

Avaya Aura Contact Center Maintenance and Troubleshooting

Avaya 3301

Version Demo

Total Demo Questions: 7

Total Premium Questions: 74

Buy Premium PDF

<https://passqueen.com>

support@passqueen.com

QUESTION NO: 1

Which two Avaya Aura Contact Center (AACC) components are supported by the capacity Assessment Tool (CapTool)? (Choose two.)

- A. License Manager
- B. Security framework
- C. Contact Center Manager Administration
- D. Avaya Media Server
- E. Avaya Aura Agent Desktop

ANSWER: A C

Explanation:

CapTool supports capacity assessment for **License Manager** and **Contact Center Manager Administration**. These are AACC server-side components whose resource requirements must be validated during solution design, deployment, and maintenance. CapTool collects and evaluates the relevant system-capacity information so that the host environment can be assessed against the requirements associated with the enabled AACC applications and the anticipated contact-center workload. For License Manager, this ensures that the licensing service is included in the capacity planning of the AACC deployment. For Contact Center Manager Administration, the assessment addresses the administration application's server role and its required platform resources. Using CapTool before implementation or when expanding an existing deployment helps administrators identify whether the server configuration is appropriate for the intended solution scale and supports a more predictable installation or upgrade outcome. Avaya publishes product documentation and deployment guidance through the [Avaya Documentation portal](#); current product notices, downloads, and support resources are available through [Avaya Support](#).

QUESTION NO: 2

Which two SIP components are normally associated with registering a user address and maintaining the address binding? (Choose two.)

- A. Registrar
- B. Location Service
- C. Redirect Server
- D. RTP Relay
- E. Media Gateway

ANSWER: A B

Explanation:

Registrar and **Location Service** are associated with SIP registration. A SIP registrar receives REGISTER requests and processes the registration information supplied by the user agent. The resulting binding between an address-of-record and its current contact address is stored in the location service.

A proxy server routes SIP requests, and a redirect server returns alternative destination information to a client. Although these components can use registration information, they do not perform the registrar and location-service functions described in the question. SIP registration architecture is described in [RFC 3261, Section 10](#).

QUESTION NO: 3

Which three SIP header elements are used together to identify a SIP dialog after it has been established? (Choose three.)

- A. Call-ID
- B. From tag
- C. To tag
- D. CSeq
- E. Via

ANSWER: A B C

Explanation:

A SIP dialog is identified by the combination of the **Call-ID**, the local tag from the **From** header, and the remote tag from the **To** header. These values allow SIP entities to associate later in-dialog requests, such as BYE, re-INVITE, and UPDATE, with the correct established dialog.

The CSeq header is used to order requests within a dialog, and the Via header records the transport path used by a request or response. Although both are important when analyzing SIP traces, neither forms part of the dialog identifier. Dialog identification is defined in [RFC 3261, Section 12](#).

QUESTION NO: 4

The C:\WINDOWS\system32\drivers\etc\hosts file on the Contact Center Manager Server (CCMS) contains multiple entries for each host. You have removed the duplicate entries by manually editing the file.

What should you do next to completely resolve the issue?

- A. Run the Server Configuration utility, save and apply all changes, then reboot the CCMS server.
- B. Reboot the CCMS server.
- C. Use the windows services utility to restart the MAS Configuration manager services.
- D. Run the CCMS network Configuration utility, save and apply all changes, then reboot the CCMS server.

ANSWER: C

Explanation:

Use the windows services utility to restart the MAS Configuration manager services. On a CCMS, the MAS Configuration Manager maintains and applies Contact Center configuration-related network and host-resolution information. Manually removing duplicate host records corrects the file contents on disk, but the configuration-management components can retain the previously loaded state until they are restarted. Restarting the MAS Configuration Manager services forces those components to reload the corrected hosts-file information and resume management using the cleaned entries. This is the appropriate targeted action after a manual hosts-file correction because it refreshes the affected Avaya configuration layer without requiring unrelated server-wide configuration changes. The hosts file is used by Windows name resolution as a local static mapping source, so ensuring that the service which consumes and manages this information reloads it is necessary for the correction to take full effect in Contact Center operations. For Avaya product documentation and maintenance guidance, consult the [Avaya Documentation portal](#) and the [Avaya Support portal](#).

QUESTION NO: 5

Your department has installed a backup utility client application on your co-resident Contact Center Manager Server (CCMS) server. This utility uses port 10000 for network communications. After installing the utility and rebooting the server, you begin to have issues with the Avaya Aura Contact Center (AACC) system.

What are the symptoms of this problem that you experience?

- A. The TFE service fails to start and calls are not processed.
- B. The Toolkit Name service fails to start and agents appear as "UNKNOWN" in real-time displays.
- C. The NCCT service fails to start and agents are unable to log in via the Avaya Aura Agent Desktop (AAAD).
- D. SymposiumWC.exe fails to start and supervisors are unable to log in to Contact Center Manager Administrator (CCMA).

ANSWER: B

Explanation:

The Toolkit Name service fails to start and agents appear as "UNKNOWN" in real-time displays. This is the expected symptom because Avaya Aura Contact Center reserves TCP port 10000 for the Toolkit Name service. A co-resident backup client that binds to that port first creates a listening-port conflict when the CCMS server is restarted. The Toolkit Name service consequently cannot initialize its network listener and remains unavailable.

Toolkit Name supplies the name-resolution information used by Contact Center components to associate agent and resource identities with the data presented to monitoring clients. When that service is unavailable, real-time displays cannot resolve those identities correctly and show agents as *UNKNOWN*. This is a particularly useful diagnostic signature: after a reboot, check for a process listening on TCP 10000, identify the conflicting backup utility process, and reconfigure that utility to use a non-reserved port before restarting the affected Avaya services. Port assignments and service dependencies must be preserved on a CCMS, since installing third-party software on a co-resident server can interfere with Contact Center service startup. Consult the applicable AACC maintenance documentation and product support resources at [Avaya Documentation](#) and [Avaya Support](#).

QUESTION NO: 6

You are installing Contact Center manager Administrator (CCMA) on a server that has been loaded from a prebuilt image joined to the customer's domain. The server does not have a DVD-ROM drive, so you are installing from a DVD image shared over LAN. During the installation, you encounter several error messages:

- Run-time error '-2147463168 (800005000)'; ASDI Error; an invalid directory pathnamewas passed.
- Script: D:\Avaya\Contract Center\CCMA ADAm\ADAmScripts\lceinstallADM.vbs; theserver is not operational. Code: 8007293A
- Error 0x8007203A on getObject method.

The installation proceeds through the error messages and reports success.

What should you do to ensure the integrity of the CCMA software installation?

- A. Installation of active directory lightweight Domain Services (AD-LDS) may report transient errors when installed on a server that is already a domain member, but if the installation status indicated success, all CCMA components were installed correctly. B. Disable Data Execution protection (DEP) on the server, uninstall CCMA, and then reinstall CCM
- B. Uninstall CCMA, run networkSetup.bat from the DVD image, reinstall CCMA, and then run NetworkSetupReset.bat from the DVD image.
- C. Uninstall CCMA, remove the server from the domain, rejoin it to the domain, and then reinstall the CCMA software.

ANSWER: B

Explanation:

Uninstall CCMA, run `networkSetup.bat` from the DVD image, reinstall CCMA, and then run `NetworkSetupReset.bat` from the DVD image. This is the required recovery procedure when CCMA is installed from a network-shared DVD image rather than local DVD media. The CCMA installation and its Active Directory Application Mode/Active Directory Lightweight Directory Services setup scripts rely on expected installation-media paths and related environment settings. When those prerequisites are not prepared for a LAN-based source, scripts can encounter invalid-path and directory-service connection errors even though the top-level installer subsequently reports completion.

Running `networkSetup.bat` before the reinstall prepares the server for installation from the shared image, allowing the setup routines to locate and use the required source paths consistently. Reinstalling after that preparation is essential because an installation that emitted these errors cannot be treated as a verified, intact deployment merely because the installer displayed a success status. Running `NetworkSetupReset.bat` afterward restores the temporary network-installation configuration, leaving the server in its expected operational state. This process is aligned with Avaya's documented media and support practices; consult the [Avaya Documentation portal](#) for the release-specific CCMA installation guide and [Avaya Support](#) for product advisories and installation resources.

QUESTION NO: 7

In a SIP environment, which component of Avaya Aura Contact Center (AACC) performs call processing?

- A. .NET
- B. SIP Computer Telephony Integration (CTI)
- C. SIP Gateway Manager
- D. SIP Proxy Server
- E. SIP Redirect Server

ANSWER: D

Explanation:

SIP Proxy Server is correct because it is the Avaya Aura Contact Center server-side component responsible for SIP call processing in a SIP-based deployment. It receives and processes SIP signaling, maintains call-related dialog state, and applies the contact-center call-routing and treatment decisions needed to connect, transfer, queue, or otherwise progress calls. It therefore provides the SIP signaling control point through which calls are handled as they enter and move through the contact-center environment. This role is essential to integrating SIP endpoints and SIP trunks with the contact-center application's routing logic while preserving the signaling information required for call control and reporting. The SIP Proxy Server operates as part of the AACC SIP architecture, rather than merely supplying an application runtime or an administrative integration function. Avaya's product information identifies Avaya Aura Contact Center as a solution supporting multichannel contact-center routing and call treatment; its support portal provides the product documentation and release-specific deployment material used to validate component roles. See [Avaya Contact Center](#) and [Avaya Support](#).