DUMPSBOSS.

Implementing Cisco Collaboration Cloud and Edge Solutions (300-820 CLCEI)

Cisco 300-820

Version Demo

Total Demo Questions: 26

Total Premium Questions: 269

Buy Premium PDF

https://dumpsboss.co

support@dumpsboss.co

support@dumpsboss.co
dumpsboss.co

Topic Break Down

Topic	No. of Questions
Topic 1, Cloud Collaboration and Edge Solutions	226
Topic 2, Cisco Unified Communications Manager	6
Topic 3, Cisco Collaboration Applications	16
Topic 4, Collaboration Security	21
Total	269

QUESTION NO: 1

Which two statements about Webex Hybrid Data Security are true? (Choose two.)

A. It uses customer-deployed key management components in an organization-controlled environment.

B. It protects encryption keys used for Webex App content.

C. It requires all Webex App users to connect through a VPN.

D. It replaces directory synchronization between an enterprise directory and Control Hub.

E. It provides a TURN relay for Webex meeting media.

ANSWER: A B

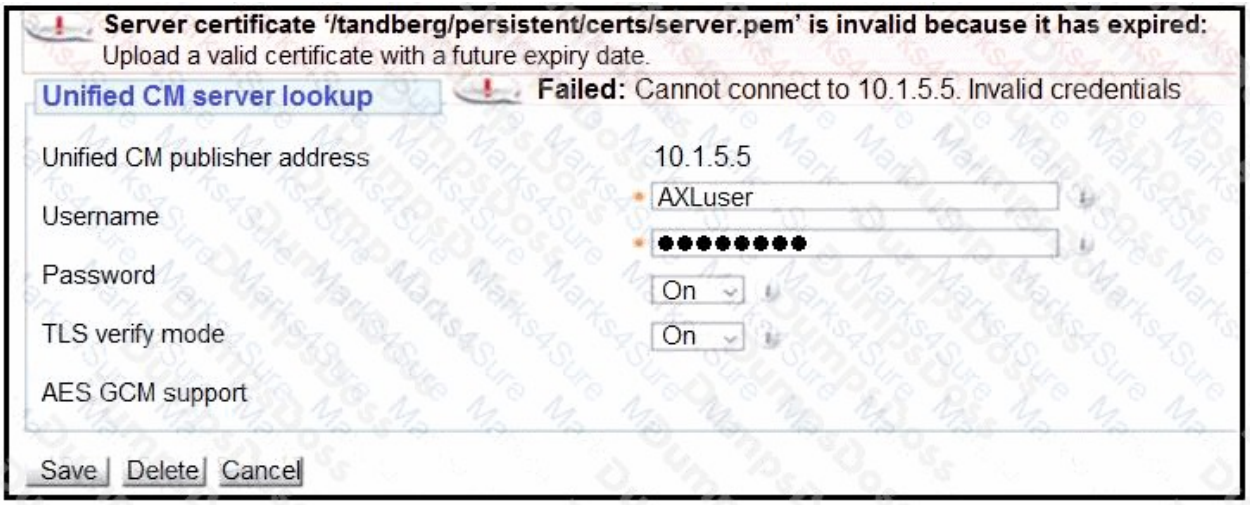
Explanation:

Webex Hybrid Data Security uses customer-deployed key management components in an organization-controlled environment. This allows the organization to retain control of key-management functions while using Webex cloud collaboration services.

Hybrid Data Security protects Webex App content encryption keys. The Webex cloud can continue to provide collaboration services, but content remains encrypted and requires access to the customer-controlled key-management environment for decryption operations.

Hybrid Data Security does not require every Webex user to connect by VPN, and it does not provide a media relay for Webex meetings. Cisco documents the architecture, key-management role, and deployment prerequisites in the Deploy Hybrid Data Security guide.

QUESTION NO: 2



Refer to the exhibit. An engineer is configuring Cisco Expressway-C to discover Cisco UCM by using an IP address and a TCP connection. After the configuration is saved, errors occur.

Which two changes must be made to resolve the errors? (Choose two.)

A. Configure an application user with Cisco Computer Telephony Integration-enabled privileges in Cisco UCM.

B. Configure an application user with Administrative XML privileges in Cisco UCM.

C. Upload a valid Cisco Tomcat certificate from the Cisco UCM to Expressway-C.

D. Set TLS verify mode to Off.

E. Configure an HTTP allow list that contains the Cisco UCM

ANSWER: B D

Explanation:

Configure an application user with Administrative XML privileges in Cisco UCM because Expressway-C uses the Cisco Unified CM Administrative XML (AXL) interface to query Unified CM configuration data during discovery. The credentials entered for the Unified CM server on Expressway-C must therefore belong to an application user that is assigned the Standard AXL API Access role (described here as Administrative XML privileges). This access allows Expressway-C to perform the required discovery and synchronization queries.

Set TLS verify mode to Off because the Unified CM server is being addressed by its IP address. With certificate verification enabled, Expressway-C validates the identity presented by Unified CM against the configured server address. A typical Cisco Tomcat certificate is issued to a DNS hostname and may not include the IP address as a valid subject alternative name. Disabling verification removes that identity-validation mismatch for this IP-address-based TCP connection, allowing Expressway-C to establish the connection and complete Unified CM discovery. Cisco documents the Unified CM server configuration and its TLS verification behavior in the Cisco Expressway Basic Configuration Deployment Guide. Cisco also documents AXL access and application-user permissions in the Cisco AXL API documentation.

QUESTION NO: 3

Refer to the exhibit. A collaboration engineer creates an allow list test file for a Mobile and Remote Access deployment. Which lines are needed to format the test in the file correctly?

A. https://myServer:8443/myPath.block, â€œmy deploymentâ€□, â€œa block testâ€□, GET

B. â€œmy deploymentâ€□, block, GET https://myServer:8443/myPath, â€œa block testâ€□

C. a block test:https:8443:GET â€œmyServer/myPathâ€□:my deployment:block

D. a block test,https:8443,GET â€œmyServer/myPathâ€□,my deployment:block

ANSWER: B

Explanation:

The correctly formatted allow-list test entry is *“my deployment”, block, GET https://myServer:8443/myPath, “a block test”*. Cisco Expressway allow-list test files use a comma-separated structure that identifies the deployment to which the test applies, specifies the expected allow-list action, defines the HTTP method and complete target URL to test, and includes a human-readable test description. In this entry, *my deployment* identifies the MRA deployment, *block* states the expected result of the allow-list evaluation, and *GET https://myServer:8443/myPath* supplies both the HTTP request method and the HTTPS destination, including its nondefault port and path. The final quoted text, *a block test*, documents the purpose of the test for administrators reviewing the test results. Quoting the deployment name and description preserves them as individual fields when they contain spaces. This format enables Expressway to parse the entry consistently and compare the configured HTTP allow-list policy with the intended MRA access behavior. Cisco publishes Expressway configuration documentation through its Expressway installation and configuration guides; MRA architecture and deployment guidance is also available in Cisco’s Expressway technical reference documentation.

QUESTION NO: 4

An organization is securing an Expressway B2B deployment against unauthorized inbound calling.

Which two configuration methods can be used to control which inbound calls are routed toward the internal network? (Choose two.)

A. Configure call policy rules to reject unauthorized destination aliases.

B. Configure restrictive search rules for approved destination patterns.

C. Enable static NAT on Expressway-C.

D. Configure a DNS zone for the internal SIP domain.

E. Disable TLS verification on the traversal zone.

ANSWER: A B

Explanation:

A call policy rule can evaluate characteristics such as source zone, destination alias, and protocol, and then explicitly allow, reject, or redirect calls. A policy rule can therefore reject unauthorized external calls before they reach internal call-control resources.

Search rules can also limit routing by matching only approved destination patterns and directing matching calls to the appropriate internal zone. Calls that do not match an authorized routing rule are not forwarded through that route. Secure deployments commonly combine restrictive search rules with call policy to implement least-privilege call routing.

Cisco documents call policy, search rules, and other dial-plan controls in the Cisco Expressway Administrator Guide.

QUESTION NO: 5

Which two types of information does Cisco Expressway back up? (Choose two.)

A. call records

B. log files

C. IP addresses

D. current call states

E. security certificates

ANSWER: C E

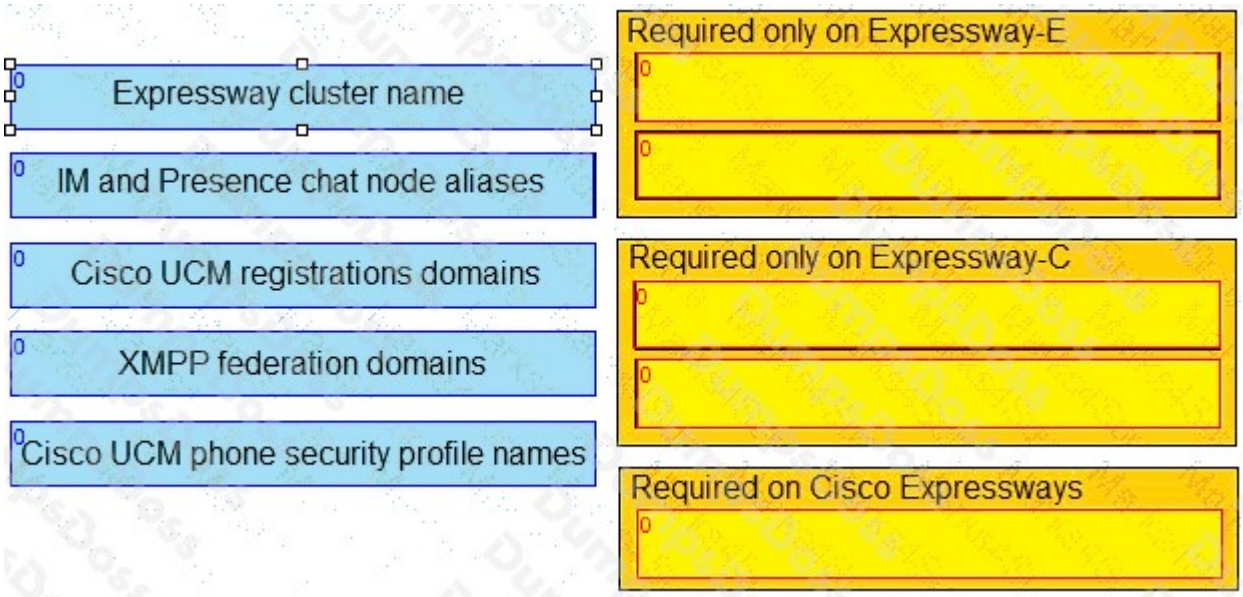
Explanation:

Cisco Expressway system backups preserve configuration information that is needed to restore the appliance's operational setup after a hardware replacement, recovery event, or migration. **IP addresses** are part of the network configuration maintained by Expressway, so they are included in the system configuration data captured by a backup. This allows the restored system to retain its configured addressing and associated network behavior, subject to the deployment's restore procedure and connectivity requirements.

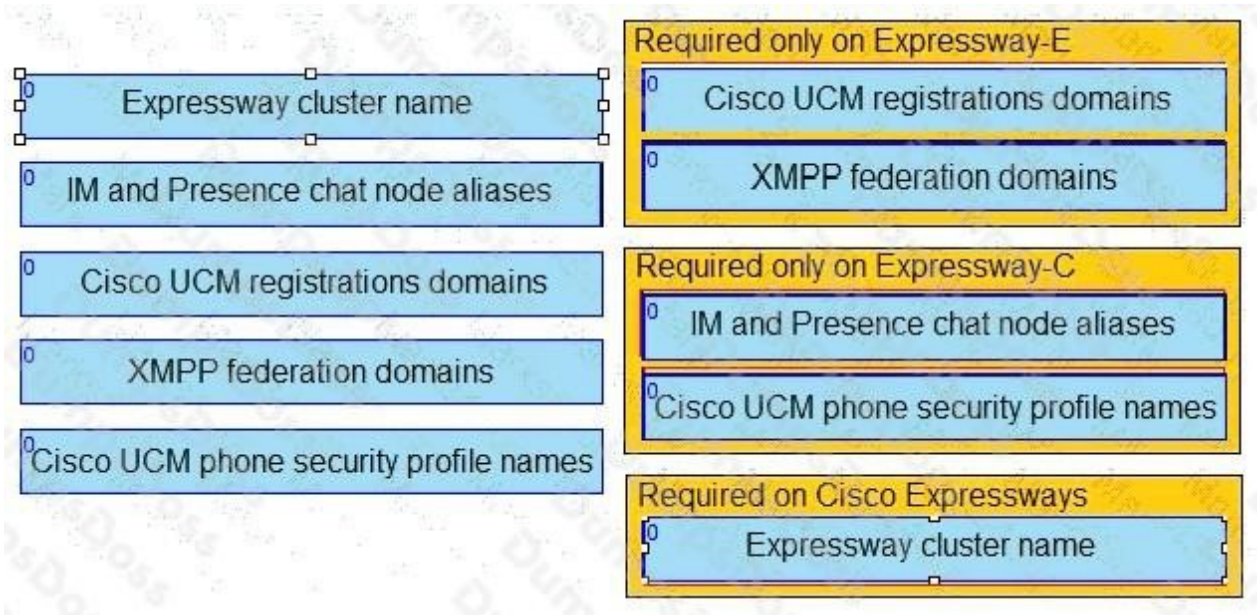
Security certificates are also backed up because Expressway depends on certificates and their associated configuration to establish trusted TLS connections for services such as Mobile and Remote Access, SIP signaling, traversal, and administrator access. Retaining this certificate information is essential to restoring the system's identity and trust relationships without rebuilding all certificate-related configuration manually. Cisco's Expressway administration documentation describes backup and restore as a mechanism for saving and recovering Expressway configuration data, including network and security-related settings. See the Cisco Expressway Administrator Guide and Cisco's Expressway maintenance documentation for backup and restore guidance.

QUESTION NO: 6 - (DRAG DROP)

Drag and drop the required SAN field items from the left onto the features within the server categories on the right.



ANSWER:



Explanation:

The SAN entries identify the DNS identities that Cisco Expressway services must present during secure TLS connections. The shared requirement is **Expressway cluster name**, because the cluster identity is relevant to the Expressway deployment itself and must be represented in the certificate SANs used by Cisco Expressway systems. Including the cluster name supports the correct certificate identity for clustered Expressway operation.

For an Expressway-E certificate, the required SANs are **Cisco UCM registrations domains** and **XMPP federation domains**. The Unified CM registration domains identify the collaboration domains that remote clients use when connecting through Mobile and Remote Access. XMPP federation domains are included on the internet-facing Expressway-E certificate because external XMPP federation peers use those domain identities when establishing secure federation connectivity.

For an Expressway-C certificate, the required SANs are **IM and Presence chat node aliases** and **Cisco UCM phone security profile names**. Chat node aliases allow the Expressway-C to validate the IM and Presence identities used for internal messaging-related integration. Unified CM phone security profile names are required because the Expressway-C participates in secure Unified CM registration and TLS trust relationships that use the configured phone security profile identity.

This division ensures that each Expressway certificate contains the service names expected by the systems with which it communicates, while the cluster name is included as a common Expressway identity. Cisco documents certificate and SAN

planning for Expressway deployments in the Cisco Expressway Certificate Creation and Use Deployment Guide and its Mobile and Remote Access deployment documentation.

QUESTION NO: 7

Which two statements about Expressway media traversal are true? (Choose two.)

A. Expressway Control is the traversal server installed in the DMZ.

B. The Expressway Edge must be put in a firewall DMZ segment.

C. Cisco Unified Communications Manager zone can be either traversal server or client.

D. The Unified Communications traversal zone can be used for Mobile and Remote Access.

E. Both Expressway Edge interfaces can be NATed.

ANSWER: B D

Explanation:

The Expressway Edge must be put in a firewall DMZ segment. Cisco's Collaboration Edge design places Expressway Edge at the network perimeter, in a DMZ, so it can securely accept connections from untrusted external networks while keeping the internal collaboration environment protected. Firewall rules permit only the required signaling and media flows between the internet, Expressway Edge, and the internal Expressway Control deployment. This placement is a fundamental part of securely providing business-to-business communications and remote access services.

The Unified Communications traversal zone can be used for Mobile and Remote Access. In an MRA deployment, Expressway Control and Expressway Edge establish a secure Unified Communications traversal zone. Remote clients connect to Expressway Edge, and Expressway Edge traverses signaling and media through that zone to Expressway Control and the internal Unified Communications services. This architecture enables off-premises users to register and use calling, messaging, and related collaboration services without requiring a traditional VPN connection. Cisco documents the Expressway deployment model and its MRA traversal-zone role in its Expressway installation and configuration guides and the Collaboration Edge Deployment Guide.

QUESTION NO: 8

An administrator is planning certificate deployment for Cisco Expressway services that use TLS.

Which two practices help ensure successful certificate validation? (Choose two.)

A. Include the connection FQDN as a Subject Alternative Name.

B. Install the issuing CA certificate chain in the appropriate trust store.

C. Use the Expressway IP address as the certificate common name.

D. Disable TLS verification on all zones.

E. Use a self-signed certificate for Internet-facing MRA clients.

ANSWER: A B

Explanation:

The certificate must contain the FQDN used by connecting systems in its Subject Alternative Name extension. TLS clients validate the server identity against the hostname used to establish the connection, so the relevant Expressway system name, cluster name, or service domain must be represented in the certificate.

The issuing CA chain must also be trusted by the connecting system. This normally requires the applicable root CA and any intermediate CA certificates to be installed in the relevant trust store. Without a trusted chain, clients cannot validate the certificate even when the FQDN is correctly included as a SAN.

Cisco certificate guidance for Expressway is available in the Cisco Expressway Certificate Creation and Use Deployment Guide.

QUESTION NO: 9

In a Webex Video Mesh deployment, where do Cloud-registered Webex Teams clients and devices send signaling traffic for call setup?

A. to a local Video Mesh node

B. directly to the Webex cloud

C. to an Expressway-E server

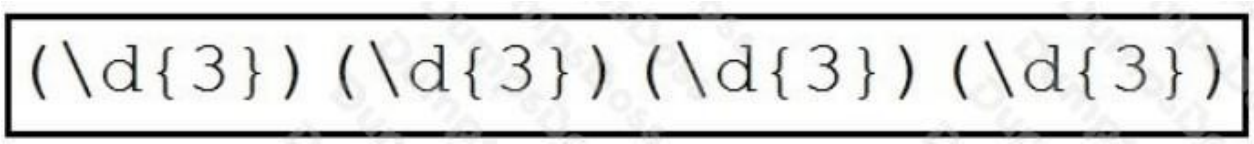
D. to a remote Video Mesh node

ANSWER: B

Explanation:

Cloud-registered Webex Teams clients and devices send call-setup signaling directly to the Webex cloud. Video Mesh is designed primarily to keep media processing and media traffic on premises when suitable Video Mesh nodes are available and have capacity. It does not replace the Webex cloud control plane for cloud-registered endpoints. The client or device first uses Webex cloud signaling to establish the meeting or call context, determine available resources, and receive instructions for the media path. When conditions permit, the Webex cloud can select an on-premises Video Mesh node to host the media; otherwise, media is handled by the Webex cloud. This separation of cloud-based signaling from locally anchored media is a central architectural characteristic of Video Mesh and allows organizations to reduce WAN bandwidth consumption while retaining the Webex cloud collaboration experience. Cisco's Video Mesh deployment documentation describes Video Mesh nodes as resources that provide local media processing, while Webex services continue to provide meeting and signaling services. See Cisco's Webex Video Mesh deployment guide and the Webex Video Mesh overview.

QUESTION NO: 10



Refer to the exhibit. Which two numbers match the regular expression? (Choose two.)

A. d20d16d20d22

B. 2091652010224

C. 209165200225

D. d209d165d200d224

E. 209165200224

ANSWER: C E

Explanation:

The regular expression shown in the exhibit requires one uninterrupted value made up of exactly twelve decimal digits. Both **209165200225** and **209165200224** satisfy that structure: each contains twelve numeric characters, with no alphabetic

characters, separators, spaces, or additional digits. The final digit does not need to be a specific value under this digit-count pattern, so values ending in either **5** or **4** match as long as the complete sequence retains the required twelve-digit length.

Regular expressions are used throughout Cisco collaboration dial-plan and call-routing configurations to identify dialed strings according to defined digit patterns. When evaluating a candidate string, the relevant checks are that every character conforms to the digit token in the expression and that the complete input meets the expression's required length. Cisco documentation on Unified Communications Manager dial-plan configuration is available from the Cisco Unified Communications Manager support documentation. For the general regular-expression syntax concepts underlying digit matching and repetition, see RFC 3402.

QUESTION NO: 11

Which configuration is required when implementing Mobile and Remote Access on Cisco Expressway?

A. IPS

B. SAML authentication

C. Cisco Unified CM publisher address

D. SSO

ANSWER: C

Explanation:

Cisco Unified CM publisher address is required because Expressway-C must establish its trusted Unified Communications connection to the Cisco Unified CM cluster before it can provide Mobile and Remote Access services. In the Expressway-C Unified CM servers configuration, the publisher is entered as the primary cluster node. Expressway-C uses this connection to discover cluster topology and service information and to support communications between externally registered MRA endpoints and internal Unified CM services. The publisher address must resolve correctly and be reachable from Expressway-C; deployments commonly use an FQDN so that DNS resolution and certificate identity validation align with the Unified CM and Expressway certificates. After the publisher is configured, Expressway-C can discover other relevant cluster nodes and apply the UC traversal configuration used by Expressway-E for MRA. This configuration is therefore foundational to an MRA deployment rather than an optional enhancement. Cisco's Expressway deployment documentation describes configuring Unified CM server details on Expressway-C as part of the required MRA setup, and Cisco's Expressway configuration-guide collection provides the release-specific procedures. See Cisco Expressway installation and configuration guides and Cisco Expressway Mobile and Remote Access Deployment Guide.

QUESTION NO: 12

How does an administrator configure an Expressway to make sure an external caller cannot reach a specific internal address?

A. block the call with a call policy rule in the Expressway-E

B. add the specific URI in the firewall section of the Expressway and block it

C. configure FAC for the destination alias on the Expressway

D. add a search rule route all calls to the Cisco UCM

ANSWER: A

Explanation:

Blocking the call with a call policy rule in the Expressway-E is correct because call policy is the Expressway feature designed to evaluate calls against administrator-defined matching conditions and take an explicit action, including rejecting a call. The administrator can create a rule that matches the protected internal destination alias or URI and, where needed, limits the rule

to calls arriving from the external-facing traversal or SIP zone. Setting the rule action to reject prevents the matching external call from being routed onward toward internal resources.

This approach provides granular control: the rule can target one exact address, a domain, or an alias pattern while allowing other authorized calls to continue through normal search-rule routing. It is also enforced at the edge, before the call reaches the internal call-control environment, which is appropriate for protecting an internal address from externally originated signaling. Cisco documents call policy as a mechanism for controlling whether calls are allowed and for defining policy rules based on call characteristics. See the Cisco Expressway Administrator Guide and Cisco's Expressway configuration guides.

QUESTION NO: 13

Which connection does the traversal zone configuration define?

A. Expressway-E and Collaboration Endpoints

B. Cisco UCS E-Series and Cisco UCM

C. Cisco UC and Cisco Unified Presence Server

D. Cisco Expressway-C and Cisco Expressway-E platforms

ANSWER: D

Explanation:

A traversal zone configuration defines the secure communications relationship between Cisco Expressway-C and Cisco Expressway-E platforms. In a typical Cisco Collaboration Mobile and Remote Access deployment, Expressway-C is placed on the internal network and integrates with Unified CM and other collaboration services, while Expressway-E is deployed in the DMZ to provide the externally reachable edge service. The traversal zone links these two Expressway systems so that signaling and media can traverse securely between the enterprise network and remote users or external participants.

The configuration is created as a neighbor zone on Expressway-C and a corresponding traversal-server zone on Expressway-E. It uses mutual TLS authentication, usually with certificates whose names match the configured zone peer addresses, to establish a trusted connection. This zone is fundamental to Expressway traversal because it provides the controlled path through the firewall boundary without directly exposing internal collaboration infrastructure to the Internet. Cisco's Expressway deployment documentation describes configuring a traversal zone between the Expressway-C and Expressway-E after the systems are reachable and their certificates are in place. See the Cisco Expressway Basic Configuration Deployment Guide and the Cisco Expressway Administrator Guide.

QUESTION NO: 14

An administrator has been tasked to bulk entitle 200 existing users and ensure all future users are

automatically configured for the Webex Hybrid Calendar Service. Which two options should be used to configure these users? (Choose two.)

A. Export a CSV list of users in the Cisco Webex Control Hub, set the Hybrid Calendar Service to TRUE for users to be enabled, then import the file back to Manage Users menu in the Cisco Webex Control Hub.

B. Set up an Auto-Assign template that enables Hybrid Calendar.

C. Select the Hybrid Services settings card in the Cisco Webex Control Hub and import a User Status report that contains only users to be enabled.

D. On the Users tab in the Cisco Webex Control Hub, check the box next to each user who should be enabled, then click the toggle for the Hybrid Calendar service to turn it on.

E. From Cisco Webex Control Hub, verify the domain that your Hybrid Calendar users will use, whichautomatically activates them for the service.

ANSWER: A B

Explanation:

Exporting a CSV list of users in Cisco Webex Control Hub, setting the Hybrid Calendar Service value to TRUE, and importing the file is the appropriate bulk-management method for the 200 existing users. Control Hub supports bulk modification of user service assignments through a CSV export/import workflow, allowing the administrator to update the Hybrid Calendar entitlement for many existing accounts in one operation rather than changing users individually. Cisco documents this process in its bulk user-service modification guidance.

Setting up an Auto-Assign template that enables Hybrid Calendar addresses the ongoing requirement for future users. Automatic license-assignment templates apply selected services when new users are created or join the organization, so the Hybrid Calendar entitlement is consistently assigned without manual intervention. Templates can be scoped appropriately, including to users associated with particular domains or groups, depending on the organization's provisioning design. Cisco's automatic license assignment documentation describes how Control Hub uses these templates to assign services to future users. Together, CSV bulk assignment remediates the current population, while the auto-assignment template maintains the desired entitlement state for new accounts.

QUESTION NO: 15

After Mobile and Remote Access is deployed with automatic service discovery, end users encounter the error "Cannot communicate with the server" when they attempt to log in to Cisco Jabber 14.0 using the company email address from within the company network. Which action must an administrator take to resolve this challenge?

A. Create _collab-edge._tcp DNS SRV record in the internal DNS.

B. Create _cisco-uds._tcp DNS SRV record in the internal DNS server.

C. Create _collab-edge._tls DNS SRV record in the public DNS.

D. Create _cisco-uds._tcp DNS SRV record in the public DNS server.

ANSWER: B

Explanation:

Create `_cisco-uds._tcp` DNS SRV record in the internal DNS server. When Cisco Jabber users sign in from the corporate network using their email address, Jabber performs internal service discovery to locate Cisco Unified Communications Manager services. The required DNS Service (SRV) record is `_cisco-uds._tcp.<domain>`, where the domain is derived from the user's sign-in address. This record directs Jabber to the Unified CM node that provides the User Data Service, allowing Jabber to obtain its service profile, configuration, and communications service information. The SRV record must be resolvable by the internal DNS infrastructure used by corporate clients and must point to an appropriate Unified CM publisher or subscriber node configured for UDS. Once internal DNS returns the correct UDS destination, Jabber can complete automatic discovery and sign in successfully without requiring a manually specified server address. Cisco distinguishes this internal discovery mechanism from Mobile and Remote Access discovery, which is intended for clients connecting from outside the organization. See Cisco's Cisco Jabber 14.0 feature configuration documentation and the Cisco Jabber installation and configuration guides.

QUESTION NO: 16

Where can the administrator manage a Webex tenant?

A. Cisco Webex administrator portal

B. Cisco Webex management portal

C. Cisco Webex control panel

D. Cisco Webex Control Hub

ANSWER: D

Explanation:

Cisco Webex Control Hub is the centralized, web-based administration portal for a Webex organization (tenant). An administrator uses Control Hub to manage organizational settings, including users and licenses, authentication and domains, devices, messaging, meetings, calling services, security policies, compliance features, analytics, and troubleshooting. It provides a single management plane for Webex cloud services and allows administrators to assign roles with the appropriate scope of administrative privileges. In collaboration deployments, Control Hub is also the primary place to configure and monitor hybrid and cloud-connected services, as applicable to the organization's Webex subscriptions. Cisco documentation explicitly describes Control Hub as the interface for administering Webex services and users, making it the correct location to manage a Webex tenant. See the Cisco Webex Control Hub administration documentation and Cisco's Control Hub overview.

QUESTION NO: 17

What are two reasons why port 8443 is unreachable from the Internet to the Expressway-E? (Choose two.)

A. The MRA license is missing on the Expressway-E.

B. The Unified Communications zone is down.

C. Transform is not configured on Expressway-E.

D. The SRV record for _cisco-uds is misconfigured.

E. The firewall is blocking the port.

ANSWER: B E

Explanation:

The firewall is blocking the port is correct because Mobile and Remote Access requires inbound TCP port 8443 to be permitted from Internet-based clients to the Expressway-E. This port carries the HTTPS traffic used by remote Cisco Jabber and Webex App clients to access Unified Communications services through MRA. If an Internet-edge firewall, access-control list, security policy, or NAT configuration does not allow and correctly forward TCP 8443 to the Expressway-E external interface, external clients cannot establish the required connection.

The Unified Communications zone is down is also correct because MRA depends on a working traversal relationship between Expressway-E and Expressway-C, as well as the Unified Communications services reachable through that deployment. A down Unified Communications zone indicates that the required service path is unavailable. Consequently, Expressway-E cannot provide the MRA service to Internet clients, and connections to the external MRA HTTPS service fail from the user perspective. Cisco's MRA deployment guidance identifies TCP 8443 as the external client HTTPS port and requires the Expressway traversal and Unified Communications connectivity to be operational. See the Cisco Expressway installation and configuration guides and the Cisco Expressway configuration guide.

QUESTION NO: 18

Which two functions are supported by Cisco Webex Device Connector? (Choose two.)

A. Synchronize Cisco Unified Communications Manager-managed devices to Control Hub

B. Migrate supported Cisco Unified Communications Manager devices to Webex cloud registration

C. Provide SIP media traversal for Mobile and Remote Access clients

D. Replace Cisco Unified Communications Manager as on-premises call control

E. Provide PSTN connectivity for Webex Calling users

ANSWER: A B

Explanation:

Cisco Webex Device Connector can synchronize Cisco Unified Communications Manager-managed devices to Webex Control Hub. This workflow gives administrators inventory visibility and access to supported Webex cloud management capabilities while retaining Unified CM registration.

Cisco Webex Device Connector can also assist with migrating supported Cisco Unified Communications Manager-registered devices to Webex cloud registration. During this workflow, the administrator prepares eligible devices and moves their registration from Unified CM to the Webex cloud.

Device Connector is not a call-control system and does not act as a media traversal relay. Cisco documents the supported synchronization and migration workflows in the Webex Device Connector documentation.

QUESTION NO: 19

Which step is required when configuring Cisco Webex Hybrid Message Service?

A. Register Expressway-C Connector Hosts to the Cisco Webex Cloud.

B. Register Expressway-C to Cisco Unified Communications Manager.

C. Add Expressway-C and Cisco United CM to the Cisco Webex Cloud.

D. Add Cisco Unity Connection to Expressway-E.

ANSWER: A

Explanation:

Register Expressway-C Connector Hosts to the Cisco Webex Cloud. is required because the Hybrid Message Service uses an on-premises connector host to create a secure, outbound connection between the organization's messaging environment and the Webex cloud. During deployment, the administrator generates an activation code in Control Hub and uses it to register the Expressway-C connector host with Cisco Webex. This registration establishes the host's identity, associates it with the Webex organization, and allows the cloud service to manage the Hybrid Message connector configuration. The connector host then provides the integration path needed for users to access supported on-premises messaging capabilities through Webex without requiring inbound firewall openings. Registration is therefore a foundational deployment task that must occur before the Hybrid Message connector can be activated and used. Cisco's Hybrid Services deployment documentation describes connector-host registration and activation as part of establishing hybrid connectivity; see the Cisco Webex Hybrid Message Service Deployment Guide and the Webex Hybrid Services Deployment Guide.

QUESTION NO: 20

Which two considerations must be made when using Expressway media traversal? (Choose two.)

A. It is possible to NAT both Expressway-E interfaces

B. The Unified Communications traversal zone should be used for MRA

C. The Expressway-E must be put in a firewall DMZ segment

D. Expressway Control is the traversal server installed in the DMZ

E. Cisco UCM zone should be either traversal server or client

ANSWER: B C

Explanation:

The Unified Communications traversal zone should be used for MRA because it is the dedicated, secure relationship between Expressway-C and Expressway-E that supports Mobile and Remote Access services. This zone type is configured specifically for Unified Communications signaling and associated media traversal requirements, allowing remote endpoints to register and use collaboration services through the Expressway pair without requiring a VPN. The traversal relationship also

enables Expressway-C to remain on the trusted internal network while Expressway-E provides the externally reachable edge function.

The Expressway-E must be put in a firewall DMZ segment because it is the internet-facing component that accepts communications from untrusted external networks and relays permitted signaling and media toward the internal collaboration environment. Locating it in a DMZ provides network separation and lets firewall policy tightly control the required inbound and outbound ports between the internet, Expressway-E, Expressway-C, and Unified Communications services. Cisco's deployment guidance describes Expressway-E as the public-facing edge system and Expressway-C as the internal system, with a secure traversal connection between them. See Cisco's Expressway Basic Configuration Deployment Guide and the Cisco Expressway configuration guides.

QUESTION NO: 21

An engineer is supporting an existing Cisco Collaboration deployment that has internal and external home users using the solution without VPN. Business usage also includes B2B calling for voice and video. Suddenly the engineer receives a report that one of the home office users cannot use the Cisco Jabber client, and shortly after, a few more reports come in for the same error. What must the engineer check first to resolve this issue?

A. client logs of the users

B. real-time monitoring toll logs for problems

C. alarms on the Cisco Expressways

D. alarms on the Cisco UCM Cluster

ANSWER: C

Explanation:

alarms on the Cisco Expressways should be checked first because Cisco Expressway is the shared edge component that enables both VPN-less remote access for Cisco Jabber through Mobile and Remote Access and business-to-business voice/video connectivity. Multiple home users reporting the same issue in quick succession points to a common service or infrastructure condition rather than an isolated endpoint problem. Expressway alarms provide an immediate view of operational conditions that can affect client registration and service access, such as traversal-zone failures, Unified Communications service connectivity issues, certificate problems, DNS-related conditions, resource exhaustion, or other system faults. Checking the alarm state first lets the engineer quickly determine whether the incident correlates with a failure on the component serving these external collaboration workflows and identifies the relevant fault details for remediation. Cisco documents Expressway as the edge platform used for Mobile and Remote Access, while its administrator guidance identifies alarms as a primary operational monitoring mechanism. See the Cisco Expressway Administrator Guide and Cisco's Expressway installation and configuration guides.

QUESTION NO: 22

After an engineer implements load balancing in the Cisco CMS cluster, they observe that shortly after the second Call Bridge is added to the cluster, calls into a space randomly disconnect when the calls are from endpoints registered with Cisco UCM. Which action resolves the issue?

A. Enable "Accept Out-of-dialog REFER" on the SIP Trunk security profile.

B. Enable "Accept Unsolicited Notification" on the SIP Trunk security profile.

C. Enable "Accept Presence Subscription" on the SIP Trunk security profile on Cisco UCM.

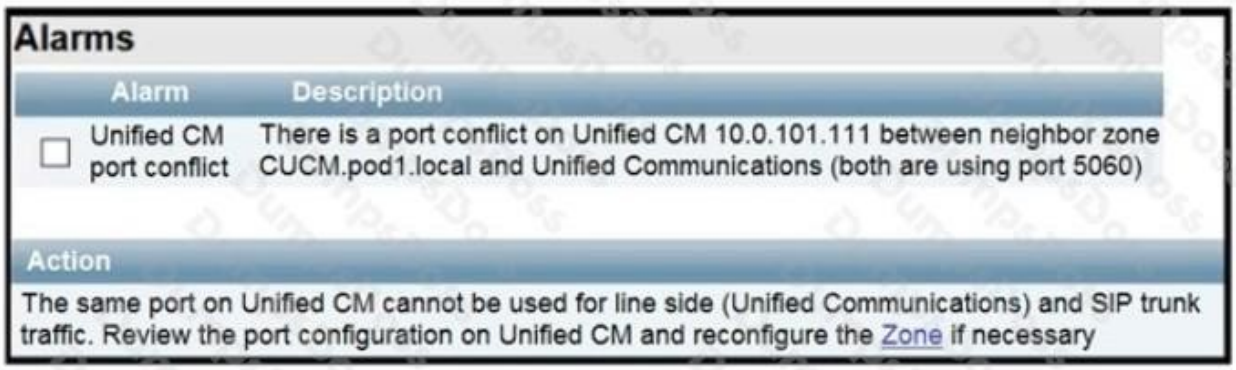
D. Enable "Accept Replaces Header" on the SIP Trunk security profile on Cisco UCM.

ANSWER: D

Explanation:

Enable "Accept Replaces Header" on the SIP Trunk security profile on Cisco UCM. In a Cisco Meeting Server cluster, Call Bridges coordinate clustered calls and may need to move or re-anchor call signaling between Call Bridges as part of load balancing and call distribution. This operation uses the SIP `Replaces` header to associate a new SIP dialog with and replace an existing dialog cleanly. Cisco Unified Communications Manager must explicitly allow the `Replaces` header on the SIP trunk security profile used for communications with Cisco Meeting Server. If it is not accepted, CUCM cannot process the dialog replacement required during these clustered call operations, which can manifest as seemingly random call disconnections after an additional Call Bridge begins handling calls. Enabling this setting allows CUCM to honor the SIP dialog replacement and preserves the call as CMS performs the necessary signaling transition between cluster members. Apply the updated security profile to the relevant SIP trunk and reset the trunk if CUCM requires it for the change to take effect. Cisco documents this CUCM SIP trunk requirement for CMS clustered deployments in its deployment guidance: Cisco Meeting Server Installation and Configuration Guides. CUCM configuration details are also available through Cisco Unified Communications Manager Configuration Guides.

QUESTION NO: 23



Refer to the exhibit. Mobile and remote access is being added to an existing B2B deployment and is failing. When the administrator looks at the alarms on the Expressway-C, the snippets are shown. Which configuration action should the administrator take to fix this issue?

A. The listening port on the Expressway-C for SIP TCP must be changed to a value other than 5060

B. The listening port on the Expressway-C for SIP TLS must be changed to a value other than 5061

C. The listening port on the Cisco UCM for the Expressway-C SIP trunk must be changed to something other than 5060 or 5061

D. The listening port on the Cisco UCM for the Expressway-C SIP trunk is set to something other than 5060 or 5061. It must be set to 5060 for insecure and 5061 for secure SIP

ANSWER: A

Explanation:

The listening port on the Expressway-C for SIP TCP must be changed to a value other than 5060. When Mobile and Remote Access is enabled on an Expressway-C that is already configured for business-to-business calling, Cisco identifies a port-use conflict when the Expressway-C SIP TCP listening port remains at its default port of 5060. This condition prevents the combined B2B and MRA deployment from operating as intended and generates the related Expressway-C alarm. Configure the Expressway-C SIP TCP listener with an available, nondefault TCP port appropriate for the deployment. Any dependent SIP routing configuration, including the Unified CM SIP trunk destination port where applicable, must then be aligned with the newly configured Expressway-C listening port so that SIP signaling continues to reach Expressway-C correctly. This separates the relevant signaling behavior and allows MRA services to be enabled alongside the existing B2B configuration. Cisco's MRA deployment guidance describes the Expressway-C and Unified CM integration requirements, while the Expressway Administrator Guide documents the SIP listener configuration controls. See the Cisco Expressway Mobile and Remote Access Deployment Guide and the Cisco Expressway Administrator Guide.

QUESTION NO: 24

Which two items are configured when deploying a B2B collaboration solution? (Choose two.)

A. SIP trunk between Cisco Unified Communications Manager and Cisco Expressway-C

B. search rules in Cisco Expressway-E

C. SIP trunk between Cisco Unified Communications Manager and Cisco Expressway-E

D. traversal client on a Cisco Expressway-E

E. DNS zone on a Cisco Expressway-C

ANSWER: A B

Explanation:

A **SIP trunk between Cisco Unified Communications Manager and Cisco Expressway-C** is configured because Expressway-C is the internal, trusted edge component that integrates directly with the Unified Communications Manager call-control domain. The SIP trunk provides the signaling path through which internally registered endpoints can place business-to-business calls toward the Expressway deployment, and it also supports routing calls received from external organizations into Unified Communications Manager.

search rules in Cisco Expressway-E are configured to define how B2B signaling is routed at the internet-facing edge. Search rules evaluate the called address and select an appropriate target zone or route, allowing Expressway-E to direct inbound federation calls toward the traversal connection and to apply the intended B2B call-routing behavior. This routing logic is a core part of controlling how external SIP video and voice calls traverse the collaboration edge securely.

Cisco documents the Expressway-C and Expressway-E roles, including Unified Communications Manager integration and B2B call routing, in the Cisco Expressway configuration guides. Cisco's Basic Configuration Deployment Guide also describes configuring call-routing policy through zones and search rules.

QUESTION NO: 25

What should an engineer use to create users for a Cisco Jabber Cloud Deployment?

A. Cisco Webex Administration Tool

B. Cisco UCM

C. Cisco Webex Directory Connector

D. Cisco Unified IM and Presence Server

ANSWER: A

Explanation:

Cisco Webex Administration Tool is the correct choice because Cisco Jabber Cloud deployments use the Webex cloud administration portal to provision and manage the organization's Jabber users. An administrator can create user accounts directly in the administration interface, assign the appropriate services and licenses, and manage user identity information needed for cloud-based Jabber access. This makes the Webex administration environment the authoritative administrative location for creating users in a Jabber Cloud organization. Cisco's Jabber Cloud deployment guidance identifies the Cisco Webex Administration Tool as the interface used to add and administer users for the cloud service. In current Cisco terminology, this administration experience is provided through Control Hub, which supports adding users manually, in bulk, or through directory synchronization. The key point is that the users are created in the Webex cloud organization rather than being created solely in an on-premises calling or presence system. See Cisco's Jabber Cloud and Hybrid Deployments guide and the Cisco Webex Control Hub user-management documentation.

QUESTION NO: 26

Which user management method uses the Webex Directory Connector to add and synchronize users to the Control Hub organization?

A. Synchronize from Active Directory.

B. Synchronize from Azure AD.

C. Synchronize from "Add using People API'.

D. Synchronize from Okta.

ANSWER: A

Explanation:

Synchronize from Active Directory. is correct because Cisco Webex Directory Connector is an on-premises application designed to connect an organization's Microsoft Active Directory to Webex Control Hub. An administrator installs the connector on a Windows system that can access the Active Directory domain, configures the directory source and synchronization attributes, and then performs synchronization to create or update users in the Control Hub organization. The connector can synchronize key identity information such as names, email addresses, and other supported user attributes, helping organizations maintain Webex user accounts from their established enterprise directory rather than managing each account manually. Directory Connector also supports scheduled and incremental synchronization, so changes made in Active Directory can be reflected in Control Hub over time. This method is particularly appropriate for organizations that use on-premises AD as their authoritative user directory and want to integrate that directory with Webex identity management. Cisco's Directory Connector deployment documentation describes Active Directory as the directory source used by the connector and details the configuration and synchronization workflow. See the Cisco Webex Directory Connector Deployment Guide and Configure Cisco Directory Connector for synchronization.