# 71300X Q&As

Avaya Aura Communication Applications Integration Exam

## Pass Avaya 71300X Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

**https://www.pass4itsure.com/71300x.html**

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Avaya Official Exam Center

Instant Download After Purchase
100% Money Back Guarantee
365 Days Free Update
800,000+ Satisfied Customers

**QUESTION 1**

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.

Correct Answer: C

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

**QUESTION 2**

In the Avaya Session Border Controller for Enterprise (SBCE), before a traffic carrying Network Interface (A1 or B1) can be pinged, to which state do you have to toggle the status on Device Specific Settings > Network Management / Interfaces?

A. Enabled

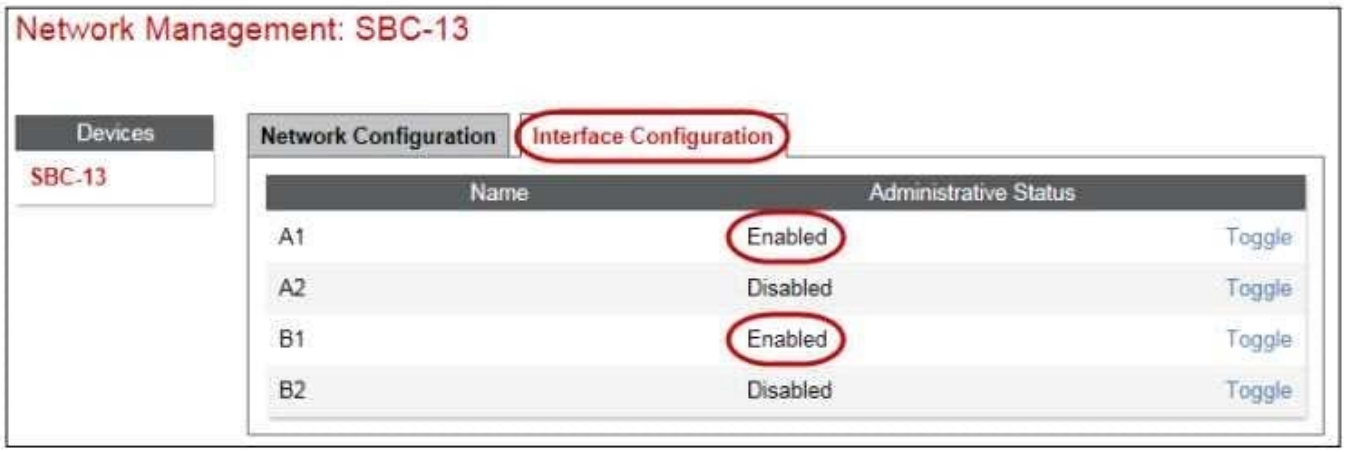
B. In-Service

C. Accept Service

D. Active

Correct Answer: A

Commission the SBC--SBC Configuration 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 203

**QUESTION 3**

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

Correct Answer: BDE

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 4**

You need to connect Avaya BreezeTM platform that is hosting Avaya Aura Presence Services Snap-in with Avaya Aura Session Manager (SM).

Which three are needed? (Choose three.)

A. ports UDP 5060 and TLS 5061

B. one Entity Link from SM to Avaya Aura Presence Services Snap-in

C. one Entity Link from SM to Avaya BreezeTM

D. TLS 5061 and TLS 5062

E. ports TCP 5060 and UDP 5060

Correct Answer: BCD

BD: Administering Entity Link between Presence Services Cluster SIP Entity and Session Manager Procedure

1.

On the System Manager web console, navigate to Elements > Routing > Entity Links.

2.

In the Name field, enter a name for Entity Link.

3.

In the SIP Entity 1 field, select the Session Manager instance.

4.

In the Protocol field, select TLS.

5.

In the Port field, type 5062. Note: Note that this port number cannot be the same as the port number administered in "Administering Entity Link between Avaya Breeze and Session Manager". CD: Administering Entity Link between Avaya Breeze and Session Manager. About this task Create an En2tity Link to connect Session Manager to Avaya Breeze. You must administer separate Entity Links for Avaya Breeze servers in order to open SIP listeners on the designated ports. Session Manager requires a Listen Port with the Listen Port as 5061, Protocol as TLS, and Default Domain as the login domain of endpoint devices. Without this, PPM will fail for SIP endpoints. References: Avaya Aura Presence Services Snap-in Reference. Release 7.0.1 (December 2016), pages 25-26
https://downloads.avaya.com/css/P8/documents/101013646

**QUESTION 5**

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

A. Verify that Avaya BreezeTM 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 BreezeTM instance.

D. Verify that Avaya BreezeTM is licensed.

Correct Answer: B

See step 8 and step 9 below.

Repairing replication between Avaya BreezeTM 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 BreezeTM.

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 BreezeTM and Presence Services are displayed.

6.

Select Avaya BreezeTM, 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 BreezeTM and Presence Services must be re-administered, because System Manager Enrollment Password was configured during deployment of Avaya BreezeTM. b. Open an SSH session to the Avaya BreezeTM 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

Latest 71300X Dumps 71300X VCE Dumps 71300X Practice Test