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

Before running the initTM -f command from the Avaya Breeze?server CLI, what should be verified?

A. Verify that the Avaya Breeze?is configured as a Managed Element in Avaya Aura System Manager.

B. Verify that an enrollment password is configured in Avaya Aura System Manager, and that it has not expired.

C. Verify that a valid certificate is installed on the Avaya Breeze?server.

D. Verify that the Avaya Breeze?server is licensed.

Correct Answer: B

The initTM -f command is used to initialize the trust management between the Avaya Breeze?server and the Avaya Aura System Manager. This command requires an enrollment password that is configured in the System Manager web interface, under Security > Enrollment Password. The enrollment password has a validity period that can be set by the administrator. If the enrollment password has expired, the initTM -f command will fail. Therefore, before running the initTM -f command, you should verify that the enrollment password is configured and valid12

QUESTION 2

How does an Avaya Workplace client learn about a Survivability Server assigned in its User Profile?

A. An Avaya Workplace client receives this information from the AADS via the Dynamic Configuration.

B. The Survivability Server details must be manually configured in the Avaya Workplace client.

C. An Avaya Workplace client receives this information from the Session Manager (SM) via PPM.

D. An Avaya Workplace client receives this information from the System Manager (SMGR) via Data Replication Service (DRS).

Correct Answer: A

An Avaya Workplace client learns about a Survivability Server assigned in its User Profile from the Avaya Aura Device Services (AADS) via the Dynamic Configuration. TheDynamic Configuration is a set of parameters that are sent by the AADS to the Avaya Workplace client during login or registration. The Dynamic Configuration contains information such as the SIP domain, SIP proxy, SIP registrar, and Survivability Server for the Avaya Workplace client. The Survivability Server is an Avaya Aura Communication Manager instance that provides call processing and voice mail access for the Avaya Workplace client in case of a network failure or loss of connectivity with the core servers34

QUESTION 3

Which statement about the Application Enablement Services (AES) certificate management is true?

A. AES is shipped with a self-signed server identity certificate which can be used indefinitely.

B. AES provides an integrated Certificate Authority (CA) which can be used to generate a self-signed server identity certificate.

C. AES is shipped with a default certificate which is valid for one year, and a customer- provided server identity certificate must be installed before the default certificate expires.

D. AES does not require a server identity certificate as it communicates only via H.323.

Correct Answer: C

The statement that is true about the Application Enablement Services (AES) certificate management is that AES is shipped with a default certificate which is valid for one year, and a customer-provided server identity certificate must be installed before the default certificate expires. A server identity certificate is a file that contains information about the identity and public key of a server, such as AES. A server identity certificate is used to authenticate the server to other entities that communicate with it using HTTPS or SIP over TLS. A server identity certificate is signed by a Certificate Authority (CA), which is an entity that issues and verifies certificates. AES uses certificates for various purposes, such as securing web access, enabling HTTPS-based APIs, encrypting SIP signaling, and supporting mutual authentication with endpoints or servers. AES comes with a default self- signed certificate that can be used for testing or demonstration purposes. The default certificate is valid for one year from the date of installation. After one year, the default certificate expires and needs to be replaced with a valid customer-provided certificate from a trusted CA. To install a customer-provided certificate on AES, you need to use tools such as OpenSSL or Keytool to generate a Certificate Signing Request (CSR), submit it to a CA, obtain a signed certificate from the CA, and upload it to AES using the web interface or CLI.

QUESTION 4

Which CLI tool is used to trace messages in real-time as they pass through the Avaya Session Border Controller for Enterprise (ASBCE)?

A. start trace

B. tracesbc

C. tracePackets

D. SIPtracer start

Correct Answer: B

The CLI tool that is used to trace messages in real-time as they pass through the Avaya Session Border Controller for Enterprise (ASBCE) is tracesbc. The tracesbc tool is a CLI tool that runs on the SBC component of the ASBCE server and captures and displays SIP messages and media statistics for calls that traverse the ASBCE server. You can use various filters and options to specify which calls or messages you want to trace. For example, you can filter by source or destination IP address, port, protocol, or call ID. You can also specify how long you want to run the trace and how many messages you want to display. The tracesbc tool can help you troubleshoot and diagnose issues with SIP registration and call setup.

QUESTION 5

Avaya Session Border Controller for Enterprise (ASBCE) can be deployed on the Kernel- based Virtual Machine (KVM) infrastructure. What is the template file type to be used for the KVM deployment?

A. OVA

B. QCOW2

C. OVF

D. EC2

Correct Answer: B

Avaya Session Border Controller for Enterprise (ASBCE) can be deployed on the Kernel-based Virtual Machine (KVM) infrastructure. KVM is a virtualization technology that allows multiple operating systems to run on a single physical machine. To deploy ASBCE on KVM, you need to use a template file that contains the ASBCE software image and configuration parameters. The template file type to be used for KVM deployment is QCOW2, which stands for QEMU CopyOn-Write version 2. QCOW2 is a file format for disk images that can be used by QEMU, which is an open source emulator and virtualizer that can run KVM virtual machines. QCOW2 files support features such as compression, encryption, snapshots, and backing files