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.pass4itsure.com/500-444.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which signed certificate is less administration in environments with many servers, such as CCE?

A. Self-signed

B. Certificate Authority (CA)

C. 3rd party signed

D. Security Authority (SA)

Correct Answer: B

The signed certificate that is less administration in environments with many servers, such as CCE, is the Certificate Authority (CA) signed certificate. This type of certificate is signed by a trusted Certificate Authority (CA), which eliminates the need to manually manage each server\\'s certificate. The CA signed certificate is also more secure than a self-signed or third-party signed certificate, as the CA has verified the identity of the certificate\\'s owner and can revoke it if necessary. Security Authority (SA) signed certificates are not commonly used in CCE environments.

QUESTION 2

What should be deployed to provide a web-based administrative interface even though Unified CCE provides Configuration Manager as the legacy User Interface for administrators?

A. WebSetup

B. Contact Centre Management Portal (CCMP)

C. LDAP Plugin

D. Single Pane of Glass (SPOG)

Correct Answer: D

Single Pane of Glass (SPOG) is a web-based administrative interface that provides administrators with an intuitive and unified view of the entire contact center environment. It is designed to provide administrators with a single interface to manage all aspects of the contact center, including agents, skills, queues, and reports. SPOG provides a more user-friendly interface than the legacy Configuration Manager, making it easier for administrators to manage the contact center environment. Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucce/spog/10_5_1/cce_b_spog-admin-guide-1051.html

QUESTION 3

Which three features does Cisco Unified Border Element provide when CCE and Cisco Unified Customer Voice Portal are used? (Choose three.)

A. Silent Monitor inbound voice calls

B. NAT for address hiding D Demarcation point between networks

C. Record calls by forking the media using build-in-bridge

D. Secure communication using flow around mode

E. Normalize SIP messages using SIP profiles

Correct Answer: BDE

Cisco Unified Border Element (CUBE) is a network element that provides a number of features for securing and controlling voice, video, and data communications when Cisco Unified Communications Manager (CUCM) and Cisco Unified Customer Voice Portal (CVP) are used. NAT for address hiding: CUBE provides Network Address Translation (NAT) capabilities that allow you to hide the internal IP addresses of the CVP and CUCM servers from the public Internet. This is useful for security and compliance reasons, as it makes it harder for hackers to identify and attack these servers. Demarcation point between networks: CUBE acts as a demarcation point between the customer network and the service provider network. This allows for secure and controlled communication between the two networks. Normalize SIP messages using SIP profiles: CUBE can normalize SIP messages using SIP profiles, which allows it to ensure that incoming SIP messages conform to a specific format and contain the necessary headers and parameters. This can help to improve the reliability and security of SIP-based communications. Silent Monitor inbound voice calls: CUBE does not provide silent monitor feature, it is a feature of CUCM that allows a supervisor to listen in on an agent\\'s call without the agent or the caller knowing. Record calls by forking the media using build-in-bridge: CUBE does not provide this feature, it is a feature of CUCM that allows for call recording by forking the media through a built-in bridge. References: Cisco Unified Border Element Configuration Guide (https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cube/12_5/cube_12_5_configuration_guide/cube_12_5_configuration_guide_chapter_01.html)

QUESTION 4

Which two certificates need to be uploaded to VOS servers for CA Signed certificate management? (Choose two.)

A. CA Certificate:tomcat

B. CA Signed Certificate from CSR Request:tomcat

C. 3rd party signed Certificate

D. CA Certificate:tomcat-trust

E. CA Signed Certificate from CSR Request:tomcat-trust

Correct Answer: AD

These two certificates need to be uploaded to VOS servers for CA Signed certificate management. The CA Certificate is used to verify the authenticity of the server and the CA Signed Certificate from the CSR Request is used to generate the server\\'s private key. The tomcat-trust certificate is used by the server to trust other SSL certificates. Reference: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/tutorial-certificate-management#upload-the-certificates

QUESTION 5

Which two certificates do the Cisco Finesse primary and secondary servers accept when HTTPS protocol is used to access the administration console or agent desktop in Cisco Finesse? (Choose two.)

A. Domain validation certificate

B. Digital certificate

C. Self-signed certificate

D. Certificate authority certificate

E. Root certificate

Correct Answer: BD

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cust_contact/contact_center/finesse /finesse_1151/Admin/guide/CFIN_BK_C0CD262D_00_cisco-finesse-administration-guide-1151/CFIN_BK_C0CD262D_00_cisco-finesseadministration-guide-1151_chapter_01001.pdf

When the HTTPS protocol is used to access the administration console or agent desktop in Cisco Finesse, the primary and secondary servers accept only digital certificates that are issued by a certificate authority (CA).

A digital certificate is an electronic document that uses a digital signature to bind a public key with an identity, such as the name of a person or an organization, and the certificate is issued by a trusted third party, such as a certificate authority

(CA). The digital certificate confirms the identity of the server and enables secure communication between the client and the server.

A certificate authority (CA) certificate is a type of digital certificate that is issued by a trusted third party, such as a certificate authority (CA), to verify the identity of an entity and establish trust.

References:

https://www.cisco.com/c/en/us/support/docs/voice-unified-communications/finesse/118248-configure-certificates-finesse-00.html

https://www.globalsign.com/en/ssl-information-center/what-is-a-digital-certificate/