

500-444^{Q&As}

Cisco Contact Center Enterprise Implementation and Troubleshooting

Pass Cisco 500-444 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass2lead.com/500-444.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

- ⚙️ **Instant Download** After Purchase
- ⚙️ **100% Money Back** Guarantee
- ⚙️ **365 Days** Free Update
- ⚙️ **800,000+** Satisfied Customers



QUESTION 1

Which mode can be used to display data flow in the Script?

- A. Edit Mode
- B. Monitor Mode
- C. Quick Edit Mode
- D. Browse Mode

Correct Answer: B

Monitor Mode is a feature of the Packaged CCE Script Editor that allows you to view the flow of data through the script. This can be used to troubleshoot any issues with the script and ensure that it is functioning properly. Edit Mode is used to edit the Script, Quick Edit Mode is used to quickly edit basic script elements, and Browse Mode is used to view the data elements available in the Script.

QUESTION 2

What are two roles of a Certificate Authority (CA) in a trusted third-party CA certificate? (Choose two.)

- A. to provide validation of certificate requests
- B. to issue a CA signed Identity certificates
- C. to provide domain validation certificate
- D. to import the root CA certificate to each component
- E. to generate a new Certificate Signing Request (CSR)

Correct Answer: AB

A. to provide validation of certificate requests: A CA is responsible for verifying the identity of an entity before issuing a certificate. This includes verifying the entity's identity, such as by checking government-issued identification or business

registration documents.

B. to issue a CA-signed Identity certificates: After validating the entity's identity, the CA issues the certificate, which is signed by the CA's private key. This certificate can be used to authenticate the identity of the entity, establish trust and

secure communication.

References:

<https://tools.ietf.org/html/rfc5280>

<https://www.globalsign.com/en/ca-services/what-is-a-ca/>

QUESTION 3

What are two considerations for Active Directory (AD)? (Choose two.)

- A. user interface available
- B. Remote Access Control is available for software
- C. Read-Only Domain Controllers (RODC) are supported
- D. global catalogs are required at each AD site
- E. supports multi-domain, single AD Forest topology

Correct Answer: CE

Two considerations for Active Directory (AD) are that Read-Only Domain Controllers (RODC) are supported and that it supports multi-domain, single AD Forest topology. RODC are used to provide secure access to AD data in remote locations, and the multi-domain, single AD Forest topology allows multiple domains to be managed from a single AD forest. Additionally, global catalogs are required at each AD site to enable efficient searches across the entire AD forest. AD does not provide a user interface, but Remote Access Control is available for software that is used to manage and administer the AD environment.

QUESTION 4

Which service must be restarted after modifying the Java Keystore on the CVP servers?

- A. Cisco CVP Call server
- B. Cisco CVP VXML server
- C. Client license service
- D. Cisco CVP WebServicesManager

Correct Answer: D

The WebServicesManager is responsible for managing the secure communication between the CVP servers and the clients, and it requires a valid Java Keystore to function properly. Restarting the service after making changes to the

Keystore ensures that the changes take effect. The other services listed (Cisco CVP Call server, Cisco CVP VXML server, and Client license service) are not related to the Java Keystore and do not require restarting after making changes to

it.

References:

[1] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_8_5/configuration/guide/ccce85cfg/ccce85cfg_chapter_0101.html

[2] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_8_5/configuration/guide/ccce85cfg/ccce85

QUESTION 5

What are two ways to deploy security certificates in CCE? (Choose two.)

- A. Certificate Authority (CA)
- B. 3rd party signed
- C. Security Authority (SA)
- D. Digitally signed
- E. Self-signed

Correct Answer: AD

Two ways to deploy security certificates in CCE are Certificate Authority (CA) and Digitally Signed. A Certificate Authority (CA) is an organization that issues digital certificates to authenticate the identity of a user or service. A digitally signed

certificate is one that is digitally signed by the entity that is issuing it, such as the Certificate Authority. This ensures that the certificate is not tampered with or altered in any way.

References:

[1] https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/crs/express_8_5/configuration/guide/ccce85cfg/ccce85cfg_chapter_0501.html

[2] <https://tools.ietf.org/html/rfc4158>

[Latest 500-444 Dumps](#)

[500-444 PDF Dumps](#)

[500-444 Study Guide](#)