

Avaya Aura Core Components Support Certified Exam

Avaya 72201X

Version Demo

Total Demo Questions: 8

Total Premium Questions: 80

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, Avaya Aura® Communication Manager	36
Topic 2, Avaya Aura® Session Manager	23
Topic 3, Avaya Aura® System Manager	7
Topic 4, Mix Questions	14
Total	80

QUESTION NO: 1

What documents are expected to be filled out by customers/partners before contacting support in Avaya 's Diagnostic Methodology program?

- A. Problem Clarification
- B. Cause
- C. Knowledge Management
- D. Details/Findings
- E. Problem Statement
- F. Troubleshooting steps taken

ANSWER: A D E

Explanation:

Avaya's Diagnostic Methodology is intended to ensure that a support request begins with a clear, reproducible technical description and the evidence already gathered by the customer or partner. The required pre-contact documentation therefore starts with **Problem Statement**, which defines the issue in concise business and technical terms, including the affected service and the observed behavior. **Problem Clarification** then refines the statement through relevant context, such as when the problem began, its scope, frequency, recent changes, and conditions under which it occurs. **Details/Findings** captures the results of the investigation performed before escalation, including observed symptoms, alarms, logs, traces, configuration information, and diagnostic results. Together, these documents give Avaya Support an actionable starting point, reduce initial information-gathering cycles, and support faster case triage and resolution. Customers and partners should use the relevant product documentation and support resources to collect the required evidence before opening or escalating a service request. Avaya's support entry point is available at [Avaya Support](#), and product documentation, including maintenance and troubleshooting guidance, is available through the [Avaya Documentation Portal](#).

QUESTION NO: 2

A SIP telephone sends an initial REGISTER request to Session Manager and receives a 401 Unauthorized response. It sends a second REGISTER request containing an Authorization header, but continues to receive 401 responses.

Which issue should be investigated first?

- A. Verify that the endpoint credentials match the authentication data in the SIP Communication Profile.
- B. Assign additional Media Server VoIP channels to Communication Manager.
- C. Increase the bandwidth limit between the endpoint Network Regions.
- D. Add a feature button assignment to the Communication Manager station.
- E. Disable the Session Manager Entity Link to force a new registration.

ANSWER: A

Explanation:

The initial 401 response is normal SIP digest-authentication behavior because the first REGISTER request normally does not contain the challenge response. Repeated 401 responses after the telephone includes an Authorization header indicate that the endpoint credentials or the corresponding SIP Communication Profile authentication data should be verified.

The first 401 does not by itself indicate a failed registration. A missing Media Server resource, WAN bandwidth allocation, or Communication Manager station button assignment would not cause digest authentication to continue failing.

QUESTION NO: 3

After a certificate renewal, Communication Manager cannot establish a TLS connection to a Session Manager SIP Entity. The TCP connection is reachable, but the TLS handshake fails. Which two conditions must be verified to restore certificate-based trust? (Choose two.)

- A. The peer identity certificate contains a name matching the configured SIP Entity name.
- B. The applicable issuing CA certificate chain is installed in the peer trust store.
- C. The SIP trunk group has sufficient licensed members.
- D. The Media Server has available VoIP channels.
- E. The signaling group is changed permanently from TLS to TCP.

ANSWER: A B

Explanation:

The identity certificate presented by a TLS peer must contain a subject name or Subject Alternative Name that matches the name configured and used by the other peer. In addition, the receiving system must trust the issuing CA certificate chain for that identity certificate. Both conditions are required for successful certificate validation during the TLS handshake.

Changing the signaling transport permanently to TCP bypasses the TLS issue rather than repairing trust. License capacity and DSP allocation do not determine whether a certificate identity can be validated.

QUESTION NO: 4

In the Avaya Aura® Core, which two modes can Communication Manager be deployed in?

- A. Call Server
- B. Hybrid Server
- C. Evolution Server
- D. Communication Server
- E. Feature Server
- F. None of the above

ANSWER: C E

Explanation:

Communication Manager supports deployment as an **Evolution Server** and as a **Feature Server** in an Avaya Aura Core environment. Evolution Server mode is the full Communication Manager call-processing deployment model. It supplies the established Communication Manager telephony feature set and call-control capabilities while participating in the Aura architecture, including integration with Aura Session Manager for SIP-based routing and services. Feature Server mode is intended for an Aura Session Manager-centric design, in which Session Manager provides the primary SIP call-routing function and Communication Manager supplies telephony features for endpoints and users that require them. This separation lets an enterprise use Aura SIP session control while retaining Communication Manager's mature feature processing where needed. These deployment terms are specifically used in Avaya Aura architecture and Communication Manager documentation to distinguish the role Communication Manager plays in the overall solution; they are not generic descriptions of a call-processing server. Avaya's product documentation portal provides the Communication Manager deployment and administration documentation describing these server roles: [Avaya Documentation Portal](#). Product documentation and release materials are also available through [Avaya Support](#).

QUESTION NO: 5

A customer calls Avaya Support stating their Session Manager (SM) is down. After doing some troubleshooting, the technician sees SM is in the Deny New Service state, and in Restricted license mode.

What does the Restricted license mode indicate in this scenario?

- A. The SM license is not accessible or does not exist.
- B. There is a license error but SM continues to function.
- C. The license 30 day grace period has expired and SM service is being denied.
- D. The license was installed incorrectly.
- E. The SM has exceeded the license capacity and is operating in restricted mode.

ANSWER: C

Explanation:

The license 30 day grace period has expired and SM service is being denied. Session Manager uses its licensing status to determine whether it can continue accepting new service. When the required license cannot be validated or obtained, Session Manager can initially operate during a limited grace period. This is intended to provide time for the administrator to restore license availability, correct the licensing configuration, or resolve communication with the Avaya licensing infrastructure without an immediate service interruption. Once that 30-day grace interval is exhausted, the system enters Restricted license mode. In this state, Session Manager transitions to Deny New Service, preventing new service activity from being established while protecting the system from operating indefinitely without valid licensing. The observed combination of Restricted license mode and Deny New Service therefore specifically identifies an expired licensing grace period, rather than merely a nonfatal license warning. Administrators should restore valid license access and confirm that the appropriate Session Manager entitlements are available before returning the server to normal service. Avaya product documentation and support resources are available through the [Avaya Documentation Portal](#) and the [Avaya Support portal](#).

QUESTION NO: 6

A customer called Avaya Support stating that shortly after some maintenance work was done, they cannot make or receive calls. Which command in Avaya Aura® Communication Manager (CM) can the administrator execute to determine if the H.248 Gateways were placed in a maintenance busy state?

- A. Status signaling group x
- B. Status health
- C. Status media-gateways
- D. Trace trunk x
- E. Status maintenance busy

ANSWER: E

Explanation:

`status maintenance busy` is the appropriate Communication Manager System Access Terminal command because it displays equipment that is currently in the maintenance-busy condition. Maintenance busy is an administrative state used to take hardware or gateway-related resources out of service safely while maintenance is being performed. If an H.248 media gateway was left in this state after work was completed, Communication Manager will not use its affected resources for normal call processing, which can directly account for users being unable to place or receive calls. Running this status command gives the administrator a focused way to verify whether maintenance-busy resources remain and to identify the affected equipment before restoring it to service through the approved maintenance procedure. This check is especially relevant immediately after planned work because the service impact can result from a gateway intentionally being busied but not subsequently released. Avaya maintains product documentation and support resources for Communication Manager

administration and maintenance at [Avaya Support](#) and provides its current technical documentation library at [Avaya Documentation](#).

QUESTION NO: 7

Several branch Network Regions reach the data center across the same constrained WAN link. Which three statements describe how a Virtual or Intervening Network Region assists with bandwidth management? (Choose three.)

- A. It represents a shared WAN constraint between physical Network Regions.
- B. It helps Communication Manager prevent aggregate WAN-link oversubscription.
- C. It supports call-admission decisions based on bandwidth available on the shared path.
- D. It provides additional DSP channels to endpoints in the branch regions.
- E. It automatically converts calls to a lower-bandwidth codec.
- F. It permits a Network Region to consume unavailable bandwidth from another region.

ANSWER: A B C

Explanation:

A Virtual or Intervening Network Region represents the shared WAN bottleneck between physical Network Regions. It allows Communication Manager to apply call-admission-control decisions against the shared path and helps prevent the aggregate bandwidth used by calls from oversubscribing that common link. This makes bandwidth administration more manageable in topologies where multiple branches traverse the same WAN resource.

A Virtual Network Region does not supply DSP resources, change endpoint codecs automatically, or permit one region to borrow bandwidth that has already been exhausted on the shared path.

QUESTION NO: 8

A customer states they are having voice quality issues when they make calls over a WAN link. You would like to see what the Quality of Service is for a call, as the customer makes the call.

Which Avaya Aura® Communication Manager (CM) SAT command will display packet loss and jitter for a call in progress?

- A. monitor station qos xxxx, where XXXX is the station number
- B. list monitor qos
- C. status station qos xxxx, where XXXX is the station number
- D. list trace station xxxx, where XXXX is the station number.
- E. status media-gateway
- F. list trace h248

ANSWER: A

Explanation:

`monitor station qos xxxx`, where XXXX is the station number is the appropriate Communication Manager SAT command for observing real-time Quality of Service statistics for an active IP call associated with a particular station. The QoS monitor uses the station extension to identify the endpoint and presents call-quality measurements reported during the call, including packet loss and jitter. This makes it especially useful when a user can reproduce a WAN-related audio problem while an administrator is connected to the SAT, because the administrator can correlate reported symptoms with the live media statistics instead of relying only on historical counters or signaling traces. Packet loss indicates RTP media

packets that failed to arrive, while jitter represents variation in packet arrival timing; both are key indicators when diagnosing poor voice quality across a WAN. The command should be run while the station has an active call so that Communication Manager has current RTP/RTCP quality information to display. Avaya documentation and product-support resources for Communication Manager administration and troubleshooting are available through the [Avaya Documentation portal](#) and [Avaya Support](#).