

Avaya Aura Communication Applications Implement Certified Exam

Avaya 71301X

Version Demo

Total Demo Questions: 9

Total Premium Questions: 93

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Avaya Aura® Communication Manager	9
Topic 2, Avaya Aura® System Manager	4
Topic 3, Avaya Aura® Session Manager	28
Topic 4, Avaya Aura® Messaging	3
Topic 5, Avaya Aura® Application Enablement Services	15
Topic 6, Avaya Aura® Conferencing	1
Topic 7, Avaya Aura® Presence Services	19
Topic 8, Mix Questions	14
Total	93

QUESTION NO: 1

An administrator is creating a SIP Entity in Avaya Aura® System Manager for an Avaya Breeze® deployment hosting Avaya Aura® Presence Services. The SIP Entity must remain valid for the clustered service rather than identify one individual Breeze server.

What should be entered in the SIP Entity IP Address field?

- A. The Avaya Breeze® server Management IP Address or FQDN
- B. The Core Platform Cluster IP Address or FQDN
- C. The General Purpose Cluster IP Address or FQDN
- D. The Avaya Breeze® server Security Module IP Address or FQDN

ANSWER: B

Explanation:

The **Core Platform Cluster IP Address or FQDN** must be entered. Presence Services is hosted on the Breeze Core Platform cluster, and the SIP Entity must identify the routable cluster service endpoint. A node management address or an individual Security Module address does not represent the clustered SIP destination used for this configuration.

QUESTION NO: 2

An Avaya Aura® Web Gateway (AAWG) virtual machine has been deployed successfully. Before System Manager can manage the AAWG instance, the administrator must establish trust management between the two systems.

Which two actions are required? (Choose two.)

- A. Create a SIP Entity for AAWG in System Manager.
- B. Run the app install command on the AAWG CLI.
- C. Configure an enrollment password in System Manager and verify that it has not expired.
- D. Restart the AAWG application after virtual-machine deployment.
- E. Run the initTM command on the AAWG CLI.

ANSWER: C E

Explanation:

The administrator must configure a current **enrollment password in System Manager** and run **initTM** from the AAWG CLI. The enrollment password authorizes the trust enrollment, and the initTM command establishes the trusted relationship with System Manager. Adding a SIP Entity or pairing Session Manager does not replace this trust-management enrollment.

QUESTION NO: 3

Which two pieces of information in an output from the show mgc command (issued on a G430/G450 Gateway CLI), indicate that the G430/G450 is operating as an Internet Friendly (Edge) Gateway as opposed to an Enterprise Gateway? (Choose two.)

- A. The Management Link Mode displays Tunnelled.
- B. The H.248 Link Mode displays IFG.
- C. The Gateway Mode displays Edge.

D. The H.248 Link Status displays UP/Encrypted.

E. The Controller displays sbc@.

ANSWER: A B

Explanation:

Management Link Mode displays Tunnelled and H.248 Link Mode displays IFG are the two mode-specific indicators that identify an Internet Friendly Gateway configuration in `show mgc` output. The management-link mode identifies how the gateway's management communications are carried. A tunnelled management link is used for the Internet-facing deployment model, where management traffic is carried through the secured gateway-control connectivity rather than using the enterprise-gateway direct management-link arrangement. The H.248 link mode is the explicit gateway-control operating-mode indicator: IFG denotes Internet Friendly Gateway operation, while an enterprise deployment uses the enterprise gateway mode. Together, these two configured mode values distinguish the intended IFG/Edge operating model from an Enterprise Gateway model. Link status is operational state information: it can help establish whether a control connection is currently available and protected, but it is not the primary configuration-mode identifier requested by the question. Avaya documentation and product resources for Communication Manager gateways and their CLI administration are available through [Avaya Support](#) and the [Avaya Documentation Portal](#).

QUESTION NO: 4

An administrator is preparing to deploy Avaya Session Border Controller for Enterprise (ASBCE) on a Kernel-based Virtual Machine (KVM) host. The virtualization team requests the Avaya virtual-disk template format before creating the virtual machine.

Which template file type should be used?

A. OVA

B. QCOW2

C. OVF

D. VHDX

ANSWER: B

Explanation:

QCOW2 is the virtual-disk image format used for an ASBCE deployment on KVM. QCOW2 is the QEMU/KVM disk-image format and is used to create the ASBCE virtual appliance on the KVM infrastructure. OVA and OVF are normally associated with other virtualization deployment methods rather than a KVM disk image.

QUESTION NO: 5

An administrator is preparing Avaya Aura[®] Communication Manager (CM) for an Application Enablement Services (AES) integration. AES must expose TSAPI call-control services to a CTI application.

Which two administration tasks must be completed on CM? (Choose two.)

A. Create a CTI user.

B. Create a SIP signaling group.

C. Create a CTI link.

D. Configure IP Services.

E. Configure a Switch Connection.

ANSWER: C D

Explanation:

Configure IP Services and **Create a CTI link** are required on Communication Manager. IP Services provides the ASAI-over-IP transport used to communicate with AES, while the CTI link defines the logical CTI relationship used by AES. A CTI user and Switch Connection are configured on AES, not on CM. A SIP signaling group does not establish the ASAI CTI integration.

QUESTION NO: 6

Which statement about the Avaya Aura® Media Server (AAMS) associated with the Avaya Aura® Web Gateway (AAWG) is true?

- A.** The AAMS is only used for calls to Avaya Spaces Calling from outside the corporate network.
- B.** When a call is established using Avaya Spaces Calling, the AAMS processes the media until the Avaya Communication Manager shuffles the call.
- C.** When Avaya Spaces Calling is used by a User to make a call to another User, the media path is always direct, bypassing the AAMS.
- D.** For a call established to or from Avaya Spaces Calling, the AAMS processes the media for the duration of the call.

ANSWER: D

Explanation:

For a call established to or from Avaya Spaces Calling, the AAMS processes the media for the duration of the call. Avaya Aura Web Gateway provides the WebRTC access component that allows Avaya Spaces Calling clients to use an organization's Avaya Aura calling environment. In this architecture, Avaya Aura Media Server is the media-processing component associated with the gateway. It terminates and processes the WebRTC media stream and interworks it with the enterprise telephony media path as required. This role applies to calls originating from Avaya Spaces Calling and calls delivered to an Avaya Spaces Calling user. AAMS remains in the media path throughout the connected call; media processing is not removed as a consequence of Communication Manager call shuffling. Maintaining AAMS media processing supports the WebRTC-to-enterprise media interworking needed by the Avaya Spaces Calling integration. Avaya's Aura documentation describes Web Gateway as part of the WebRTC client-access architecture and identifies AAMS as the associated media-server capability. See the [Avaya Documentation Portal](#) for the applicable Avaya Aura Web Gateway and Avaya Aura Media Server deployment documentation, and the [Avaya Support site](#) for product documentation and release-specific resources.

QUESTION NO: 7

Which Avaya Aura® Platform component does Application Enablement Services (AES) communicate with?

- A.** Avaya Aura® Communication Manager (CM) using SIP
- B.** Avaya Aura® Communication Manager (CM) using H.323
- C.** Avaya Aura® Session Manager (SM) using SIP
- D.** Avaya Aura® Media Server (AAMS) using H.323
- E.** Avaya Aura® Communication Manager (CM) using ASAI

ANSWER: E

Explanation:

Application Enablement Services communicates directly with Avaya Aura® Communication Manager through an Application Server Interface (ASAI) link. This ASAI connection is the core integration between the AE Services server and Communication Manager, allowing AE Services to receive call events and invoke Communication Manager call-control capabilities on behalf of applications. AE Services then exposes those capabilities to CTI clients through interfaces and APIs such as TSAPI, JTAPI, DMCC, Web Services, and related services. In practical deployments, the ASAI link is administered in Communication Manager and AE Services so that applications can monitor devices, observe call states, perform call control, and use adjunct-routing-related capabilities supported by the platform. The communication method named in the correct answer is therefore ASAI, rather than a general endpoint signaling protocol. Avaya's AE Services documentation identifies Communication Manager as the associated call-processing platform and describes the AE Services–Communication Manager ASAI integration. See the [Avaya Aura® Application Enablement Services Overview](#) and Avaya's [product documentation portal](#) for AE Services administration and integration documentation.

QUESTION NO: 8

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).

ANSWER: A

Explanation:

An Avaya Workplace client receives this information from the AADS via the Dynamic Configuration. Avaya Aura Device Services (AADS) supplies dynamic client configuration information as part of the Workplace client's sign-in and registration process. When a survivability server is associated with the user's profile, AADS includes the applicable survivability details in that delivered configuration. This lets the client discover and use the designated survivability resource without requiring the user to enter server information locally.

Dynamic configuration centralizes endpoint settings and keeps the client aligned with the user's administered profile. In addition to survivability-related data, the configuration process can provide the client with communication-service settings needed to register and operate in the Avaya Aura environment. This administration model is particularly important for resilience because the survivability assignment follows the user profile and can be managed centrally rather than maintained separately on every client device. Avaya's product documentation and support resources for Workplace and Aura Device Services are available through the [Avaya Support portal](#) and the [Avaya Documentation portal](#).

QUESTION NO: 9

Which three statements about Avaya Breeze® are true? (Choose three.)

- A. It does not require a license.
- B. It is used by Avaya, Partner, and third-party developers.
- C. It was formerly called Collaboration Pod.
- D. It allows application developers to quickly add new capabilities to their Avaya solutions.
- E. It is a development platform that enables rapid development for applications targeted to meet a customer's communications needs.

ANSWER: B D E

Explanation:

Avaya Breeze® is a communications-application development and integration platform for Avaya Aura® environments. Its core purpose is to let organizations rapidly create and deploy communication capabilities tailored to business requirements, rather than requiring every feature to be delivered as a separate, monolithic application. The statement that it is “a development platform that enables rapid development for applications targeted to meet a customer's communications needs” accurately describes this role.

The platform supports Avaya, authorized partners, and third-party developers. These developers can build and deploy Snap-ins: modular application components that consume Avaya communication services and can provide targeted capabilities such as workflow automation, messaging, conferencing, context-aware routing, and integration with external business systems. Consequently, “It is used by Avaya, Partner, and third-party developers” is correct. “It allows application developers to quickly add new capabilities to their Avaya solutions” is also correct because Snap-ins and the Breeze framework are specifically intended to speed delivery and extension of communication applications. Avaya’s product information describes Breeze as a platform for building and integrating real-time communications applications; see [Avaya Breeze product information](#) and the [Avaya Support documentation portal](#) for product documentation and deployment guidance.