Free Questions for 300-810 by certsinside

Shared by Stein on 22-07-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

A Collaboration engineer is implementing the Apple Push Notification service for Jabber clients running on iOS and has saved the configuration in Cisco UCM under Advanced Features > Cisco Cloud Onboarding What is the next step to install Cisco-managed certificates?

Options:

A- Restart the Cisco Tomcat service on all nodes in the Cisco UCM cluster

B- Restart the Cisco Tomcat service on all nodes m the IM and Presence cluster

C- Restart the Cisco XCP router service on IM and Presence

D- Restart the Cisco UCM Push Notification service.

Answer:

A

Explanation:

After configuring Apple Push Notification (APN) Service for Jabber on iOS in Cisco UCM, the next step is to restart the Cisco Tomcat service on all UCM cluster nodes for the changes to take effect and to generate and install the required Cisco-managed certificates.

Question 2

Question Type: MultipleChoice

Collaboration engineer configures Cisco UCM and Cisco IM and Presence to support Cisco Jabber Clients. The base configuration is complete The engineer successfully used all the Jabber features a test client but received certificate alerts when signing in. The engineer now wants to ensure that end users do not receive certificate alerts at login. Which two self-.... certificate must be.. with a CA-signed certificate to achieve this goal? (Choose two)

Options:

A- Tomcat

B- cup-xmpp

C- cup-xmpp-s2s

D- cup

E- IPsec

Answer:

B, C

Explanation:

Based on the information you provided and the image (though I cannot access the specific content of the image), for Cisco Jabber clients to avoid certificate trust warnings during login, two certificates need to be replaced with CA-signed certificates:

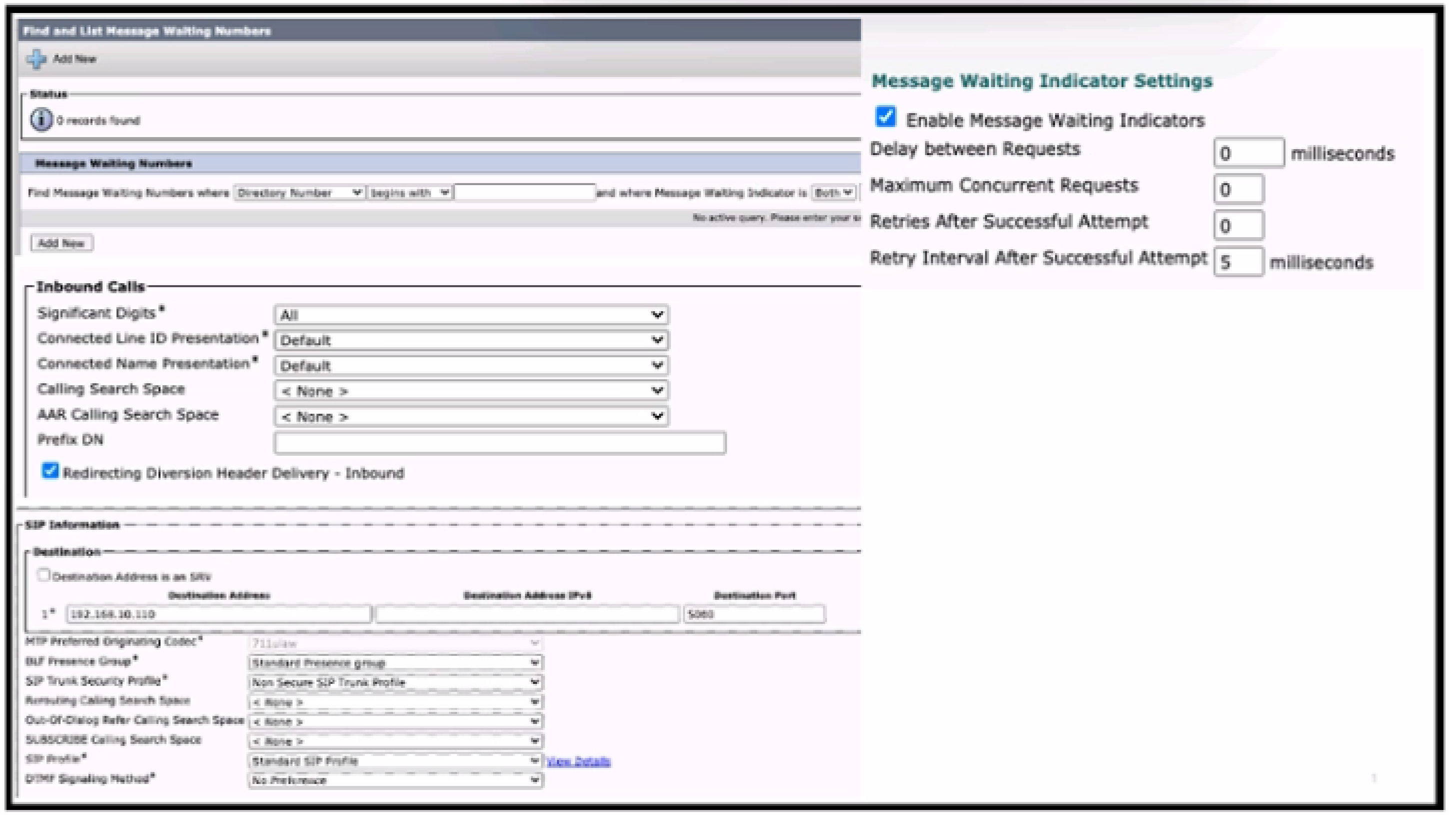
B) cup-xmpp:This certificate secures the connection between Cisco Jabber and the Cisco UCM XMPP server for instant messaging and presence functionalities.

C) cup-xmpp-s2s:This certificate secures the connection between XMPP servers for inter-cluster communication within Cisco UCM, which can also impact Jabber functionality.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



Find and List Message Waiting Numbers

Add New

Status

0 records found

Message Waiting Numbers

Find Message Waiting Numbers where Directory Number begins with and where Message Waiting Indicator is Both

No active query. Please enter your s

Add New

Inbound Calls

Significant Digits*	All
Connected Line ID Presentation*	Default
Connected Name Presentation*	Default
Calling Search Space	< None >
AAR Calling Search Space	< None >
Prefix DN	

☑ Redirecting Diversion Header Delivery - Inbound

SIP Information

Destination

□ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	192.168.10.110		5060

MTP Preferred Originating Codec*	711ulaw
BLF Presence Group*	Standard Presence group
SIP Trunk Security Profile*	Non Secure SIP Trunk Profile
Rerouting Calling Search Space	< None >
Out-Of-Dialog Refer Calling Search Space	< None >
SUBSCRIBE Calling Search Space	< None >
SIP Profile*	Standard SIP Profile
DTMF Signaling Method*	No Preference

Message Waiting Indicator Settings

☑ Enable Message Waiting Indicators

Delay between Requests	0	milliseconds
Maximum Concurrent Requests	0	
Retries After Successful Attempt	0	
Retry Interval After Successful Attempt	5	milliseconds

Refer to the exhibit A collaboration engineer is troubleshooting an issue with MWIs not working for SIP-integrated Cisco Unity Connection users on Cisco UCM Calls to the Cisco Unity Connection work. but MWIs do not light This problem affects all users on the system Which action resolves the issue?

Options:

A- Modify the SIP Trunk Security Profile on Cisco UCM.

B- Increase the Delay Between Requests timer on Cisco Unity Connection

C- Assign a Calling Search Space to the SIP Trunk on Cisco UCM

D- Configure the Message Waiting Numbers on Cisco UCM

Answer:

D

Explanation:

The scenario describes an issue where Message Waiting Indicators (MWIs) aren't lighting up for SIP-integrated Cisco Unity Connection users, even though calls reach voicemail. This points towards a configuration problem with MWI notifications on Cisco UCM.

A) Modify the SIP Trunk Security Profile on Cisco UCM:While SIP trunk security is important, it likely wouldn't affect MWI functionality in this case.

B) Increase the Delay Between Requests timer on Cisco Unity Connection:This setting might be used for other purposes but wouldn't directly address MWI notification issues on Cisco UCM.

C) Assign a Calling Search Space to the SIP Trunk on Cisco UCM:Calling Search Space defines call routing, not MWI notification.

Question 4

Question Type: **MultipleChoice**

When Cisco United Attendant Console Advanced is integrated with Cisco UCM. which Cisco UCM Service does the Cisco TSP Instance communicate with directly?

Options:

A- Cisco CTI Manager Service

B- Cisco DirSync Service

C- Cisco CallManager Service

D- Cisco TAPS Service

Answer:

C

Explanation:

Cisco Unified Attendant Console Advanced (CUACA) integrates with Cisco Unified Communications Manager (UCM) to provide advanced call handling features for attendants. CUACA communicates directly with the Cisco CallManager Service for core call routing, call control, and call state information.

Cisco CTI Manager Service:While CTI (Computer Telephony Integration) plays a role in CUACA interactions, the core communication happens through the CallManager Service.

Cisco DirSync Service:This service synchronizes directory information between UCM and other systems, but it's not directly involved in CUACA communication.

Cisco TAPS Service:TAPS (Telephony Application Programming Services) provides a development framework for UCM, not core call routing functionalities used by CUACA.

Question 5

Question Type: MultipleChoice

Which option is a prerequisite for selecting a third -party IdP for Cisco Collaboration?

Options:

A- LDAP

B- SAML 1.0

C- SAML 2.0

D- SAML 1.1

Answer:

C

Explanation:

Security Assertion Markup Language (SAML) is a widely used standard for single sign-on (SSO) and is a prerequisite for using a third-party identity provider (IdP) with Cisco Collaboration applications. While other options might be related to authentication protocols, SAML 2.0 is the current standard supported by Cisco for integration with third-party IdPs.

Question 6

Question Type: MultipleChoice

An engineer is troubleshooting an issue with Cisco Unity Connection. Users report that they receive a busy tone when they attempt to dial the voicemail pilot number. Which tool must the engineer use to view the activity on the voicemail ports as users try to place calls'

Options:

A- Remote Database Administration tools

B- Remote Up and Down utility

C- Port monitor option in Real Time Monitoring Tool

D- Application Audit logging

Answer:

C

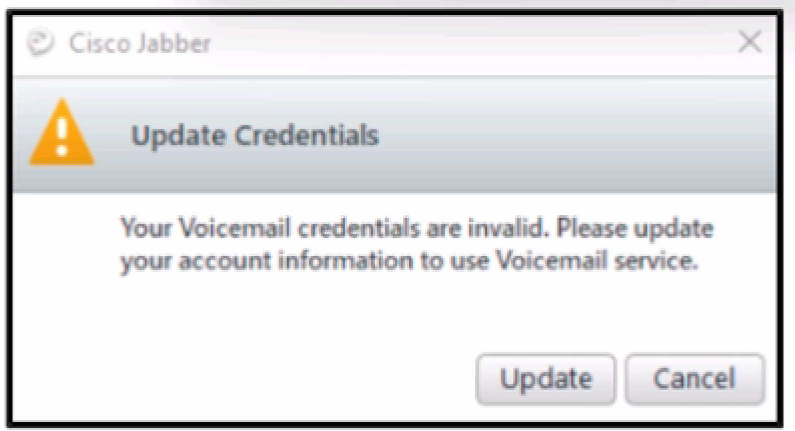
Explanation:

Troubleshooting a busy tone on the voicemail pilot number in Cisco Unity Connection typically involves analyzing voicemail port activity. The Real-Time Monitoring Tool (RTMT) within Cisco Unified Communications Manager (UCM) offers a port monitor option that allows you to monitor activity on specific ports, including voicemail ports.

Question 7

Question Type: **MultipleChoice**

Refer to the exhibit.



Cisco Jabber

Update Credentials

Your Voicemail credentials are invalid. Please update your account information to use Voicemail service.

A company integrated their newly deployed Cisco Jabber over Mobile and Remote Access with Cisco Unity Connection for voicemail access but users must manually enter their email credentials each time they log in to Cisco Jabber Which action resolves the issue?

Options:

A- Add Cisco UCM as an Authz Server on Unity Connection.

B- Add the Unity Connection Service Profile to the end users in Cisco UC Manager

C- Create a UC Service and Service Profile for Unity Connection

D- Add Unity Connection in the Expressway-C

Answer:

B

Explanation:

The image shows an error message indicating 'Your Voicemail credentials are invalid'. This suggests a configuration issue where Cisco Jabber and Unity Connection aren't properly linked for automatic credential passing. Adding the Unity Connection Service Profile to user accounts in Cisco UC Manager establishes the link and enables Single Sign-On (SSO) for voicemail access.

Question 8

Question Type: MultipleChoice

An organization wants to run on-premises instant messaging (IM), and resilience is important because this is a business-critical application for them. The organization has three locations with Cisco UCM clusters in each location. Which additional configuration is needed to meet these requirements?

Options:

A- Expand the Cisco UCM cluster with Cisco IM and Presence nodes in each location

B- Configure IMP functionality in Cisco UCM with failover. Cisco IM and Presence servers are not needed from systems release 14 X and newer.

C- Deploy a central Cisco IM and Presence server at one central location because users will log in to Cisco UCM in case of a failover

D- Deploy a minimum of two Cisco IMP servers per location, with one publisher and one subscriber connected to the existing local cluster.

Answer:

D

Explanation:

The logs don't directly address this question, but based on best practices for on-premises IM and Presence with Cisco UCM:

Disaster recovery and failover are crucial for business-critical applications like IM.

Deploying two Cisco IMP servers (one publisher, one subscriber) per location provides redundancy within each location's Cisco UCM cluster.

While Cisco UCM can potentially handle some IM functionality without a separate IM and Presence server in newer versions, Cisco IMP offers a more robust solution with features like disaster recovery.

Question 9

Question Type: MultipleChoice

Collaboration engineer is enabling desk phone control for an existing group of Cisco Jabber desktop users. The users have been granted the appropriate permissions in Cisco UCM. and the devices correctly configured in Cisco UCM. Which service must the engineer now enable?

Options:

A- Cisco CTIManager

B- Cisco XCP Authentication Service

C- Cisco Extended Functions

D- Cisco XCP Connection Manager

Answer:

D

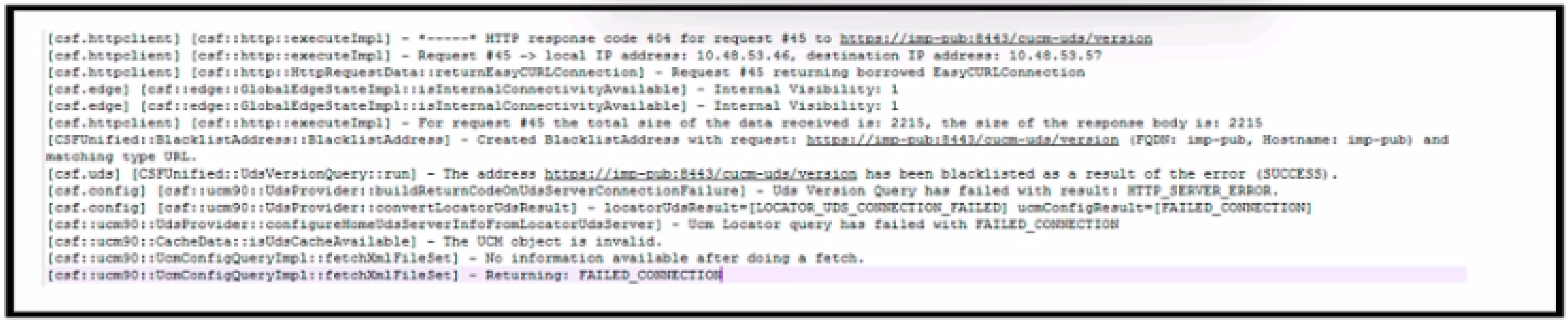
Explanation:

Enabling desk phone control for Cisco Jabber desktop users involves Cisco XCP (Extended Control Protocol). XCP Connection Manager manages the connection between Jabber and the Cisco UCM for features like desk phone control.

Question 10

Question Type: MultipleChoice

Refer to the exhibit.



```
[csf.httpclient] [csf::http::executeImpl] - *-----* HTTP response code 404 for request #45 to https://imp-pub:8443/cucm-uds/version
[csf.httpclient] [csf::http::executeImpl] - Request #45 -> local IP address: 10.48.53.46, destination IP address: 10.48.53.57
[csf.httpclient] [csf::http::HttpRequestData::returnEasyCURLConnection] - Request #45 returning borrowed EasyCURLConnection
[csf.edge] [csf::edge::GlobalEdgeStateImpl::isInternalConnectivityAvailable] - Internal Visibility: 1
[csf.edge] [csf::edge::GlobalEdgeStateImpl::isInternalConnectivityAvailable] - Internal Visibility: 1
[csf.httpclient] [csf::http::executeImpl] - For request #45 the total size of the data received is: 2215, the size of the response body is: 2215
[CSFUnified::BlacklistAddress::BlacklistAddress] - Created BlacklistAddress with request: https://imp-pub:8443/cucm-uds/version (FQDN: imp-pub, Hostname: imp-pub) and
matching type URL.
[csf.uds] [CSFUnified::UdsVersionQuery::run] - The address https://imp-pub:8443/cucm-uds/version has been blacklisted as a result of the error (SUCCESS).
[csf.config] [csf::ucm90::UdsProvider::buildReturnCodeOnUdsServerConnectionFailure] - Uds Version Query has failed with result: HTTP_SERVER_ERROR.
[csf.config] [csf::ucm90::UdsProvider::convertLocatorUdsResult] - locatorUdsResult=[LOCATOR_UDS_CONNECTION_FAILED] ucmConfigResult=[FAILED_CONNECTION]
[csf::ucm90::UdsProvider::configureHomeUdsServerInfoFromLocatorUdsServer] - Ucm Locator query has failed with FAILED_CONNECTION
[csf::ucm90::CacheData::isUdsCacheAvailable] - The UCM object is invalid.
[csf::ucm90::UcmConfigQueryImpl::fetchXmlFileSet] - No information available after doing a fetch.
[csf::ucm90::UcmConfigQueryImpl::fetchXmlFileSet] - Returning: FAILED_CONNECTION
```

A collaboration engineer is If troubleshooting Cisco Jabber for Windows login issues for clients on a corporate network with an on-premises Cisco IM and Presence server. This issue is acting all users. Which action resolves the issue?

Options:

A- Add the host 'imp-pub' to the proxy exceptions list on the users' Windows computers.

B- Restart the IM and Presence services on the host 'imp-pub'

C- Change the DNS SRV record to point to the Cisco UCM node instead of the IM and Presence node

D- Restore network connectivity to host imp-pub'

Answer:

D

Explanation:

The logs mention 'cafrumrideret codes LOCATOR_CONNECTION_FAILED' and 'CSFUnified BlacklistAddress' followed by 'imp-pub'. This indicates an issue connecting to the host 'imp-pub'. Since all users are affected, it suggests a network connectivity problem to the IM and Presence server (imp-pub) rather than individual client configurations.

Question 11

Question Type: **MultipleChoice**

Which two are two-factor authentication methods? (Choose two)

Options:

A- OAuth

B- WebView2

C- biometrics

D- username and password

E- hardware token

Answer:

C, E

Explanation:

Two-factor authentication (2FA) involves using two distinct categories of evidence to verify a user's identity. Here's why the answers are correct:

C) biometrics:Biometric factors like fingerprints, facial recognition, or voice patterns are unique to an individual and fall under the 'something you are' category of authentication.

E) hardware token:A hardware token generates a time-based code, representing 'something you have'. This code adds another layer of security.

Question 12

Question Type: **MultipleChoice**

An engineer is configuring toll fraud prevention on a Cisco Unity Connection system. The Unity Connection system is integrated with two phone systems each with its own trunk access code Which figuration blocks attempts to bypass the restriction table by dialing trunk access codes?

Options:

A- Add restriction table patterns to match applicable trunk access codes for both phone system integrations

B- Restrict the numbers that can be used for system transfers

C- Set up all restriction tables to block calls to the international operator

D- Set up restriction tables to block all calls to international numbers.

Answer:

A

Explanation:

Toll fraud prevention on Cisco Unity Connection often involves restriction tables, which define patterns of phone numbers that are allowed or disallowed. To prevent users from dialing out using trunk access codes and potentially making unauthorized long-distance calls, here's the logic:

Identify trunk access codes:Determine the specific codes that allow external calls on each phone system. These are often single-digit codes like '9'.

Add patterns to restriction tables:Within the Cisco Unity Connection restriction tables, create patterns that block any number starting with the trunk access code for each respective phone system.