Free Questions for 300-810 by dumpshq

Shared by Small on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What are two benefits of deploying OAuth in a Cisco UCM environment that uses Cisco Jabber or Cisco Webex for on-premises calling?(Choosetwo.)

Options:

A- Layers of security are added due to forced user password prompt.

B- It removes the need for Jabber and Webex clients to re-authenticate frequently.

C- Refresh tokens are encrypted.

D- It provides seamless access to resources over the life of the refresh token.

E- Token expiration can never take place, which ensures that users stay logged in.

Answer:

B, D

Explanation:

These two options are the benefits of deploying OAuth in a Cisco UCM environment that uses Cisco Jabber or Cisco Webex for on-premises calling. OAuth is an authorization protocol that allows users to grant access to third-party applications without sharing their credentials. In a Cisco UCM environment, OAuth allows Jabber and Webex clients to obtain access tokens from UCM after authenticating with their credentials once. The access tokens can then be used to access various resources, such as call control, voicemail, directory, and presence. The access tokens have a limited lifetime, but they can be refreshed using refresh tokens, which have a longer lifetime. This way, the users do not need to re-authenticate frequently and can enjoy a seamless user experience. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/12_5_1/systemConfig/cucm_b_system-configuration-guide-1251/cucm_b_system-configuration-guide-1251_chapter_0100110.html

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/jabber/11_9/Unified-CM-OAuth-Whitepaper-v17-FINAL.pdf

Question 2

Question Type: MultipleChoice

A collaboration engineer is troubleshooting MWI issues with Cisco Unity Connection and Cisco UCM. Users report that MWI lights do not work when a new message is received. After doing a packet capture, the engineer notices that Unity Connection sends a SIP Notify to Cisco UCM for MWI.Cisco UCM responds with a SIP 503 Service Unavailable message. Which action resolves the issue?

Options:

A- Configure the SIP server list on the Cisco Unity Connection port group to match the Cisco UCM device pool settings on the SIP trunk.

B- Assign the proper voicemail profile to the directory numbers on Cisco UCM.

C- Uncheck'Send Message Counts' on the phone system settings on Cisco Unity Connection.

D- Uncheck'Accept unsolicited notifications' on the SIP trunk security profile.

Answer:

A

Explanation:

This option is the correct action to resolve the issue of MWI not working when a new message is received. The SIP server list on the Cisco Unity Connection port group defines the destination addresses for SIP messages, such as MWI notifications, that Unity Connection sends to Cisco UCM. If the SIP server list does not match the device pool settings on the SIP trunk, Cisco UCM may not be able to route the MWI notifications to the correct devices, and may respond with a SIP 503 Service Unavailable message. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/integration/guide/cucm_sip/cucintcucmsip100x.pdf

https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/200453-Configure-MWI-for-SIP-Integration-Betwee.html

Question 3

Question Type: MultipleChoice

What provides device monitoring when integrating Cisco UACA and Cisco UCM?

Options:

A- SIP

B- XMPP

C- CTI/TAPI

D- AXL

Answer:

C

Explanation:

This option is the correct protocol that provides device monitoring when integrating Cisco UACA and Cisco UCM. CTI/TAPI stands for Computer Telephony Integration/Telephony Application Programming Interface, and it allows Cisco UACA to monitor and control the

devices registered to Cisco UCM. CTI/TAPI is also used for call control, call park, call pickup, and other features on Cisco UACA.
Reference:

https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucmac/cuaca/12_0_3/admin_guide/CUACA_AG_120301.pdf

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/admin/10_0_1/ccmfeat/CUCM_BK_F3AC1C0F_00_cucm-features-services-guide-100/CUCM_BK_F3AC1C0F_00_cucm-features-and-services-guide_chapter_010010.html

Question 4

Question Type: MultipleChoice

On a Cisco IM and Presence deployment, chat settings are edited, or one or more aliases are added to a chat node, but the changes are not reflected for users. Which service must be restarted for changes to be reflected?

Options:

A- TFTP Service

B- Cisco XCP Text Conference Manager Service

C- IM and Presence Manager Service

D- User Management Service

Answer:

B

Explanation:

This option is the correct service to restart for changes to chat settings or chat node aliases to be reflected for users. The Cisco XCP Text Conference Manager Service is responsible for managing chat rooms and chat sessions on the IM and Presence Service. If this service is not restarted after making changes to chat configuration, the users may not see the updated settings or aliases. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/10_5_1/CUP0_BK_CE43108E_00_config-admin-guide-imp-105/CUP0_BK_CE43108E_00_config-admin-guide-imp-105_chapter_0110.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/11_5_1/CUP0_BK_CE08159C_00_config-admin-guide-imp-1151/CUP0_BK_CE08159C_00_config-admin-guide-imp-1151_chapter_01100.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/11_5_1/cup0_b_config-and-admin-guide-1151su5/cup0_b_imp-system-configuration-1151su5_chapter_01111.html

Question 5

Question Type: **MultipleChoice**

A collaboration engineer is troubleshooting Cisco IM and Presence high availability. The system is version 10.x. The engineer has confirnd that the server recovery manager service is configured using system defaults. The engineer notices that user sessions have not fallen back to the homed nodes. What is the cause this Issue?

Options:

A- The engineer did not click the Fallback button for the redundancy group

B- The user accounts were moved to the redundant server,

C- The failed service Of server was offline longer than the Client Re-Login upper Lint setting.

D- The failed service or server has not been active for at least 30 minutes.

Answer:

C

Explanation:

This option explains why the user sessions have not fallen back to the homed nodes after the failed service or server was restored. The Client Re-Login upper limit setting determines how long the Jabber clients will attempt to re-login to their homed nodes after a failover event. If the failed service or server is offline longer than this setting, the Jabber clients will stop trying to re-login and will remain on the backup node until the administrator manually initiates a fallback or recovery. The default value for this setting is 30 minutes, but it can be changed in the Server Recovery Manager Service Parameters. Reference:

https://www.cisco.com/c/en/us/support/docs/unified-communications/unified-communications-manager-im-presence-service/200958-IM-and-Presence-Server-High-Availability.html

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/11_5_1/cup0_b_config-and-admin-guide-1151su5/cup0_b_imp-system-configuration-1151su5_chapter_0100.html

Question 6

Question Type: MultipleChoice

A collaboration engineer is implementing toll fraud prevention on Cisco Unity Connection. The engineer wants to block calls to 9005551234 for any caller that reaches the Caller System Transfer conversation. Which configuration accomplishes this goal?

Options:

A- 9005551234 blocked the Default System Transfer Restriction

B- 9005551234 blocked the Default Outdial Restriction Table

C- 900 blocked on the default Transfer Restriction Table

D- 900 blocked on the Default Outdial Restriction Table

Answer:

C

Explanation:

This option blocks calls to 9005551234 for any caller that reaches the Caller System Transfer conversation, which is one of the ways that Cisco Unity Connection can transfer calls outside. The default Transfer Restriction Table is associated with the default System Call Handler class of service, which is used by the Caller System Transfer conversation. Blocking 900 on this table prevents toll fraud by restricting calls to any number that starts with 900, which are usually premium-rate numbers. Reference:

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/10x/security/guide/10xcucsecx/10xcucsec020.html

https://www.cisco.com/c/en/us/support/docs/unified-communications/unity-connection/119337-technote-cuc-00.html