# 71301X Q&As

Avaya Aura Communication Applications Implement Certified Exam

## Pass Avaya 71301X Exam with 100% Guarantee

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

**https://www.pass4itsure.com/71301x.html**

100% Passing Guarantee
100% Money Back Assurance

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

**QUESTION 1**

Which two configuration steps must be performed on the Avaya Aura Communication Manager (CM) for integrating it with the Application Enablement Services (AES), and enabling the TSAPI link? (Choose two.)

A. Create a CTI user.

B. Configure IP Services.

C. Create a Signaling Group.

D. Create a CTI link.

E. Configure Switch Connection.

Correct Answer: BD

To integrate Avaya Aura Communication Manager (CM) with Application Enablement Services (AES), and enable the TSAPI link, you need to perform two configuration steps on CM: Configure IP Services and Create a CTI link. These steps

are necessary to establish a connection between CM and AES using ASAI protocol, which is a proprietary protocol that provides access to various CTI features of CM. A TSAPI link is a logical connection between CM and AES that allows

TSAPI applications to use ASAI features through AES. To configure IP Services and Create a CTI link on CM, you need to use these screens:

The "ip-services" screen: This is a screen that allows you to create and manage IP services on CM, such as ASAI-IP or C-LAN. You can access this screen using the System Access Terminal (SAT) interface of CM. On this screen, you need

to specify a service type, node name, local node, local port, remote node, remote port, remote domain name, service state, and service link for each IP service. For integrating with AES, you need to create an ASAI-IP service that points to the

node name of an AES server.

The "cti-link" screen: This is a screen that allows you to create and manage CTI links on CM, which are logical connections between CM and CTI servers, such as AES. You can access this screen using the System Access Terminal (SAT)

interface of CM. On this screen, you need to specify a name, number, type, and password for each CTI link. For integrating with AES, you need to create a CTI link of type ADJ-IP that matches the switch CTI link number on AES.

**QUESTION 2**

You are obtaining identity certificates and encryption keys from a Certificate Authority (CA) for installation on the Avaya Session Border Controller for Enterprise (ASBCE).

Which statement about installing the identity certificate and encryption key files on the ASBCE is true?

A. The filenames of the identity certificate (.pern or .crt file) and the encryption key (.key file) must match.

B. Both the identity certificate and the encryption key files must be provided in a .zip archive for the installation on the ASBCE.

C. It must be rebooted before the identity certificate and the encryption key installation.

D. The filename of the identity certificate (.pern or .crt file) must be different from the filename of the encryption key (.key file).

Correct Answer: D

When installing the identity certificate and encryption key files on the Avaya Session Border Controller for Enterprise (ASBCE), you need to follow this rule: The filename of the identity certificate (.pem or .crt file) must be different from the filename of the encryption key (.key file). An identity certificate is a file that contains information about the identity and public key of an entity, such as a server or an endpoint. An encryption key is a file that contains information about the private key of an entity, which is used to encrypt and decrypt data. The identity certificate and encryption key files are obtained from a Certificate Authority (CA) or generated by yourself using tools such as OpenSSL. When installing these files on the ASBCE server, you need to make sure that they have different filenames, otherwise they will overwriteeach other and cause errors. For example, you can name them as sbce-cert.pem and sbce-key.key respectively.

**QUESTION 3**

In the context of Avaya Aura Presence Services, what is a Watcher?

A. It represents a user whose device is sending status on their behalf using a Publish message.

B. It represents a Presence information about a user that the system reports.

C. It is a user who is subscribing to the current and future presence status of another user.

D. It is a user who requests a one-time view of another user\\'s current presence status. However, it does not get the future presentity updates.

Correct Answer: C

In the context of Avaya Aura Presence Services, a Watcher is a user who is interested in the presence information of another user, called a Presentity. A Watcher sends a Subscribe message to the Presence Services snap-in on the Avaya Breeze?server, requesting to receive notifications about the current and future presence status of the Presentity. The Presence Services snap-in then sends a Notify message to the Watcher, containing the presence information of the Presentity. The Watcher can use this information to decide how and when to communicate with the Presentity12

**QUESTION 4**

Which two statements describe the steps for deploying the Avaya Presence Services snap- in? (Choose two.)

A. Install the Presence Services snap-in onto the Breeze?server.

B. Load the Presence Services snap-in to System Manager.

C. Load the Presence Services snap-in into the Breeze?cluster.

D. Install the Presence Services snap-in, and then load it onto the Breeze?server.

Correct Answer: BC

The steps for deploying the Avaya Presence Services snap-in are as follows:

Download the Presence Services snap-in software bundle from the Avaya Support website.

Log in to System Manager and navigate to Elements > Inventory > Manage Elements.

Select the Breeze?cluster where you want to deploy the Presence Services snap- in and click Edit.

In the Snap-ins tab, click Add Snap-in and browse to the location where you saved the Presence Services snap-in software bundle.

Select the Presence Services snap-in file and click Open. Click Commit to load the Presence Services snap-in to System Manager. Navigate to Elements > Inventory > Cluster Administration. Select the Breeze?cluster where you loaded the

Presence Services snap-in and click Manage Snap-ins.

In the Snap-ins tab, select the Presence Services snap-in and click Activate/Upgrade/Downgrade.

Click OK to load the Presence Services snap-in into the Breeze?cluster

**QUESTION 5**

Which statement describes how an H.248 signaling link connects the Internet Friendly (Edge) Gateway to the Avaya Communication Manager (CM)?

A. It is transported using HTTPs/REST via the Avaya Session Border Controller for Enterprise (ASBCE).

B. It is transported using HTTPs using port 443.

C. It is tunnelled using TCP port 2944 and secured using TLS.

D. It is transported using TCP port 80 and secured using a VPN connection to the Avaya Session Border Controller for Enterprise (ASBCE).

Correct Answer: C

An H.248 signaling link connects the Internet Friendly (Edge) Gateway to Avaya Communication Manager (CM) by tunneling H.248 messages using TCP port 2944 and securing them using TLS. H.248 is a protocol that defines how media

gateway controllers control media gateways for supporting multimedia streams across different networks, such as IP networks and PSTN networks. An H.248 signaling link is a logical connection between an H.248 controller and an H.248

gateway that allows exchanging H.248 messages for controlling media streams. In an Internet Friendly (Edge) Gateway scenario, CM acts as an H.248 controller and ASBCE DBE acts as an H.248 gateway. To connect an H.248 signaling

link between CM and ASBCE DBE, these steps are performed:

CM initiates a TCP connection to ASBCE DBE using port 2944, which is reserved for H.248 over TLS.

CM and ASBCE DBE negotiate TLS parameters and exchange certificates for mutual authentication and encryption.

CM and ASBCE DBE establish a secure TLS session over TCP port 2944. CM and ASBCE DBE exchange H.248

messages over TLS session for controlling media streams.