

Avaya Aura Communication Applications Support Certified

Avaya 72301X

Version Demo

Total Demo Questions: 11

Total Premium Questions: 110

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Avaya Aura® Communication Manager	5
Topic 2, Avaya Aura® Session Manager	32
Topic 3, Avaya Aura® System Manager	17
Topic 4, Avaya Aura® Messaging	18
Topic 5, Avaya Aura® Application Enablement Services	14
Topic 6, Avaya Aura® Call Center Elite	1
Topic 7, Avaya Aura® Experience Portal	1
Topic 8, Mix Questions	22
Total	110

QUESTION NO: 1

The WebRTC snap-in is showing a yellow caution icon under License Mode.

What does this error mode indicate?

- A. The license was installed incorrectly.
- B. The license 30 day grace period has expired.
- C. There is a license error but the snap-in continues to function.
- D. The snap-in license has expired and is out of service.

ANSWER: C

Explanation:

There is a license error but the snap-in continues to function. In the WebRTC snap-in License Mode status display, the yellow caution state denotes an error condition that requires administrative attention but does not stop the snap-in from operating. This status is intended to distinguish a licensing issue that is being tolerated temporarily from a service-stopping license condition. Administrators should investigate the license configuration and resolve the reported issue promptly, because the caution indication identifies that the licensing state is not fully valid even though WebRTC functionality remains available. The status icon therefore communicates both the presence of a licensing problem and the current operational impact: continued service. Avaya's WebRTC Snap-in documentation describes the License Mode indicators and their meanings, including the caution/error state. See the [Avaya WebRTC Snap-in documentation](#) and the [Avaya Support portal](#) for the applicable product documentation and licensing guidance.

QUESTION NO: 2

A customer reports that they cannot place calls to the Public Network using the SIP Service Provider after a technician had finished fixing an issue in the Session Border Controller (SBC).

Within Avaya SBC, in which three places do you check the configuration of the SIP Trunks? (Choose three.)

- A. PPM Services
- B. Media Interface
- C. Routing Configuration
- D. Signaling Interfaces
- E. Server Configuration

ANSWER: C D E

Explanation:

For a SIP Service Provider trunk on Avaya Aura Session Border Controller for Enterprise, the relevant configuration is distributed across server, signaling, and routing functions. **Server Configuration** is where the SBC's server-side connectivity and service-provider server information is reviewed, including the network context required to reach the provider. This establishes the SBC's ability to communicate with the external SIP infrastructure.

Signaling Interfaces define the SIP-facing interface characteristics used by the trunk, such as the local signaling address, transport protocol, listening port, and interface assignment. These settings must correspond to the provider-facing connectivity and are essential for SIP requests and responses to traverse the SBC correctly.

Routing Configuration determines how calls are matched and sent toward the SIP Service Provider. Reviewing routing policies, destination selection, and associated signaling entities confirms that Public Network dialed numbers are directed to the appropriate provider trunk after they enter the SBC. Together, these three areas validate reachability, SIP signaling, and call-path selection. Avaya's current product documentation is available through the [Avaya Documentation portal](#) and the [Avaya Support portal](#).

QUESTION NO: 3

Refer to the exhibit.

SIP endpoint 101-1112 is updating its Presence status with the Avaya Aura® Presence (PS).

Based on the exhibit, which statement about the message flow is true?

- A. Avaya Aura® Presence sends Notify to the telephone via Avaya Aura® Session Manager.
- B. Phone sends Register message to Avaya Aura® Session Manager via Avaya Session Border Controller for Enterprise.
- C. The telephone sends Subscribe message to Avaya Aura® Session Manager via Avaya Session Border Controller for Enterprise.
- D. Avaya Aura® Presence sends Notify to the SIP endpoint via Avaya Session Border Controller for Enterprise.

ANSWER: A

Explanation:

Avaya Aura® Presence sends Notify to the telephone via Avaya Aura® Session Manager. Presence uses SIP event mechanisms to distribute presence-state changes to interested, subscribed SIP endpoints. In an Avaya Aura deployment, Session Manager is the SIP routing and integration layer between endpoints and application servers, including Presence Services. When Presence Services has a changed state to report for the endpoint or a presence resource it monitors, it generates a SIP NOTIFY event message. Session Manager applies its routing and location information to deliver that NOTIFY request to the registered telephone.

This flow reflects the separation of application and session-routing roles in Avaya Aura: Presence Services supplies the presence capability and event notification, while Session Manager provides the SIP signaling path to the endpoint. The notification reaches the telephone using the endpoint's registered contact and the Session Manager routing infrastructure. Avaya's Aura documentation describes Session Manager as the central SIP routing component for users, endpoints, and application servers, and identifies Presence Services as the component that provides presence information and presence event support. See [Avaya Aura® Presence Services documentation](#) and [Avaya Aura® Session Manager documentation](#).

QUESTION NO: 4

A SIP endpoint can register with Avaya Aura® Session Manager, but calls sent from the endpoint to an application fail only when TLS is used. The administrator needs Session Manager-side diagnostic detail for the TLS negotiation.

Which tool should be used?

- A. traceSM
- B. traceSBC
- C. statapp
- D. SMnetSetup

ANSWER: A

Explanation:

`traceSM` is the Session Manager command-line tracing utility and includes options for detailed TLS-handshake troubleshooting. It provides Session Manager-side evidence for certificate validation, TLS negotiation, and secure SIP connection failures. Trace Viewer can be used to examine collected traces, but it does not replace `traceSM` as the Session Manager trace-collection utility.

QUESTION NO: 5

A browser-based WebRTC client is located behind Network Address Translation (NAT). The customer requires the client to gather candidate addresses, test available media paths, and use a relay when a direct media path cannot be established.

Which three technologies support these requirements? (Choose three.)

- A. ICE
- B. HTTPS
- C. TURN
- D. SRTCP
- E. STUN

ANSWER: A C E

Explanation:

ICE coordinates candidate gathering and connectivity checks. **STUN** assists an endpoint in discovering its public-facing mapped address, and **TURN** provides relay connectivity when a direct path cannot be used. HTTPS can protect web signaling, while SRTCP protects RTCP traffic, but neither performs the stated NAT-traversal functions.

QUESTION NO: 6

In Avaya Aura® 7 the Avaya Session Border Controller for Enterprise (SBCE) license is installed on a System Manager (SMGR) WebLM server. The EMS points to the WebLM server using a URL.

What is the correct syntax of the URL where 135.xxx.xxx.xxx. is the IP address of the SMGR WebLM server?

- A. https://135.xx.xxx.xx:8443/WebLM/LicenseServer
- B. https://135.xx.xxx.xx:8080/LicenseServer
- C. https://135.xx.xxx.xx:52233/WebLM/LicenseServer
- D. https://135.xx.xxx.xx/WebLM

ANSWER: C

Explanation:

The correct WebLM server URL is **https://135.xx.xxx.xx:52233/WebLM/LicenseServer**. In an Avaya Aura 7 deployment where Session Border Controller for Enterprise is configured to obtain its entitlement from WebLM hosted on System Manager, EMS must be given the complete secure WebLM LicenseServer endpoint. This includes the `https` protocol, the WebLM HTTPS service port 52233, and the required `/WebLM/LicenseServer` path. The path identifies the WebLM licensing service rather than simply the System Manager web interface, allowing SBCE EMS to communicate with the licensing server and retrieve or validate license capacity. The configured address must be reachable from the SBCE management network, and the SBCE must trust the certificate presented by the WebLM service if certificate validation is enabled. Use the actual System Manager WebLM IP address or resolvable hostname in place of the sample address. Avaya's SBCE product documentation and support resources are available through the [Avaya Session Border Controller for Enterprise support page](#) and the [Avaya Documentation Portal](#).

QUESTION NO: 7

Which two methods can be used to determine the status of the Switch/CTI Link between Avaya Aura®

Communication Manager (CM) and Avaya Aura® Application Enablement Services (AES)? (Choose two.)

- A. Observe the AES Alarm Report.

- B. Run an ASAI test on AES.
- C. Observe the CM dashboard.
- D. Observe the AES dashboard.
- E. Run the `status aesvcs cti-link` command on CM.

ANSWER: B E

Explanation:

Running an ASAI test on AES is a direct method of validating the operational path used by the Application Enablement Services server to communicate with Communication Manager. The ASAI test exercises the AE Services-to-switch interface and reports whether the relevant CTI connectivity is available, making it useful when investigating whether applications can receive CTI events or issue CTI requests through the configured switch connection.

The `status aesvcs cti-link` command on Communication Manager is also an authoritative status check from the switch side. It displays the state of the AE Services CTI link and provides operational information for the administered connection. Using this command together with the AES ASAI test verifies the link from both endpoints: the Communication Manager administration and service state, and the AE Services ability to use the ASAI interface. This is especially valuable after administration changes, service restarts, network interruptions, or during CTI application troubleshooting.

Avaya publishes AE Services product documentation and administration guidance through the [Avaya Application Enablement Services support page](#) and makes related technical documentation available in its [documentation repository](#).

QUESTION NO: 8

A customer called in stating they cannot place WebRTC calls. You discover that when the WebRTC snap-in sends an Invite to Avaya Aura® Media Server (AAMS), Avaya Breeze™ is not sending the correct information in the Request URI to match a regular expression in Session Manager.

Where do you configure the Media Server URI (`ce-msml@avaya.com`) that Avaya Breeze™ will send to AAMS via Avaya Aura® Session Manager (SM)?

- A. Use Avaya Aura® System Manager web GUI to access the Engagement Development Platform >Configuration > Attributes.
- B. Use SSH to Avaya Breeze™ and edit the `/etc/config.properties` file.
- C. Use Avaya Aura® System Manager web GUI to access the Inventory > Manage Elements, and then edit the Avaya Breeze™ element.
- D. Use Avaya Aura® System Manager web GUI to access the Engagement Development Platform >Configuration > Avaya Aura® Media Server.

ANSWER: D

Explanation:

Use Avaya Aura® System Manager web GUI to access the Engagement Development Platform > Configuration > Avaya Aura® Media Server. This is the centralized Avaya Breeze administration location for the Avaya Aura Media Server integration settings, including the Media Server URI that Breeze uses when it creates the SIP INVITE toward AAMS through Session Manager. Setting the URI to the value expected by the Session Manager routing regular expression, such as `ce-msml@avaya.com`, ensures that the request URI is presented in the required format and can be matched by the configured routing logic. This configuration is an Engagement Development Platform setting because it governs how Breeze services and snap-ins address the media server; it is not a per-element inventory property or an operating-system file configuration. After changing the URI, normal operational practice is to save and apply the configuration and verify the resulting SIP signaling, so that the INVITE Request-URI reaching Session Manager contains the configured media-server address. Avaya documentation and product resources are available through the [Avaya Support portal](#) and the [Avaya Aura Platform product page](#).

QUESTION NO: 9

A support team has completed Discipline 4 of the 8D Troubleshooting Methodology and has verified the root cause of an intermittent SIP service failure. The team is now performing Discipline 5.

Which two activities are appropriate during Discipline 5? (Choose two.)

- A. Select actions that eliminate the verified root cause.
- B. Verify that the proposed actions are effective and do not create unacceptable side effects.
- C. Implement the selected corrective actions throughout the production environment.
- D. Define actions to prevent recurrence across comparable systems.
- E. Recognize the team contribution after closure of the investigation.

ANSWER: A B

Explanation:

Discipline 5 is used to choose and verify permanent corrective actions. The actions must address the verified root cause rather than merely contain the symptom, and they should be evaluated for effectiveness and unacceptable side effects before broad implementation. Implementing the selected actions occurs in the following discipline, while preventing recurrence is addressed later in the process.

QUESTION NO: 10

Which three protocols assist the WebRTC functionality to overcome the Network Address Translations (NAT) challenges? (Choose three.)

- A. ICE
- B. SRTCP
- C. TURN
- D. HTTPS
- E. STUN

ANSWER: A C E

Explanation:

ICE, TURN, and STUN are the core WebRTC technologies used together to establish media connectivity when endpoints are behind Network Address Translation devices. Interactive Connectivity Establishment (ICE) is the coordination framework: it gathers possible network paths, exchanges those candidates with the remote endpoint, tests them, and selects a working candidate pair for the connection. Session Traversal Utilities for NAT (STUN) lets an endpoint discover the public-facing transport address and port mapping assigned by a NAT device. That information enables direct peer-to-peer connectivity whenever the network topology permits it. Traversal Using Relays around NAT (TURN) provides a relay allocation when direct paths cannot be established, such as with restrictive or symmetric NAT behavior and firewall policies. WebRTC implementations use ICE candidate gathering and connectivity checks, with STUN and, where required, TURN servers supplying the candidate types needed for resilient call setup. This combination is fundamental to reliable browser-based real-time voice and video sessions across private and public networks. The WebRTC specification describes ICE as the mechanism for establishing connectivity and identifies STUN/TURN servers as sources of candidates; the IETF ICE specification also defines the use of STUN and TURN for NAT traversal. See the [W3C WebRTC specification](#) and [RFC 8445: ICE](#).

QUESTION NO: 11

A customer reports that they cannot place WebRTC calls. You discover there is a problem with communication between Avaya Breeze™ and the Avaya Aura® Media Server (AAMS).

Where in Avaya Breeze™ do you set/check the User ID for Restful TLS authentication?

- A. Use the System Manager (SMGR) web GUI to access Breeze > Configuration > Avaya Aura Media Server
- B. Use the System Manager (SMGR) web GUI to access Breeze > Cluster Administration > General > Cluster Attributes
- C. Use the System Manager (SMGR) web GUI to access Breeze > Configuration > Attributes
- D. Use the System Manager (SMGR) web GUI to access Breeze > Server Administration > Dashboard

ANSWER: B

Explanation:

Use the System Manager (SMGR) web GUI to access Breeze > Cluster Administration > General > Cluster Attributes. This is the cluster-level location in Avaya Breeze where the Avaya Aura Media Server RESTful authentication settings are administered, including the user identity used when Breeze connects to the media server through its secured REST interface. Because the value applies to the Breeze cluster's integration with Avaya Aura Media Server, it belongs in the general cluster attributes rather than in an individual server dashboard or a generic configuration view.

For WebRTC call processing, Breeze must be able to request and control media resources from Avaya Aura Media Server. The configured RESTful TLS user identity is therefore an important integration value to validate when communication between those components is failing. Confirm that the User ID is present and matches the account configured on the media-server side, then verify the associated credentials and certificate trust configuration according to the release-specific deployment documentation. Avaya publishes current product documentation through its [Documentation Portal](#); product support, advisories, and downloads are available from [Avaya Support](#).