QUESTIONS & ANSWERS
Kill your exam at first Attempt

KILL EXAMS

Avaya

7130X

Avaya Aura Communication Applications Integration

QUESTION: 62
What are three ways of accessing Avaya Aura® Application Enablement Services (AES) to perform administration? (Choose three.)

A. with an Open X.11 terminal window
B. with web access
C. with remote access using Rlogin
D. with local access using a system console
E. with remote access using SSH

Answer: B, D, E

Explanation:
B: You can use a Web browser to access the Application Enablement Services Management Console (AE Services Management Console).
DE: Administrators can access the AE Services Linux shell (command prompt) either locally using a system console or remotely using a secure shell (ssh) client. This access method applies primarily to AE Services Technicians (craft users) who perform specific tasks, such as viewing trace logs, installing patches, and so forth.

References:
Avaya Aura® Application Enablement Services Administration and Maintenance Guide , page 52 https://downloads.avaya.com/css/P8/documents/100171737

QUESTION: 63
After running the Install wizard on Avaya Session Border Controller for Enterprise (SBCE), you added a Public outside IP address to the B1 interface. You try to ping this IP address from a PC in the same subnet but it falls. What would you do first to resolve the issue?

A. Restart Applications.
B. Set the Default Gateway router IP address, navigate to the Interfaces and Enable the B1 Interface.
C. Reboot SBCE.
D. Navigate to Device Specific Settings > Network Management > Interfaces and Enable the B1 interface.

Answer: D

Explanation:
The interface might need to be enabled.
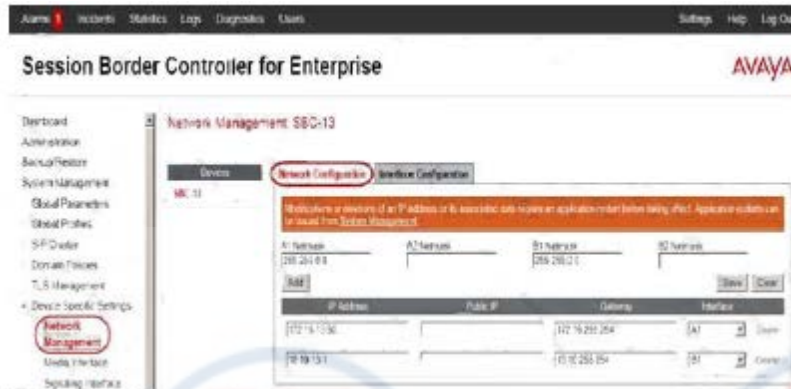
2. Click on the Interface Configuration tab.

3. Click the Toggle link for both the A1 and the B1 interfaces. The Administrative Status for both A1 and B1 changes to Enabled

References:
Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 204

QUESTION: 64
In Avaya Aura® Communication Manager (CM) for TSAPI, which type of CTI-link needs to be configured?

A. ASAI-IP
B. TSAPI-IP
C. ADJ-IP
D. DMCC-IP

Answer: C

Explanation:
The Avaya AES server forwards CTI requests, responses, and events between Invision CTI Server and Communication Manager. The Avaya AES server communicates with Communication Manager over an AES link. Within the AES link, CTI links may be configured to provide CTI services to CTI applications such as Invision CTI.
Step 1: Enter the display system-parameters customer-options command. On Page 3, verify that Computer Telephony Adjunct Links is set to y.
Step 2: Enter the add cti-link m command, where m is a number between 1 and 64, inclusive.
Enter a valid Extension under the provisioned dial plan in Avaya Communication Manager, set the Type field to ADJ-IP, and assign a descriptive Name to the CTI link. Etc.

References:
Application Notes for Invision CTI with Avaya Aura® Communication Manager and Avaya Aura® Application Enablement Services – Issue 1.0, page 6
https://www.devconnectprogram.com/fileMedia/download/edd26666-ae98-4f15-9a2a-a156d0807160

QUESTION: 65
Which statement about the SIP Entities to support Avaya Aura® Presence Services is true?

A. Only one SIP Entity is built of Type = "Presence Services", which uses the SM100 IP address of the Avaya Breeze™ node.
B. Only one SIP Entity is built of Type = "Engagement Development Platform", which uses the SM100 IP Address of the Avaya Breeze™ node.
C. Two SIP Entities are built to the same SM100 IP address of each node. One is of Type = "Engagement Development Platform", and the other is of Type = "Other".
D. Two SIP Entities are built to the same SM100 IP address of each node. One is of Type = "Engagement Development Platform", and the other is of Type = "Presence Services".

Answer: B

QUESTION: 66
To log on the one-X® Communicator to Avaya Aura® Presence Services server, what do you enter in the IM and Presence / Server field of the one-X® Communicator?

A. the management IP-Address of FQDN of Avaya Breeze™ server
B. the management IP-Address of FQDN of Avaya Aura® Session Manager (SM)
C. the SM100 IP-Address of FQDN of Avaya Aura® Session Manager (SM)
D. the SM100 IP-Address or FQDN of Avaya Breeze™ server

Answer: C

Explanation:
The SIP one-X Communicator needs to be configured to use a specific protocol and port when registering to Session Manager.Enter the IP address of the Session Manager virtual SM-100 card for Session Manager SIP Element.

References:
Application Notes for Configuring Avaya AuraTM Presence
Services 6.0 with Avaya AuraTM Session Manager 6.0, and Avaya AuraTM
Communication Manager for one-XTM Communicator clients as part of Avaya Unified
Communication Mobile Worker Solution – Issue 1.0, page 30
https://www.devconnectprogram.com/fileMedia/download/dba93412-03c6-4fda-8d6a-280ae2193d6f

QUESTION: 67
In which location is the AAMS URI 'ce-msml@avaya.com' configured?

A. Elements > Breeze > Configuration > HTTP Security and as a Regular Expression
B. Elements > Breeze > Configuration > HTTP Security and as a Dial Pattern
C. Home > Elements > Breeze > Configuration > Avaya Aura® Media Server and as a Dial Pattern
D. Home > Elements > Breeze > Configuration > Avaya Aura® Media Server and as a Regular Expression

Answer: D

Explanation:
Creating the Avaya Aura Media Server Routing Pattern Procedure
1. On System Manager, click Elements > Routing > Routing Policies.
2. Click New.
3. Type a Name for the Routing Policy.
4. From the SIP Entity as Destination field, click Select.
5. Select the Avaya Aura®
Media Server SIP Entity that you created.
Select the Local Host Name FQDN SIP Entity if you are using High Availability for the Avaya Aura® Media Server routing.

6. Click Commit.
7. Navigate to Home > Elements > Routing > Regular Expressions and click New.
8. In the Pattern field, type ce-msml@<sip-domain>.* This sip-domain value must match:
• The SIP domain that you entered in the Home > Elements > Routing > Domains page.
• The default SIP domain that you entered on the Avaya Breeze™ Cluster Administration page.
9. Click Commit https://downloads.avaya.com/css/P8/documents/101014426

References:
Deploying Avaya Breeze, Release 3.1, (September 2016), page 55

QUESTION: 68
In Avaya Aura® Messaging 6.3, which statement is true about Avaya Aura® Messaging (AAM) capacities of a system utilizing the Standard Capacity (non-High Capacity) Message Store template?

A. One Message Store Server supports up to 60000 user mailboxes and you can have 5 active + 1 Redundant Application Servers in a cluster.
B. One Message Store Server supports up to 6000 user mailboxes and you can have 3 active + 1 Redundant Application Servers in a cluster.
C. One Message Store Server supports up to 600 user mailboxes and you can have 5 active + 1 Redundant Application Servers in a cluster.
D. One Message Store Server supports up to 1000 user mailboxes and you can have 3 active + 1 Redundant Application

Answer: B

Explanation:
Dedicated AxC/Directory server: A physical server that manages notification capabilities and the LDAP database and provides communications between application servers and the thirdparty storage server. This server also stores user properties and name and greeting recordings.
Not all configurations require a dedicated AxC/Directory server because the AxC/Directory role runs on the Avaya- provided message store. You only need a dedicated AxC/Directory server for:

References:
Avaya Aura® Messaging Overview and Specification, Release 6.3.2 (January 2015) , page 20 https://downloads.avaya.com/css/P8/documents/101004642

QUESTION: 69

How many Server Flows and/or Subscriber Flows are required for SIP Trunking?
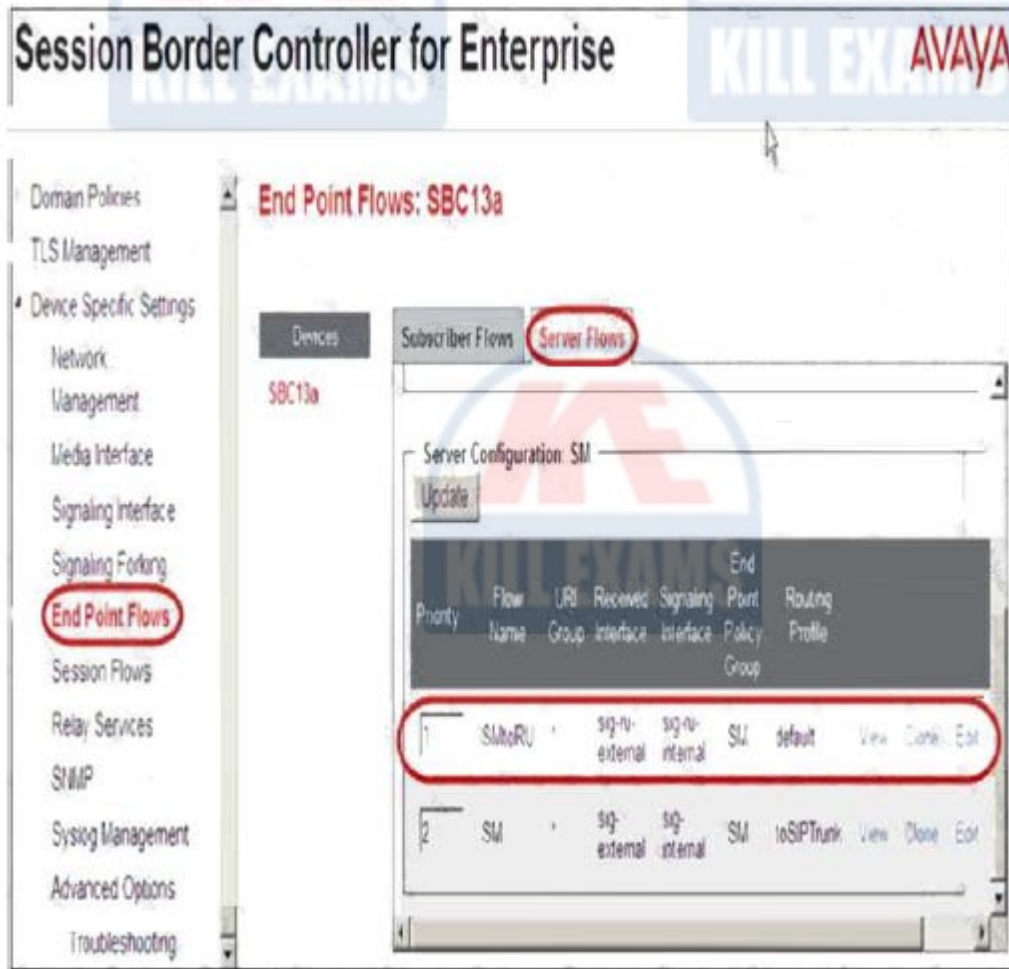
A. one Subscriber Flow and two Server Flows
B. a minimum of two Subscriber Flows
C. one Subscriber Flow and one Server Flow
D. a minimum of two Server Flows

Answer: A

Explanation:
Two types of flows need to be defined for the proper routing of SIP messages from and to the endpoints and the SIP server.
Example, Server Flows:

References:
Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 540, 546

QUESTION: 70

To allow trust between Avaya Aura® System Manager (SMGR) and Avaya Aura® Messaging (AAM), there is a password set when you add the Trusted Server on AAM. This password must match with the password also configured in SMGR.
Which statement about the password in SMGR is true?

A. It needs to match the Enrollment Password.
B. It needs to match the admin password used to login to SMGR using a web browser.
C. It needs to match the Attributes of the Messaging Managed Element in the Inventory.
D. It needs to match the root password used to login to SMGR command line.

Answer: C

Explanation:
Configuring Messaging in the normal operational mode Before you begin
* Add both the primary and secondary servers as Trusted Servers in the Messaging system.
* Update the Login, Password, and Confirm Password fields with the appropriate trusted server defined on the Messaging system.
Procedure
1. Log on to the Messaging system that System Manager manages.
2. Add the secondary System Manager server as Trusted Servers in the Messaging system.
3. Log on to the secondary System Manager server.
4. On the System Manager web console, click Services > Inventory.
5. In the left navigation pane, click Manage Elements.
6. On the Manage Elements page, select the Messaging system that you want to change to the secondary System Manager server.
7. Click Edit.
8. On the Attributes tab, fill the Login, Password, and Confirm Password fields with the corresponding name and password of the Messaging trusted server.
9. Click Commit.
10. Click Inventory > Synchronization > Messaging System, and select the required Messaging element.
11. Click Now.
The secondary System Manager server retrieves all data from Messaging and is now ready to administer and manage Messaging.

References:
Administering Avaya Aura System Manager for Release 6.3.11 and later, Release 6.3,
Issue 8 (November 2016), page 104
https://downloads.avaya.com/css/P8/documents/101008185