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.certbus.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 core components are required for calls that originate from Cisco Unified Communications Manager to Cisco Unified CVP using Comprehensive mode when using microapps?

A. CUCM: CTI Route Port, SIP Trunk, ICM: CVP Type 2 VRU, CUBE. VXML Gateway

B. CUCM: CTI Route Point and SIP Trunk, ICM: CVP Type 2 VRU and Network VRU labels, VXML Gateway

C. CUCM: CTI Route Port and SIP Trunk, ICM: CVP Type 10 VRU and Network VRU labels, VXML Gateway

D. CUCM: CTI Route Point and SIP Trunk, ICM: CVP Type 10 VRU and Network VRU labels, VXML Gateway

Correct Answer: B

For calls that originate from Cisco Unified Communications Manager (CUCM) to Cisco Unified CVP using Comprehensive mode when using microapps, core components that are required include a CUCM CTI Route Point and SIP Trunk, an ICM CVP Type 2 VRU, Network VRU labels, and a VXML Gateway. CVP Type 10 VRUs are not required for such calls.

QUESTION 2

Which CLI command manages the Java Keystore Certificate in Windows CCE servers?

A. PROCMON

B. OPENSSL

C. System CLI

D. Keytool

Correct Answer: D

Keytool is the command-line tool used to manage the Java Keystore Certificate in Windows CCE servers. This tool is used to create, import, and export certificates for use with Java applications. It can also be used to view the certificate request, as well as to modify the certificate\\'s friendly name and store name. This can be useful for managing Java Keystore Certificates on Windows CCE servers. Reference: https://docs.oracle.com/cd/E19509-01/820-3503/gghji/index.html

---

QUESTION 3

What are two components of Cisco VOS? (Choose two.)

A. Finesse

B. CCE

C. CUIC

D. CVP

E. ECE

Correct Answer: BD

Cisco VOS (Virtualized Operating System) is a cloud-based platform that enables service providers to deliver real-time voice, video, and data services to their customers. The two core components of Cisco VOS are Cisco CCE (Customer Care Environment) and Cisco CVP (Customer Voice Portal). CCE is a cloud-based contact center solution that provides organizations with the ability to manage customer interactions and deliver personalized experiences. CVP is a cloud-based voice portal that enables organizations to create automated customer service experiences. Finesse, CUIC, and ECE are not components of Cisco VOS.

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 tasks of a PCCE initialization under Unified CCE PG? (Choose two.)

A. Creates the CUCM Peripheral Gateway (PG) with the CUCM PIM.

B. Creates just VRU PG; VRU PIMs need to be added manually.

C. Creates the Media Routing PG (MR PG) with three MR PIMs.

D. Downloads JTAPI from the Unified Communications Manager and installs it on the Unified CCE PG.

E. Downloads JTAPI from the Unified Communications Manager, but manually need to be installed in the Unified CCE PG.

Correct Answer: CD

QUESTION 6

Which telephony deployment is between a TDM trunk and a VOIP?

A. CUCM

B. CUBE

C. Voice gateway (VGW)

D. CUSP

Correct Answer: C

The telephony deployment between a TDM trunk and a VOIP is a voice gateway (VGW). A voice gateway is a hardware or software device that acts as a bridge between a TDM trunk and a VOIP network. It allows TDM and VOIP calls to be connected and terminated, and can also provide additional features such as call routing, call forwarding, call waiting, and call recording. CUCM, CUBE, and CUSP are not involved in this type of deployment.

QUESTION 7

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/

QUESTION 8

Which type of machine will run an automated deferred sync job?

A. Principal AW machine

B. AW client machine

C. Secondary AW machine

D. AW/HDS machine

Correct Answer: D

An AW/HDS machine is a hybrid of an AW client machine and a Secondary AW machine, and it is used to run automated deferred sync jobs. These jobs are typically used to transfer data between two or more AW machines, and the AW/HDS

machine acts as the intermediary, making sure that all of the data is kept up-to-date and in sync.

References:

[1] https://www.oracle.com/webfolder/technetwork/tutorials/obe/fmw/oim/11gR2-PS3/OIM_11gR2_PS3_Installation/OIM_11gR2_PS3_Installation_Step2.html

[2] https://doc s.oracle.com/cd/E24628_01/doc.121/e28814/config_hds_aw.htm

[3] https://docs.oracle.co m/en/middleware/lifecycle/12.2.1.4/core/one-time-processes-deferred-synchronization-jobs.html

QUESTION 9

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 10

Where can the SAML Certificate Expiry details be checked in PCCE Web Administration Manager (S.RO.G)?

A. Features -> Context Service

B. Infrastructure Settings -> License Management

C. Features -> Single Sign-On

D. Infrastructure Settings -> Device Configurations -> Identity Services

Correct Answer: C

The SAML Certificate Expiry details can be checked in the PCCE Web Administration Manager (S.RO.G) under the Features -> Single Sign-On menu. This menu can be used to view the certificate details, such as the issuer, validity period,

and expiry date. This can be useful for ensuring that the certificate does not expire before its intended use.

Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/pccx/pccx_11_0_ 1/pccx_b_pccx-web-admin-manager-guide-110/pccx_b_pccx-web-admin-manager-guide_chapter_011.html