DUMPSBOSS.

# Avaya AuraCore Components Implement Certified Exam

## Avaya 71201X

## Version Demo

**Total Demo Questions: 9**

**Total Premium Questions: 99**

**Buy Premium PDF**

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

QUESTION NO: 1

Which two conditions should be verified before placing an Avaya Aura Session Manager (SM) into Accept New Service state? (Choose two.)

**A.** The trust relationship with System Manager should be established.

**B.** The required SIP Entity Links should be in service.

**C.** A local System Manager backup must be completed.

**D.** The Session Manager must be configured as a Certificate Authority.

**E.** All Communication Manager translations must be exported to a USB device.

**ANSWER: A B**

**Explanation:**

Before a Session Manager is placed into **Accept New Service**, administrators should verify that the Session Manager has a healthy managed relationship with System Manager and that its required SIP connectivity is operational. In particular, the **trust relationship with System Manager should be established** so that the instance can be administered and receive configuration. The **required SIP Entity Links should be in service** so that the Session Manager can route signaling to its configured peers. A server should not be placed into production service solely because its virtual machine is powered on or because a local backup has completed. See the Avaya Documentation Portal for Session Manager deployment and service-state procedures.

**QUESTION NO: 2**

Which two does an Avaya Aura Session Manager (SM) store in its registrar database during registration? (Choose two.)

**A.** Location (IP Address)

**B.** User Language preference

**C.** SIP Uniform Resource Identifier (URI)

**D.** SIP endpoint type

**E.** User Time Zone

**ANSWER: A C**

**Explanation:**

During SIP registration, Avaya Aura Session Manager acts as a SIP registrar and creates a registration binding that associates the user's address-of-record with the endpoint's reachable contact location. The SIP Uniform Resource Identifier (URI) identifies the registered user or address-of-record, allowing Session Manager to determine the identity to which requests are addressed. The location (IP Address) represents the endpoint contact information needed to route subsequent SIP signaling to the device at its currently registered network location. This registration state is fundamental to Session Manager's ability to locate a user dynamically after the user's endpoint sends a REGISTER request, including when that endpoint's reachable address changes. SIP registration behavior is defined by the IETF as the mapping of an address-of-record to one or more contact addresses; see RFC 3261, Section 10. Avaya identifies Session Manager as the component that provides SIP session control and endpoint registration within Avaya Aura; see the Avaya Aura Session Manager product page.

**QUESTION NO: 3**

Which feature of Avaya Aura Session Manager (SM) makes it possible to communicate with non-Avaya Aura Third-Party Call Servers such as a CS1000?

**A.** Adaptation Module

**B.** CS1000 Convertor

**C.** Regular Expression

**D.** CS1000 Switcher

**ANSWER: A**

**Explanation:**

Adaptation Module is correct because Avaya Aura Session Manager uses adaptation modules to interwork with SIP-based, non-Avaya Aura call-control systems, including the CS 1000. The module adapts signaling and routing behavior between Session Manager's Aura environment and the specific SIP implementation of the third-party or legacy call server. This capability lets Session Manager include those systems within the enterprise session-routing architecture while accommodating differences in SIP headers, numbering formats, feature interactions, and protocol behavior. In practical deployments, the adaptation is associated with the relevant SIP entity and supports the routing of calls between Aura components and the external call server through Session Manager. It is therefore the Session Manager feature specifically intended to enable this form of interoperability, rather than a generic dialing-rule mechanism or a separate CS 1000 conversion/switching function. Avaya's Session Manager interoperability material identifies adaptation as the mechanism used for integration with supported third-party call servers. See the Avaya DevConnect reference material at Avaya DevConnect and the Avaya Documentation Portal for Session Manager deployment and interoperability documentation.

## QUESTION NO: 4

Which statement about making Avaya Aura Communication Manager (CM) work successfully as a feature server for CM SIP Endpoints (AST Endpoints) is true?

**A.** CM does not support SIP Endpoints in Avaya Aura 10.1.

**B.** CM must be added as an Application in an Application Sequence.

**C.** Endpoints must register directly with CM.

**D.** CM must be added as an Application Sequence assigned to the CM Managed Element.

**ANSWER: D**

**Explanation:**

CM must be added as an Application Sequence assigned to the CM Managed Element. In an Avaya Aura deployment using Session Manager, CM provides call processing and feature services for the SIP endpoint while Session Manager provides the SIP registration and routing context. System Manager represents CM as a managed element and uses an Application Sequence to define the feature-server application path associated with that CM instance. Assigning the Application Sequence to the CM Managed Element links the appropriate CM feature-server configuration to the managed CM system, allowing Session Manager to route endpoint service requests and calls to CM according to the administered sequence.

This association is an important part of the System Manager provisioning model: the application sequence is not merely created globally; it must be associated with the relevant CM managed element so the correct feature server is selected for the deployment. Once the CM managed element, application sequence, SIP entities, and routing-related administration are aligned, CM can deliver its endpoint call features while the SIP endpoint remains registered through the Aura Session Manager architecture. Avaya product documentation and support resources are available through Avaya Documentation and Avaya Support.

## QUESTION NO: 5

When performing a backup through the SMI Web interface, which two backup methods are valid for Avaya Aura Communication Manager (CM) 10.1? (Choose two.)

**A.** USB

**B.** SFTP

**C.** DVD

**D.** SCP

**ANSWER: B D**

**Explanation:**

SFTP and SCP are the supported remote, secure file-transfer methods for saving a Communication Manager backup from the System Management Interface (SMI) web interface. During the backup workflow, the administrator supplies the remote server information and destination path, and SMI transfers the generated backup archive to that server using the selected secure protocol. Both methods protect the backup transfer through encrypted SSH-based connectivity, making them appropriate for carrying potentially sensitive system configuration, translations, announcements, and other backup data across the network. Administrators should ensure that the selected remote account has permission to create files in the configured destination directory, that name resolution and network routing are available from the CM server, and that the SSH service and required credentials are configured on the target backup host. A successful backup should also be verified at the destination and included in the organization's recovery and retention process. Avaya's product documentation and support resources provide the applicable Communication Manager administration guidance for backup and restore procedures: Avaya Documentation and Avaya Support.

## QUESTION NO: 6

During SIP Digest authentication for a station registration, which two SIP headers are normally involved in the challenge-and-response exchange? (Choose two.)

**A.** WWW-Authenticate

**B.** Authorization

**C.** Contact

**D.** Via

**E.** Record-Route

**ANSWER: A B**

**Explanation:**

**WWW-Authenticate** and **Authorization** are correct. Session Manager returns a 401 Unauthorized response containing a WWW-Authenticate header to challenge the endpoint. The endpoint then sends a subsequent REGISTER request containing an Authorization header with the calculated Digest credentials.

This exchange is normal SIP registration behavior. The Contact header identifies the endpoint contact location, but it is not the Digest credential response. The Via header supports SIP request and response routing and is not used to carry Digest authentication credentials. See RFC 3261, Section 10 and the Avaya Documentation Portal.

## QUESTION NO: 7

Which Avaya Aura Communication Manager (CM) SAT command is used to display the administered data for station extension 4500?

**A.** status station 4500

**B.** display station 4500

**C.** list station 4500

**D.** change station 4500

**ANSWER: B**

**Explanation:**

`display station 4500` is correct because the `display station` SAT command opens the station form for the specified extension in read-only mode. The displayed form includes the station type, port assignment where applicable, COS and COR assignments, feature-button administration, coverage information, and other station-specific settings.

The `change station` command is used to modify an existing station, while `status station` displays operational status rather than the complete administered station record. See the Avaya Documentation Portal for Communication Manager administration and SAT command references.

## QUESTION NO: 8

You have configured Avaya Aura Communication Manager (CM) as a Managed Element in Avaya Aura System Manager (SMGR), but discover that changes made to translations using SAT are not being updated in the SMGR copy of the CM database.

Which check box on the Inventory screen has not been checked for the CM element?

**A.** Inform SMGR Of SAT Changes

**B.** Sync With SMGR

**C.** Enable Notifications

**D.** Send Updates To SMGR

**ANSWER: A**

**Explanation:**

**Inform SMGR Of SAT Changes** is the required Inventory setting. System Manager maintains a copy of the Communication Manager translation data for administration and management purposes. When an administrator makes a translation change directly on Communication Manager through the System Access Terminal (SAT), that change originates outside the normal System Manager provisioning workflow. Selecting this check box enables Communication Manager to inform System Manager that SAT-originated translation activity has occurred, allowing System Manager to update its managed-element database copy and preserve consistency between the systems.

This setting is especially important in environments where both System Manager-based administration and direct SAT administration are used. Without notification of SAT changes, System Manager can retain an out-of-date representation of the Communication Manager configuration even though the translation was successfully applied on Communication Manager itself. After enabling the setting, administrators should allow the notification and update process to complete before relying on the System Manager inventory data for subsequent administration or reporting. Avaya product documentation and technical resources are available through the Avaya Documentation portal and Avaya Support.

## QUESTION NO: 9

To enable an Avaya Aura Session Manager (SM) to be administered and maintained in a SIP Domain, which step must be performed?

**A.** Add SM as an Instance.

**B.** Add SM as a Serviceability Agent.

**C.** Add SM as a Managed Element.

**D.** Check the Enable box on the SM Entity page.

**ANSWER: C**

**Explanation:**

**Add SM as a Managed Element.** This is the required System Manager administration step that establishes Session Manager as a managed component in the Avaya Aura environment. A managed element represents a managed network application or device and provides System Manager with the connection details and administrative relationship needed to perform ongoing management functions. After the Session Manager is added as a managed element, System Manager can communicate with it for supported configuration, monitoring, and maintenance activities. This relationship is distinct from SIP-domain routing configuration: Session Manager entities and instances are used in the broader Session Manager setup, but registering the server as a managed element is the foundational action that enables System Manager to administer and maintain that Session Manager. The managed-element definition normally includes the Session Manager's network identity and the administrative credentials required for System Manager access, so it should be created with accurate host and security information before continuing with related configuration tasks. Avaya's Session Manager documentation and product resources describe Session Manager's integration with System Manager and its managed administration model. See the Avaya reference material at Avaya DevConnect documentation and the Avaya Aura Session Manager support page.