Manage Elements

Pairing Session Manager with an Avaya Aura® Device Services node

1. On the home page of the System Manager Web console, in **Elements**, click **Session Manager -> Session Manager Administration**

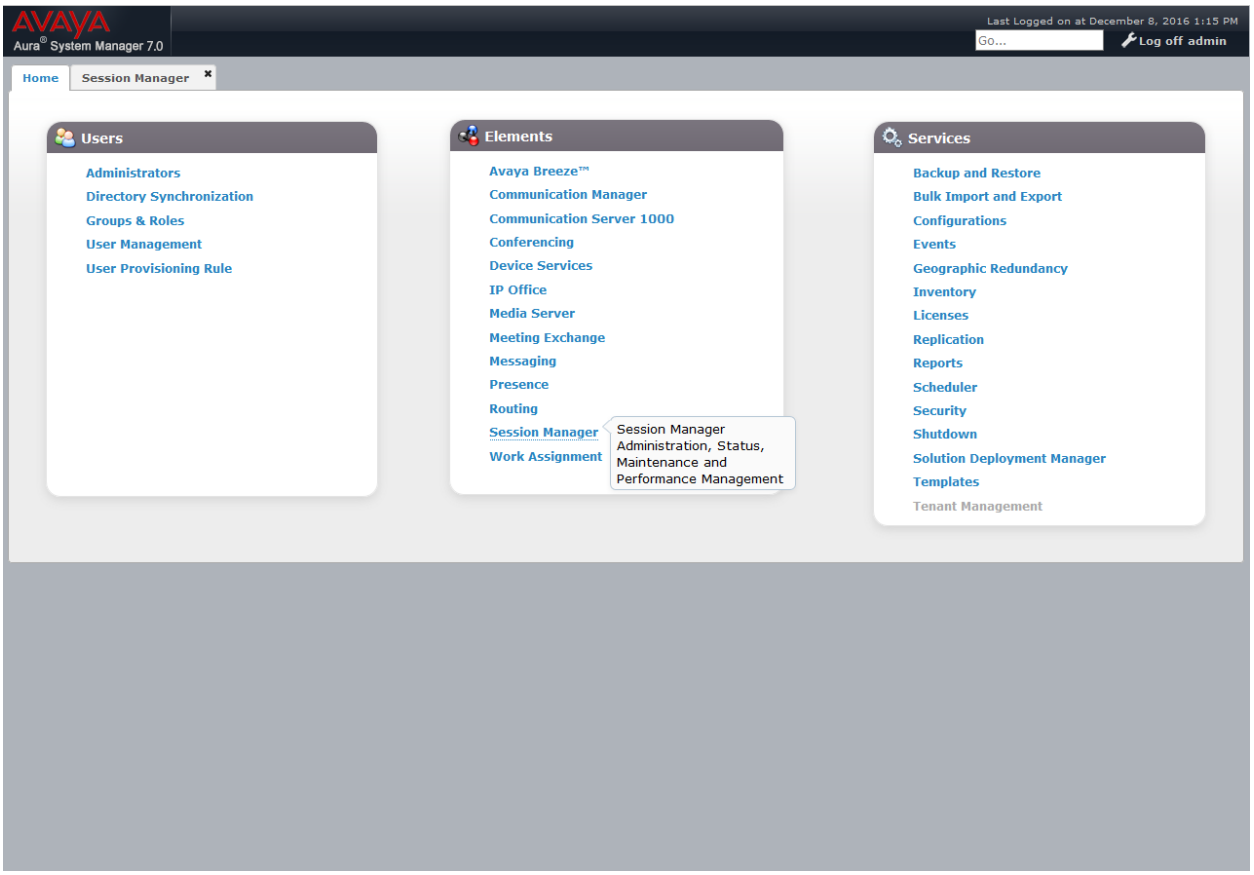


Figure 35: Session Manager Administration

2. On the Session Manager Administration page, click the **Session Manager Instances** tab. In the Session Manager Instances section, select a Session Manager instance, and click **Edit.** The system displays the Edit Session Manager page.

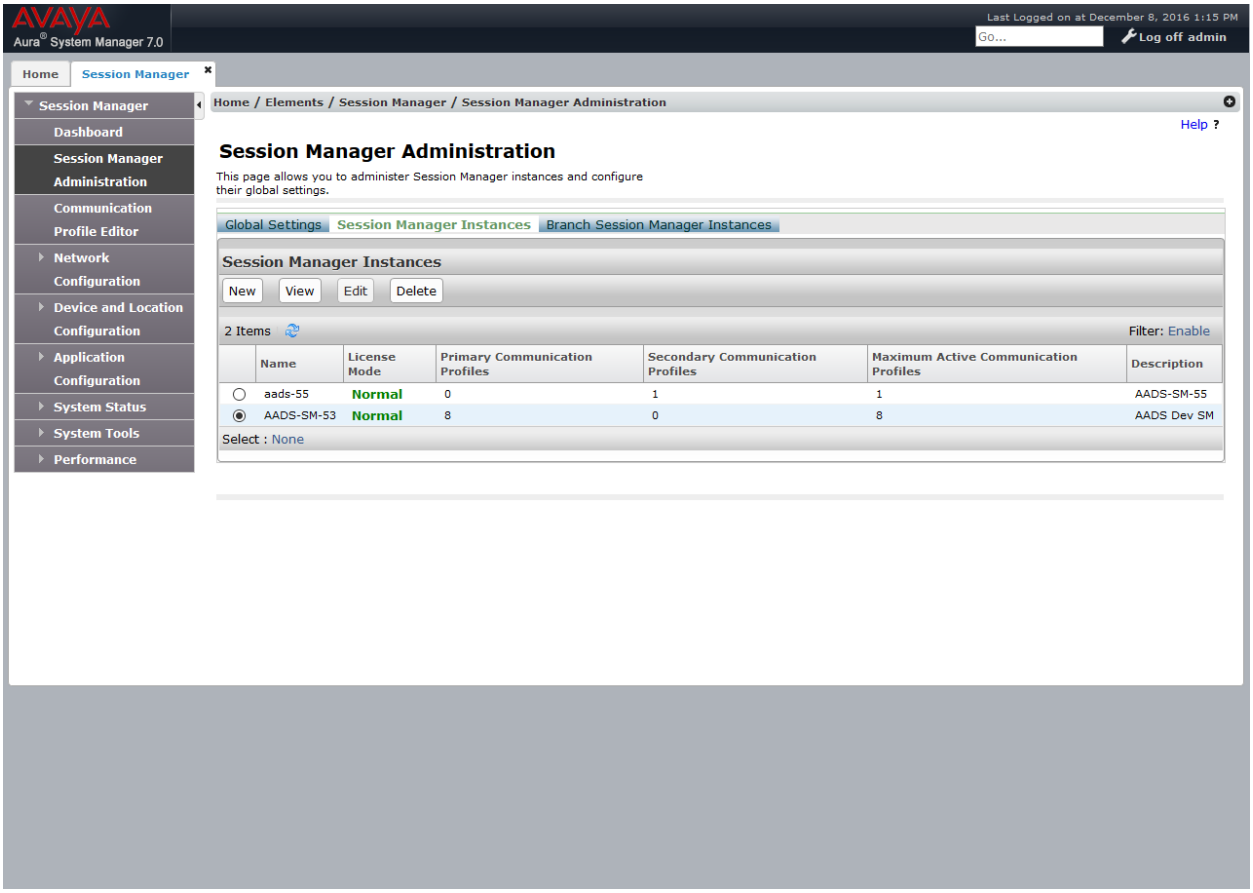


Figure 36: Session Manager Instances

3. From **Data Center** select a data center **if one is not already assigned.** If you do not assign the Session Manager instance to a data center, the system displays the following message: Session Manager must be assigned to a Data Center to pair with an Avaya Aura® Device Services Server.

4. From **Avaya Aura Device Services Pairing** field, select an Avaya Aura® Device Services server to pair with Session Manager.

5. Click **Commit.**

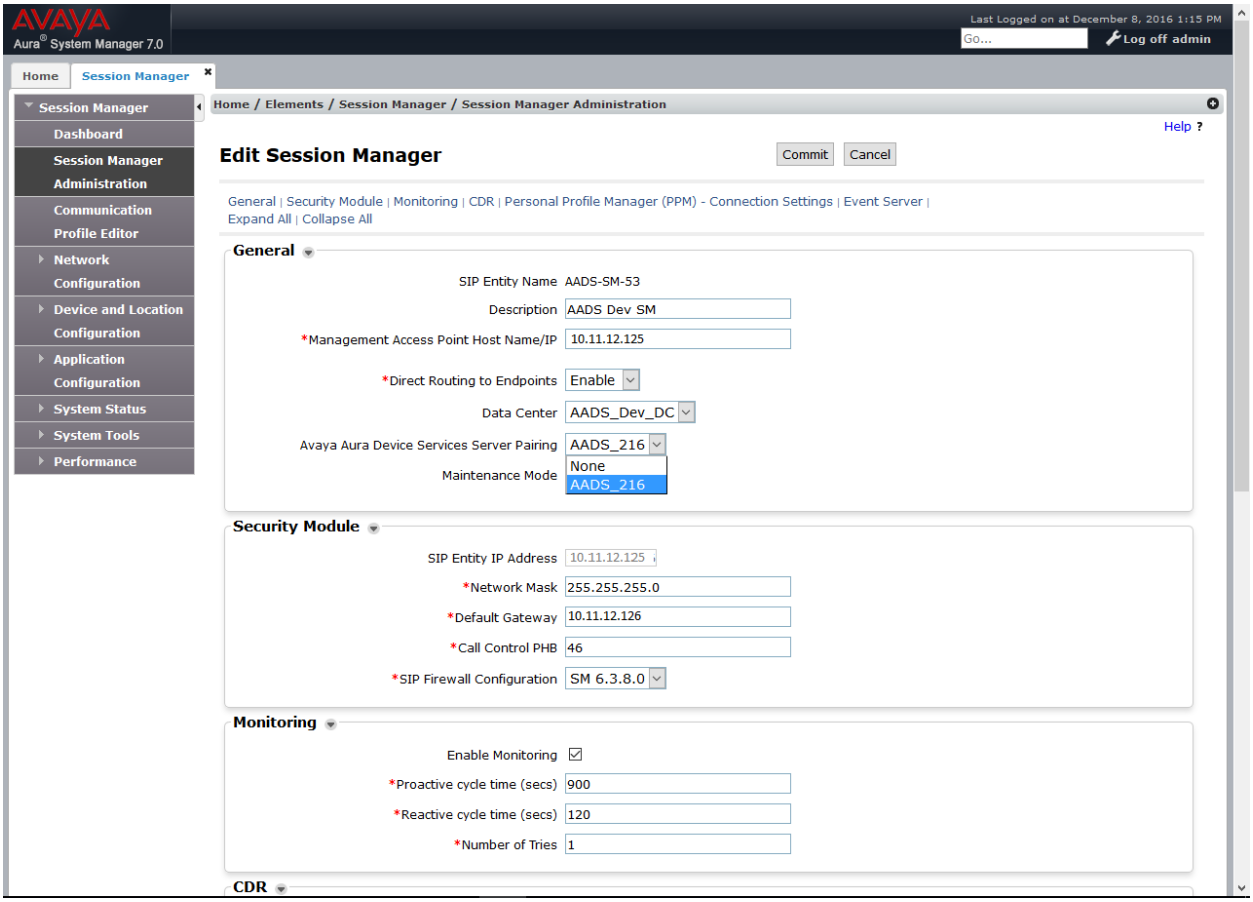


Figure 37: Avaya Aura® Device Services Pairing

Installation of Avaya Aura® Device Services (Standalone)

Pre-installation check

1. In System Manager Web Console -> Session Manager - > Dashboard and check the Session Manager status. Ensure all the Session Managers in the cluster are up and running.

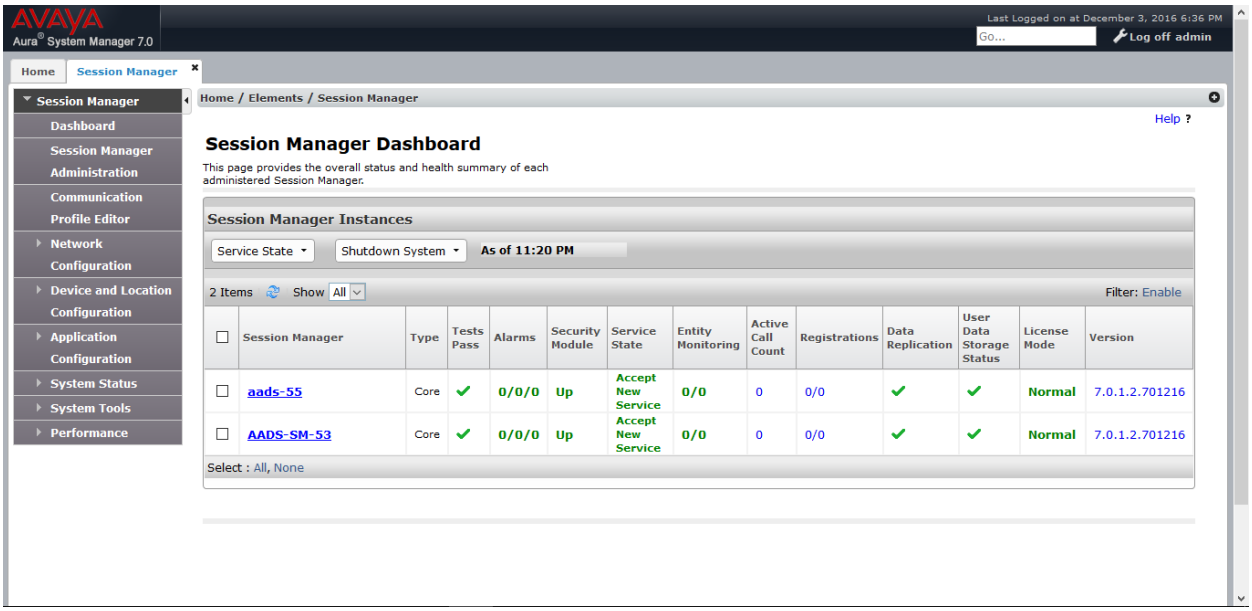


Figure 38: Session Manager Dashboard

Additionally, we can also login to Session Manager nodes using putty and execute below command to check the service status.

```
[craft@aads-sm-53 ~]$ statapp
Watchdog          9/  9 UP
logevent         13/ 13 UP
ncsd              4/  4 UP
postgres-db      31/ 31 UP
mgmt            215/215 UP
WebSphere       220/220 UP
CDRService       16/ 16 UP
cassandra       122/122 UP
sal-agent        47/ 47 UP
secmod            4/  4 UP
```

Start Avaya Aura® Device Services installation

1. Go to the Avaya directory by typing cd /opt/Avaya
2. Run the command **app install**
3. The system launches a blue installation tool.
4. Steps to be performed in the blue configuration tool:
    a. Select the **Cluster Configuration** menu and ensure that the **Initial cluster node** option is set to y (yes). To return to the previous menu, select **Return to Main Menu** and press **Enter**.

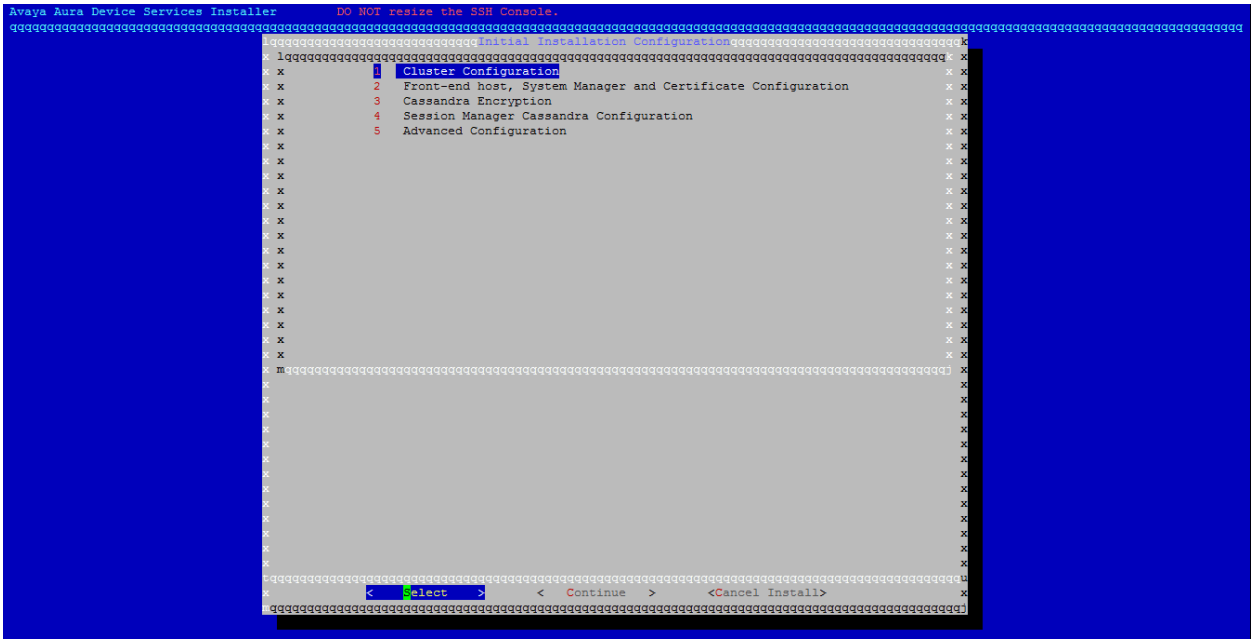


Figure 39: Cluster Configuration

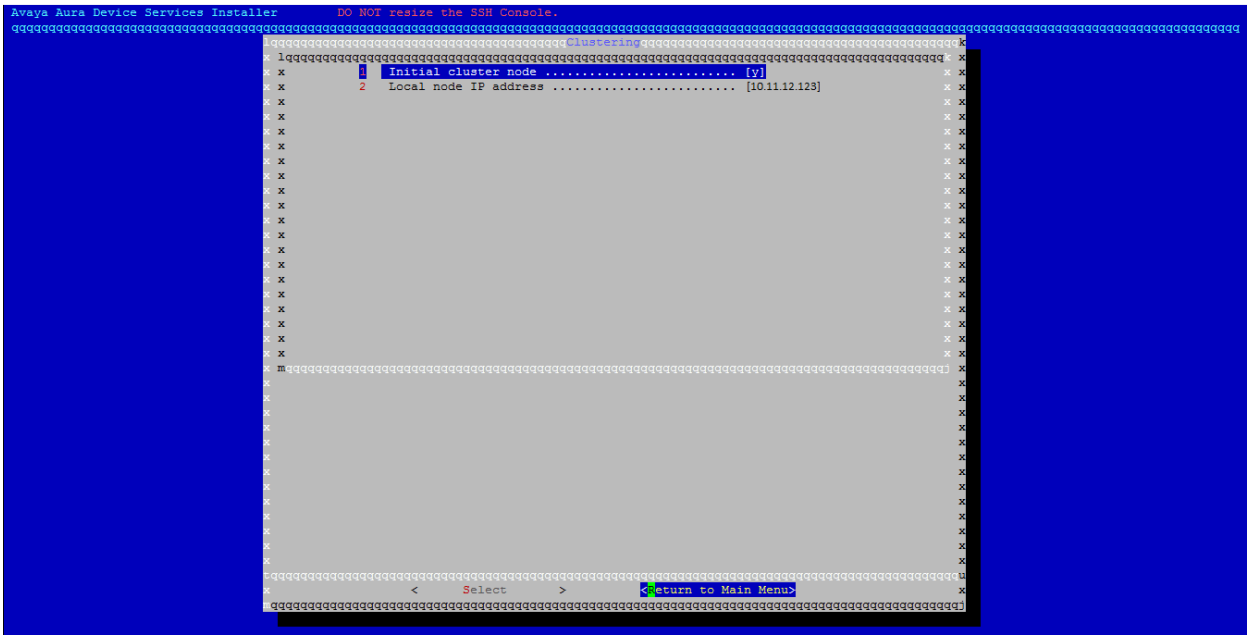


Figure 40: Initial Cluster Node

b. Select the Front-end host, System Manager and Certificate Configuration menu and configure the settings that are accessible from the menu.

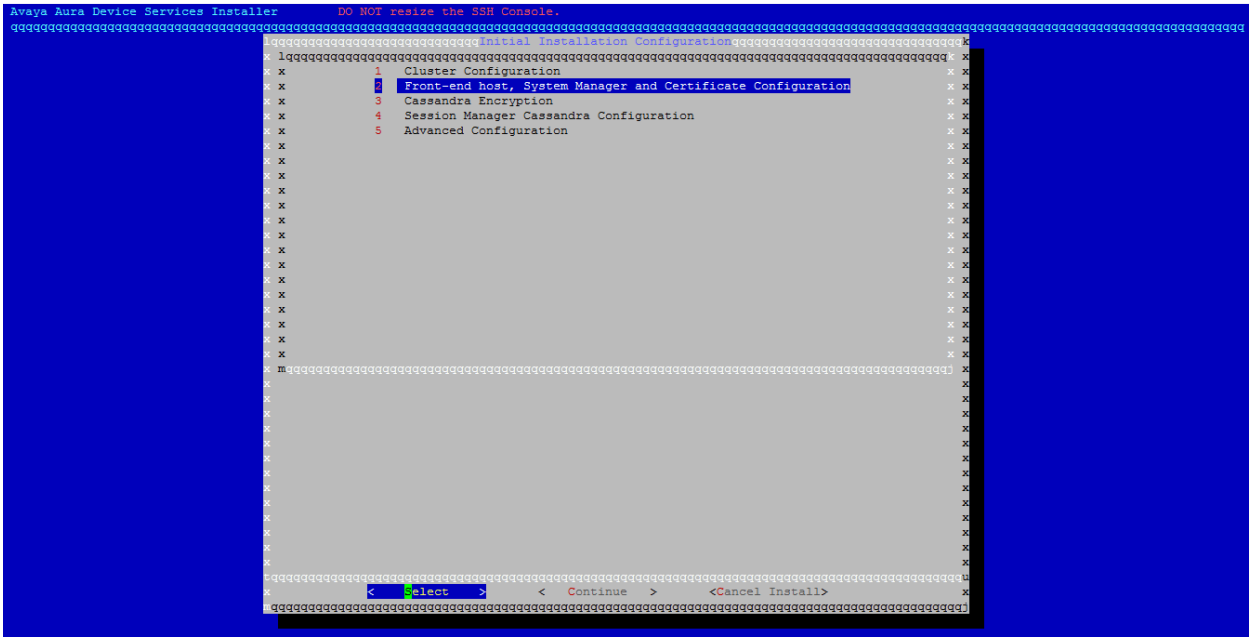


Figure 41: Initial Installation Configuration

c. Type **Front-end FQDN**– If you need to extend the system to an AADS cluster; it is advised to use the hostname corresponding to the virtual IP.

d. If you plan to have a standalone AADS, this field will be same as the Local frontend host.

e. Type the **System Manager** details. Keystore password must be 6 or more characters. This must be same on all nodes in cluster.

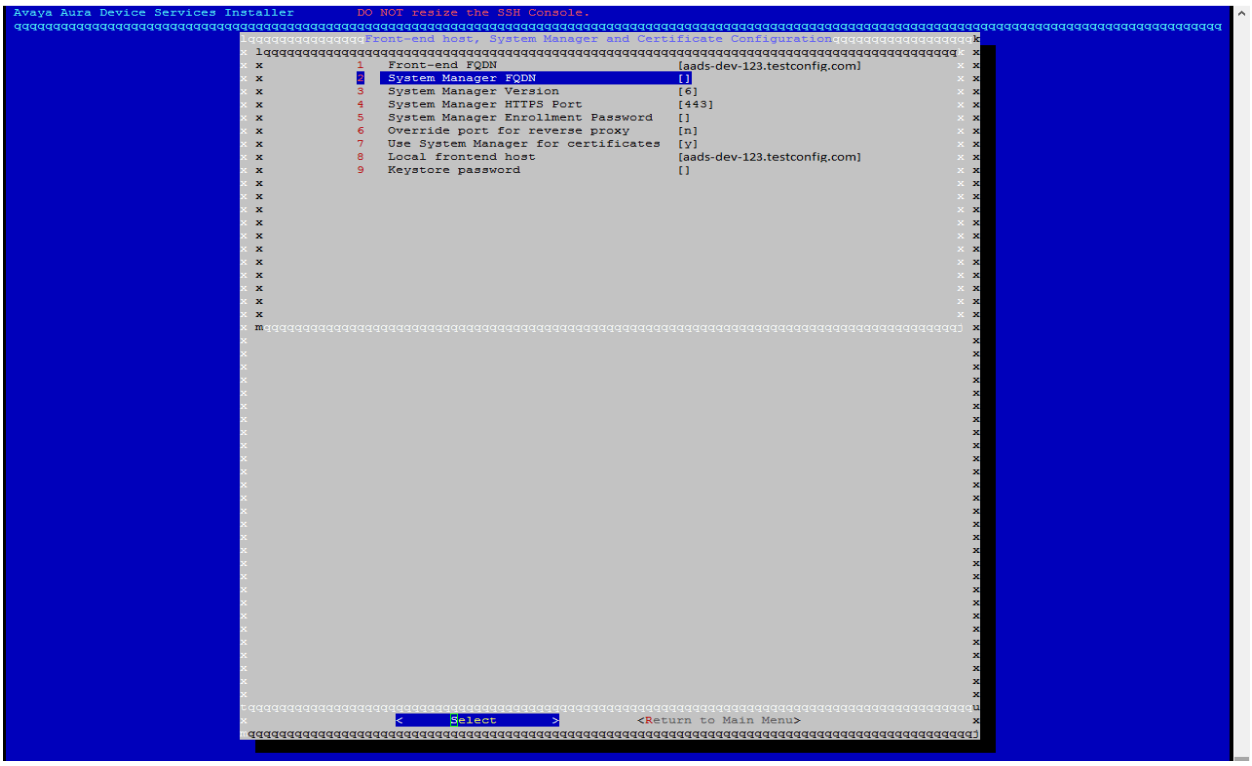


Figure 42: System Manager FQDN

Enter SMGR FQDN and press **OK**. The installer will try to check if the provided hostname is valid or not.

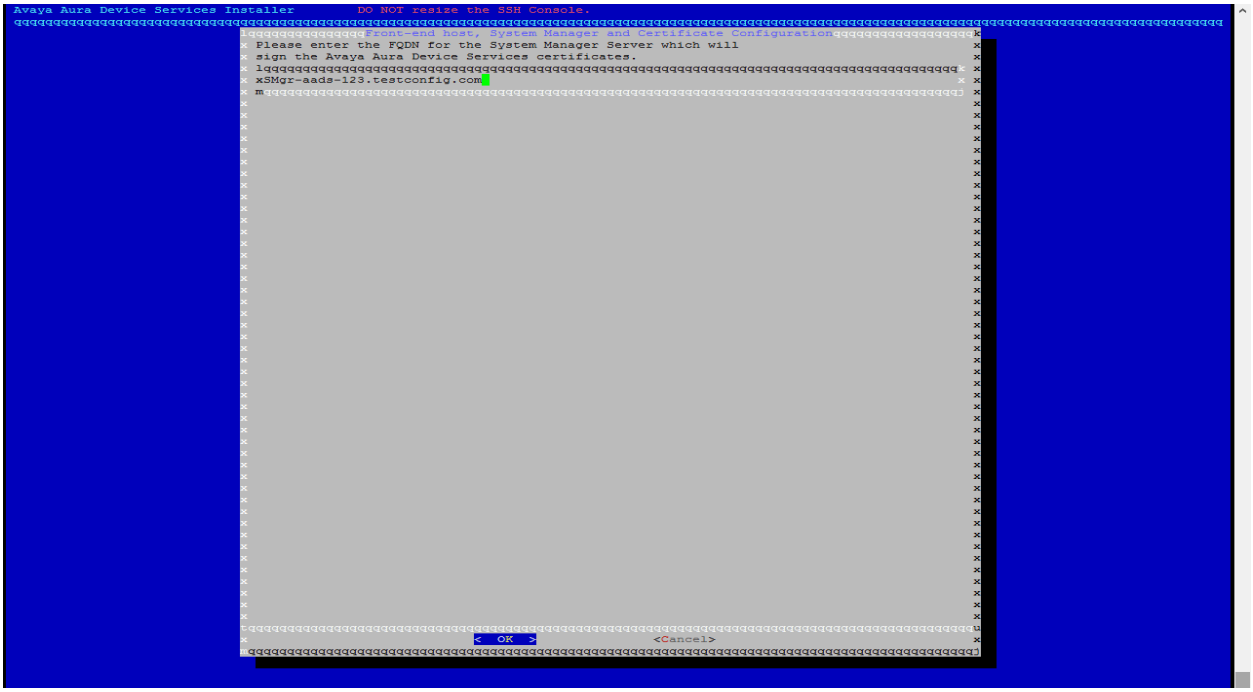


Figure 43: System Manager FQDN

Press **<OK>.**

Figure 44: SMGR Connectivity check

f. After entering all the details **Return to Main Menu**.

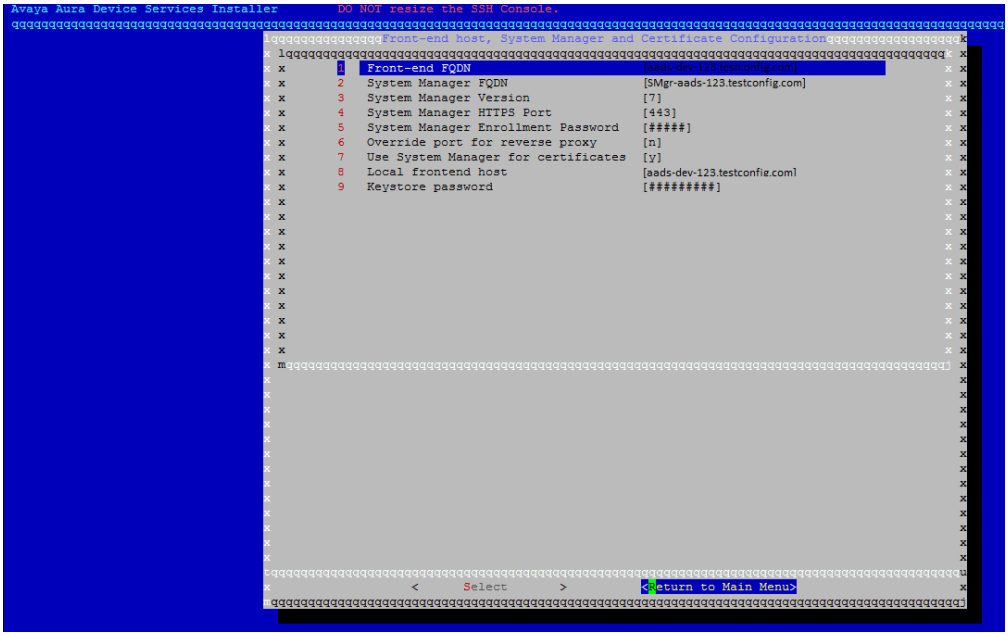


Figure 45: Front-end host, System Manager and Certificate Configuration

Note:

At this point if System Manager is not being used for certificate, follow the procedure given here Configuring Certificates without System Manager.

g. Session Manager Cassandra Configuration – Type the Session Manager Management and Asset IP.

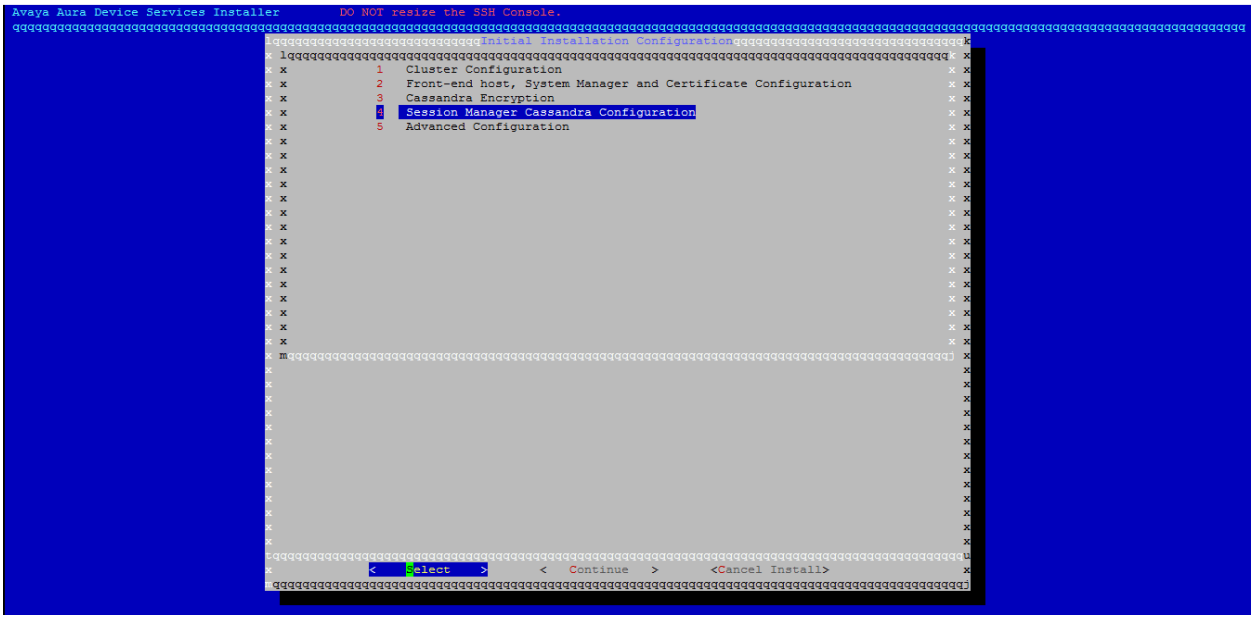


Figure 46: Initial Installation Configuration

h. Leave Cassandra Encryption and Advanced Configuration unchanged. Press **Continue**.

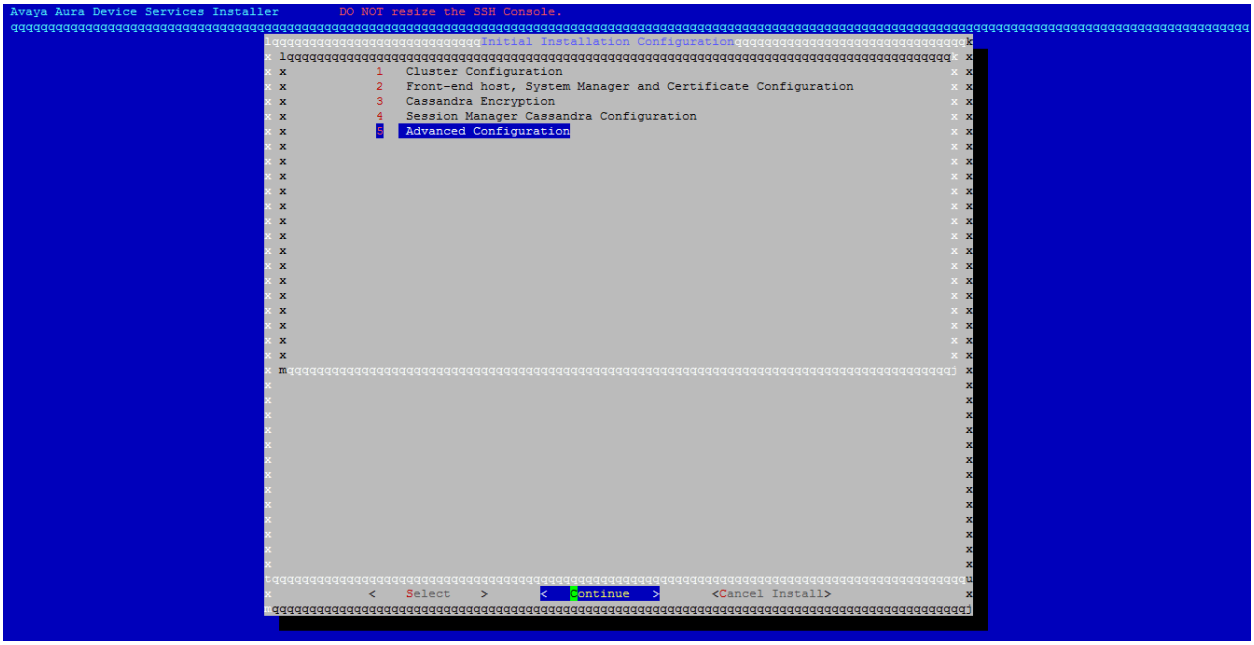


Figure 47: Advanced Configuration

i. The installer performs pre-install checks. Press **Continue**.

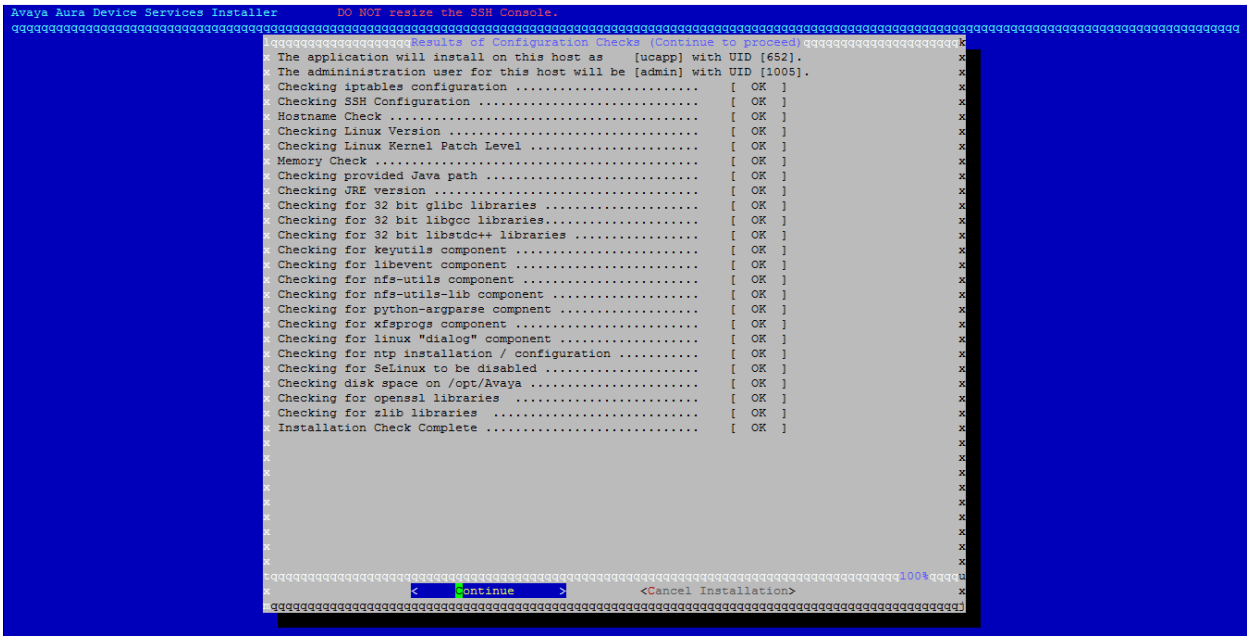


Figure 48: Results of Configuration Checks

j. Read the End User License Agreement. Press **Accept** to accept the EULA.

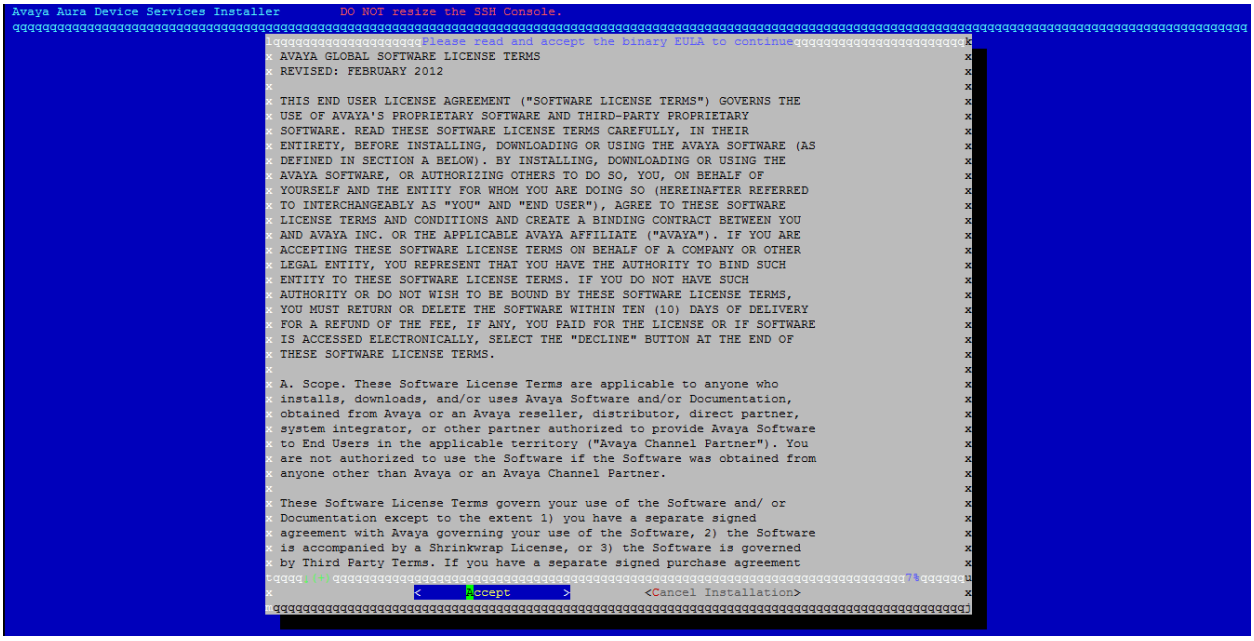


Figure 49: End User License Agreement

k. The system configures the other settings such as required RPMs, download certificates from System Manager, creates database schema, and does the required initial configuration required for the Avaya Aura® Device Services server installation. Select **Continue** to finish the installation.

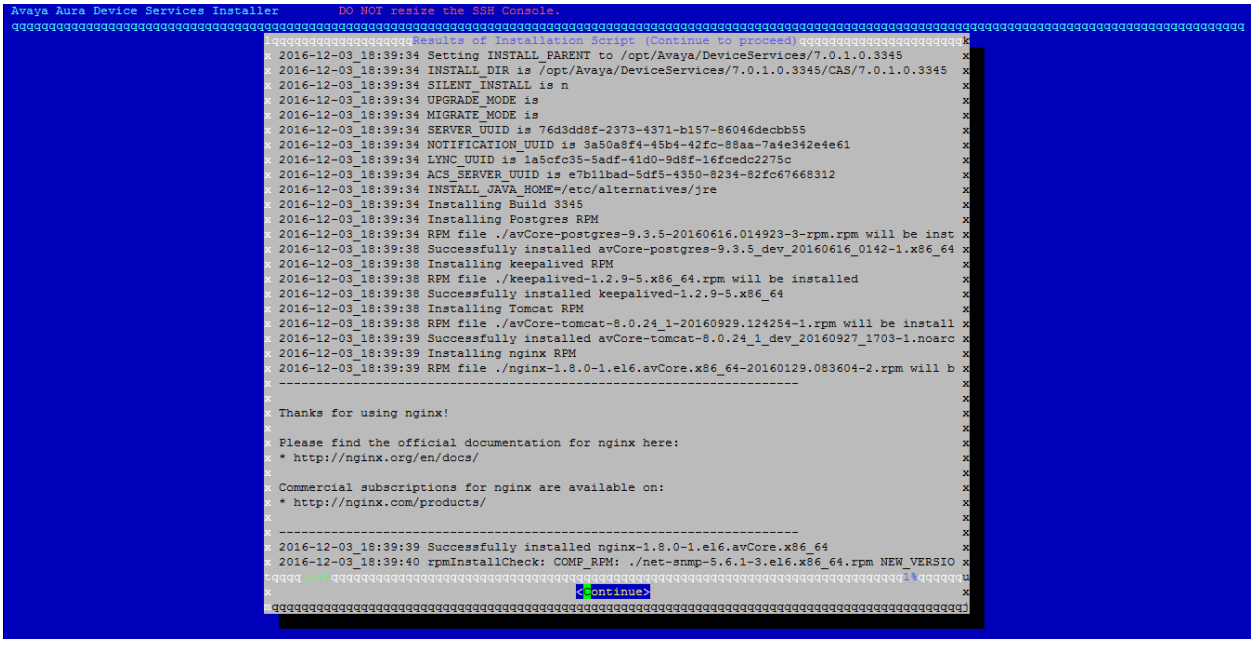


Figure 50: AADS server installation

l. Select LDAP Configuration

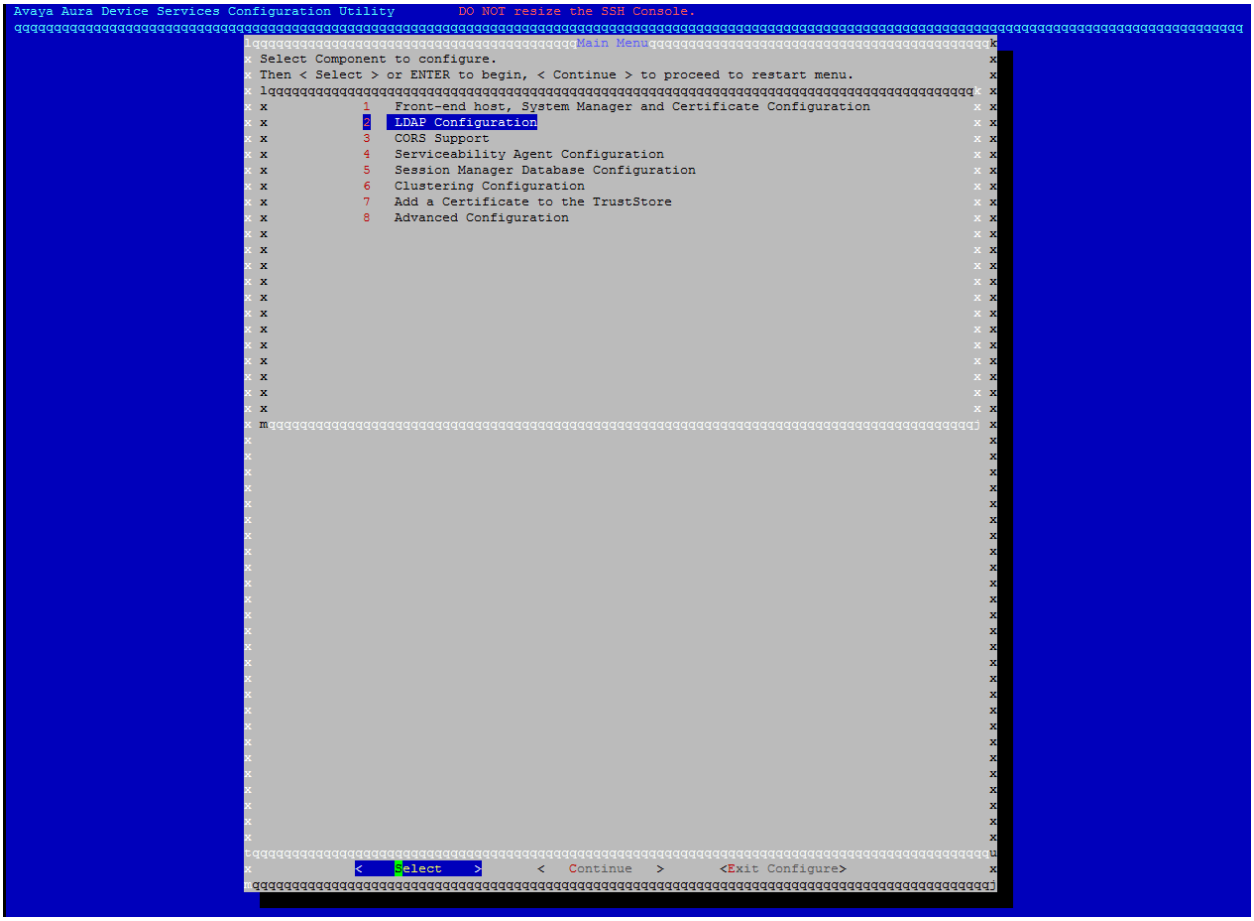


Figure 51: LDAP configuration

1. On the LDAP configuration page type values for each parameter manually.

Note:

Do not cut/copy paste values in these fields, it might introduce some invalid characters such as spaces in between.

2. After entering the values for each field manually navigate to **Advanced LDAP parameters** and click **Select**.

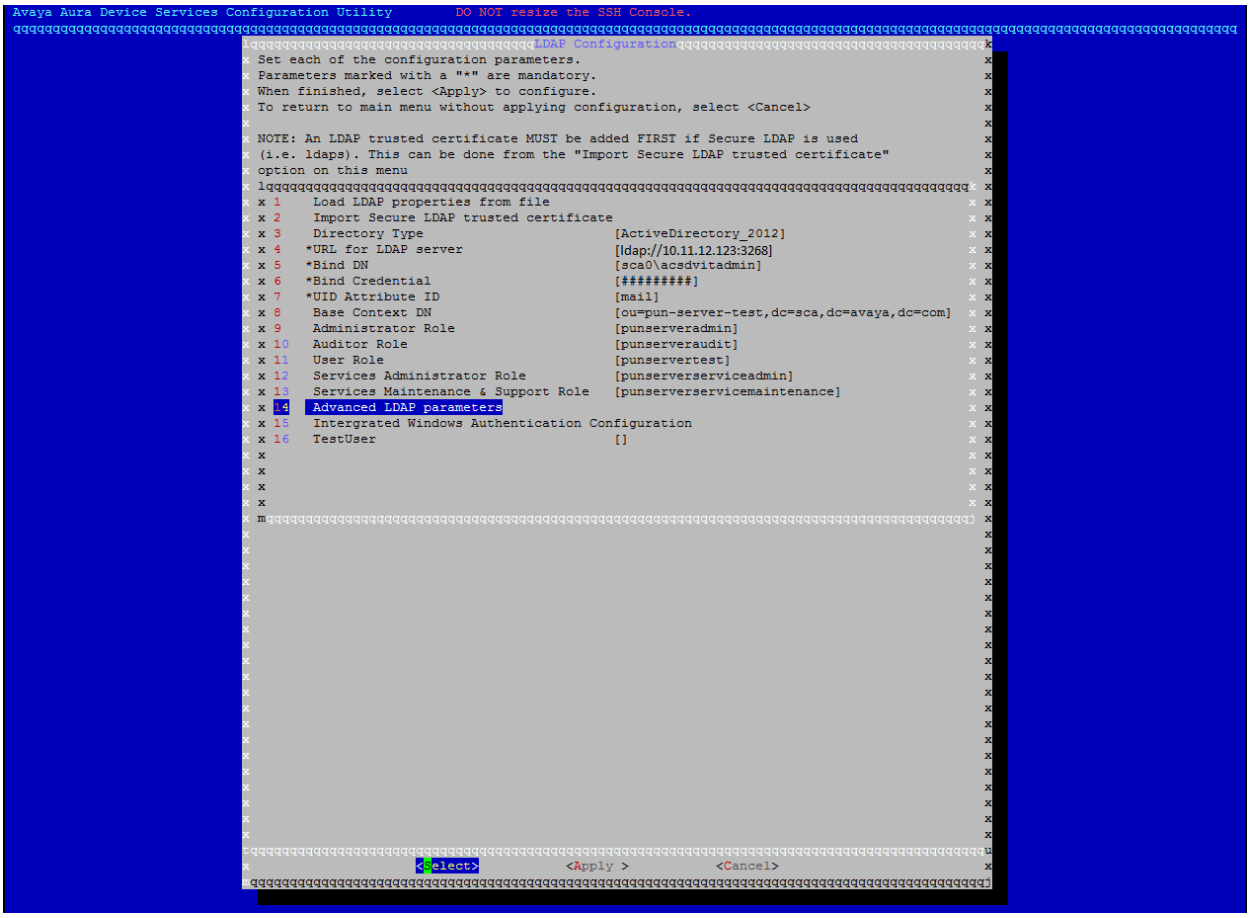


Figure 52: Advanced LDAP configuration

3. In the **Advanced LDAP parameter** screen, verify the default values for the parameters and update if required. Select **Return to previous menu** and press **Enter**.

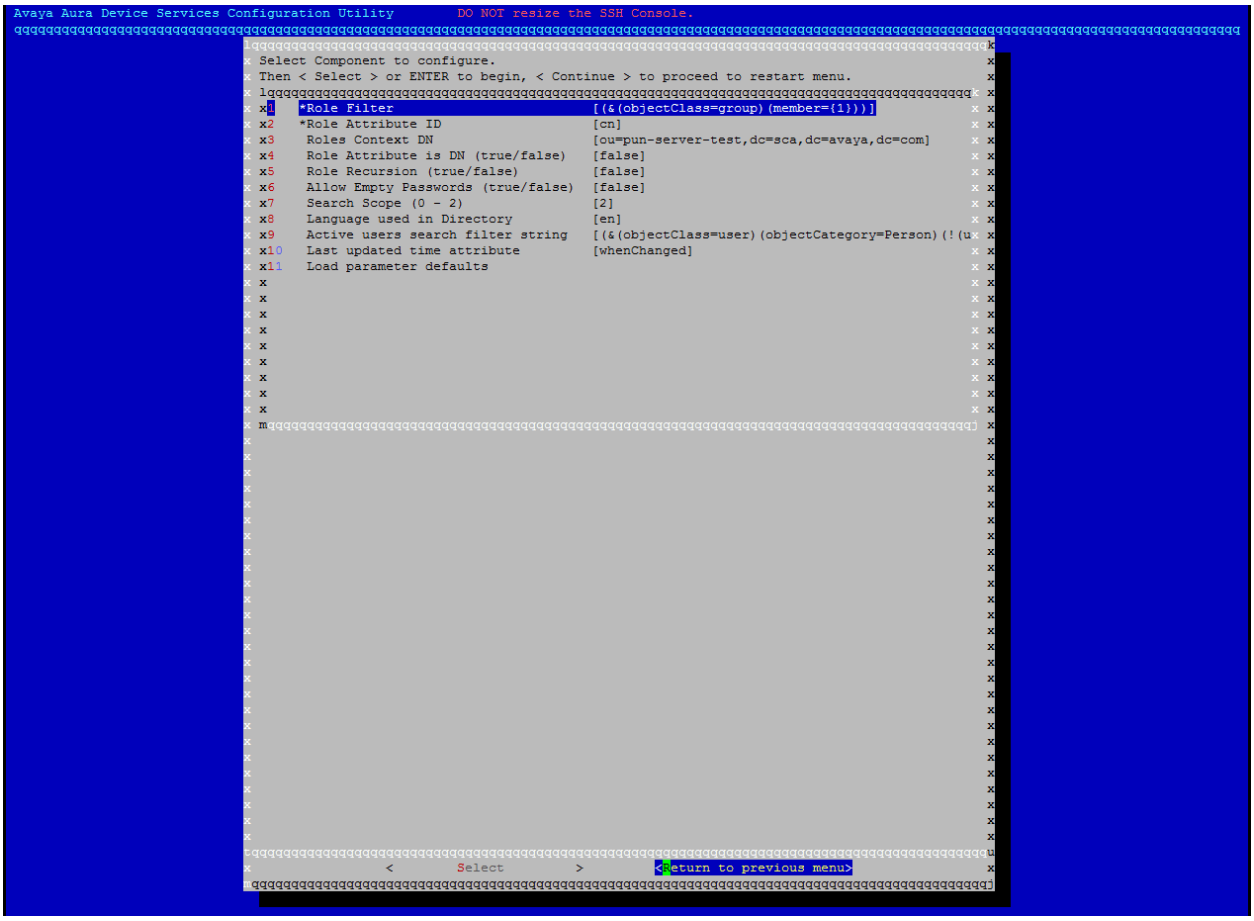


Figure 53: Advanced LDAP configuration

4. Navigate to **TestUser** field and click **Select**.

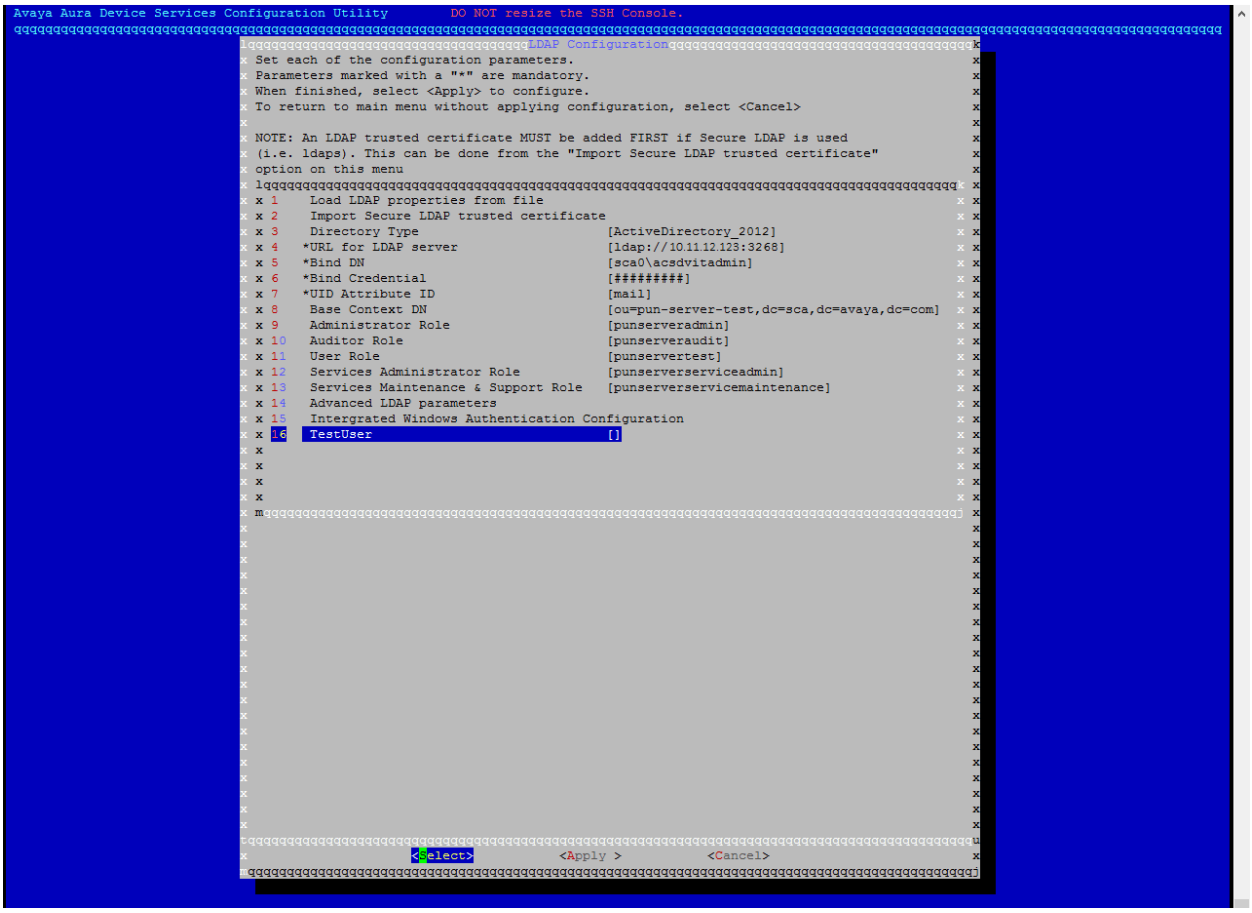


Figure 54: TestUser Selection

5. Add a LDAP test user. This will allow better validation of the LDAP parameters provided.
6. The **TestUser** must be a valid user on LDAP and should be present in the provided **Base Context DN.** The LDAP user should correspond to the **UID Attribute ID** provided.

   For example: If UID Attribute ID is sAMAccountName, in the TestUser field enter the sAMAccountName of the user
7. After typing the value, click **OK**.

Note:

TestUser may be left blank, in that case enhanced validation for LDAP parameters will not be performed.

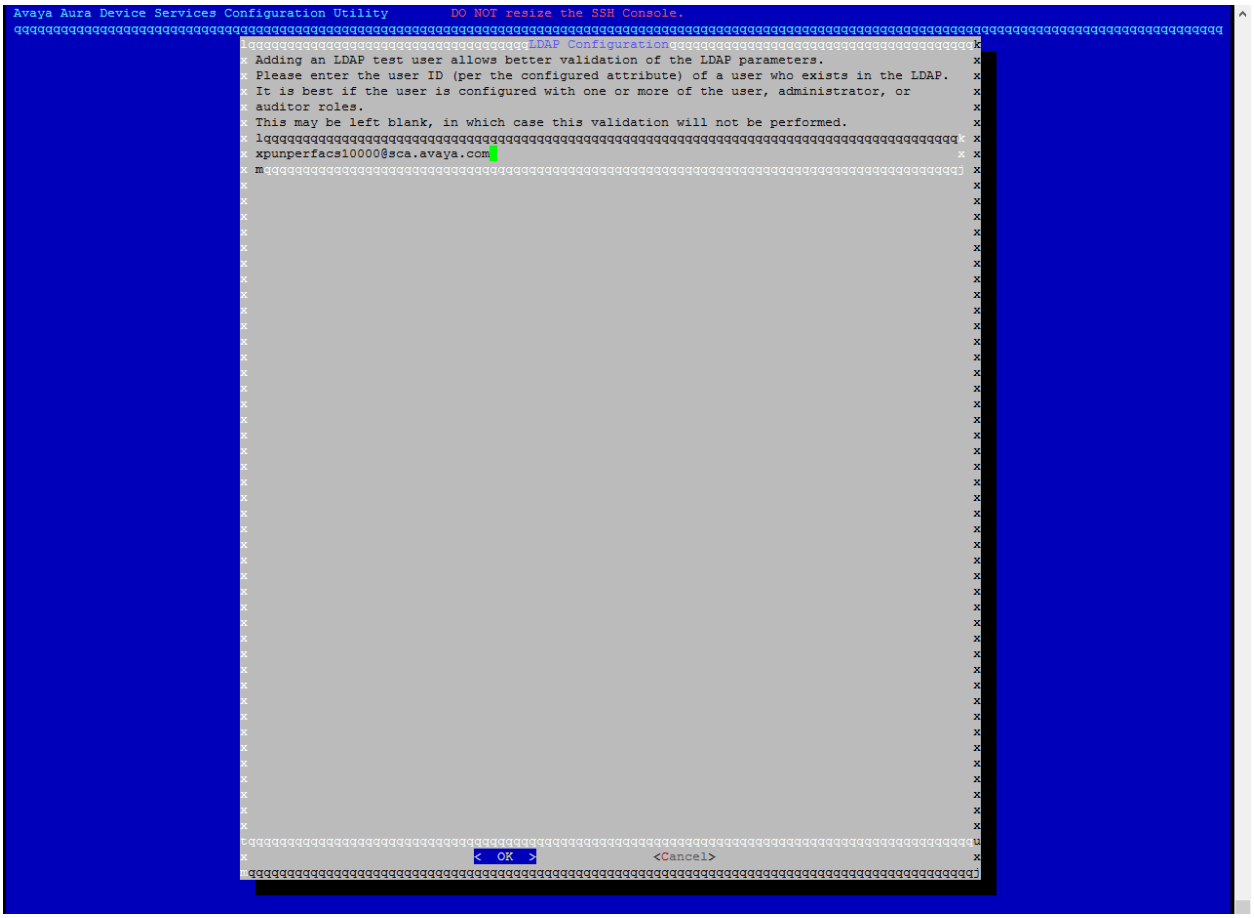


Figure 55: LDAP TestUser

8. Click **Apply**.

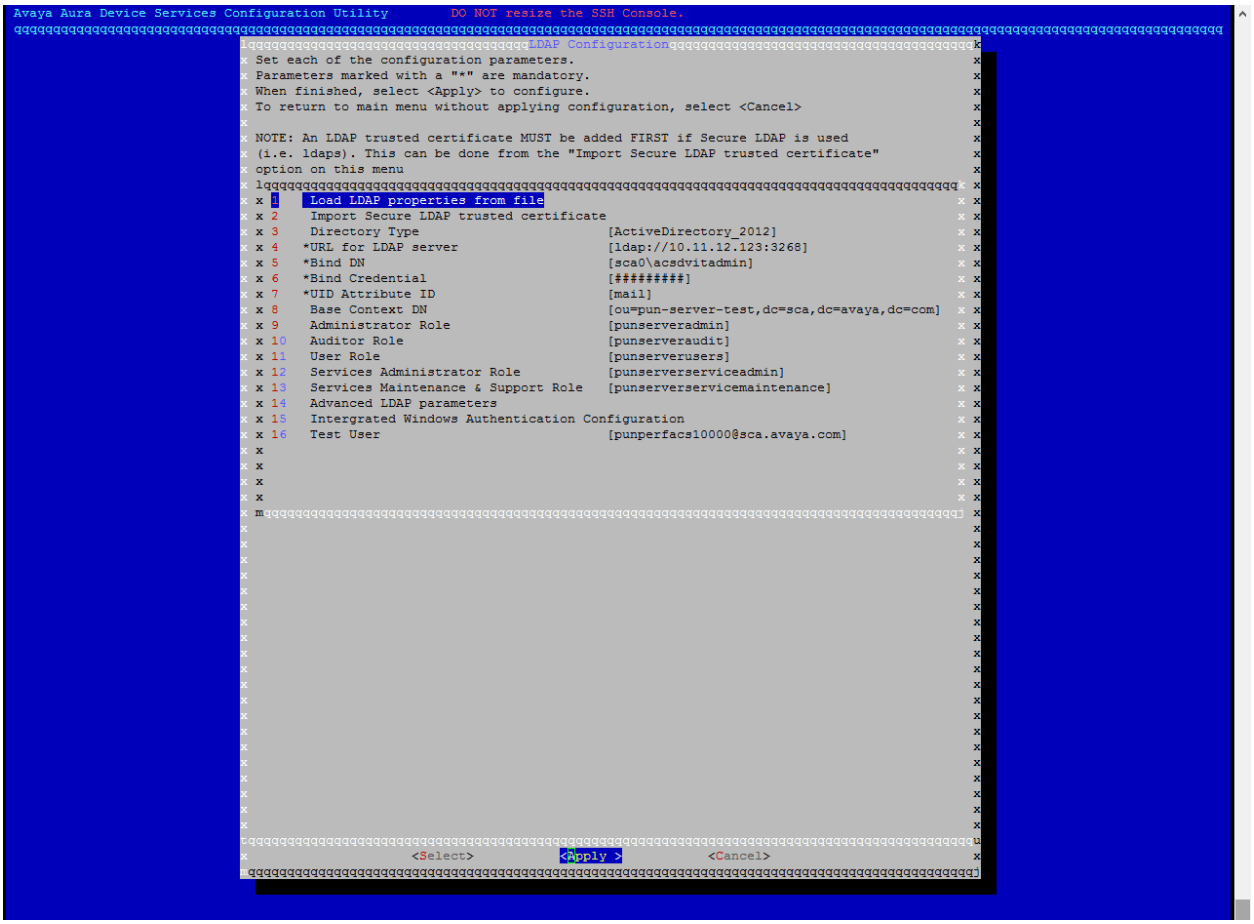


Figure 56: LDAP TestUser

9. Click **Yes**. LDAP configuration is saved.

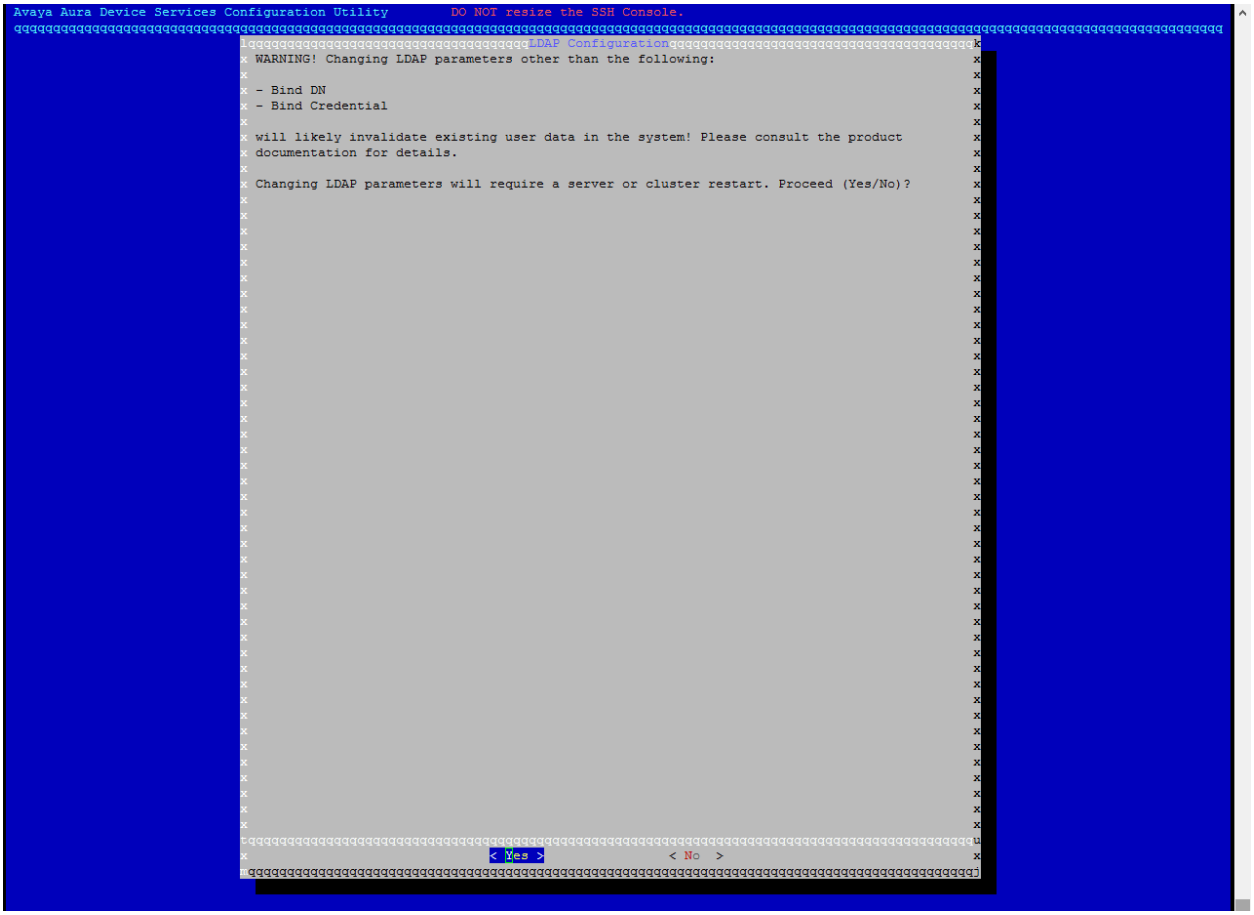


Figure 57: LDAP TestUser

10. Click Continue.

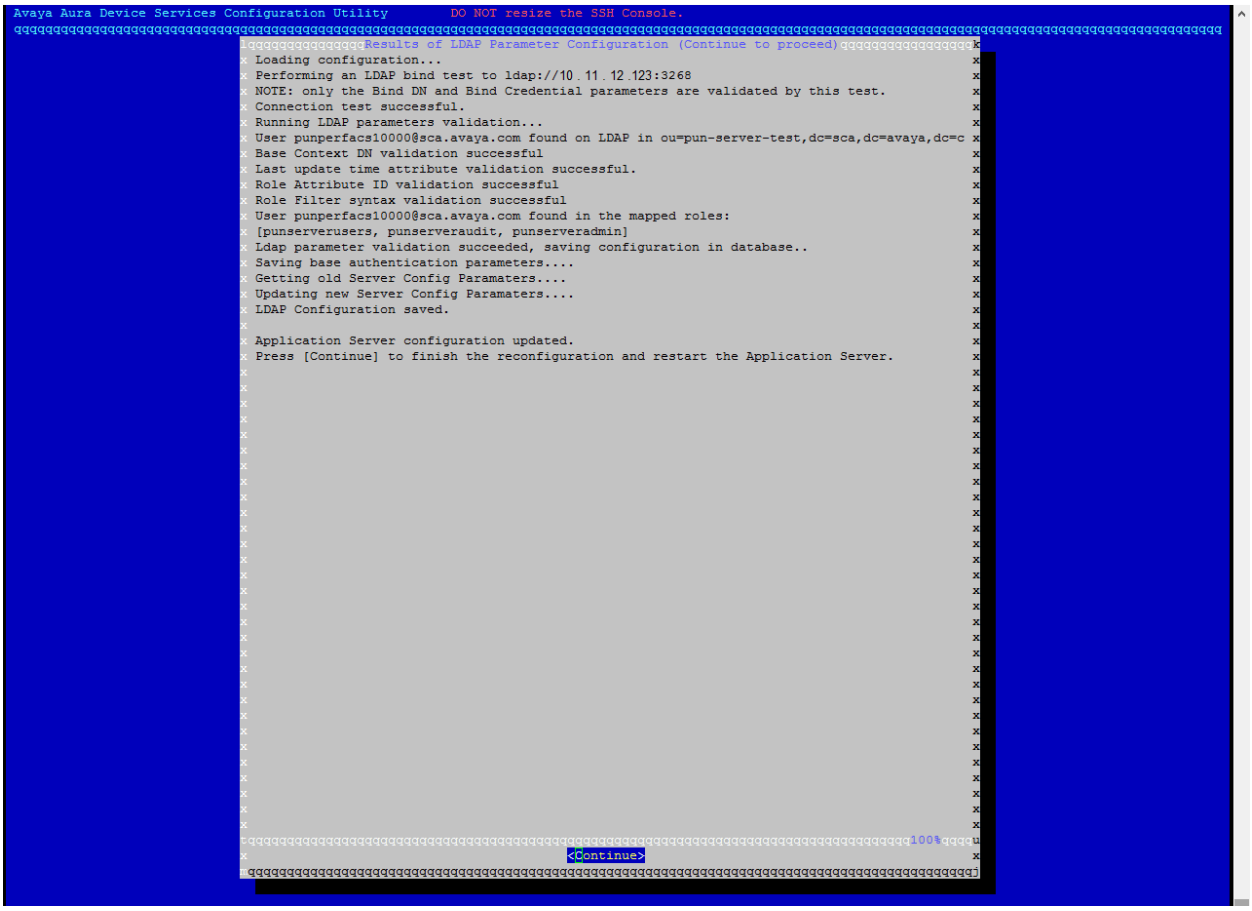


Figure 58: LDAP Configuration saved

m. Leave CORS Configuration and Serviceability Agent Configuration fields unchanged.

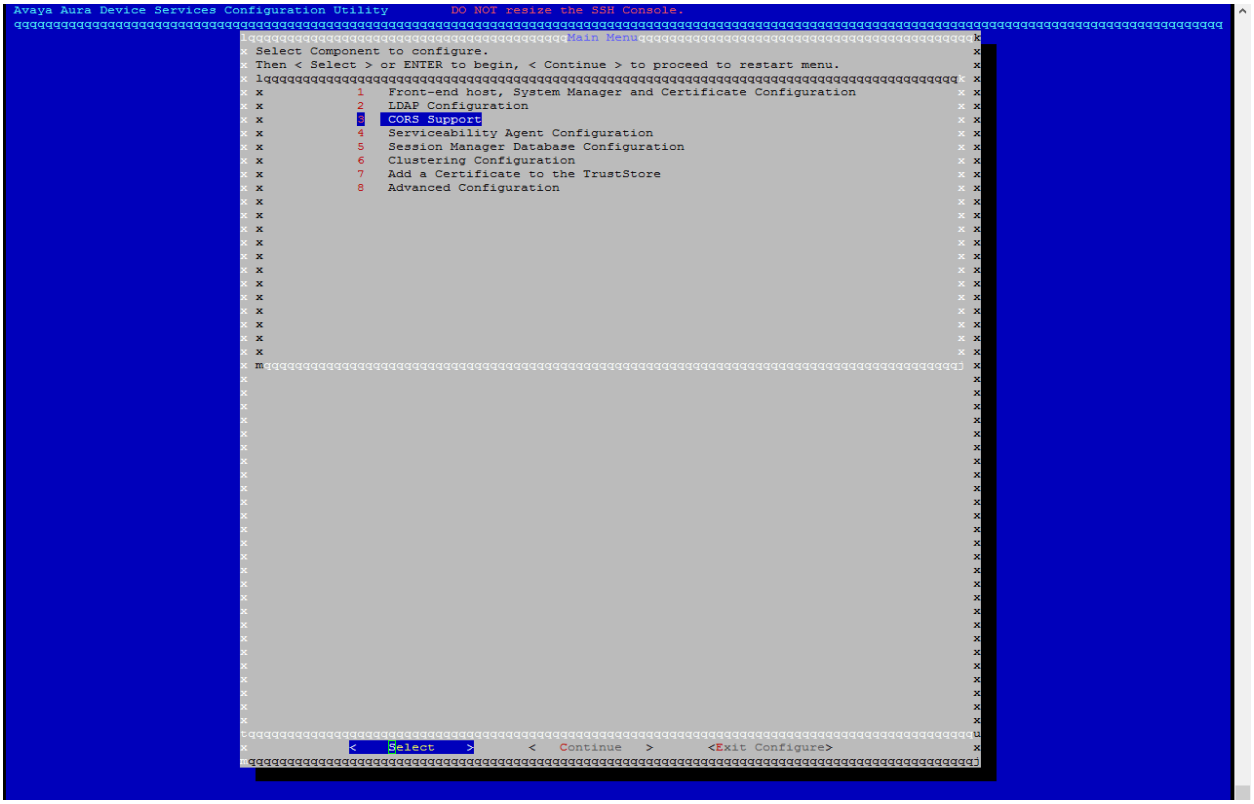
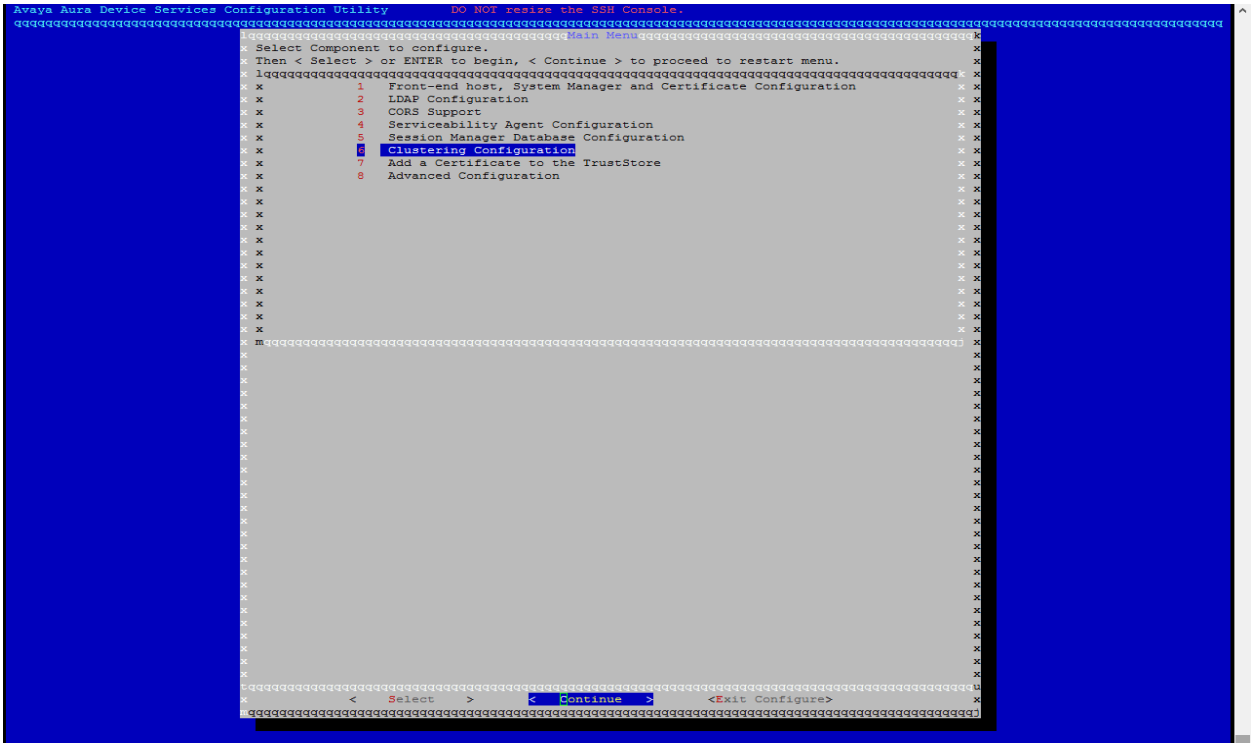


Figure 59: CORS Configuration and Serviceability Agent Configuration

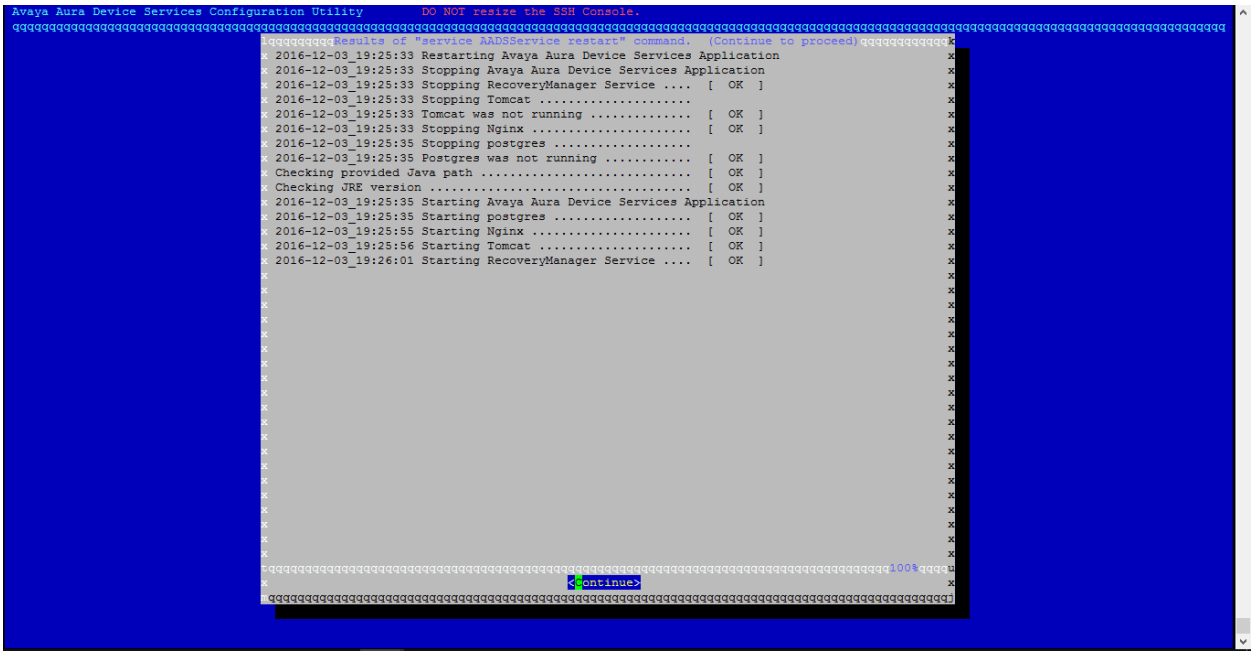
n. Press Continue.



o. After you configure the mandatory settings, you must restart the Avaya Aura® Device Services. The system prompts for AADS service restart. Press **Yes**.

Figure 60: AADS Service restart

p. Press Continue.



q. The Avaya Aura® Device Services installation is complete.

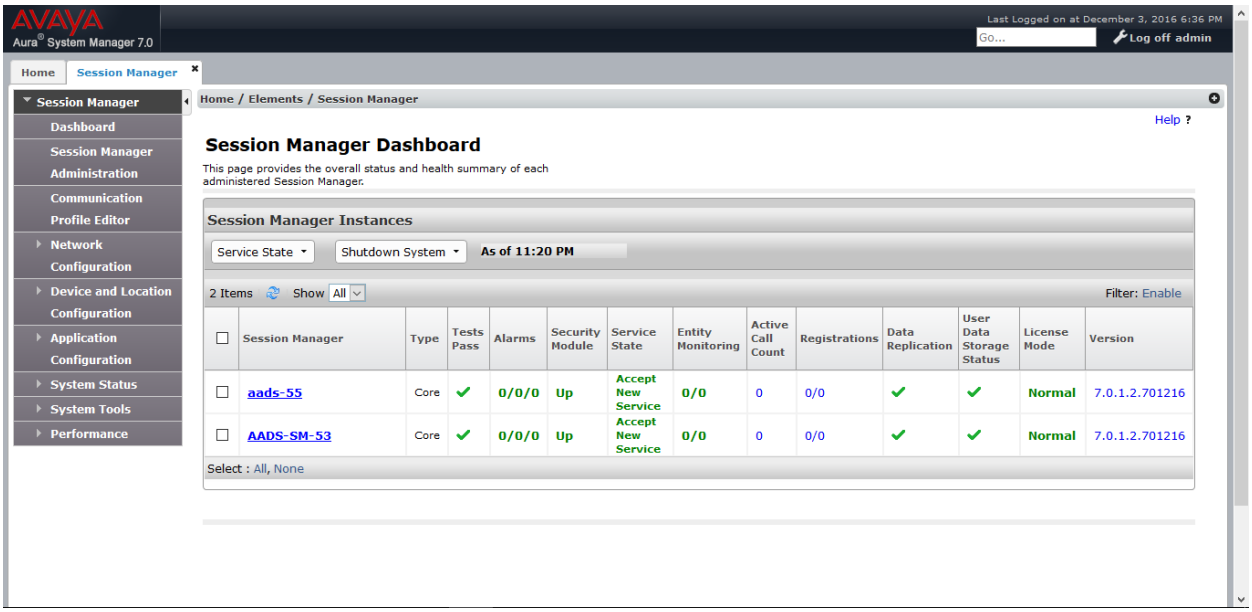
```
2017-01-25_18:33:57 ############################################################

2017-01-25_18:33:57 Installation log file is at /opt/Avaya/DeviceServices/7.0.1.1.162/../.AADSInstallLogs/AADS_Install_2017-01-25_17:06:00.log

2017-01-25_18:33:57 Avaya Aura Device Services components have been installed.
2017-01-25_18:33:57 If errors occurred during post-install configuration (see output above),
2017-01-25_18:33:57 please run the following command to configure (or re-configure) the product

2017-01-25_18:33:57     sudo /opt/Avaya/DeviceServices/7.0.1.1.162/CAS/7.0.1.1.162/bin/configureAADS.sh

2017-01-25_18:33:57 Completing Avaya Aura Device Services Installation

2017-01-25_18:33:57 Please run the following command to verify AADS system installation status:

2017-01-25_18:33:57    sudo /opt/Avaya/DeviceServices/7.0.1.1.162/CAS/7.0.1.1.162/misc/clitool-acs.sh postInstallSystemVerification

2017-01-25_18:33:57 ############################################################

[admin@aads216 ~]$
```

Installation of Avaya Aura® Device Services (Cluster)

Installing seed node

Pre-installation check

1. On System Manager Web Console-> Session Manager - > Dashboard check the Session Manager status. Ensure that all the Session Manager instances are up and running.



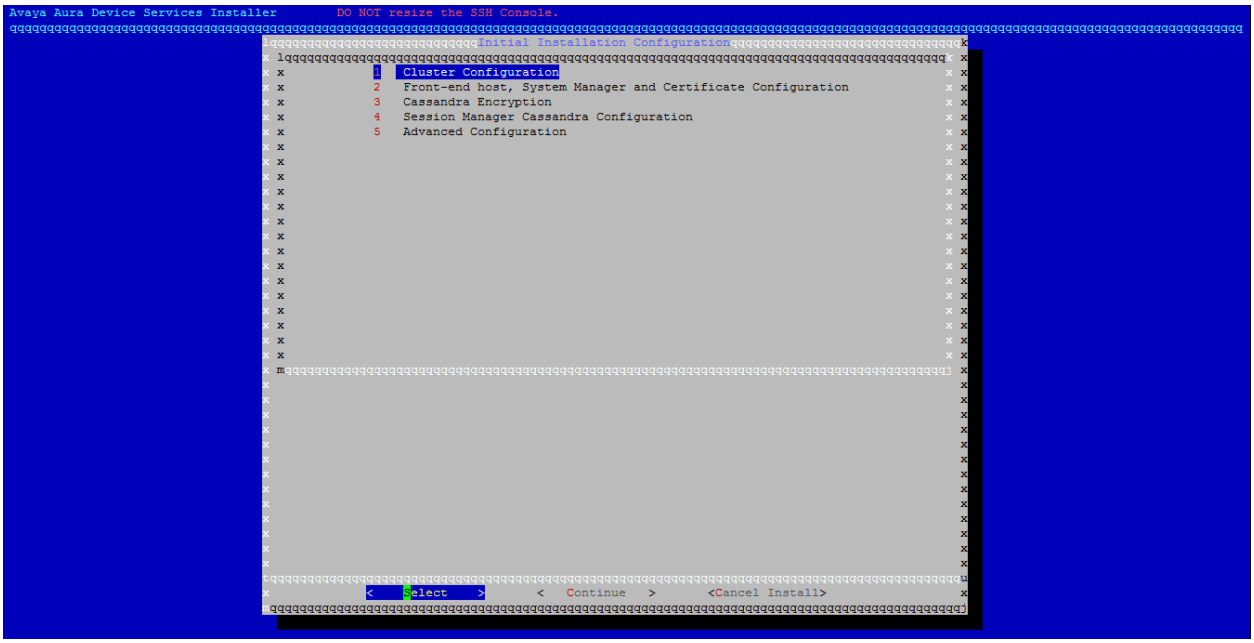
Additionally, you can also login to SM nodes using putty and execute the following command to check the service status.

```
[craft@aads-sm-53 ~]$ statapp
Watchdog          9/  9 UP
logevent         13/ 13 UP
ncsd              4/  4 UP
postgres-db      31/ 31 UP
mgmt            215/215 UP
WebSphere       220/220 UP
```

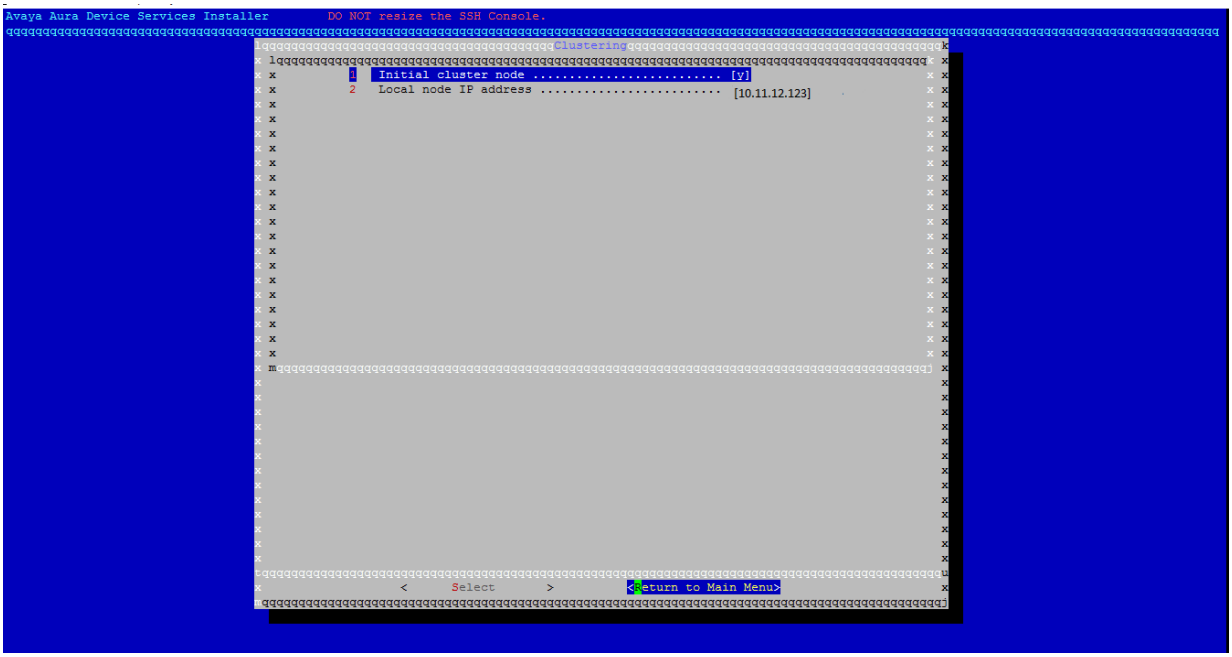
CDRService 16/ 16 UP
cassandra 122/122 UP
sal-agent 47/ 47 UP
secmod 4/ 4 UP

Start Avaya Aura® Device Service Installation

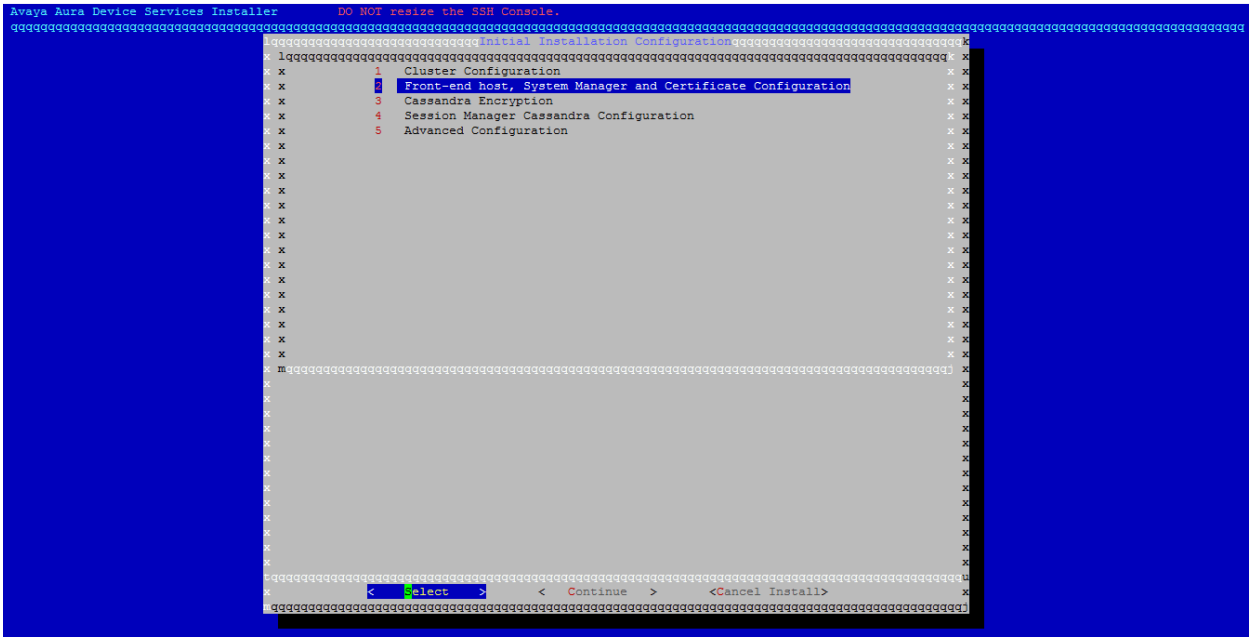
1. Go to the Avaya directory by using cd /opt/Avaya
2. Run the command **app install**
3. The system displays a blue installation tool.
4. Steps to be performed in the blue configuration tool:
    a. Cluster configuration



b. Set Initial cluster node to [y]. Press <Return to Main Menu>

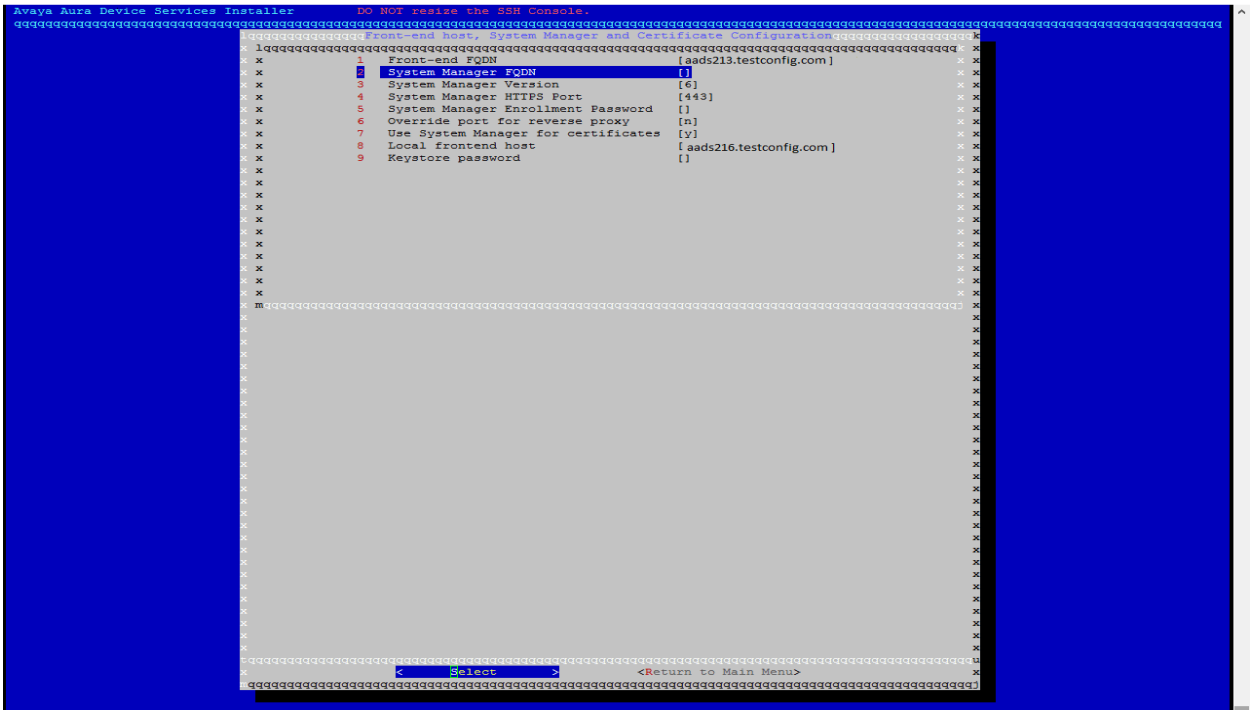


c. Front-end host, System Manager and Certificate Configuration

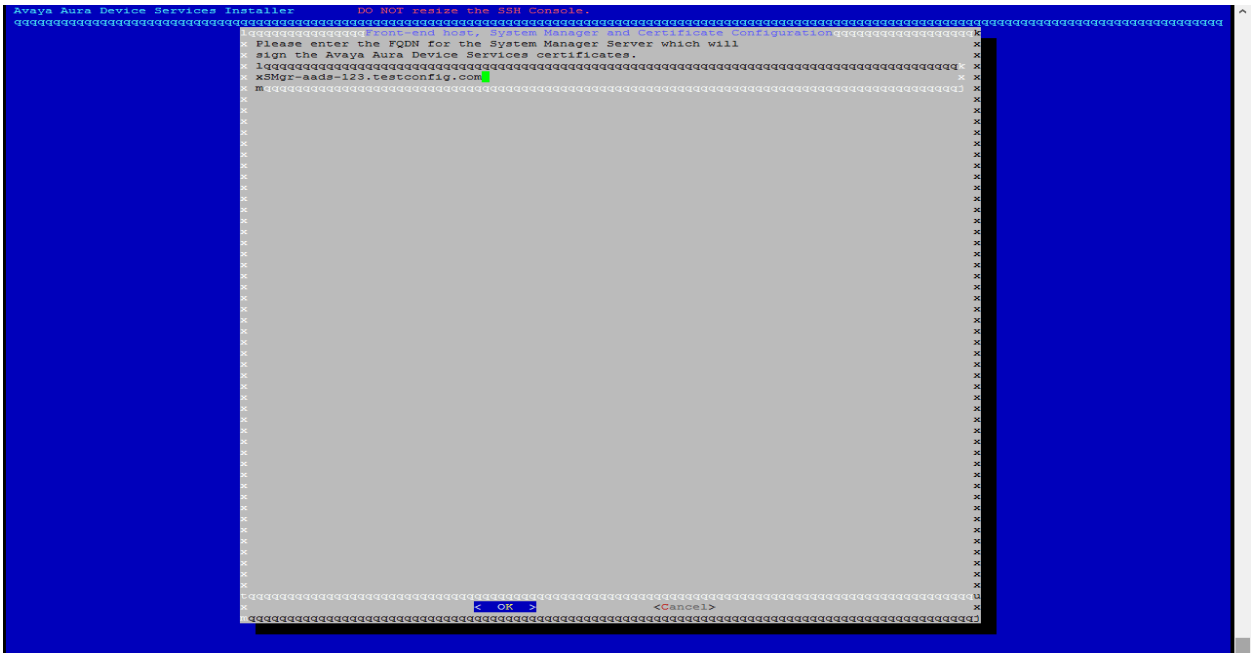


d. Enter Front-end FQDN– If you think you would need to extend the system to an AADS cluster; it is advisable to use the hostname corresponding to the virtual IP. If you are planning to have a standalone AADS, this field will be same as the Local frontend host.

e. Enter the System Manager details in this screen. Keystore password should be 6 or more characters. This should be same on all nodes in cluster.



Enter SMGR FQDN and press **OK**. The installer will try to check if the provided hostname is valid or not.

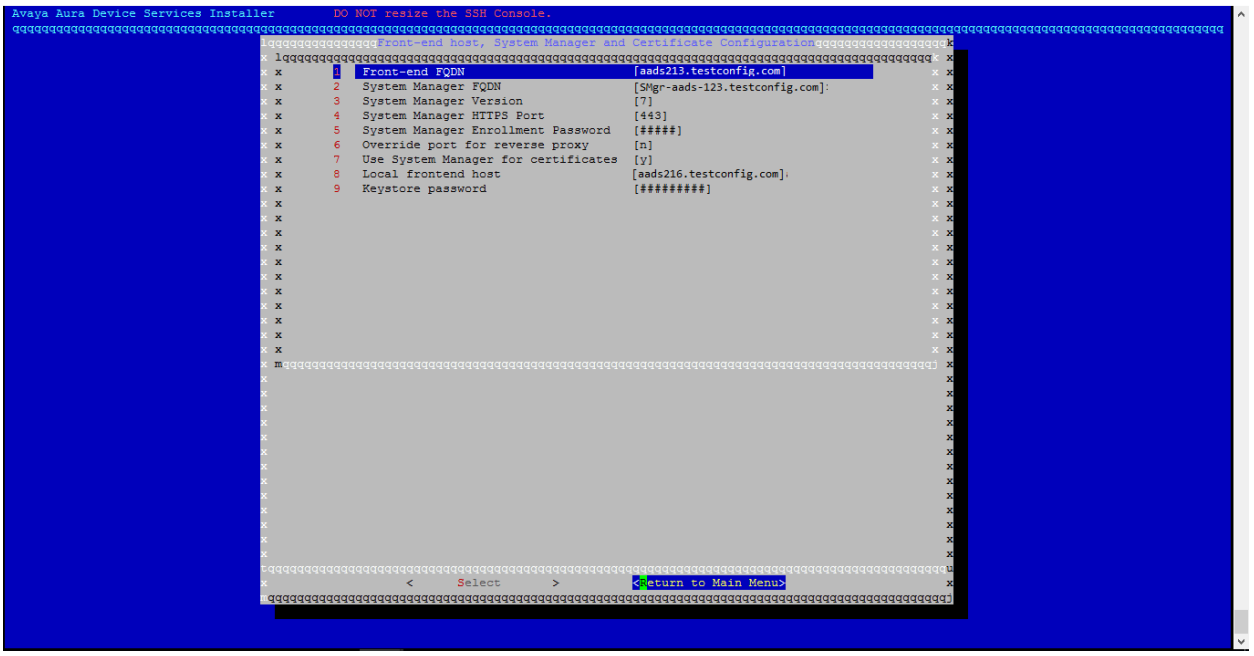


Press **<OK>.**

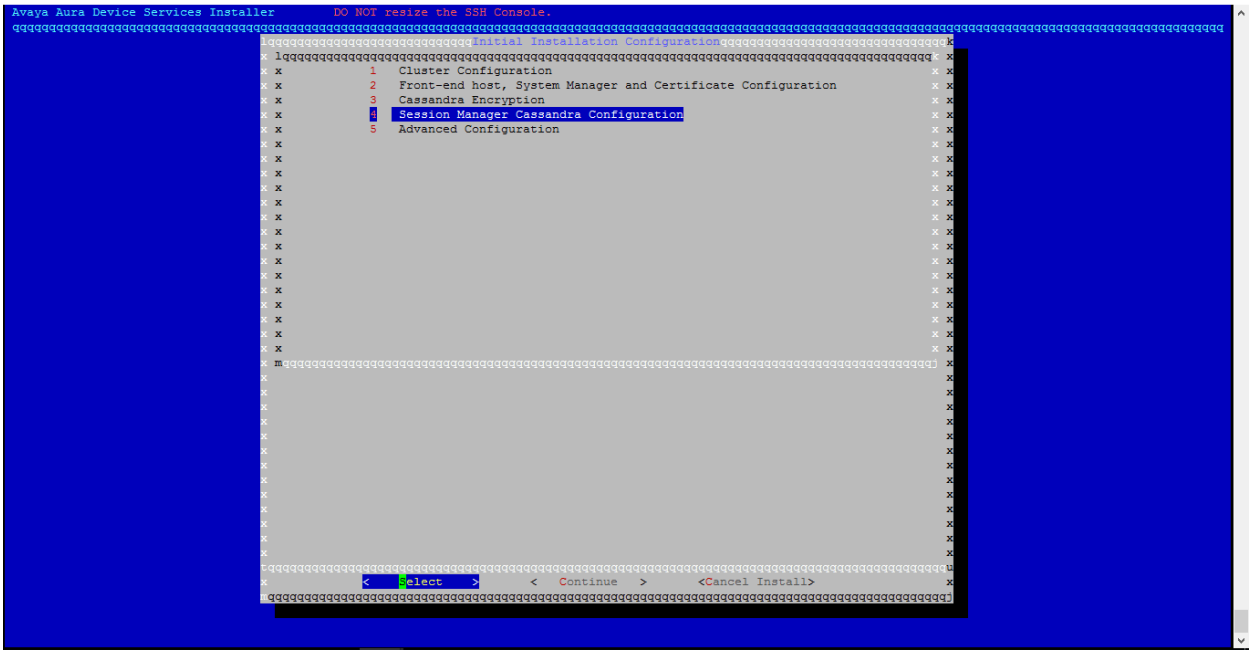
f. After entering all the details <Return to Main Menu>

Note:

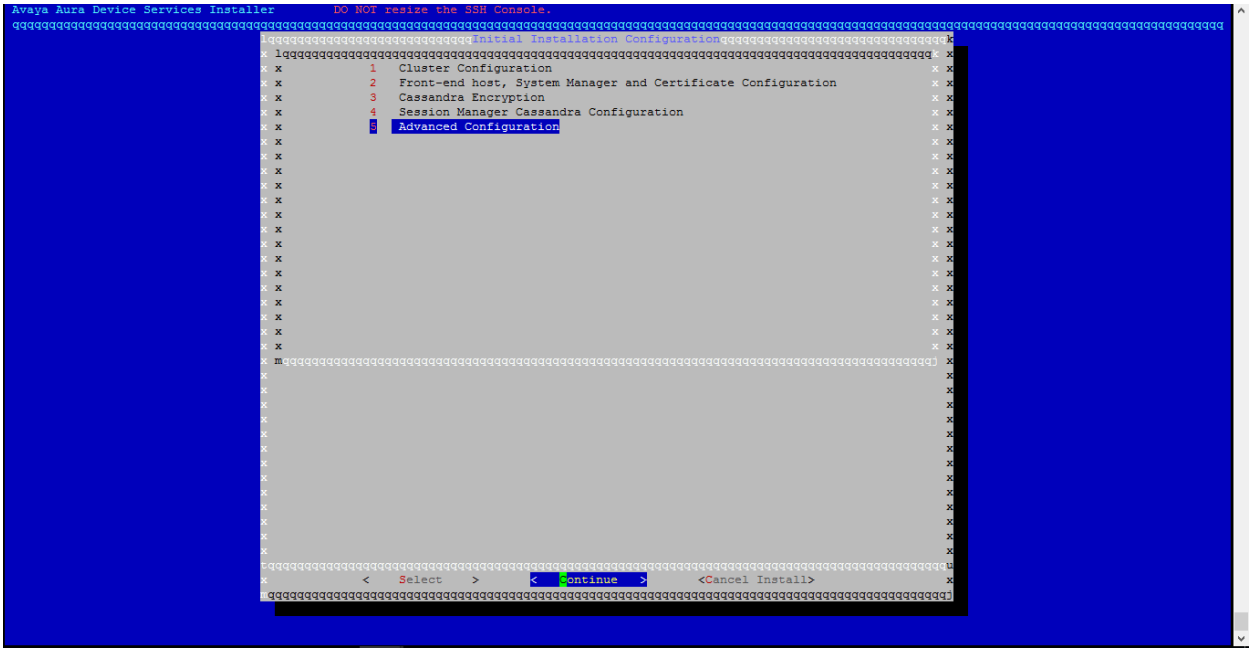
If System Manager is not being used for certificate, follow the procedure given here Configuring Certificates without System Manager.



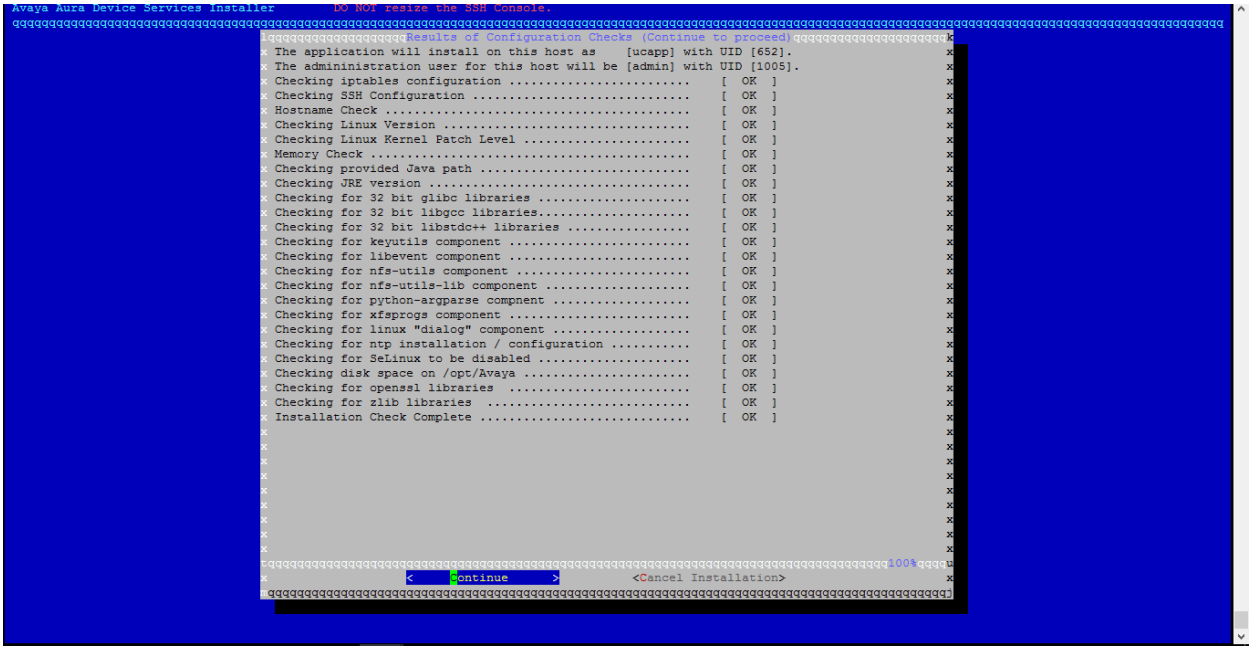
g. Session Manager Cassandra Configuration –Provide Session Manager Management and Asset IP here.



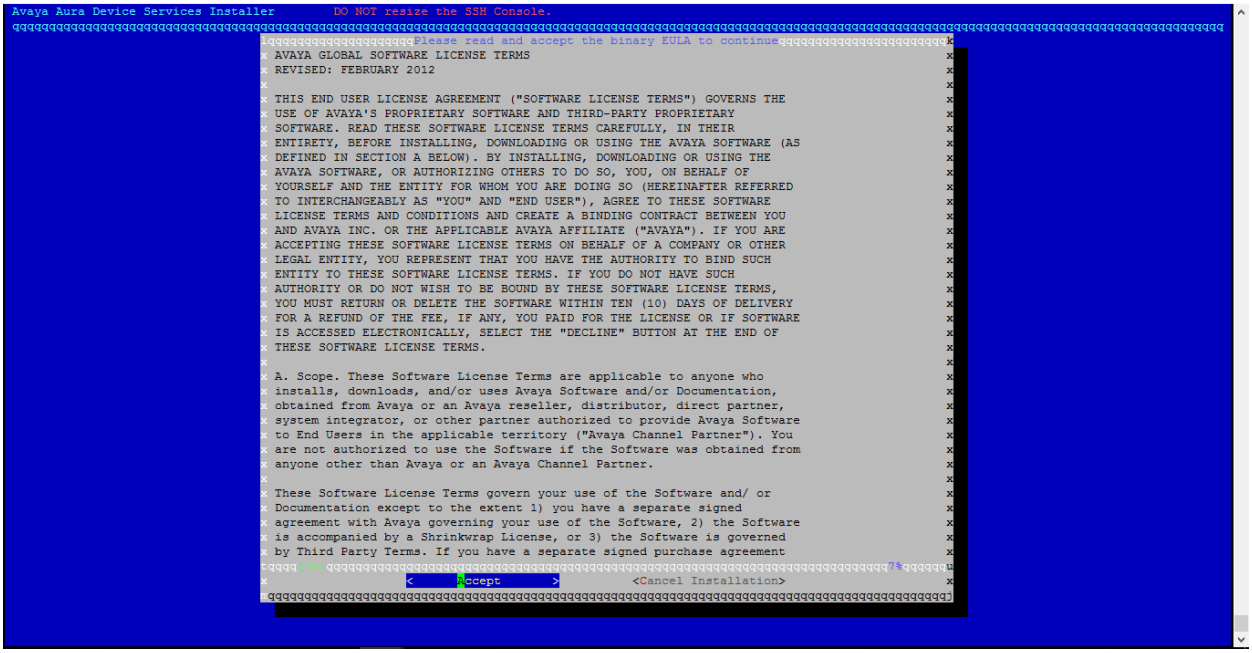
h. Leave Cassandra Encryption and Advanced Configuration unchanged. Press <Continue>



i. The installer will perform pre-install checks . Press <Continue>

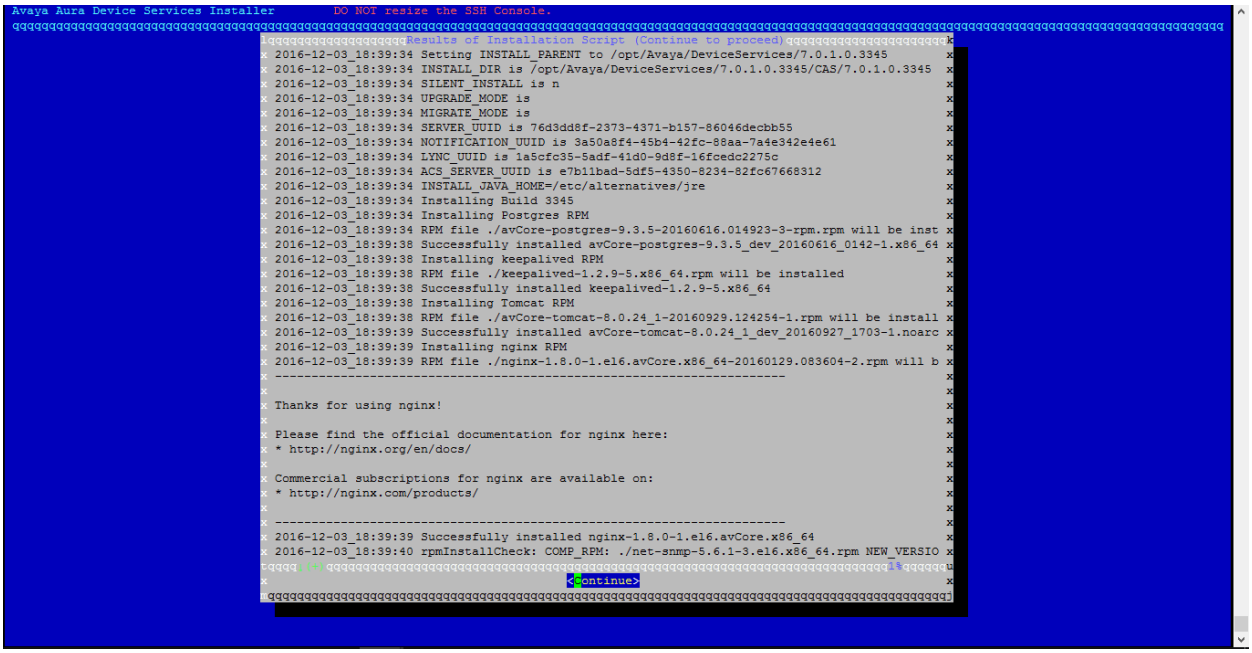


j. Press <Accept> to accept the EULA.

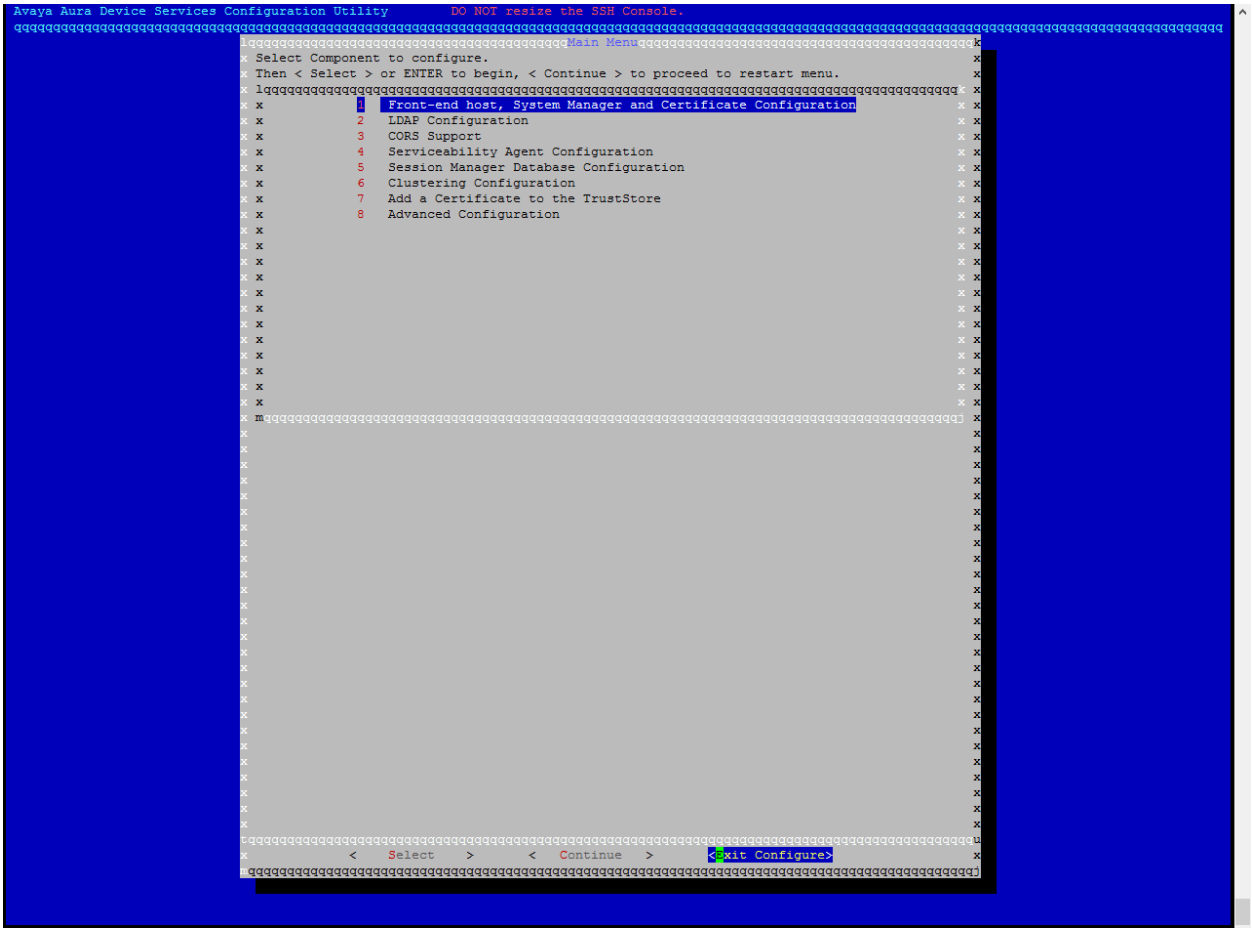


k. AADS installation will begin now. It will install the required RPMs, download certificates from System Manager, Create database schema and do the required initial configuration. The screen will show the progress.

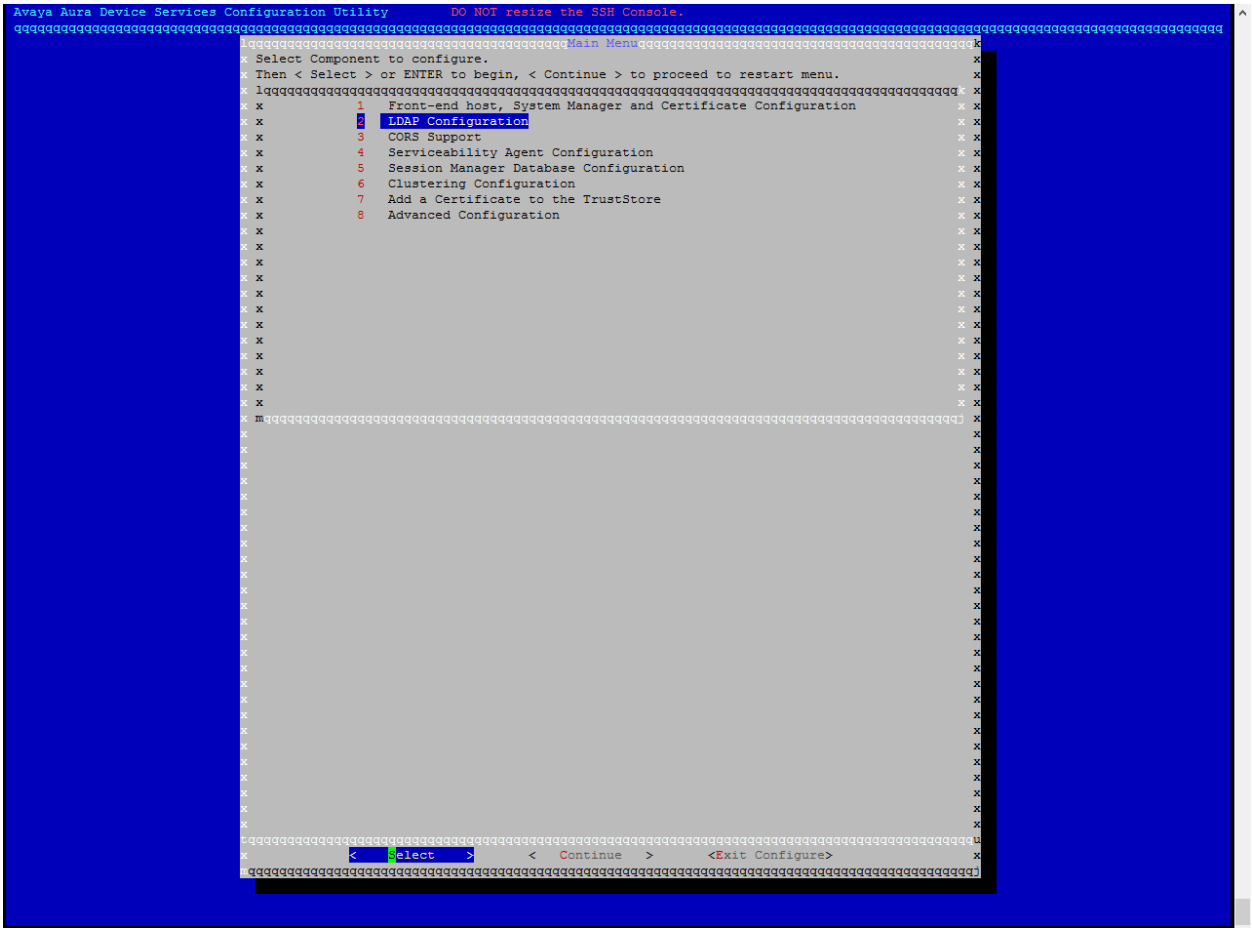
l. Once this step is complete, the following screen will be displayed. Press <Continue>



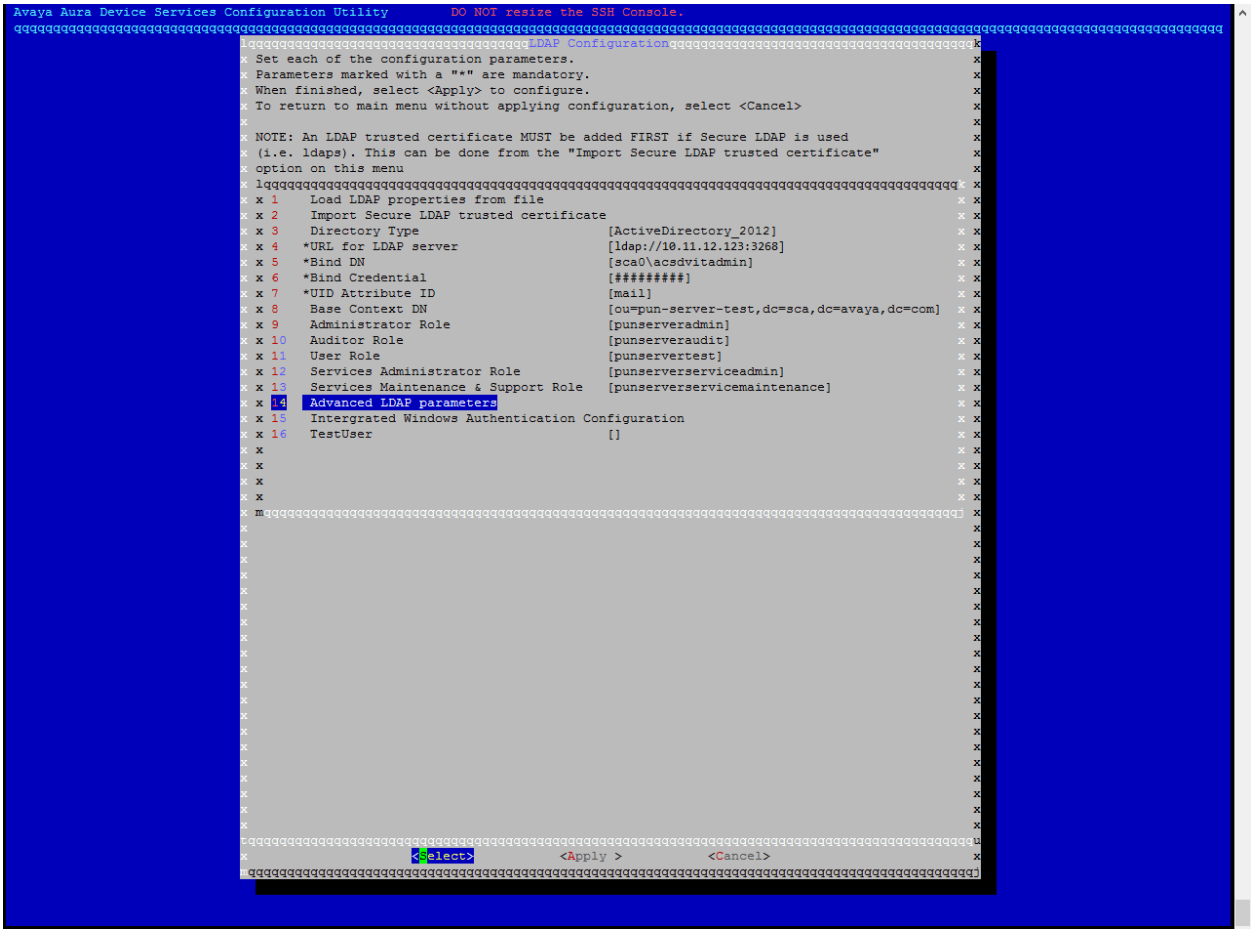
m. The system displays the following screen.



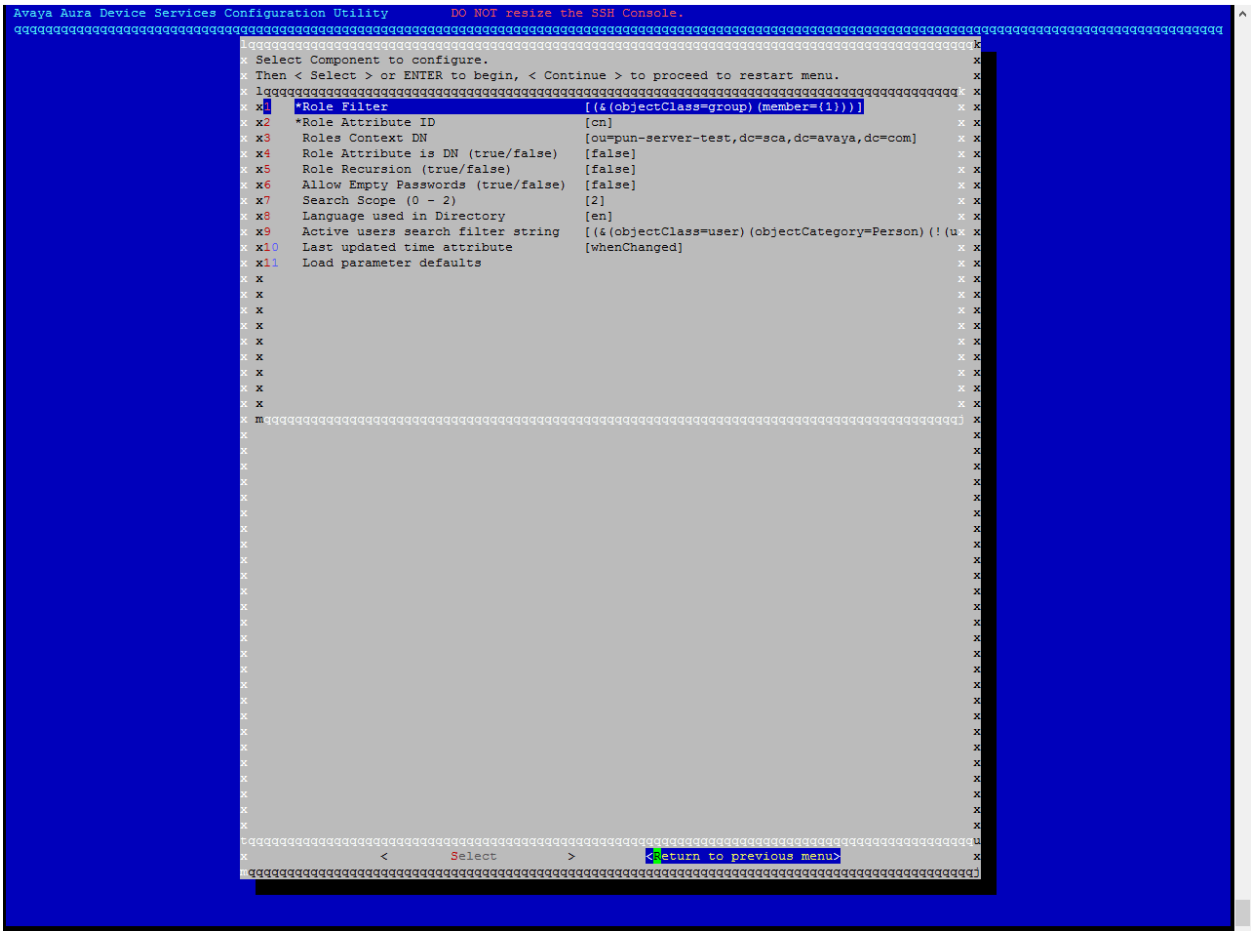
n. Go to LDAP Configuration menu.



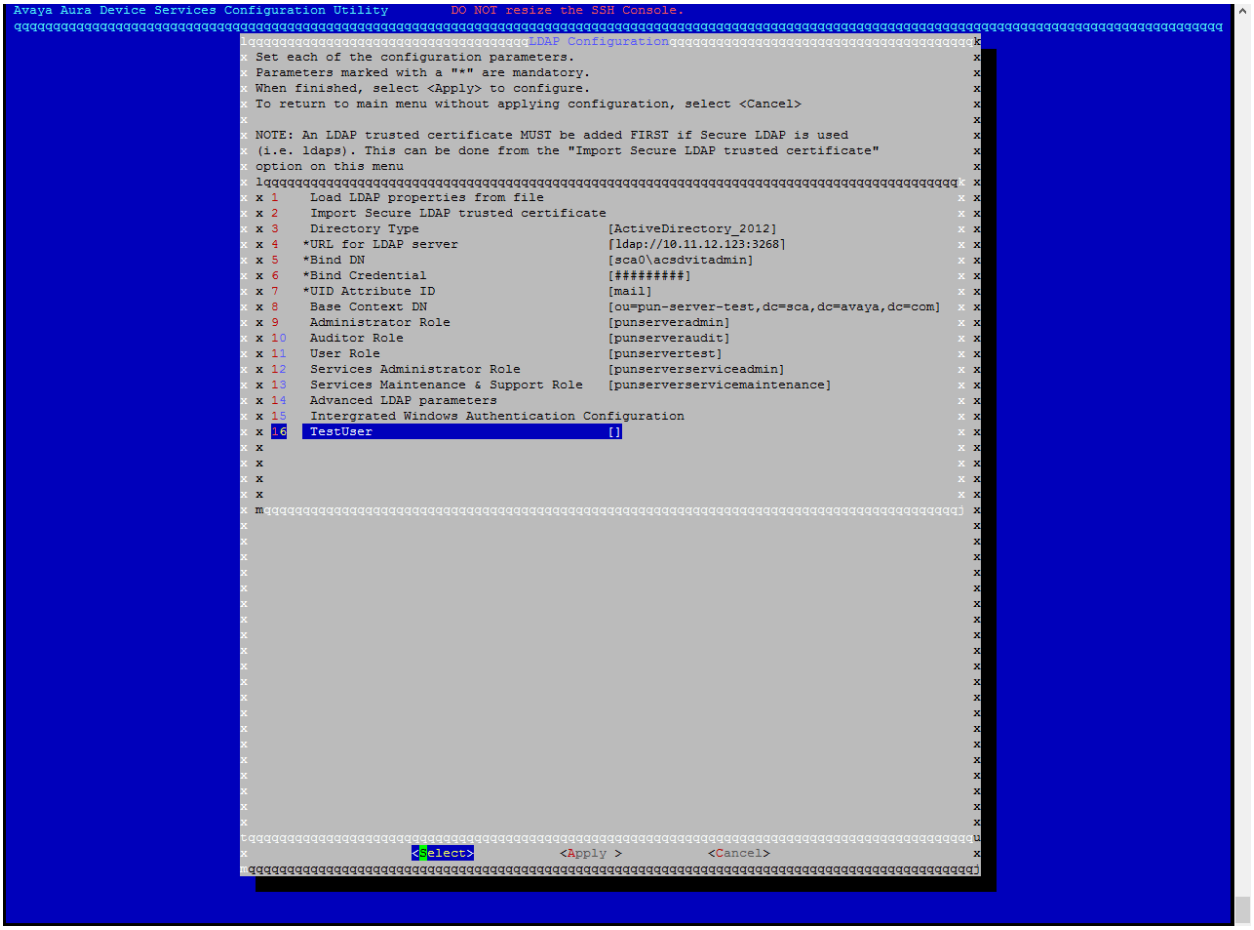
11. Provide LDAP details (Do not cut/copy paste values in these fields, it might introduce some invalid characters such as spaces in between). Enter the values for each field manually.
12. After entering the values in below screen, click **Advanced LDAP parameters.**


Avaya Aura Device Services Configuration Utility
DO NOT resize the SSH Console.
LDAP Configuration
Set each of the configuration parameters.
Parameters marked with a "*" are mandatory.
When finished, select <Apply> to configure.
To return to main menu without applying configuration, select <Cancel>
NOTE: An LDAP trusted certificate MUST be added FIRST if Secure LDAP is used
(i.e. ldaps). This can be done from the "Import Secure LDAP trusted certificate"
option on this menu
1 Load LDAP properties from file
2 Import Secure LDAP trusted certificate
3 Directory Type [ActiveDirectory_2012]
4 *URL for LDAP server [ldap://10.11.12.123:3268]
5 *Bind DN [sca0\acsdvitadmin]
6 *Bind Credential [#########]
7 *UID Attribute ID [mail]
8 Base Context DN [ou=pun-server-test,dc=sca,dc=avaya,dc=com]
9 Administrator Role [punserveradmin]
10 Auditor Role [punserveraudit]
11 User Role [punservertest]
12 Services Administrator Role [punserverserviceadmin]
13 Services Maintenance & Support Role [punserverservicemaintenance]
14 Advanced LDAP parameters
15 Intergrated Windows Authentication Configuration
16 TestUser []
<Select>
<Apply >
<Cancel>

13. Default values for Advanced LDAP parameters are already provided. Edit the fields if you use some other configuration, and press <Return to previous menu>.



14. Go to **TestUser** field and click <Select>

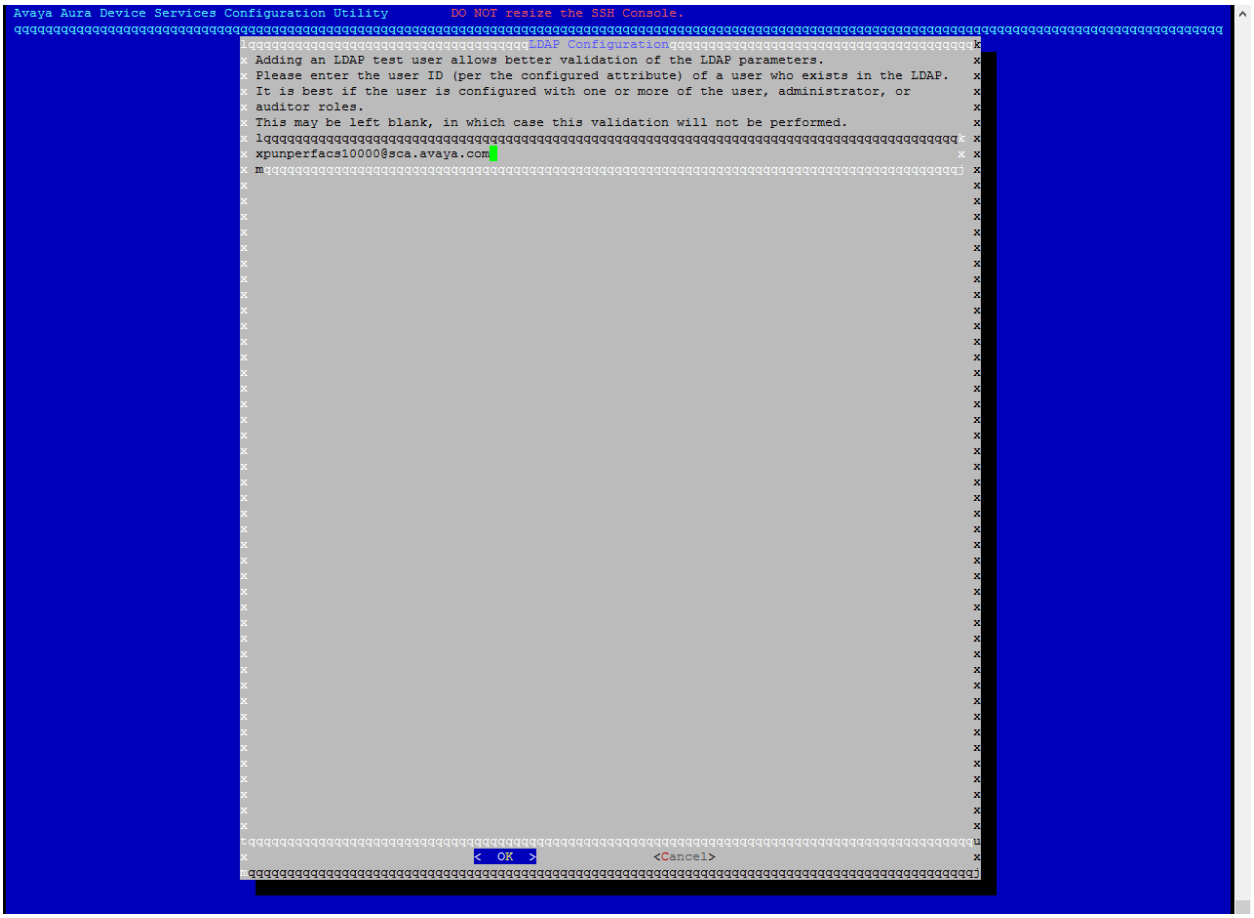


15. Add a LDAP test user. This will allow better validation of the LDAP parameters provided.
16. The **TestUser** must be a valid user on LDAP and should be present in the provided **Base Context DN.** The LDAP user should correspond to the **UID Attribute ID** provided.

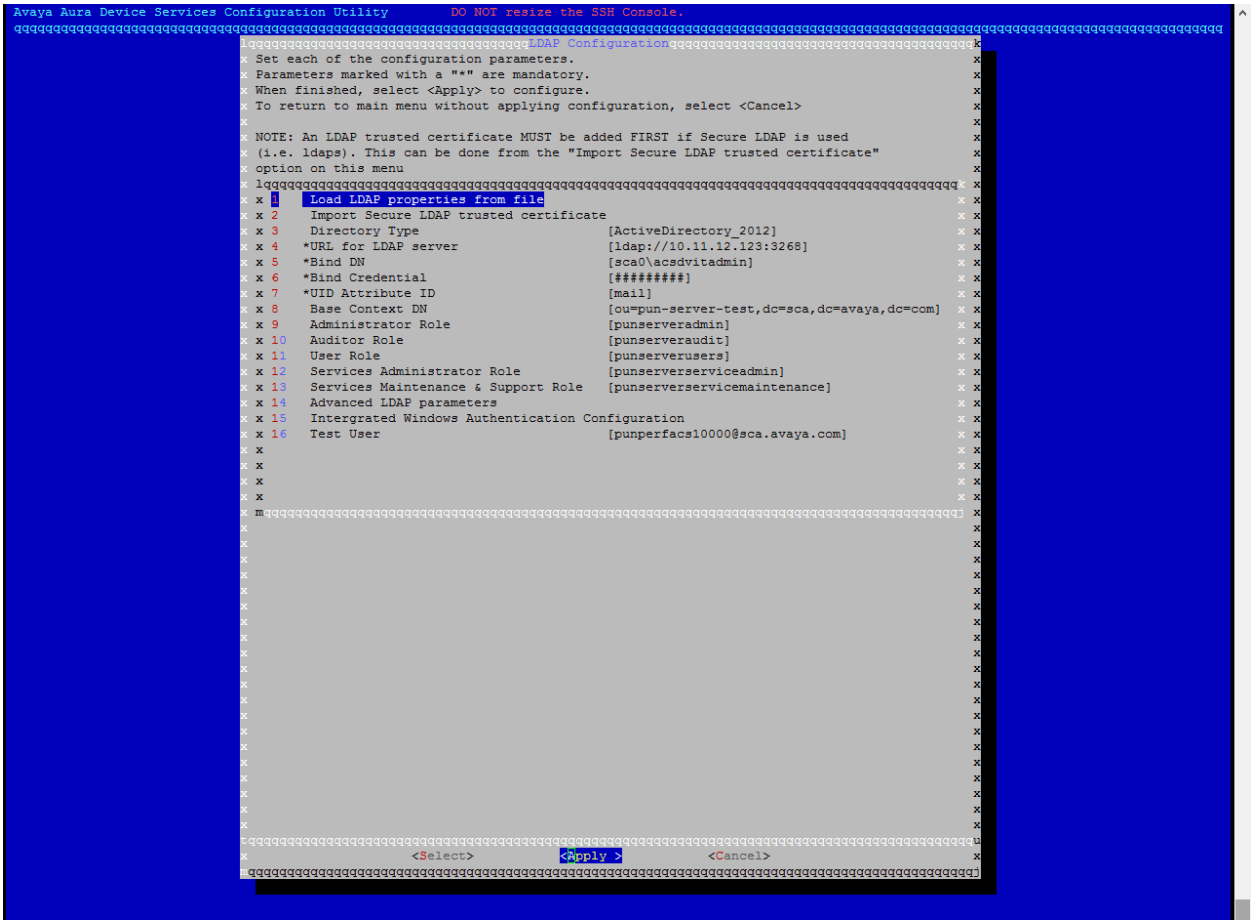
    For example: If UID Attribute ID is sAMAccountName, in the TestUser field enter the sAMAccountName of the user

17. After entering the value, click <OK>

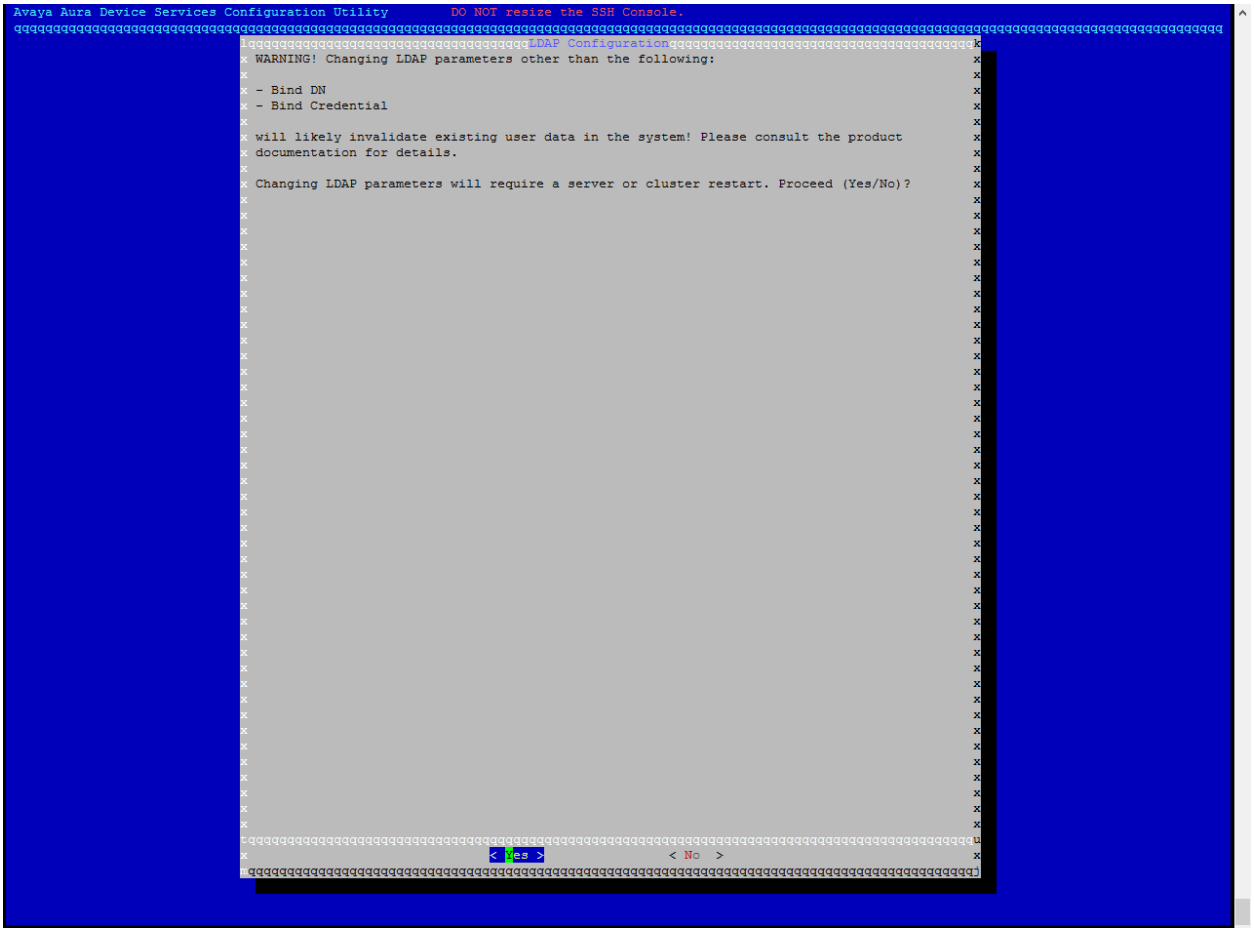
Note: TestUser may be left blank, in that case enhanced validation for LDAP parameters will not be performed.


Avaya Aura Device Services Configuration Utility
DO NOT resize the SSH Console.
LDAP Configuration
Adding an LDAP test user allows better validation of the LDAP parameters.
Please enter the user ID (per the configured attribute) of a user who exists in the LDAP.
It is best if the user is configured with one or more of the user, administrator, or
auditor roles.
This may be left blank, in which case this validation will not be performed.
xpunperfacs10000@sca.avaya.com
< OK >
<Cancel>

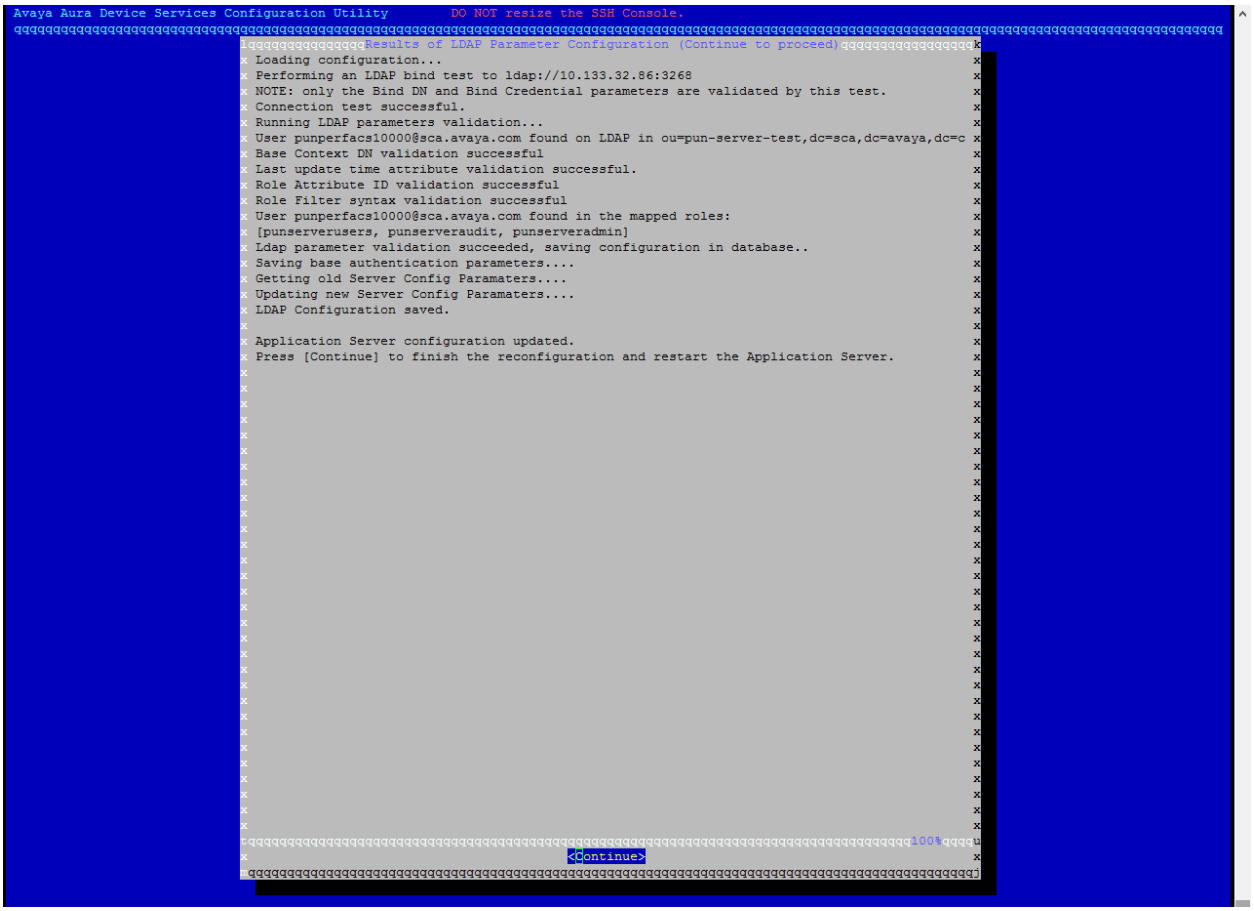
18. Click <Apply>.



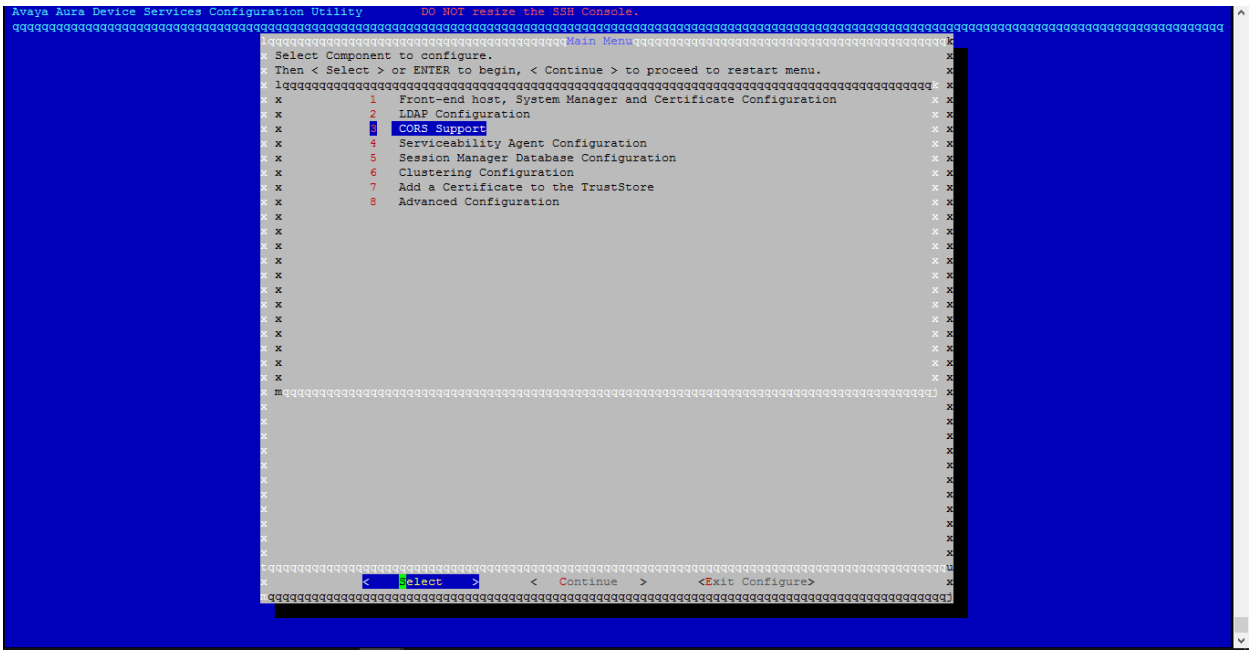
19. Click <Yes>


Avaya Aura Device Services Configuration Utility
DO NOT resize the SSH Console.
LDAP Configuration
WARNING! Changing LDAP parameters other than the following:
- Bind DN
- Bind Credential
will likely invalidate existing user data in the system! Please consult the product documentation for details.
Changing LDAP parameters will require a server or cluster restart. Proceed (Yes/No)?
< Yes >
< No >

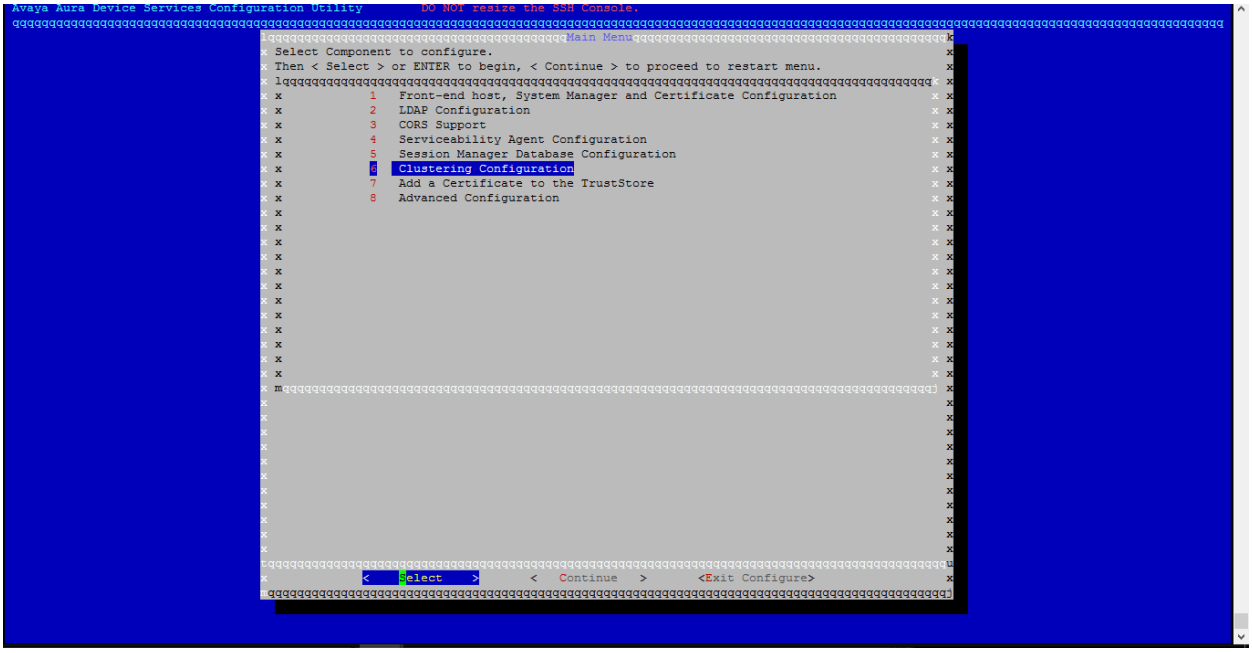
20. LDAP configuration is saved. Click <Continue>.



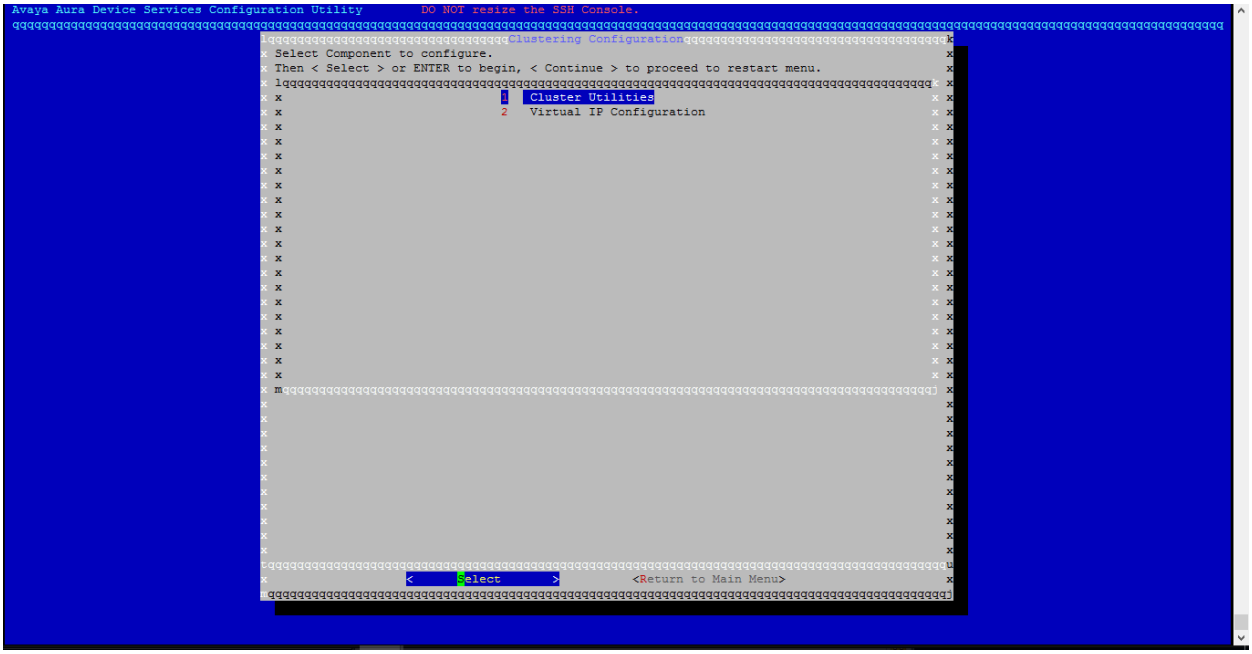
o. Leave CORS Support and Serviceability Agent Configuration unchanged.

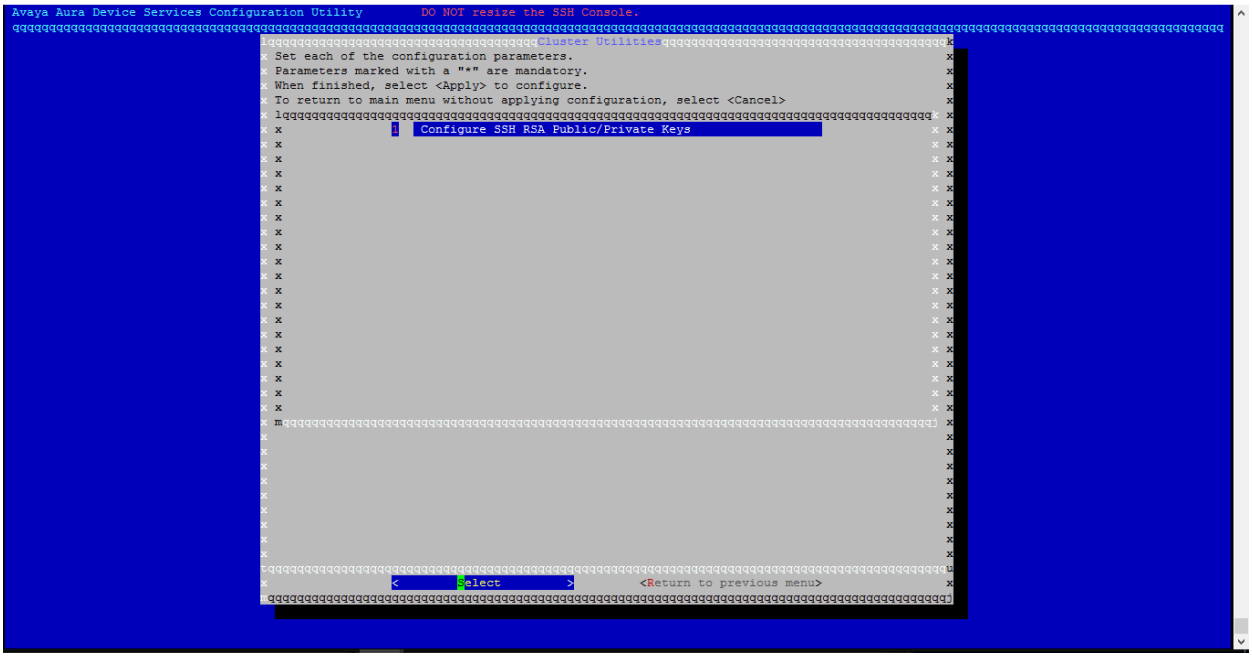


p. Go to Clustering Configuration.



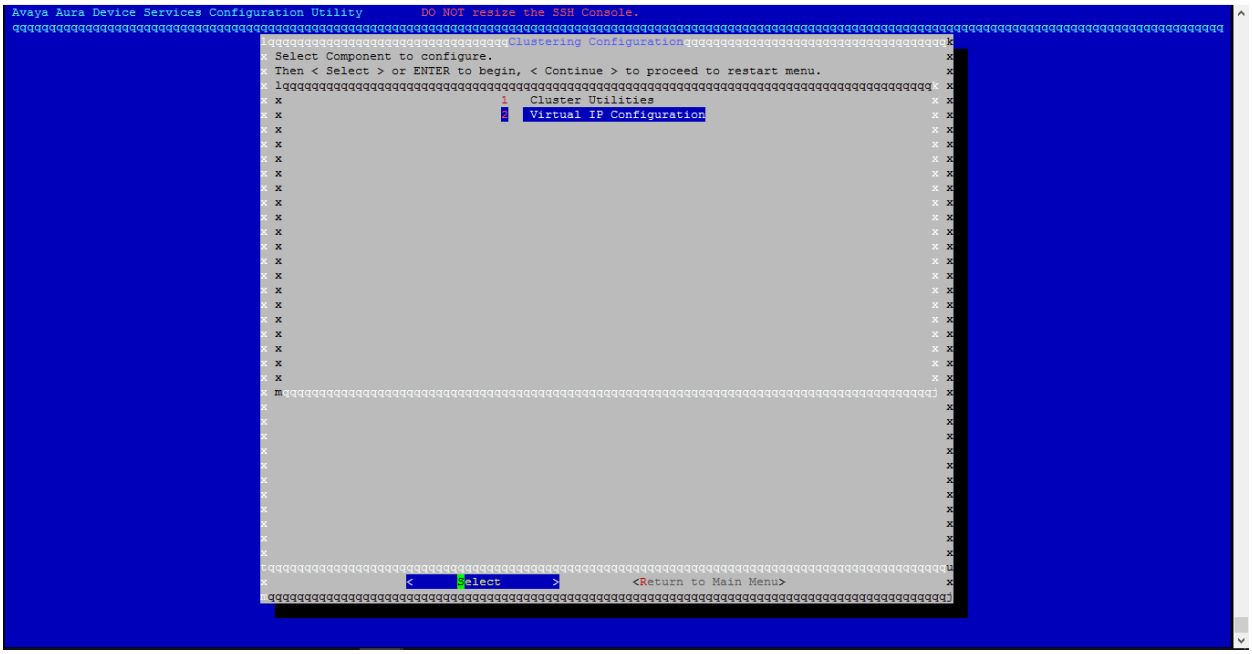
q. Go to Cluster Utilities to configure SSH RSA public/private keys.



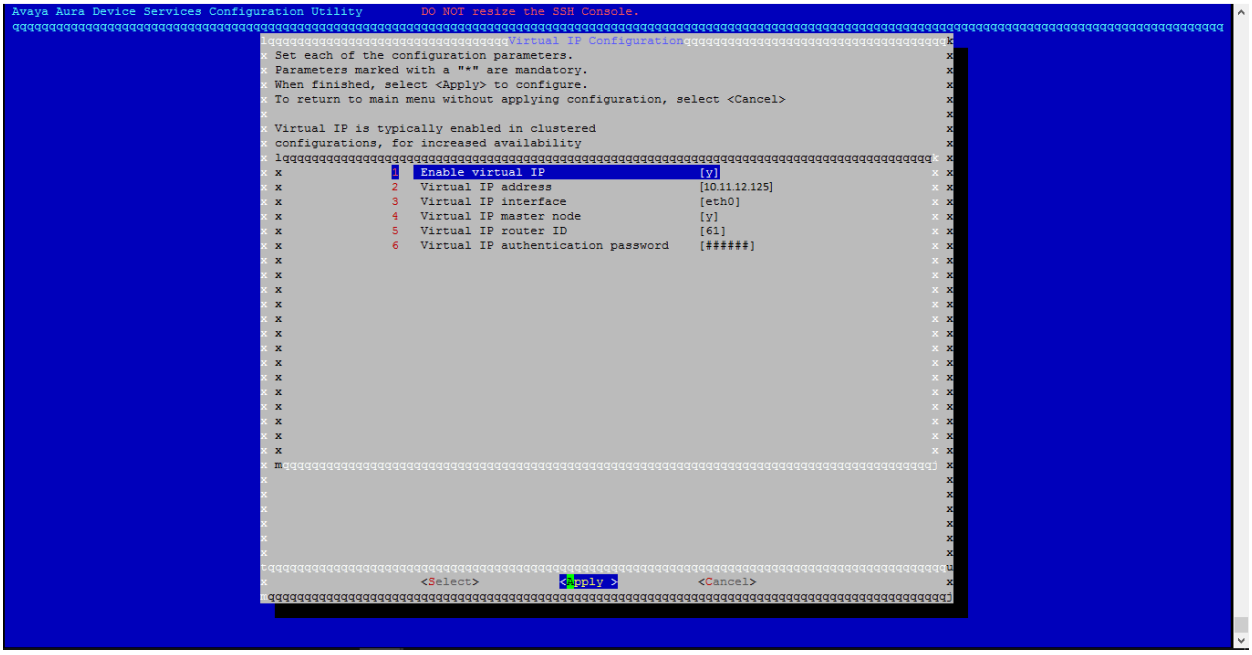



```
Add additional hosts to the list? (y/n) [n]: y
Enter a new host identifier using the syntax user@192.168.0.33 or user@server.abc.com
If the user name is omitted (e.g. just 192.168.0.33), it will be requested later.
When finished, enter a blank line by pressing the Enter key

Enter a new host identifier, blank when finished: 10.11.12.124
Enter a new host identifier, blank when finished:

User for 10.11.12.124 []: admin
2016-12-03_20:01:18 Hosts are:
2016-12-03_20:01:18 admin@10.11.12.124
2016-12-03_20:01:18 admin@10.11.12.123
2016-12-03_20:01:18 checking for existing private key
SSH RSA key exists, replace with a new one? (y/n) [n] y
2016-12-03_20:01:21 generating new private key due to request
2016-12-03_20:01:21 New key requested, generated new key
2016-12-03_20:01:21 Local Keys are at /home/admin/.ssh/id_rsa and /home/admin/.ssh/id_rsa.pub
2016-12-03_20:01:21 Configuring Remote User admin on Host 10.11.12.124
2016-12-03_20:01:21
2016-12-03_20:01:21 If or when prompted to "continue connecting", please enter "yes"
2016-12-03_20:01:21 When prompted for password, please enter password for admin@10.11.12.124
2016-12-03_20:01:21
The authenticity of host '10.11.12.124      (10.11.12.124)' can't be established.
RSA key fingerprint is bd:7d:62:ce:b0:09:aa:e2:81:c0:c2:8b:65:94:5a:10.
Are you sure you want to continue connecting (yes/no)? yes
Password:
Password:
2016-12-03_20:01:40 Configuring Local  User admin on Host 10.11.12.123
2016-12-03_20:01:40 Copying known_hosts file to User admin on Host 10.11.12.124
Password:
2016-12-03_20:01:48 Copying known_hosts file to User admin on Host 10.11.12.123
SSH RSA configuration is complete.  <Enter> to continue:
```

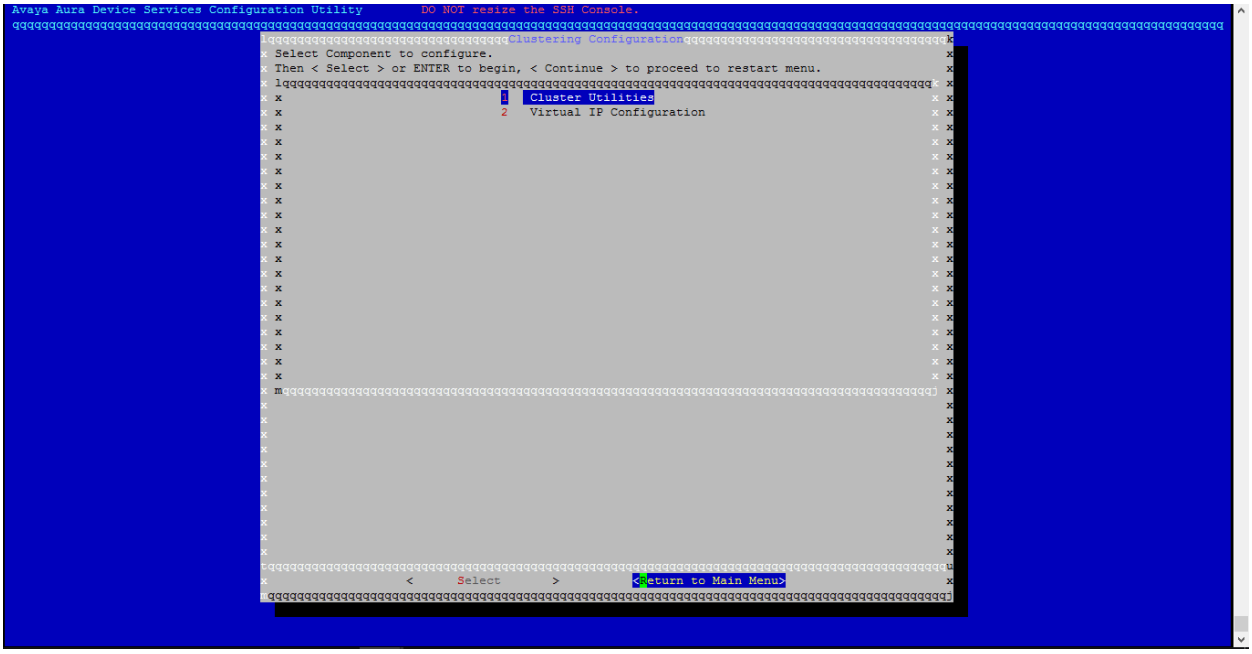
r. Go to Virtual IP Configuration



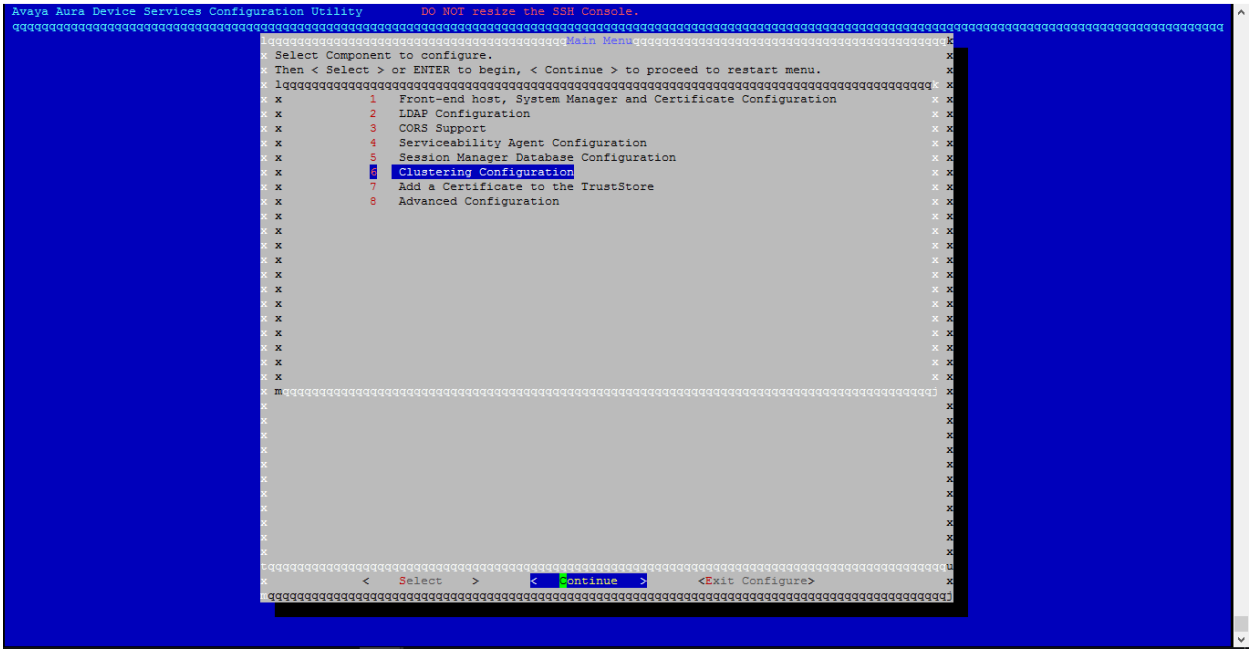
s. Enter virtual IP details and set Virtual IP master node to [y]. Virtual IP authentication password should be same on all the nodes in cluster. Press <Apply>.



t. Press <Return to Main Menu>.

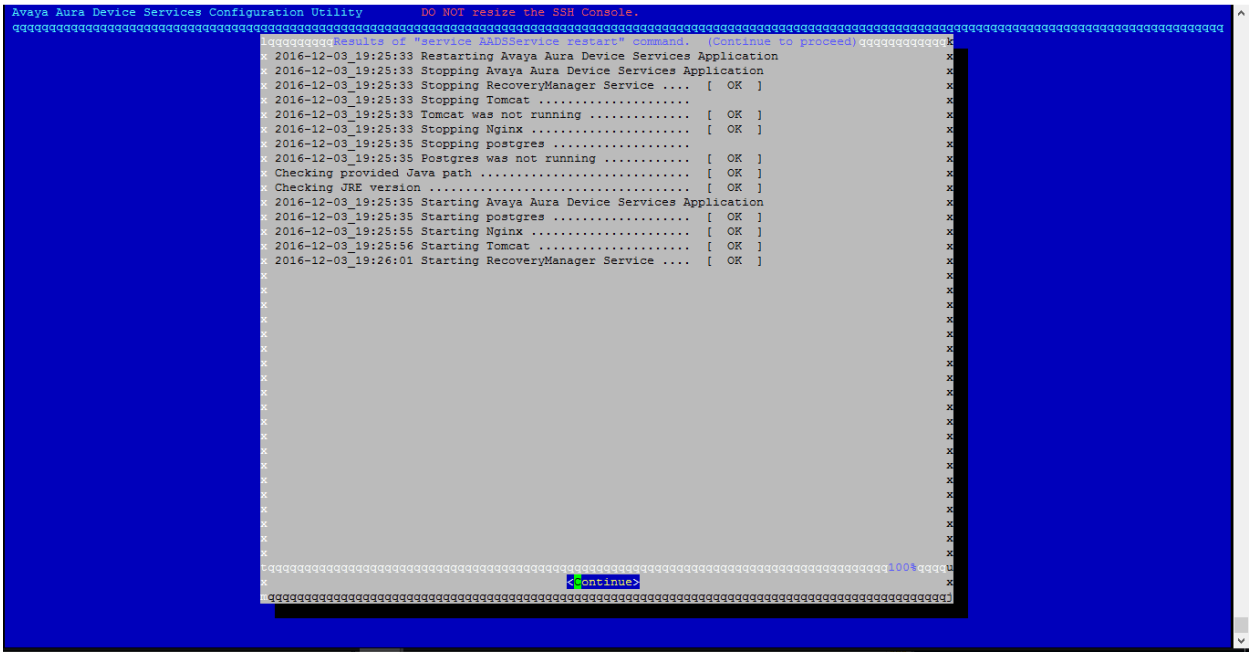


u. Press <Continue>.

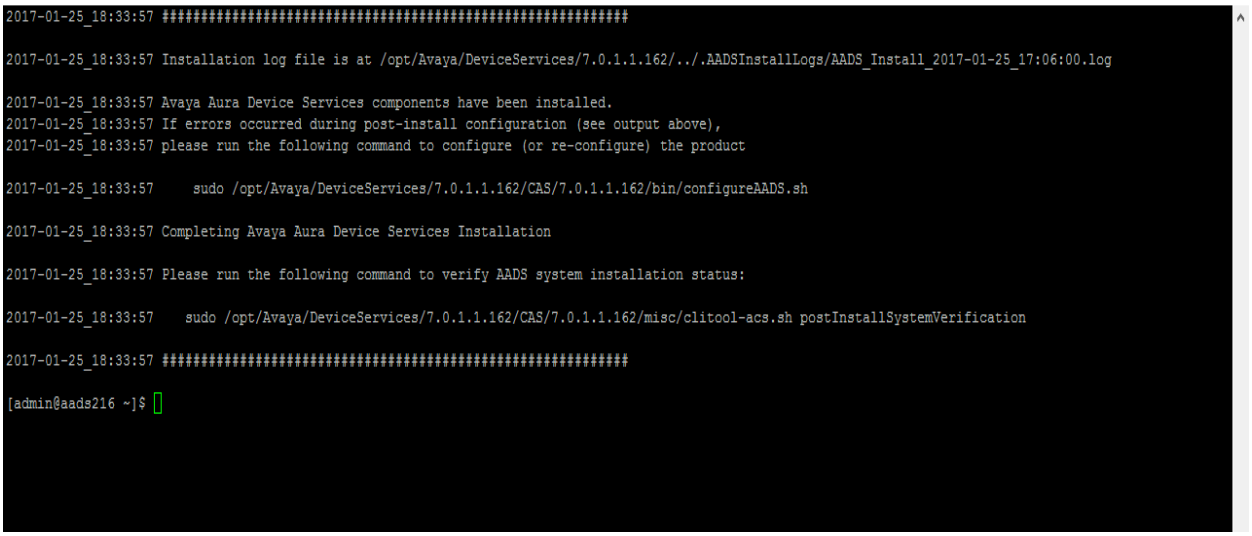


v. The installer prompts for AADS service restart. Press <Yes>.

w. Press <Continue>.

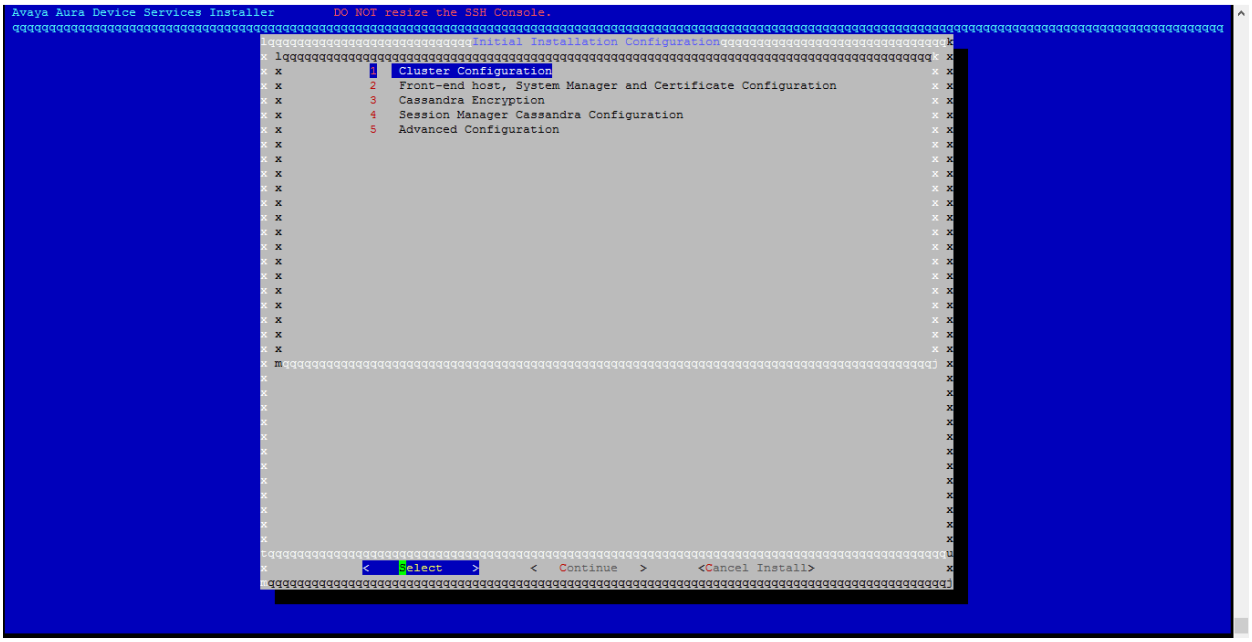


x. The Avaya Aura® Device Services installation is complete.

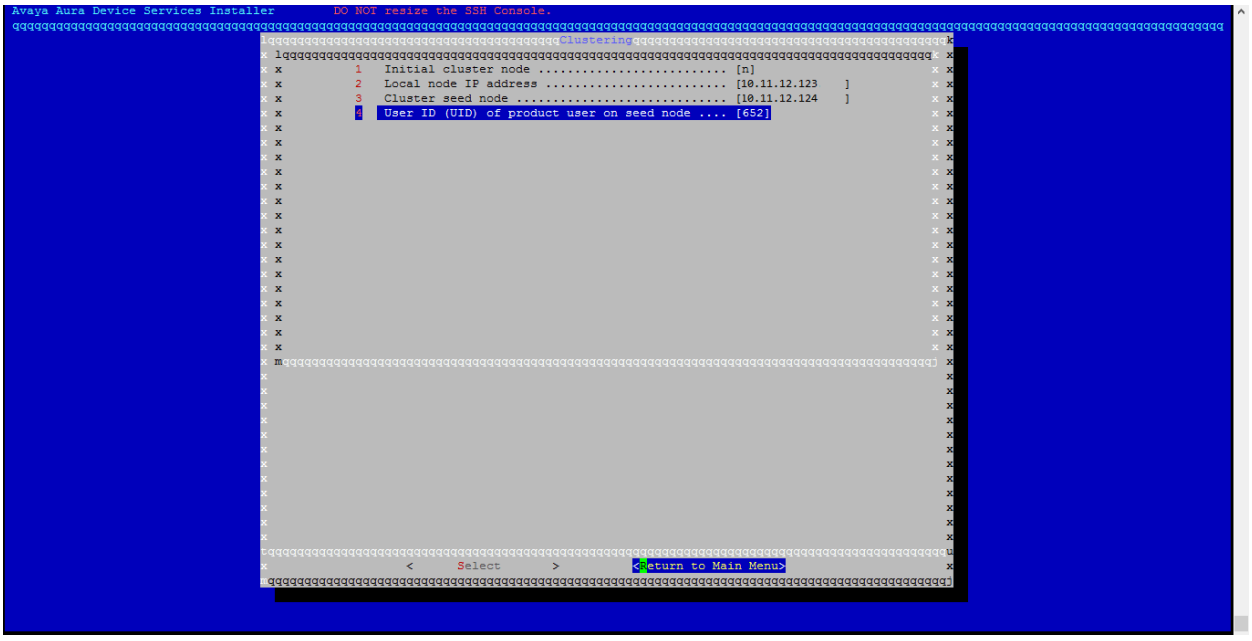


Installing other node

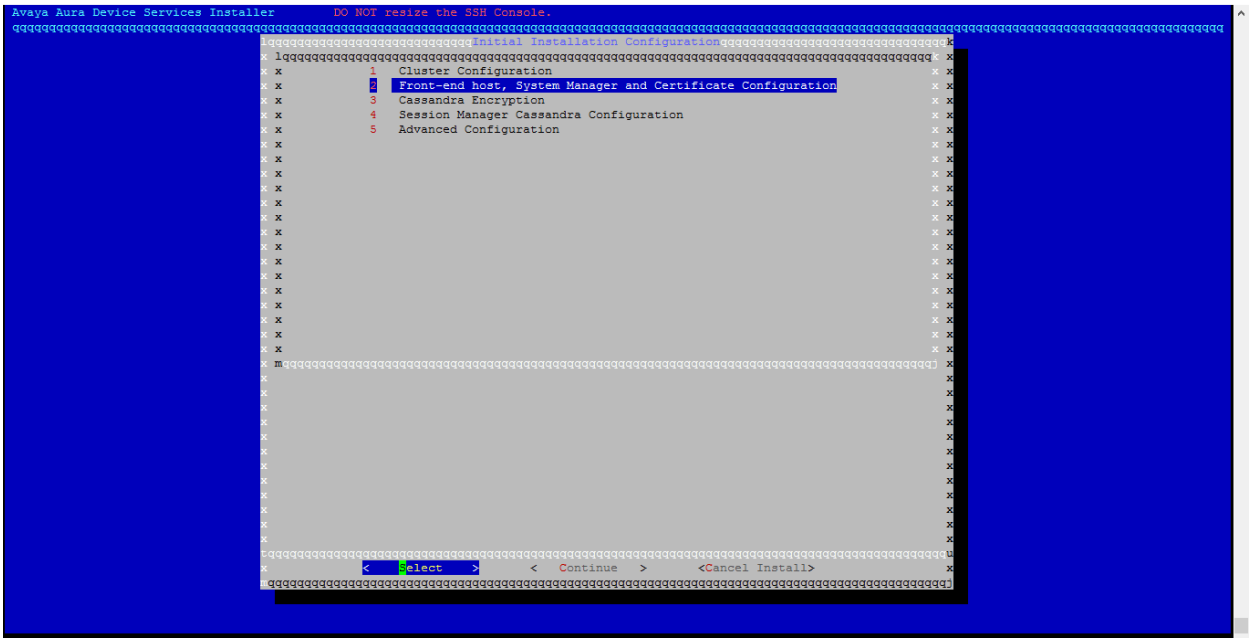
1. Go to the Avaya directory by using cd /opt/Avaya
2. Run the command **app install**
3. The system displays a blue installation tool.
4. Steps to be performed in the blue configuration tool:
    a. Cluster configuration



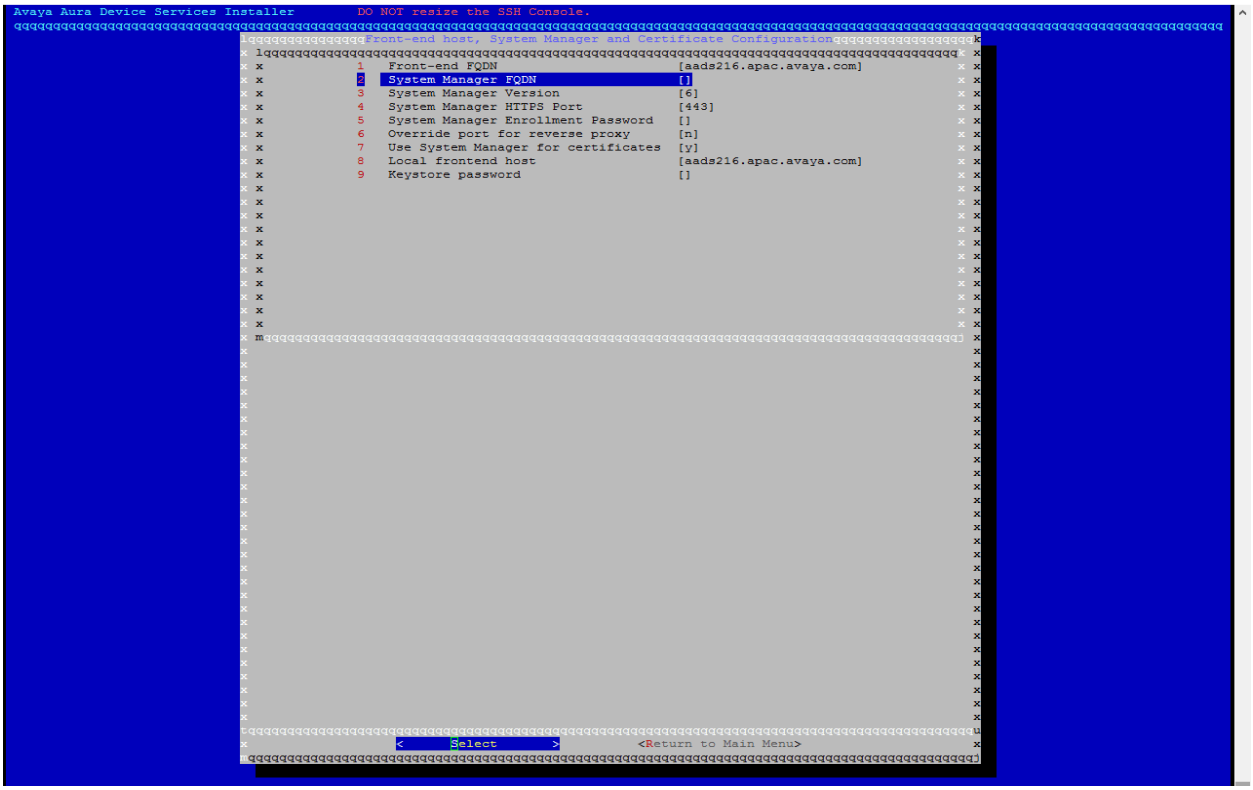
    b. Set Initial cluster node to [n]. Provide Cluster seed node IP. Press <Return to Main Menu>.



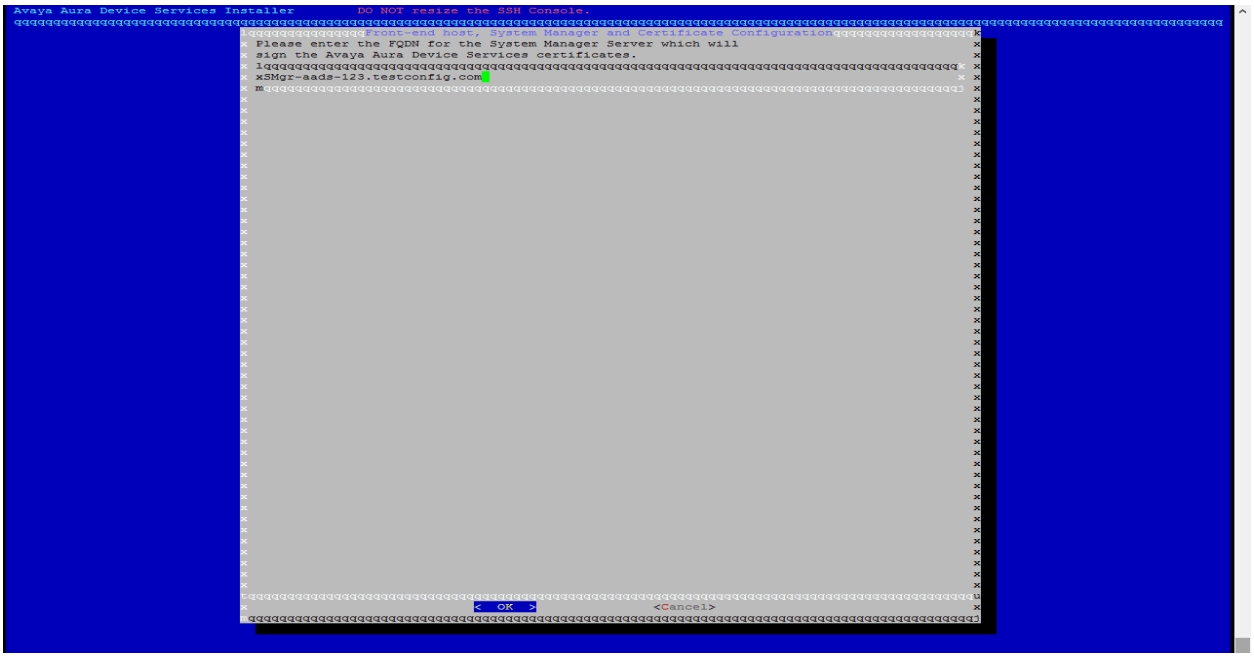
c. Front-end host, System Manager and Certificate Configuration.



d. Enter the System Manager details in this screen. Keystore password should be 6 or more characters. This should be same as the one provided on seed node.

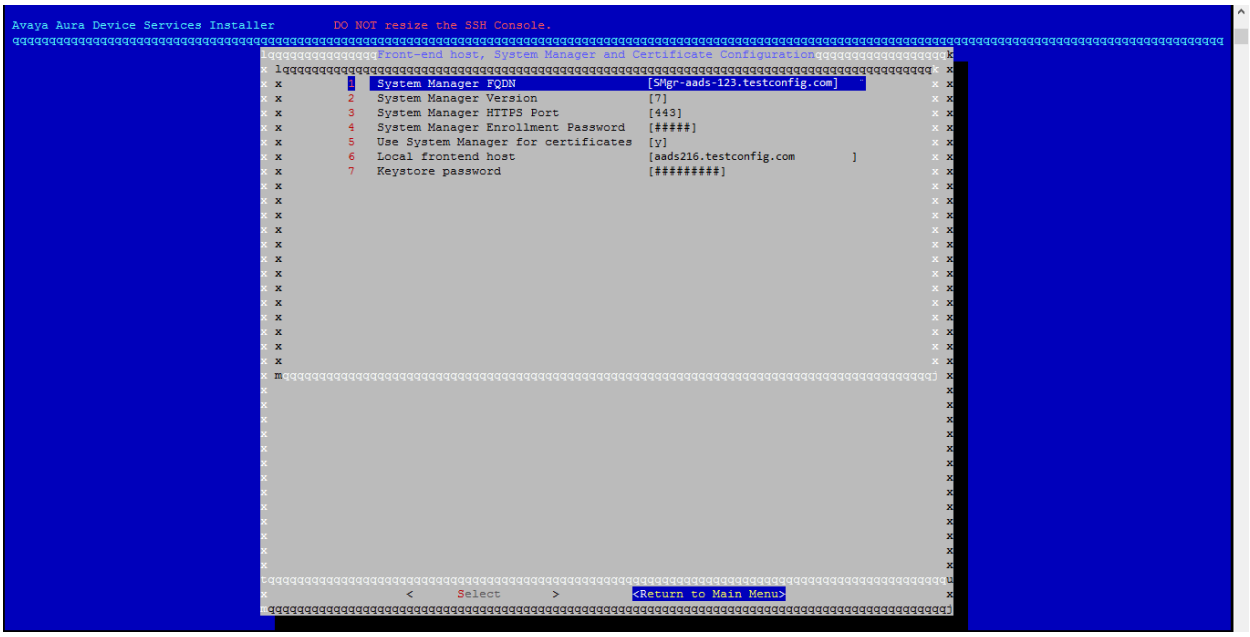


Enter SMGR FQDN and press **<OK>**. The installer will try to check if the provided hostname is valid or not.

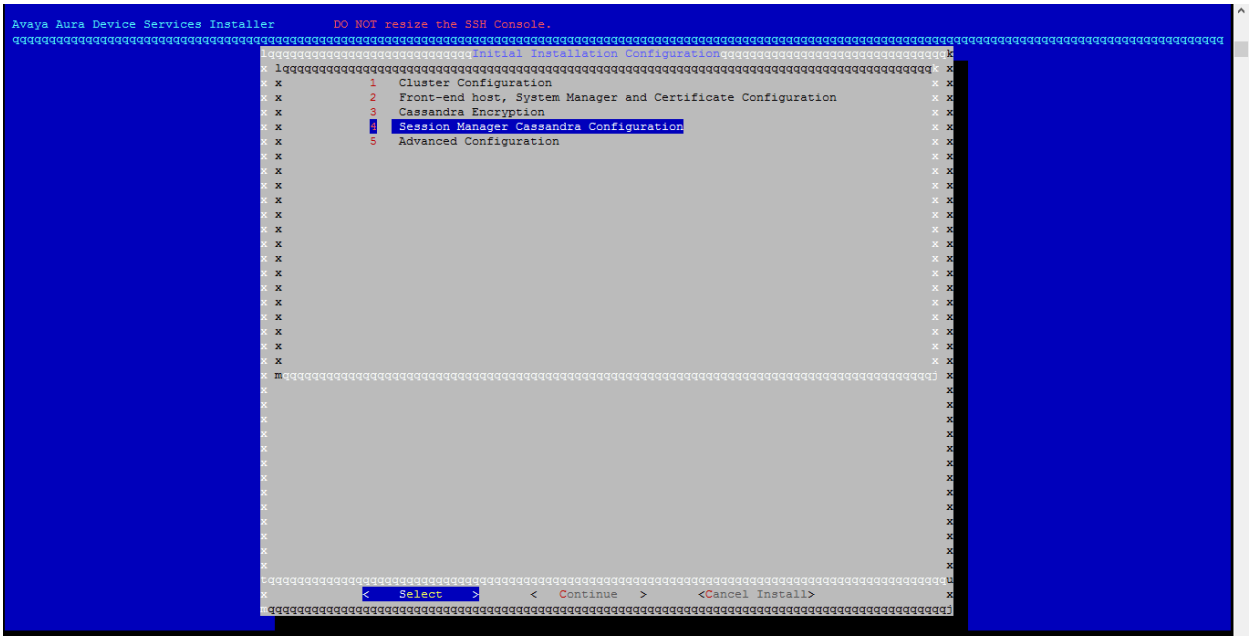


Press **<OK>**

e. After entering all the details <Return to Main Menu>.

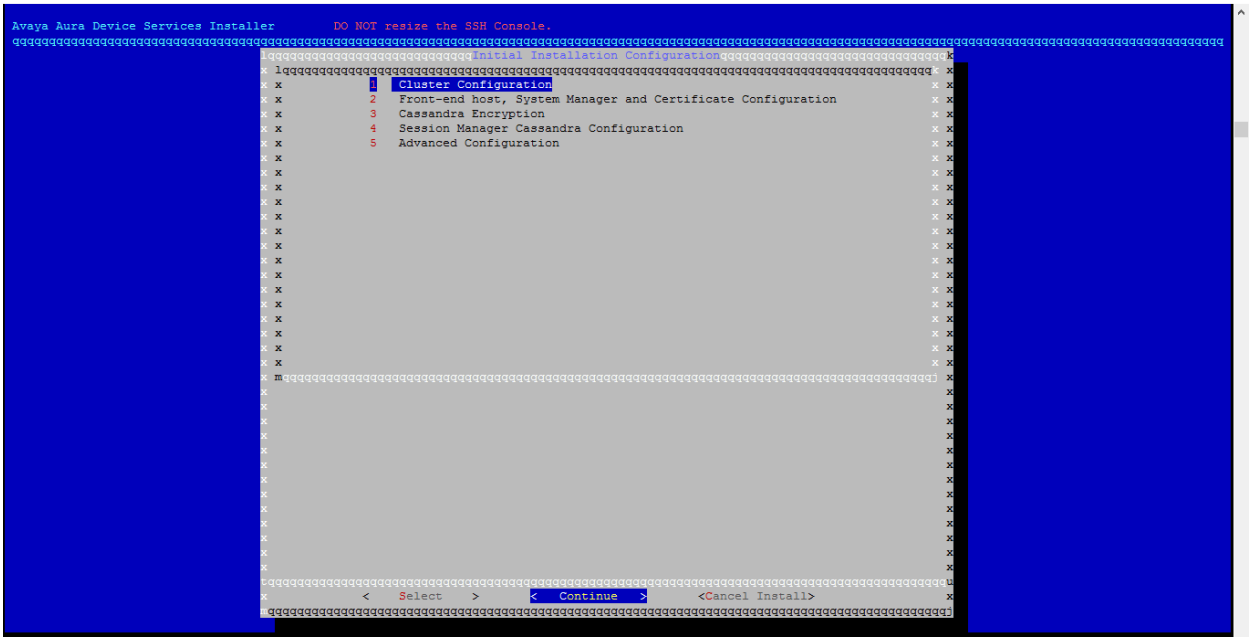


5. Session Manager Cassandra Configuration – Provide Session Manager Management and Asset IP here.

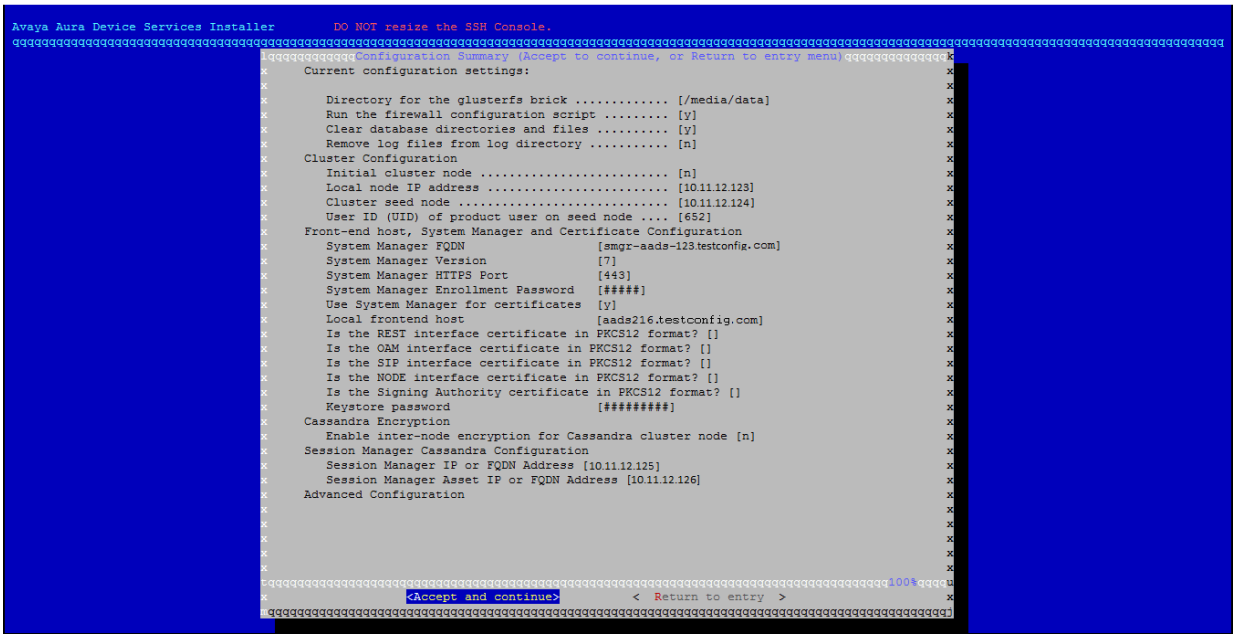



Avaya Aura Device Services Installer
DO NOT resize the SSH Console.
1 Session Manager IP or FQDN Address [10.11.12.125]
2 Session Manager Asset IP or FQDN Address [10.11.12.126]
< Select >
<Return to Main Menu>

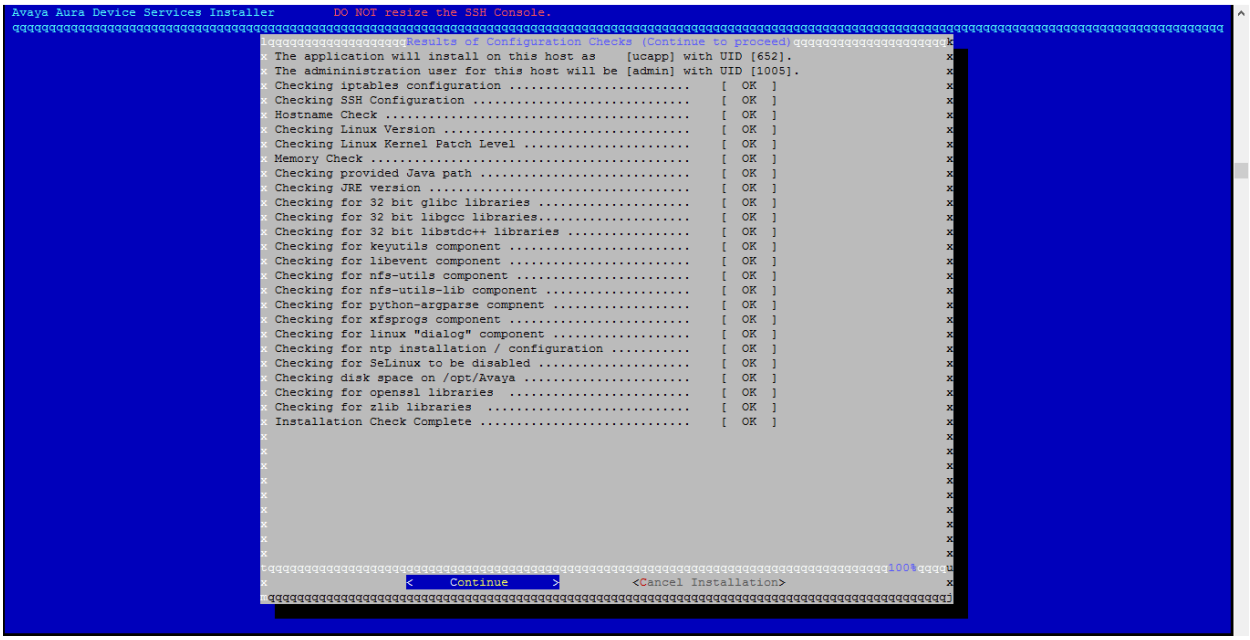
6. Leave Cassandra Encryption and Advanced Configuration unchanged. Press <Continue>.



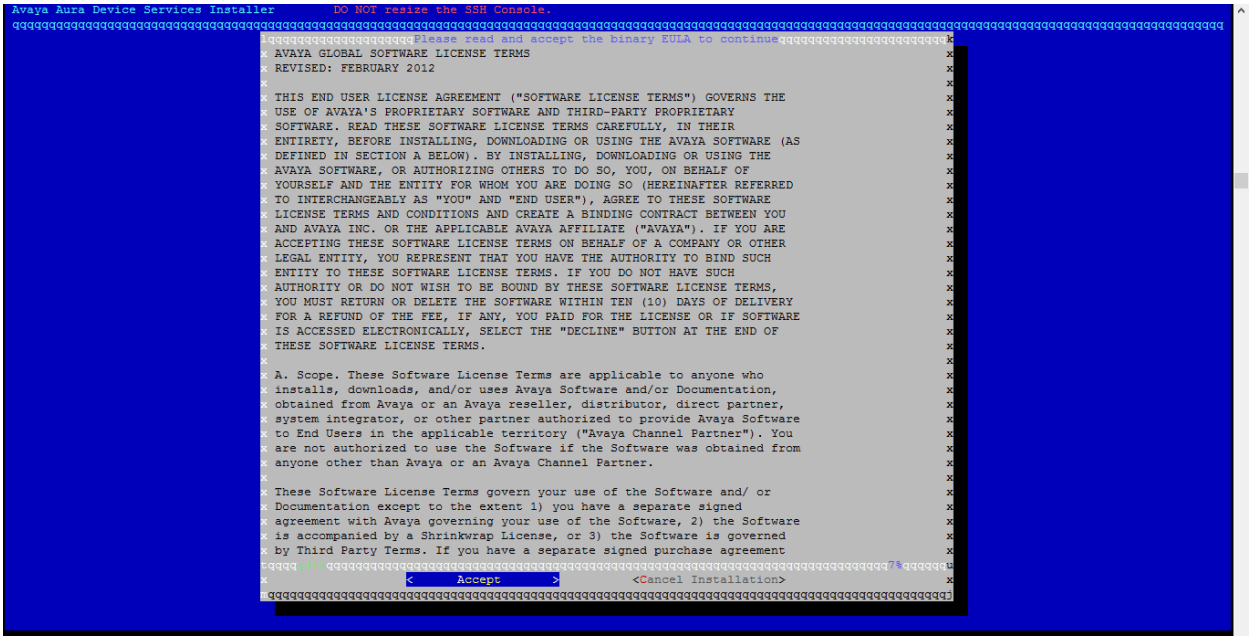
7. Check the values on the screen. Press <Accept and continue>.



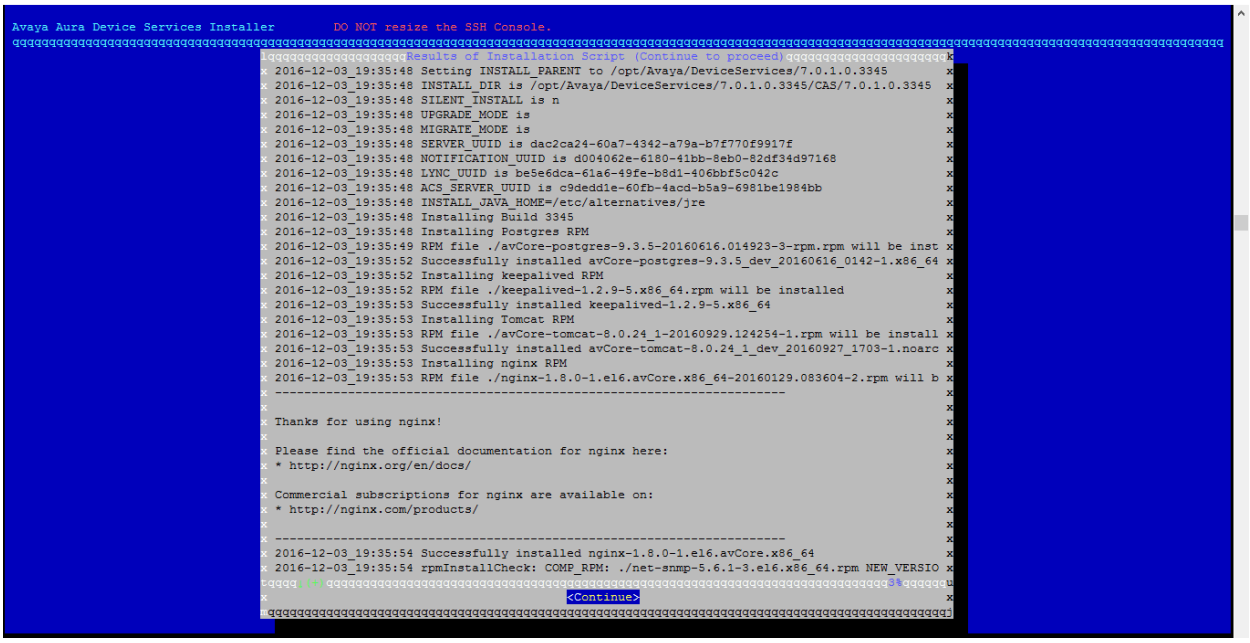
8. The installer will perform pre-install checks . Press <Continue>.



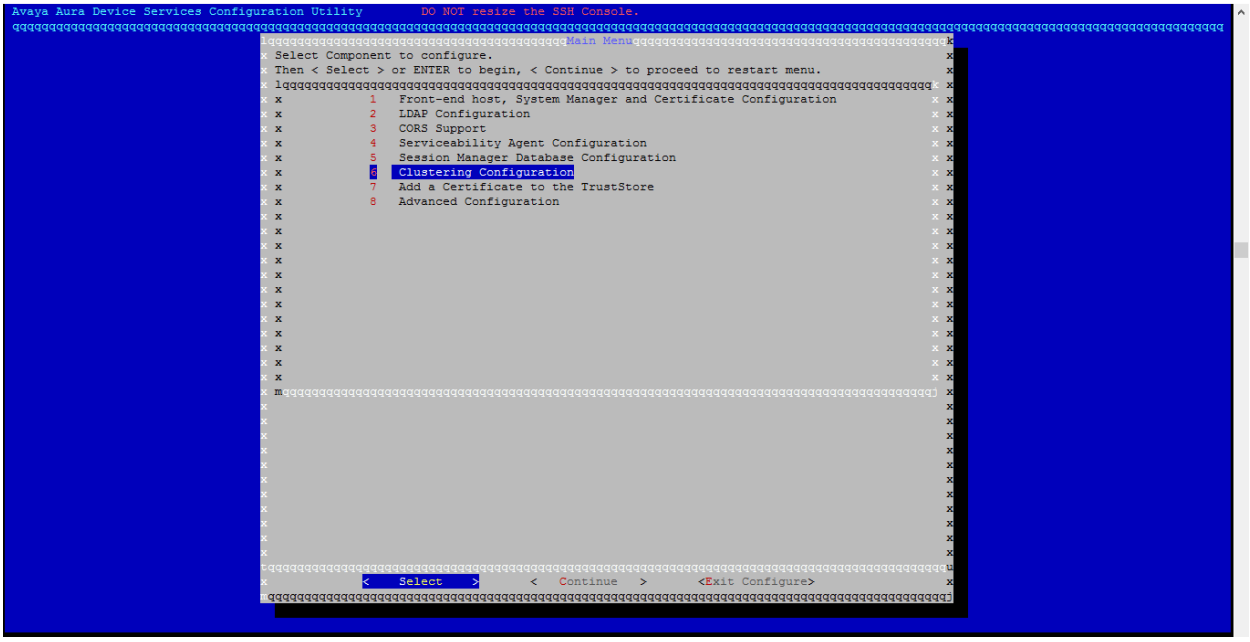
9. Press <Accept> to accept the EULA.



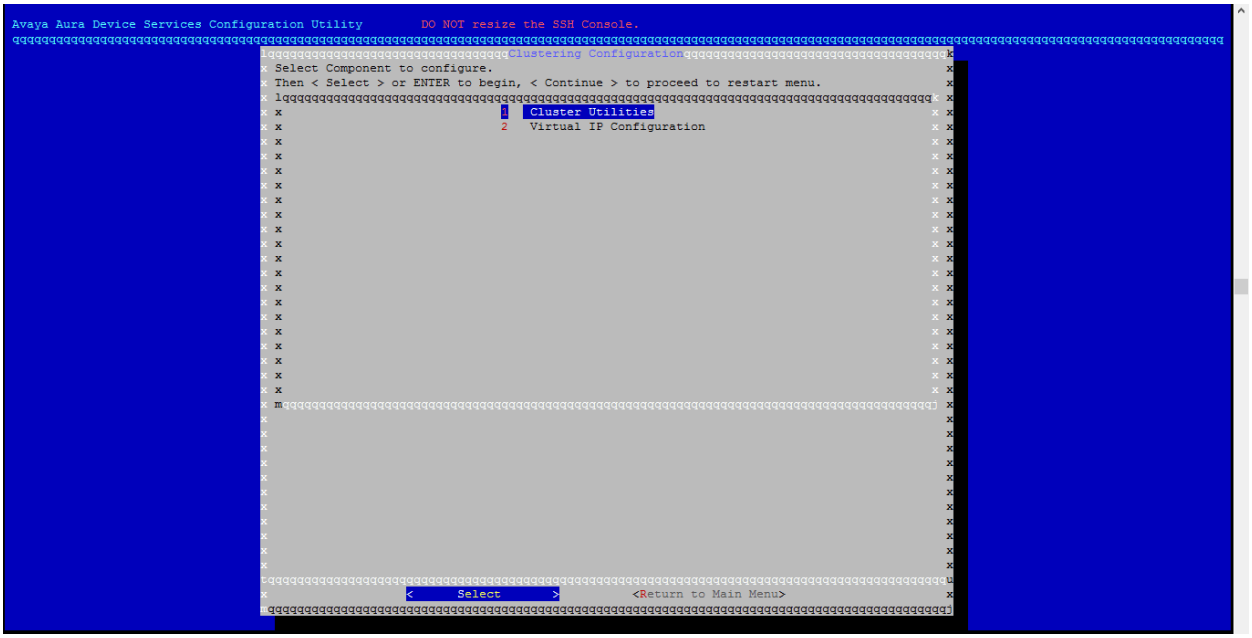
10. AADS installation will begin now. It will install the required RPMs, download certificates from System Manager and do the required initial configuration. The screen will show the progress.
11. Once this step is complete, below screen will be displayed. Press <Continue>.

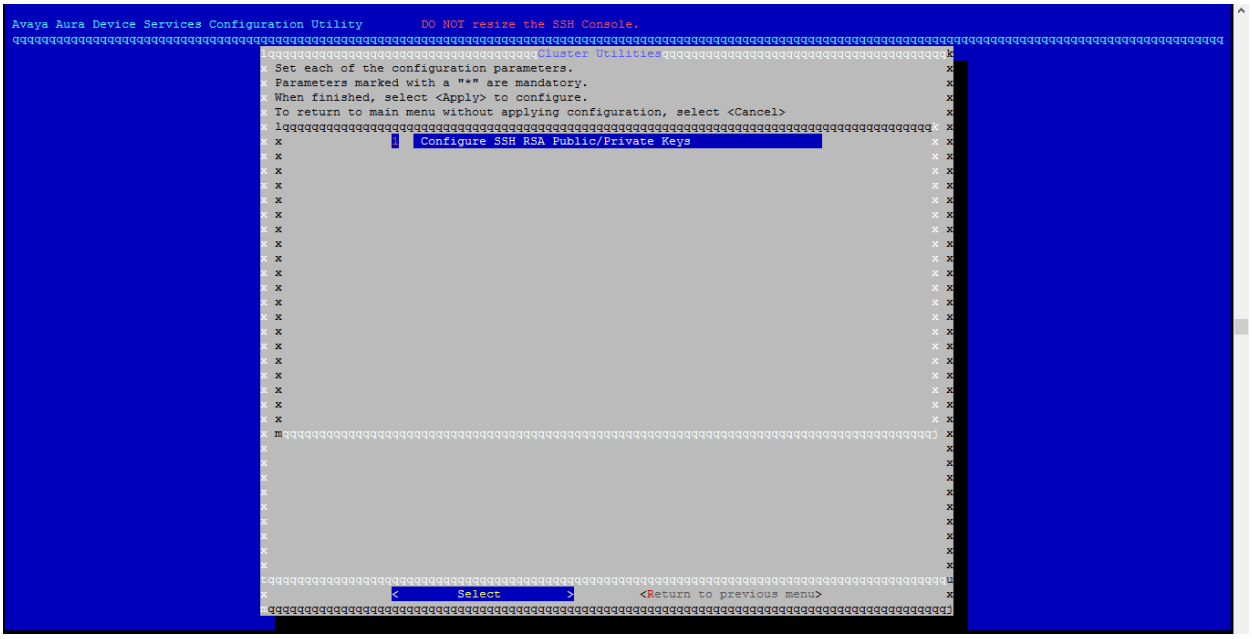


12. The below screen will be displayed. Go to Clustering Configuration menu.



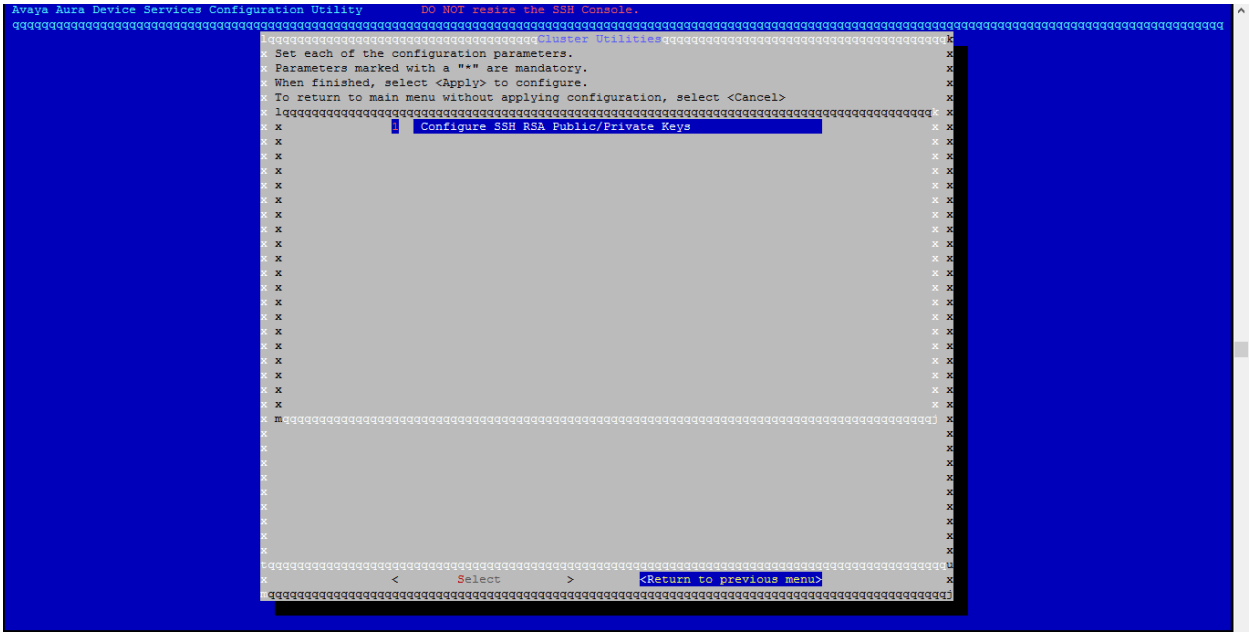
13. Go to Cluster Utilities to configure SSH RSA public/private keys.



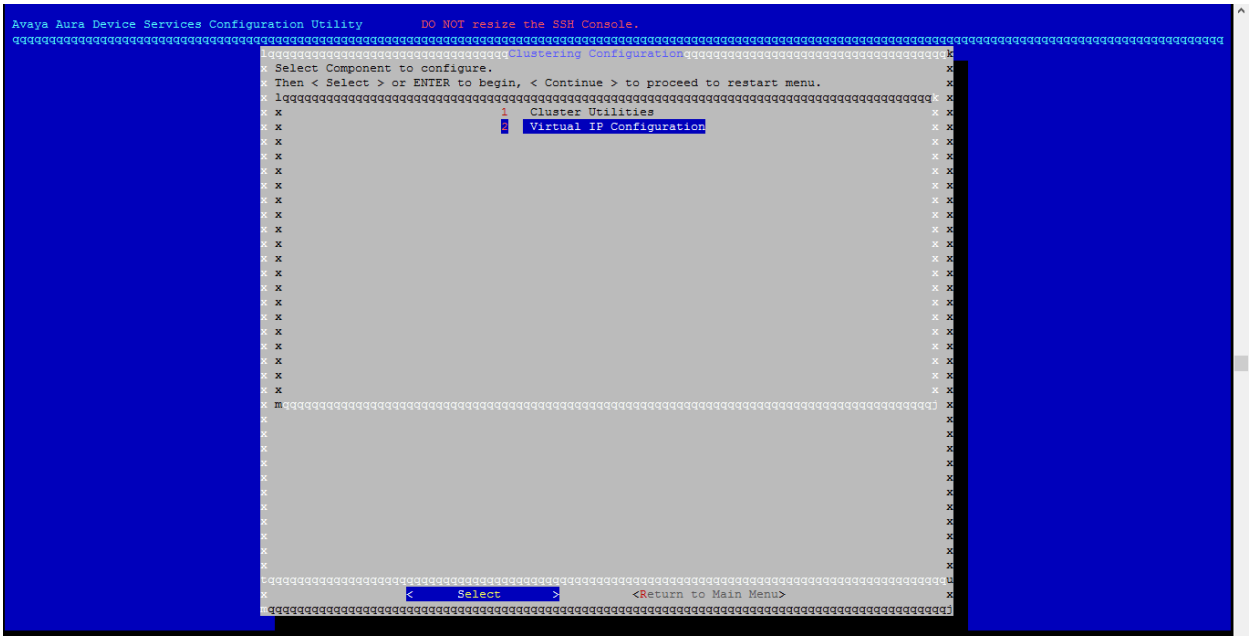


```
Add additional hosts to the list? (y/n) [n]: y
Enter a new host identifier using the syntax user@192.168.0.33 or user@server.abc.com
If the user name is omitted (e.g. just 192.168.0.33), it will be requested later.
When finished, enter a blank line by pressing the Enter key

Enter a new host identifier, blank when finished: 10.11.12.124
Enter a new host identifier, blank when finished:

User for 10.11.12.124 []: admin
2016-12-03_20:01:18 Hosts are:
2016-12-03_20:01:18 admin@10.11.12.124
2016-12-03_20:01:18 admin@10.11.12.123
2016-12-03_20:01:18 checking for existing private key
SSH RSA key exists, replace with a new one? (y/n) [n] y
2016-12-03_20:01:21 generating new private key due to request
2016-12-03_20:01:21 New key requested, generated new key
2016-12-03_20:01:21 Local Keys are at /home/admin/.ssh/id_rsa and /home/admin/.ssh/id_rsa.pub
2016-12-03_20:01:21 Configuring Remote User admin on Host 10.11.12.124
2016-12-03_20:01:21
2016-12-03_20:01:21 If or when prompted to "continue connecting", please enter "yes"
2016-12-03_20:01:21 When prompted for password, please enter password for admin@10.11.12.124
2016-12-03_20:01:21
The authenticity of host '10.11.12.124      (10.11.12.124)' can't be established.
RSA key fingerprint is bd:7d:62:ce:b0:09:aa:e2:81:c0:c2:8b:65:94:5a:10.
Are you sure you want to continue connecting (yes/no)? yes
Password:
Password:
2016-12-03_20:01:40 Configuring Local  User admin on Host 10.11.12.123
2016-12-03_20:01:40 Copying known_hosts file to User admin on Host 10.11.12.124
Password:
2016-12-03_20:01:48 Copying known_hosts file to User admin on Host 10.11.12.123
SSH RSA configuration is complete.  <Enter> to continue:
```

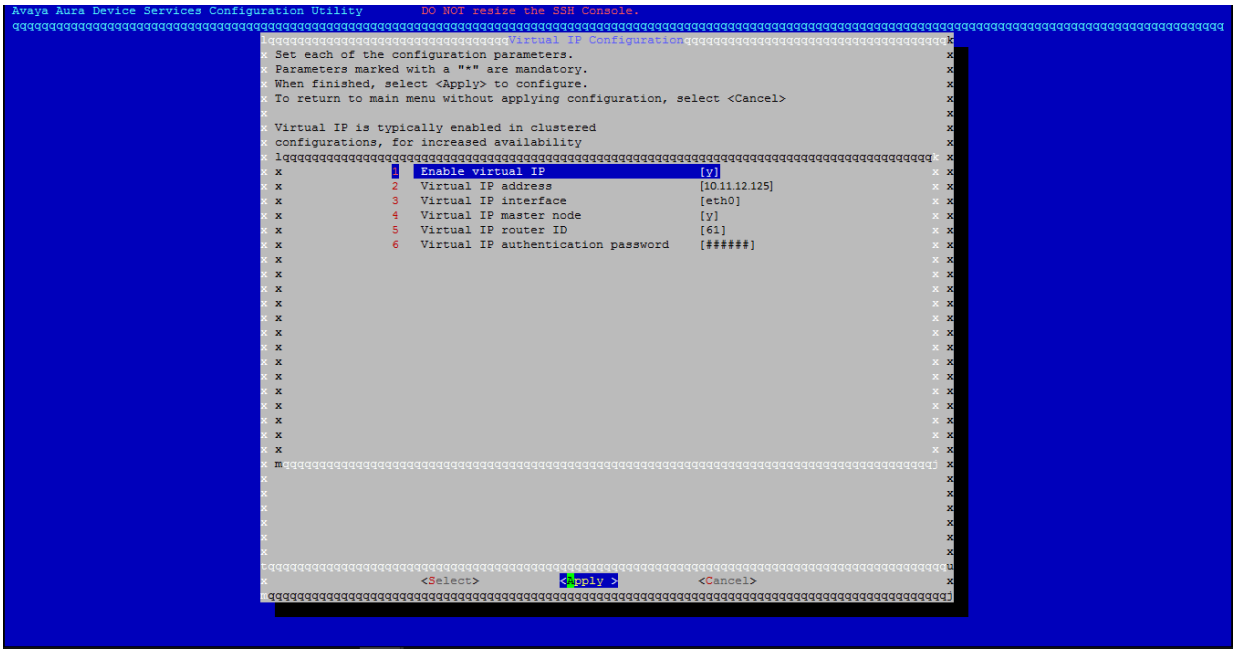
14. Press <Return to previous menu>.



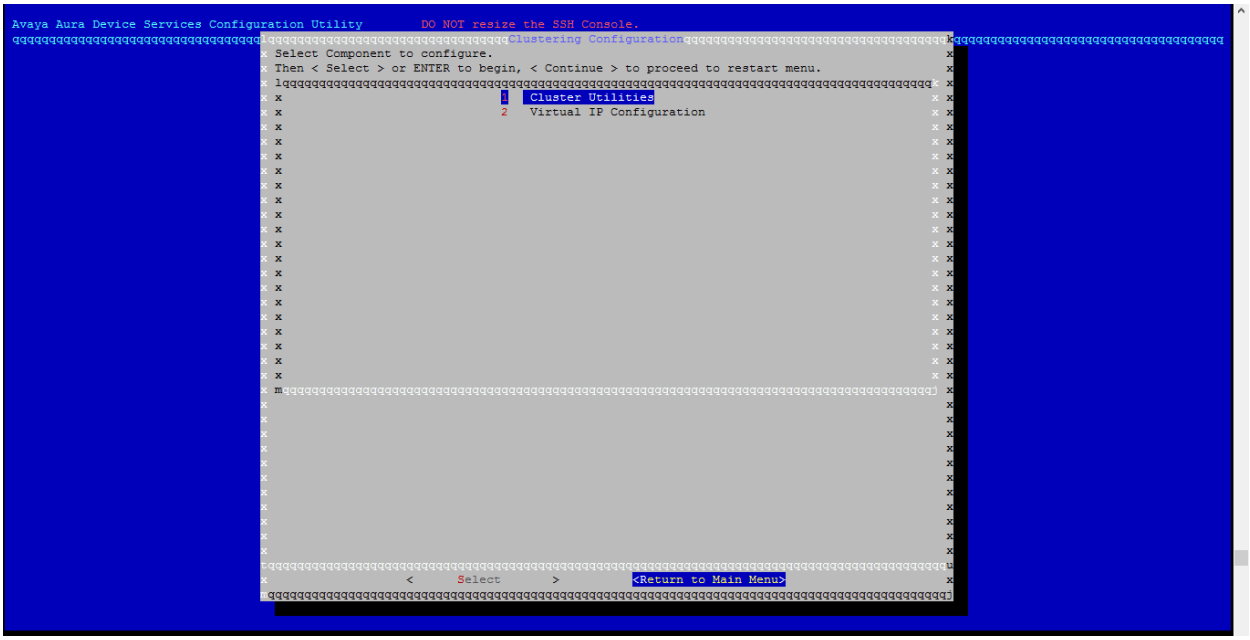
15. Go to Virtual IP Configuration.



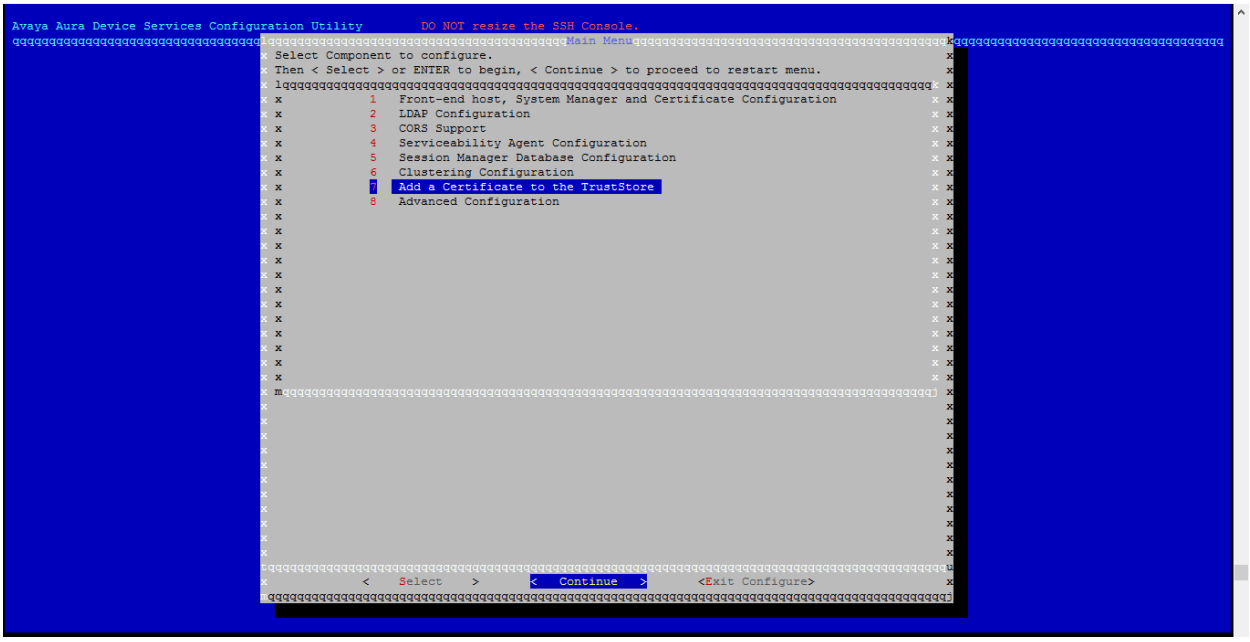
16. Enter virtual IP details and set Virtual IP master node to [n]. Virtual IP authentication password should be same as that on seed node. Press <Apply>.



17. Press <Return to Main Menu>.

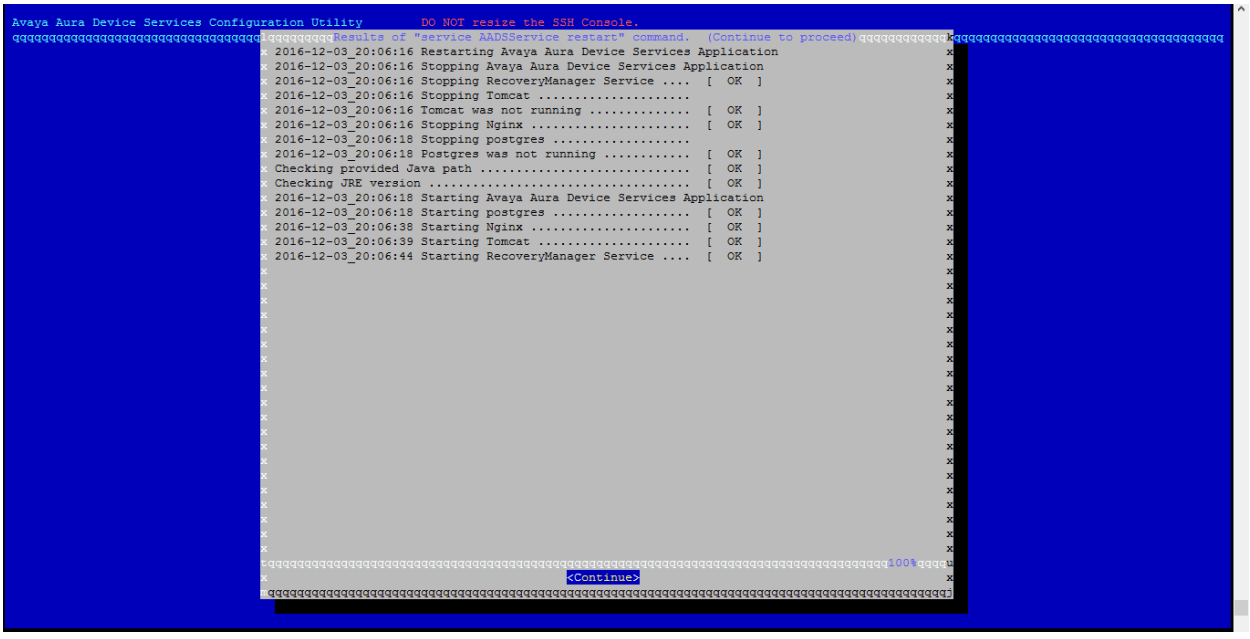


18. Press <Continue>.

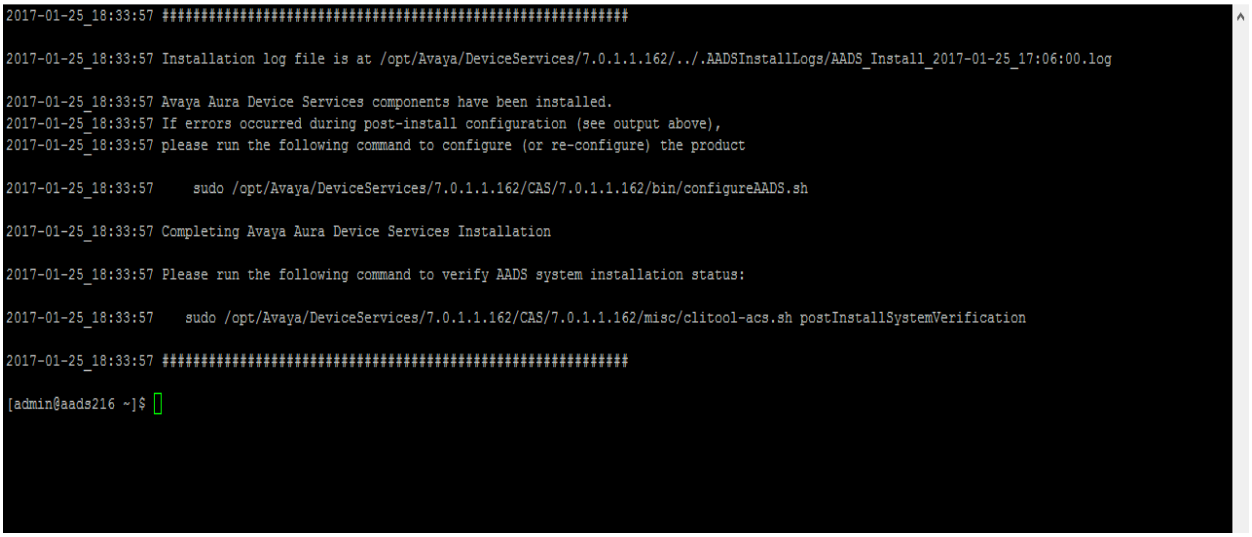


19. The installer will prompt for AADS service restart. Press <Yes>.

20. Press <Continue>.

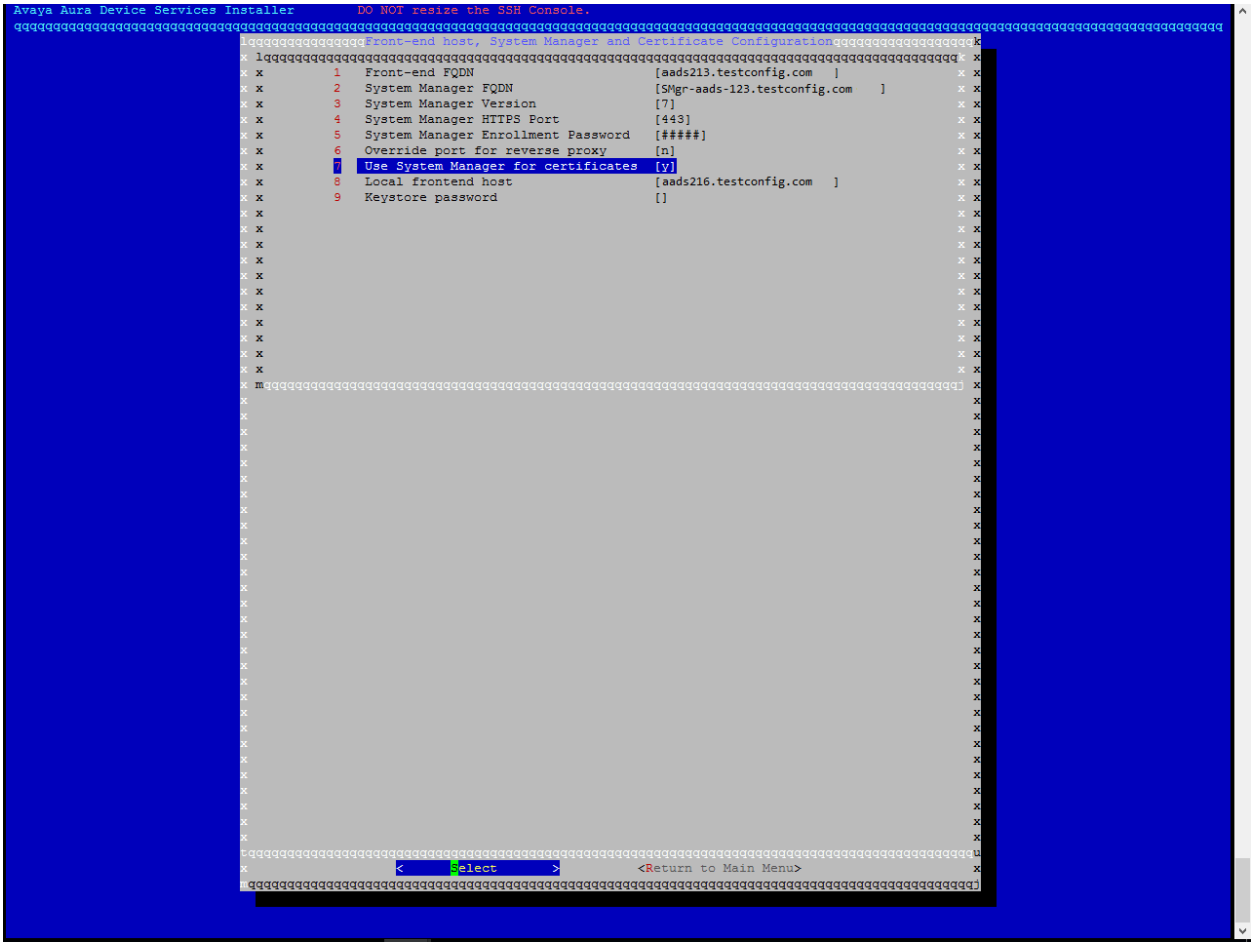


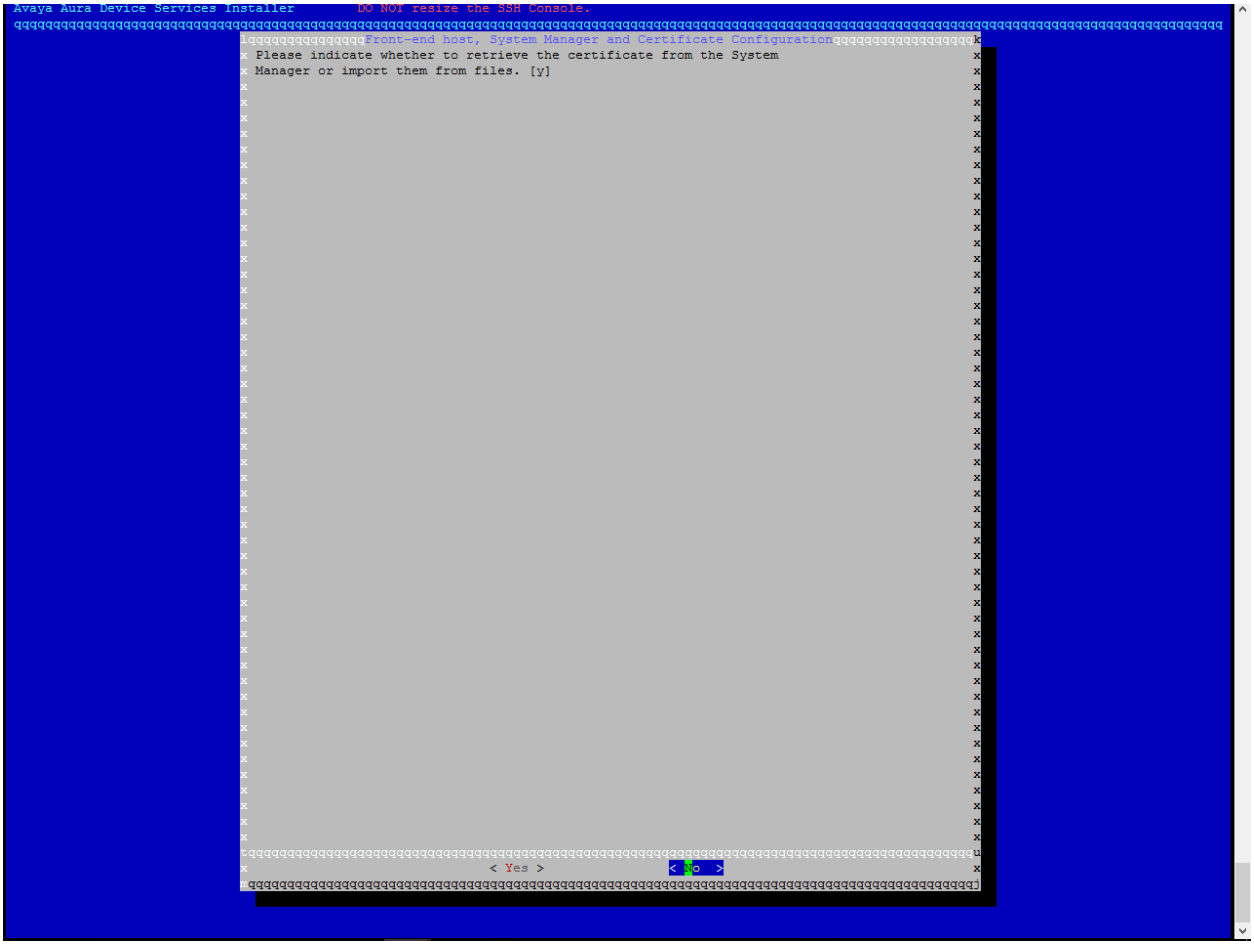
21. The Avaya Aura® Device Services installation is complete.



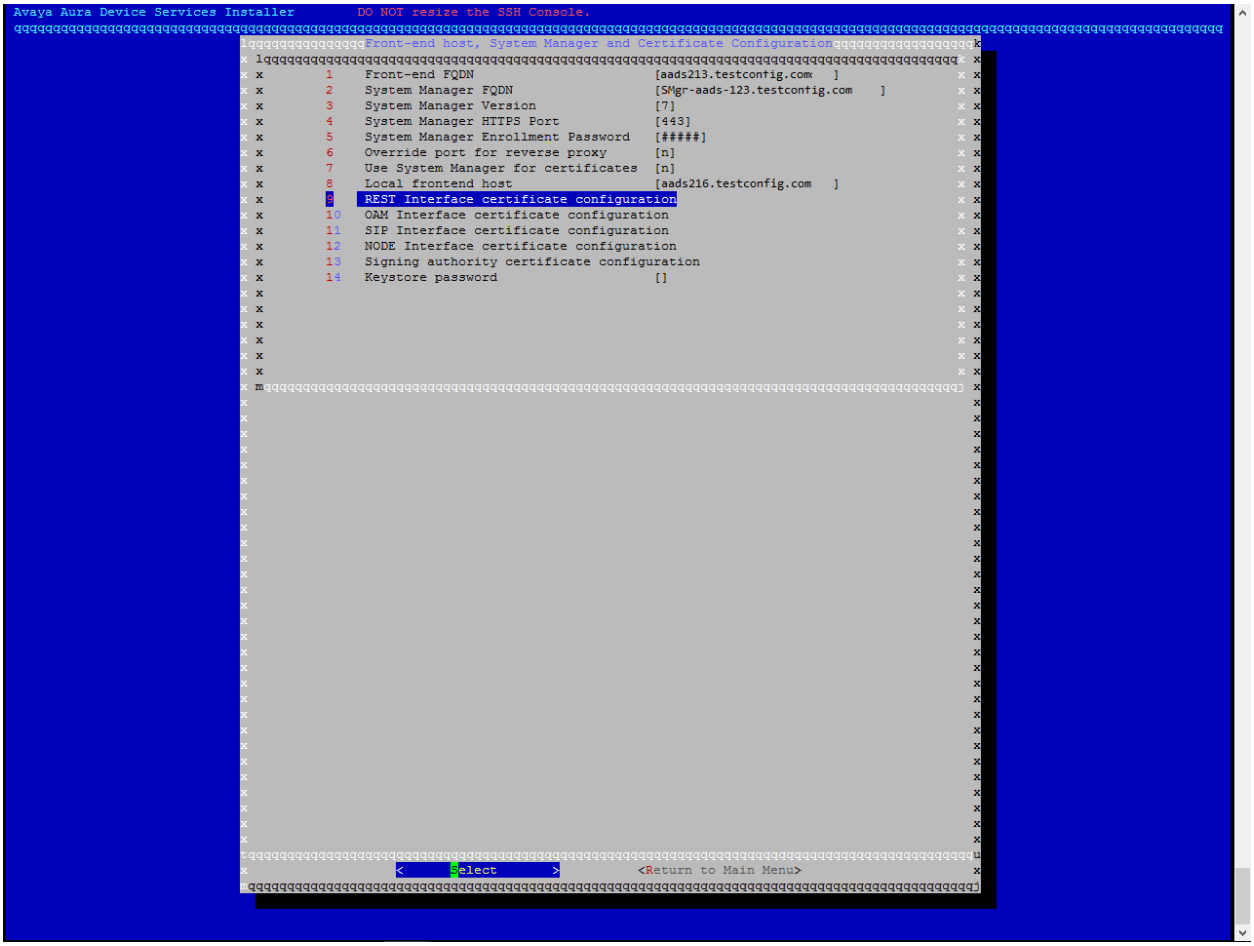
Configuring Certificates without System Manager

1. If System Manager is not being used for certificates, you need to import the certificate from files.
2. Go to “Use System Manager for certificates” menu and select <No>

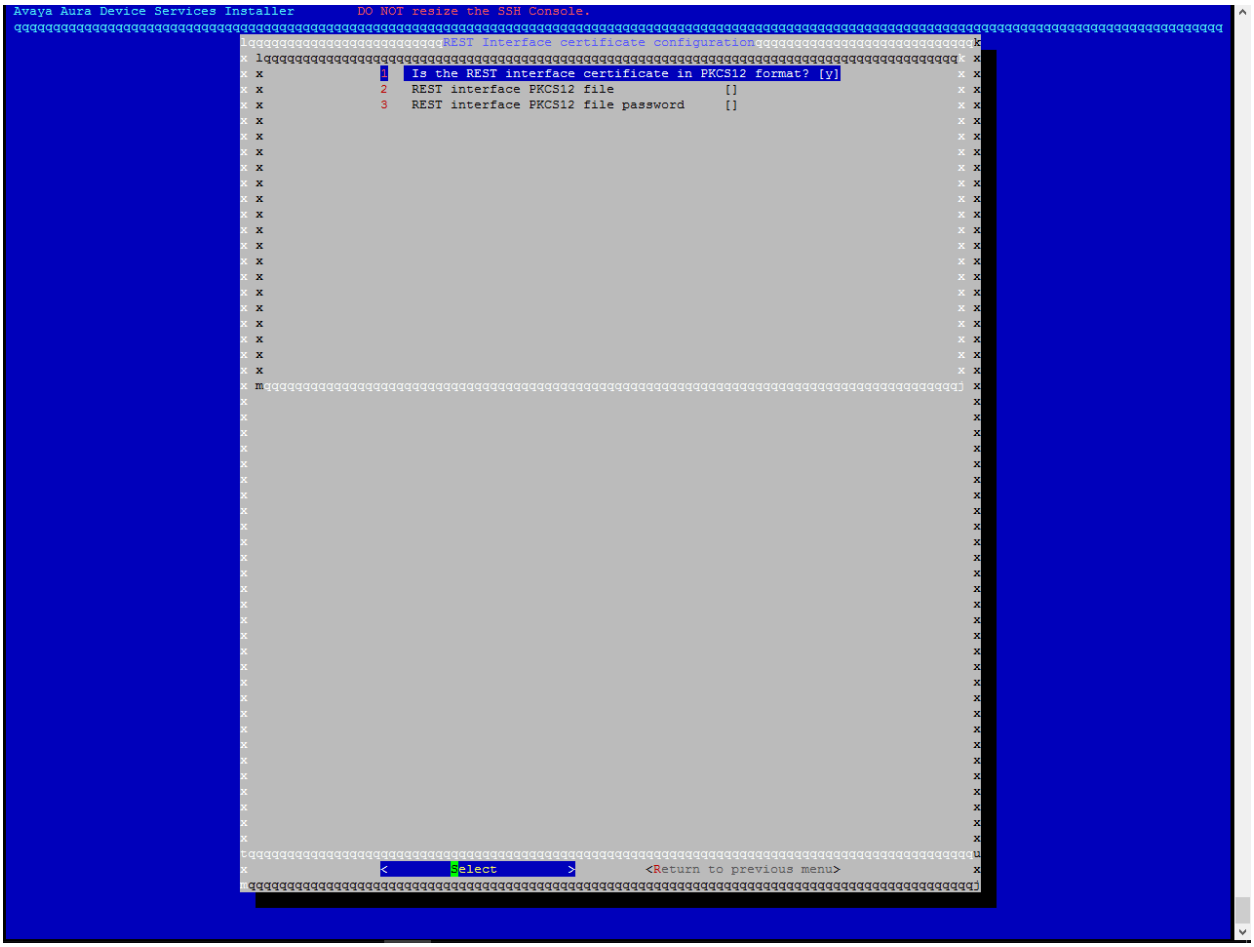


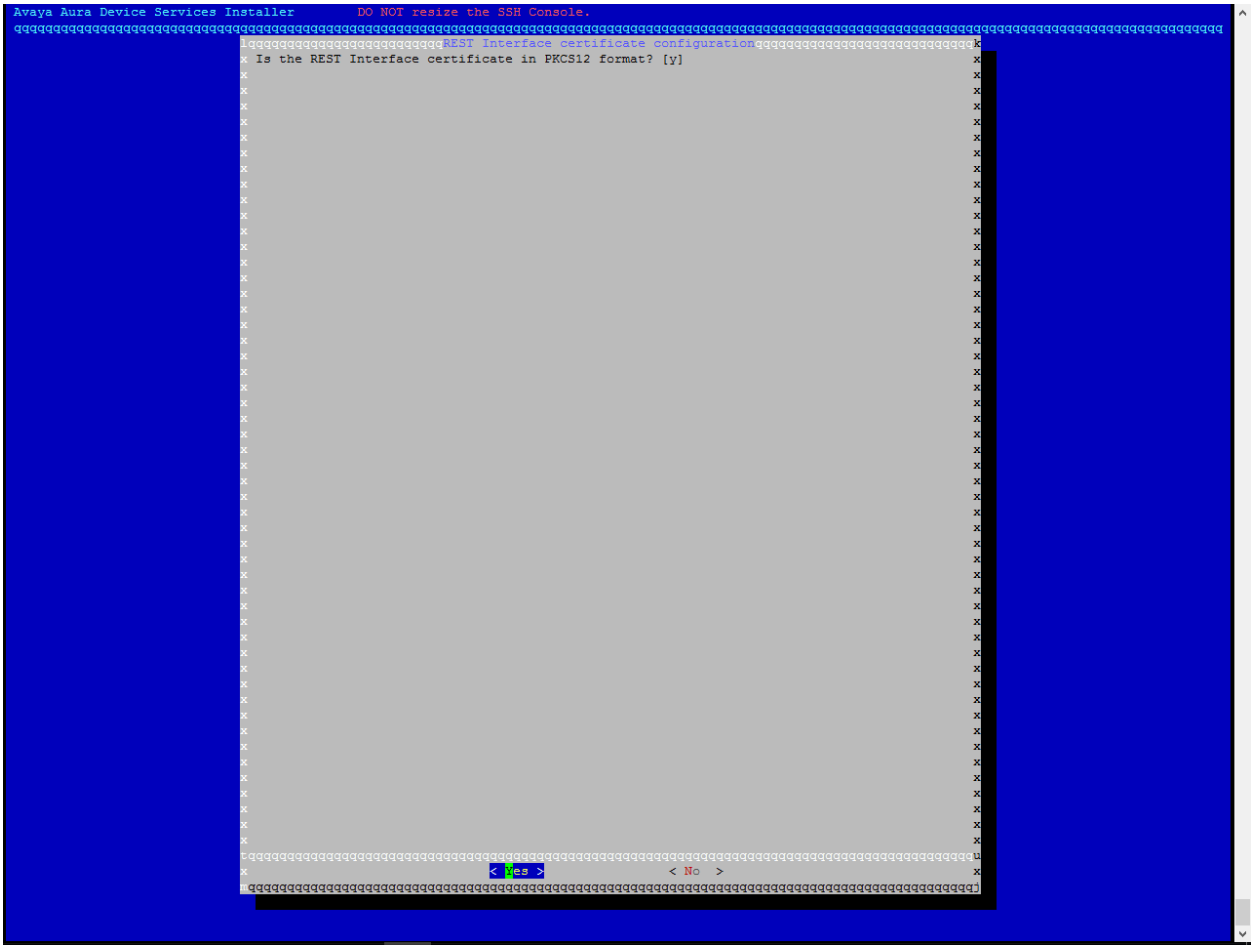

Avaya Aura Device Services Installer
DO NOT resize the SSH Console.
Front-end host, System Manager and Certificate Configuration
Please indicate whether to retrieve the certificate from the System Manager or import them from files. [y]
< Yes >
< No >

3. New menu items will be displayed (9 to 13) to provide a certificate file and import certificate.

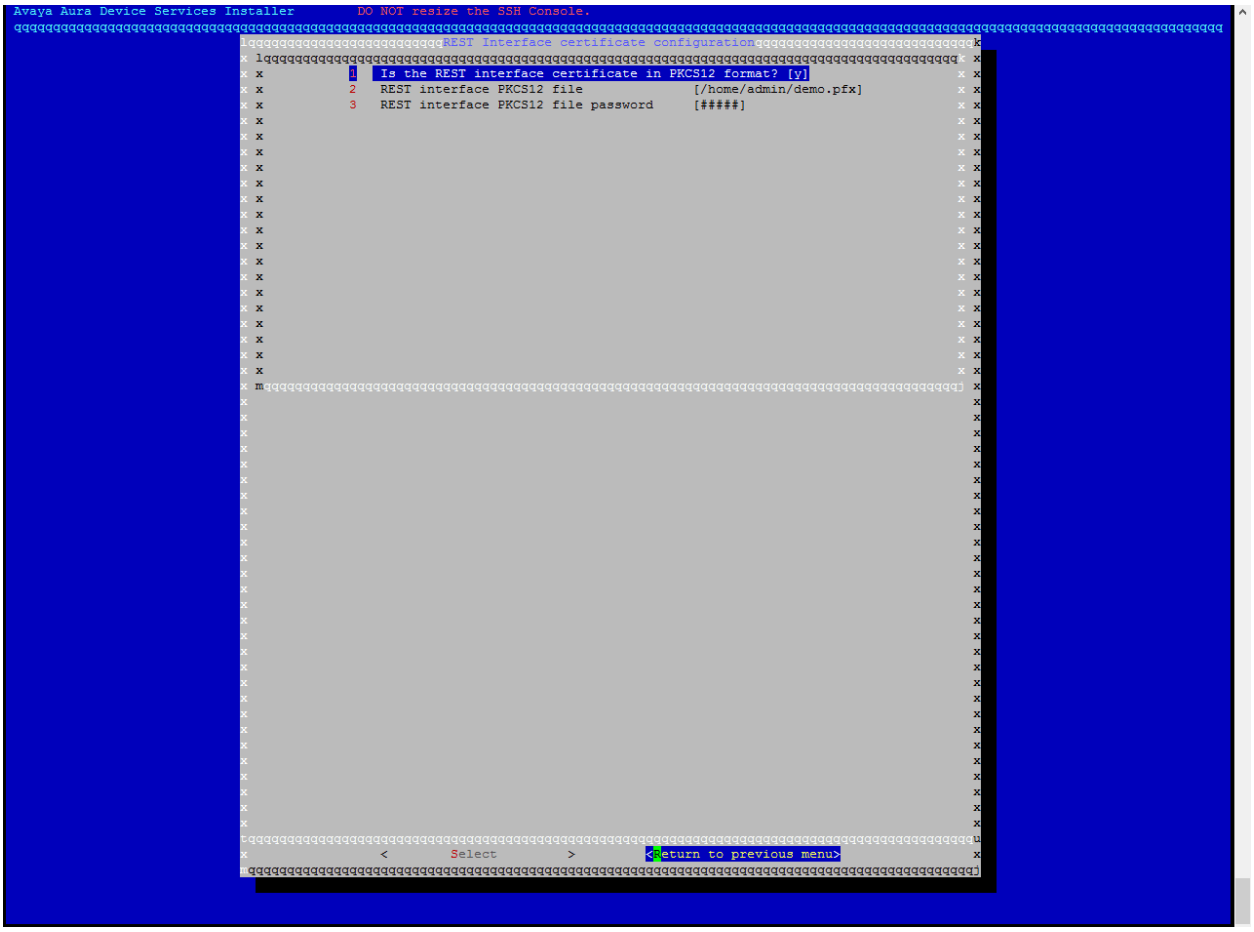


4. Select “Rest Interface certificate configuration” menu and provide the certificate file.

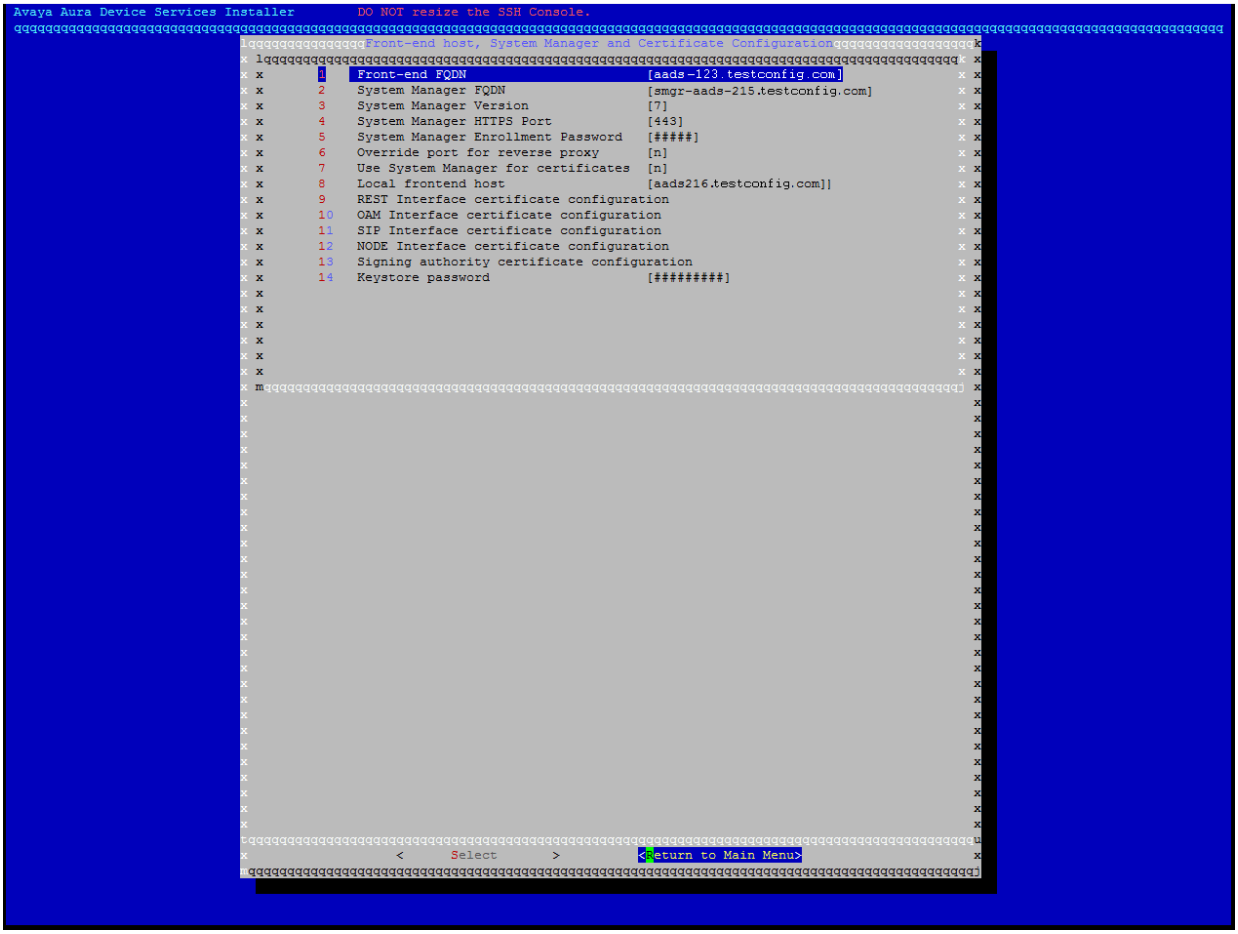



Avaya Aura Device Services Installer
DO NOT resize the SSH Console.
REST Interface certificate configuration
Is the REST Interface certificate in PKCS12 format? [y]
< Yes >
< No >

5. Provide the path of the certificate file, password and press <Return to previous menu>



6. Similarly provide the certificate configuration for remaining menu items (10-13) and press <Return to Main Menu>



Go back to Installation steps.