

100% Money Back
Guarantee

Vendor:Avaya

Exam Code:71300X

Exam Name:Avaya Aura Communication Applications
Integration Exam

Version:Demo

QUESTION 1

To which other component does the Avaya Aura Application Enablement Services (AES) Switch Connections connect?

- A. Avaya Aura Media Server (AAMS) using H.323
- B. Avaya Aura Session Manager (SM) using SIP
- C. Avaya Aura Communications Manager (CM) using H.323
- D. Avaya Aura Communications Manager (CM) using SIP

Correct Answer: C

Adding a switch connection

The procedure include the following steps:

1. From the AE Services Management Console main menu, select Communication Manager Interface > Switch Connections.
2. On the Switch Connections page, in the Add Connection field, type a switch connection name (for example Switch1)

For the Secure H323 Connection check box, do one of the following:

*

For Communication Manager 6.3.6 or later and TLS for the H.323 Signaling Channel (normally associated with FIPS Mode), select the Secure H323 Connection check box.

*

For any previous release of Communication Manager without TLS for the H.323 Signaling Channel, uncheck the Secure H323 Connection check box.

Etc.

References: Avaya Aura Application Enablement Services Administration and Maintenance Guide, page

73

<https://downloads.avaya.com/css/P8/documents/100171737>

QUESTION 2

Which component converts WebRTC Media Stream to SIP Media Stream?

- A. HTTP Reverse Proxy

B. Avaya Aura Media Server (AAMS)

C. STUN/TURN server

D. G.450/430 or G.650 Medpro board

Correct Answer: C

Provisioning Avaya Aura Media Server for the WebRTC Snap-in. Procedure

1.

Log in to the Avaya Aura

Media Server Element Manager.

2.

Check that Avaya Aura

Media Server nodes and routes are set up correctly.

See Deploying Avaya Breeze™ for details on configuring Avaya Aura Media Server for Avaya Breeze™.

3.

Go to System Configuration > Server Profile > General Settings, enable Firewall NAT Tunneling Media Processor and then click Save.

4.

Go to System Configuration > Signaling Protocols > SIP > General Settings, enable Always use SIP default outbound proxy, and then click Save.

Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Accounts and create a TURN/STUN account. This account ID and password must match the account created on the Avaya SBCE.

6. Go to System Configuration > Media Processing > ICE > TURN/STUN Servers > Servers to add the TURN/STUN connection to the Avaya SBCE server

Etc.

References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 23 <https://downloads.avaya.com/css/P8/documents/101013939>

QUESTION 3

An Avaya Aura Messaging (AAM) server intended to store Voice Messages in Avaya Message Store Mode, and you are

configuring that server for integration with an Avaya Aura Core. In Messaging Administration > Server Settings > Server Role/AxC Address, which Server Role must be chosen at the "Roles for this server" field?

- A. Application Only
- B. Storage Only
- C. Storage and Application
- D. AMSM

Correct Answer: C

QUESTION 4

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

Correct Answer: D

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@.* 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 5

What is the process for Web browsing to the AES Management Console, and logging in with the default account and default password?

- A. Error! Hyperlink reference not valid. Management IP Addr>:8443, then enter login=craft password=crftpw
- B. Error! Hyperlink reference not valid. Management IP Addr> then enter login=admin password=admin01
- C. Error! Hyperlink reference not valid. Management IP Addr> then enter login=admin password=admin
- D. Error! Hyperlink reference not valid. Management IP Addr> then enter login=cust password- custpw

Correct Answer: D

Log in to the AE Server as the default administrator (cust). Make sure that the URL begins with "https://" and the host name or IP address of the AE Services Server is correct.

References: Avaya Aura Application Enablement Services Administration and Maintenance Guide,

Release 6.3 (June 2014), page 56

<https://downloads.avaya.com/css/P8/documents/100171737>

QUESTION 6

What should be verified before running the initTM -f command on the Command Line Interface of Avaya Breeze™ platform (formerly known as Engagement Development Platform (EDP))?

- A. Verify that Avaya Breeze™ is configured as a Managed Element in Avaya Aura System Manager.
- B. Verify that an enrollment password is configured on System Manager and that it has not expired.
- C. Verify that a valid Certificate is installed on the Avaya Breeze™ instance.
- D. Verify that Avaya Breeze™ is licensed.

Correct Answer: B

See step 8 and step 9 below.

Repairing replication between Avaya Breeze™ and System Manager Procedure

1.
On the System Manager web console, navigate to Services > Replication.
2.
In Replica Group column, click CollaborationEnvironment_3.1.
3.
In Replica Node Host Name column, locate Avaya Breeze™.
4.
Verify that the status of the Synchronization Status field is green. If not, go to Step 5.
5.
If Presence Services Snap-in has been deployed, in the Product column, verify that both Avaya Breeze™ and Presence Services are displayed.
6.
Select Avaya Breeze™, and click Repair.
7.
After 2?5 minutes, verify that the status of the Synchronization Status field is green. If not, go to Step 8.
8.
Verify that Enrollment Password is not expired.
 - a.
Navigate to Services > Security.
 - b.
In the navigation pane, click Certificates > Enrollment Password.
9. If the Enrollment Password is expired:

a.

Enter a password, and click Commit. It is highly recommended that the same password must be used. Otherwise, Avaya Breeze™ and Presence Services must be re-administered, because System Manager Enrollment Password was configured during deployment of Avaya Breeze™. b. Open an SSH session to the Avaya Breeze™ Management Module IP address as sroot.

c.

On the command line interface, enter `initTM -f`.

d.

When prompted for the enrollment password, enter the password that you provided in Step 9a.

e.

Repeat Step 1 to Step 6. References: Avaya Aura Presence Services Snap-in Reference, Release 7.0.1 (December 2016), page <https://downloads.avaya.com/css/P8/documents/101013646>

QUESTION 7

In which two locations is the Switch Password configured?

- A. In `ip-services` form on Avaya Aura Communication Manager (CM) and in `TSAPI link` on Avaya Aura Application Enablement Services (AES)
- B. In `ip-services` form on Avaya Aura Communication Manager (CM) and in `Switch Connection` on Avaya Aura Application Enablement Services (AES)
- C. In `cti-link` form on Avaya Aura Communication Manager (CM) and in `Switch Connection` on Avaya Aura Application Enablement Services (AES)
- D. In `cti-link` form on Avaya Aura Communication Manager (CM) and in `TSAPI link` on Avaya Aura Application Enablement Services (AES)

Correct Answer: B

Enabling AE Services refers to administering the transport link between Communication Manager and AE Services. Procedure

1.

Type change `ip-services`. Communication Manager displays the IP SERVICES form

2.

Complete Page 1 of the IP SERVICES form

3.

Complete Page 3 of the IP SERVICES form as follows. a. In the AE Services Server field, type the name of the AE Services server b. In the Password field, create a password. This is the password that the AE Services administrator must set on the AE Server (Communication Manager Interface > Switch Connections > Edit Connection > Switch Password). The passwords must exactly match on both Communication Manager and the AE Services server.

References: Avaya Aura Application Enablement Services Administration and Maintenance Guide, Release 6.3 (June 2014) , page 26 <https://downloads.avaya.com/css/P8/documents/100171737>

QUESTION 8

What identifies that the Avaya Breeze™ server is using Identity Certificates that have been signed by Avaya Aura System Manager (SMGR)?

- A. if the Issuer Name states "O=AVAYA, OU=MGMT, CN= System Manager CA" for the Security Module SIP Identity Certificate
- B. if the replication status is showing `Synchronized` with a green background color
- C. if a successfully installed WebRTC snap-in is used
- D. if the Entity Link between Avaya Aura Session Manager (SM) and Avaya Breeze™ server is up

Correct Answer: A

QUESTION 9

Which statement about Avaya Aura Presence Services 7.x snap-in licensing is true?

- A. It requires an instance-license.
- B. It requires a per-user license.
- C. It does not require a license to work.
- D. It requires a license file for each snap-in installed.

Correct Answer: C

Presence Services snap-in does not require a license to work. References: Avaya Aura Presence Services Snap-in Reference. Release 7.0.1 (December 2016), page [https://downloads.avaya.com/css/P8/ documents/101013646](https://downloads.avaya.com/css/P8/documents/101013646)

QUESTION 10

To set Timers, URI Manipulation, and Header Manipulation that the Avaya Session Border Controller for Enterprise (SBCE) will use when signaling to the far-end server; a profile like "avaya-ru" is provided by default.

When configuring the Server Configuration, you must link to which type of Global profile?

- A. Signaling
- B. Routing

C. Topology Hiding

D. Server Interworking

Correct Answer: D

The standard Avaya profile "avaya-ru" is cloned for the Call Server Interworking Profile. The Interworking function of the Global Profiles feature enables the SBCE to function in an enterprise VoIP network using different SIP protocols.
References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012), page 339

QUESTION 11

Which statement about the SIP Entities to support single node 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 = "Avaya Breeze", 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 = "Avaya Breeze", and the other is of Type = "Presence Services".

D. Two SIP Entities are built to the same SM100 IP address of each node. One is of type = "Avaya Breeze", and the other is of Type = "Other".

Correct Answer: B

QUESTION 12

Before SIP Trunking configuration can begin, which state must the Avaya Session Border Controller for Enterprise (SBCE) be in?

A. Registered

B. Provisioned

C. Commissioned

D. Ready

Correct Answer: C

Prerequisite Conditions for SIP Trunking

Starting point for SIP-trunking administration:

System Management > Installed tab shows SBC(s) Commissioned indicates a successful initial console configuration.

References: Avaya Aura Session Border Controller Enterprise Implementation and Maintenance (2012),
page 302