



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.passapply.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

Avaya Aura Presence Services 7.x is implemented on Avaya Breeze™ (formerly known as Engagement Development Platform (EDP)).

When looking at Elements > Engagement Development Platform > Service Management, which status would you expect for a Presence Services snap-in that is ready to support Avaya Aura Presence Services?

- A. Loaded
- B. Installed
- C. Accepting
- D. Active

Correct Answer: C

Enabling Avaya Breeze cluster running Presence Services Before you begin Ensure that the Avaya Breeze™ servers running the Presence Services are recovered / powered up. Procedure

1.

On the System Manager web console, navigate to Elements > Avaya Breeze > Cluster Administration.

2.

Select the Presence Services cluster, and change the Cluster State to Accept New Service. References: Avaya Aura Presence Services Snap-in Reference. Release 7.0.1 (December 2016), page <https://downloads.avaya.com/css/P8/documents/101013646>

QUESTION 2

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 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>

QUESTION 3

The Avaya WebRTC solution uses the web intensively to make media calls from a standard web browser in the internet, into internal and secure communication premises in the enterprise. Which statement about security between the Enterprise-edge and those standard Web browsers in the internet is true?

- A. A trust relationship based on certificates must be built to make WebRTC work.
- B. No trust relationship exists between enterprise edge security and web browsers; therefore, the security strategy is based on an Authorization Token instead.
- C. There must be a VPN connection between the Web Browser and the Enterprise-edge to build a WebRTC link.
- D. WebRTC only works within the Enterprise network. External Web Browsers must connect through an Avaya Session Border Controller for Enterprise (SBCE) via a SIP trunk.

Correct Answer: B

Validation of the authorization token. The WebRTC Snap-in will validate the authorization token created and encrypted by the web server. If the snap-in can decrypt the token and ensure that the time stamp is valid, it knows that the incoming HTTP request is valid. The time stamp will usually be short lived; on the order of 5- 10seconds to protect against replay attacks. References: Avaya WebRTC Snap-in Reference, Release 3.1 (May 2016), page 27 <https://downloads.avaya.com/css/P8/documents/101013939>

QUESTION 4

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 5

For an Avaya SIP telephone, working as a Remote Worker via the Avaya Session Border Controller for Enterprise (SBCE), which IP address should be configured in the Server List of the one-X?Communicator?

- A. the SBCE Internal Interface allocated for Mobile Workspace Endpoint



- B. the SBCE External Interface allocated for Mobile Workspace Endpoint
- C. the Internal Avaya Aura Session Manager SM100 IP Address
- D. the Avaya Aura Session Manager External Interface allocated for Mobile Workspace Endpoints.

Correct Answer: D

Remote Worker Avaya one-X Communicator Configuration The following screens illustrate Avaya one-X Communicator administration settings for the Remote Worker used in the reference configuration. Example:

1. On the Avaya one-X Communicator application running on the PC, click on the Settings icon on the top right to display the Settings window.
2. Click on Telephony, the General Settings window will appear. The following values were used in the reference configuration:

Under Using: select SIP (SIP must be selected; H.323 is not supported for Remote Workers).

*

Under Server List, click Add (the Add Server window to the right will appear).

*

Under Proxy Server enter 192.168.157.180 (This is one of the two "public" IP addresses for interface B1 on the Avaya SBCE used for Remote Worker access to Session Manager (public IP not used for relay services)).

Etc.

References: Configuring Remote Workers with Avaya Session Border Controller for Enterprise Rel. 6.2, Avaya Aura Communication Manager Rel. 6.3 and Avaya Aura Session Managers Rel. 6.3 - Issue 1.0, page 81

<https://downloads.avaya.com/css/P8/documents/100183254>

[71300X VCE Dumps](#)

[71300X Practice Test](#)

[71300X Study Guide](#)