300-810 Dumps

Implementing Cisco Collaboration Applications (CLICA)

https://www.certleader.com/300-810-dumps.html

NEW QUESTION 1
An engineer must configure a test user mailbox in a newly deployed Cisco Unity Express module. Which console command set reflects the correct configuration in this scenario?

A.
```
username testuser create
username testuser pin 12345
username testuser phonenumber 4001
voicemail mailbox owner testuser
```

B.
```
username testuser pin 12345
username testuser phonenumber 4001
voicemail mailbox owner testuser
```

C.
```
username testuser phonenumber 4001
username testuser pin 12345
voicemail mailbox owner testuser
```

D.
```
username testuser create
username testuser pin 12345
username testuser phonenumber 4001 testuser@labdomain.com
voicemail mailbox create testuser
```

Answer: A

NEW QUESTION 2
Which two command line arguments can you specify when installing Cisco Jabber for windows? (Choose two.)

A. CISCO_UDS_DOMAIN
B. TFTP_ADDRESS
C. VOICEMAIL_SERVER_ADDRESS
D. SERVICES_DOMAIN
E. TFTP

Answer: DE

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/jabber/11_0/CJAB_BK_D657A25F_00_deployment-installation-guide-jabber-110/CJAB_BK_D657A25F_00_deployment-installation-guide-jabber- 110_chapter_01100.html#JABW_RF_CE43EF4C_00

NEW QUESTION 3
Which Cisco IM and Presence service must be activated and running for IM Presence to successfully integrate with Cisco Unified Communications Manager?

A. Cisco DHCP Monitor Service
B. Cisco AXL Web Service
C. Self-Provisioning IVR
D. Cisco XCP Authentication Service

Answer: A

NEW QUESTION 4
Refer to the exhibit.

```
Response:
HTTP/1.1 400 Bad Request
Strict-Transport-Security: max-age=31536000
X-Frame-Options: DENY
X-Content-Type-Options: nosniff
Set-Cookie: JSESSIONID=1233ADC137E591GE144792F38123AB09; Patch=/idb/; Secure; HttpOnly
TrackingID: FOS_d0ac0d7b-f4e4-4d83-ba27-d4252e310b88
Cache-Control: no-store
Date: Mon, 06 Jan 2018 10:30:00 GMT
Accept-Ranges: bytes
Server:
Vary: Accept-Charset, Accept-Encoding, Accept-Language, Accept
Access-Control-Allow-Credentials: true
Access-Control-Allow-Headers: Accept,Authorization,Content-Type,TrackingID
Access-Control-Allow-Methods: POST,PUT,PATCH,HEAD,GET,TRACE,CONNECT,OPTIONS,DELETE
Pragma: no-cache
Content-Type: application/json;charset=UTF-8
Connection: close
Content-Length: 176

{"error_description":"The refresh token provided is expired, revoked, malformed, or invalid.","
error":"invalid_request","trackingID":FOS_a12b123c-d123-e123-a127-b420be310188"}
```

Apple Push Notification integration is configured in a Cisco Unified IM and Presence deployment and has been working property. Administrators now report the error "Push notification settings cannot be configured. 400 Bad Request." in the GUI, and HTTP logs are displaying the errors that are shown in the exhibit. Which action solves this issue?

A. Fix the network connectivity to Apple iCloud.
B. Reboot the IM&P cluster.
C. Change the HTTP proxy settings to remove errors in request syntax.
D. Update Refresh Token Manually.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/push_notifications/cucm_b_push-notifications-deployment-guide.pdf

NEW QUESTION 5
Which CLI command is used to collect traces from the Cisco Presence engine for seven days?

A. file build log cisco_presence_engine 7
B. file build log cisco_presence 168
C. file build log presence_engine 7
D. file build log presence_engine 168

Answer: A

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/im_presence/configAdminGuide/12_0_1/cup0_b_config-admin-guide-imp-1201/cup0_b_config-admin-guide-imp-1201_chapter_010101.html

NEW QUESTION 6
Refer to the exhibit.

```
[csf.cert.] [csf::cert::BaseCertVerifier:doVerifyCertificate] - About to verify the certificate.
[csf.cert.win32] [csf::cert::Win32CertVerifier:loadCertificateChain] - Certificate Chain status 0x20
[csf.cert.win32] [csf::cert::Win32CertVerifier:verifySslPolicy] - Ignoring errors due to Invalid CN
[csf.cert.win32] [csf::cert::Win32CertVerifier:verifyPolicies] - SSL Policy status 0x2148204809
[csf.cert.win32] [csf::cert::win32CertVerifier:verifyPolicies] - Basic Constraints Policy status 0x0
[csf.cert.win32] [csf::cert::win32CertVerifier:verifyCertificate] - Certificate validation response is 'invalid'
[csf.cert.] [csf::cert::BaseCertVerifier:doVerifyCertificate] - Result of platform cert verification: [UNTRUSTED_ROOT]
[csf.cert.] [csf::cert::BaseCertVerifier:checkIdentity] - About to check for an Identity Match.
[csf.cert.xmpp] [csf::cert::XmppCertVerifier:checkIdentifier] - Verifying XMPP Identity 'example.com'
[csf.cert.utils] [csf::cert::AltNameParserImpl:verifyXmpp] - Xmpp match was not found for: 'example.com'
[csf.cert.utils] [csf::cert::AltNameParserImpl:verify] - Match for 'example.com' found in dnsNames index: 1
[csf.cert.] [csf::cert::BaseCertVerifier::checkIdentifiers] - Verification of identity succeeded. Matched identifier : 'example.com'
[csf.diagnostics] [CSFDiagnostics::DiagnosticsImpl::AddRecord] - Add record task enqueued: example.com
[csf.common.PolicySet] [csf::common:PolicySet::getPolicy] - Successfully found Policy with nature IGNORE_INVALID_CERT_CONDITION
                                                          [IGNORE_REVOCATION_INFO_UNAVAILABLE_ERRORS]
[csf.cert.] [csf::cert::BaseCertVerifier::applyIgnoreInvalidCertConditionPolicy] - About to enforce ignore invalid cert condition policy.
[csf.cert] [csf::cert::IgnoreInvalidCertConditionPolicy::removeIgnoredStatuses] - No statuses have been removed from the verification status.
[csf.cert.] [csf::cert::IgnoreInvalidCertConditionPolicy::enforce] - Policy enforced
[csf.cert.] [csf::cert::BaseCertVerifier::verifyCertificateAsync] - Certificate initially verified, result: FAILURE
[csf.cert] [csf::cert::CertificateDataImpl::parseSubjectCNField] - size of Subject CN field : 16
[csf.cert] [csf::cert::CertificateDataImpl::parseSubjectCNField] - Sybject CN field : impa.example.com
[csf.common.PolicySet] [csf::common:PolicySet::getPolicy] - Sucessfully found Policy with nature INVALID_CERT_MANAGEMENT [PROMPT_USER]
```

Users report that they are prompted to accept server certificates when they initially run Cisco Jabber. An engineer removes these prompts to prevent confusion. Which statement about this scenario is true?

A. Presentation of the certificates can be disabled by setting up Cisco IM&P servers into nonsecure mode.
B. Nothing can be done to resolve this issue because certificates must be accepted by each Jabber user, per Cisco policy.
C. These certificates are self-signed certificates, so they must be added manually to the user OS certificate stores.
D. The behavior is a security breach because certificates are considered untrusted and as not coming from Cisco Collaboration servers.

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/support/docs/unified-communications/jabber-windows/116637-trouble-jabber-00.html

NEW QUESTION 7
Which SIP request type is used by Cisco Unity Connection to inform Cisco Unified Communications manager that the Message Waiting Indicator must be turned on or off for a specific line?

A. NOTIFY
B. UPDATE
C. SUBSCRIBE
D. PUBLISH

Answer: A

NEW QUESTION 8
Which two Cisco Unity Connection logs are used to troubleshoot issues with Message Waiting Indicators? (Choose two.)

A. Connection IMAP Server
B. Connection Mailbox Sync
C. Connection Notifier
D. Connection Message Transfer Agent
E. Connection Conversation Manager

Answer: DE

NEW QUESTION 9
Secure XMPP communication is required for XMPP federation with external domains and the Cisco IM and Presence. Which certificate is used for XMPP interdomain federation when connecting to an externally federated domain?

A. cup
B. cup-xmpp
C. cup-xmpp-s2s
D. Tomcat

Answer: C

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/telepresence/infrastructure/vcs/config_guide/X8-2/XMPP-Federation-with-Cisco-VCS-and-IM-and-Presence-Service.pdf

NEW QUESTION 10
Refer to the exhibit.

Users connected to the internal network report a "Cannot communicate with the server" error while trying to log in to Cisco Jabber using auto service discovery. The Jabber diagnostics and the SRV record configuration are as shown in the exhibit. The host cucm1.ccnp.cisco.com is correctly resolved by the user desktops with the Cisco Unified Communications Manager IP address. Why is the user not able to log in?

A. SRV protocol is not set up correctl
B. It should be _tls instead of _tcp.
C. Marking weight as 0 on the SRV record makes it inactive, so Jabber cannot discover the Cisco Unified CM.
D. The port specified on the SRV record is wrong.
E. The domain ccnp.cisco.com does not exist on the DNS server.

Answer: D

Explanation:
Reference: https://community.cisco.com/t5/collaboration-voice-and-video/jabber-client-login-and-login-issues/ta-p/3143446

NEW QUESTION 10
Which statement describes a role of AXL communications in the BLF Plug-in Service of the Cisco Unified Attendant Console?

A. The AXL communications allow registered attendants to log in to Cisco Unified Communications Manager and receive calls.
B. The AXL communications enable Device Resolution Manager to resolve the device statuses of operator and system devices.
C. The AXL communications is required after installation to verify that the specified CTI manager or managers and Cisco Unified Attendant Console versions match.
D. The AXL communications is required after installation to verify that the specified CTI manager or managers and Cisco Unified CM versions.

Answer: D

Explanation:
Reference: https://www.cisco.com/c/dam/en/us/td/docs/voice_ip_comm/cucmac/cuaca/12_0_4/design_guides/CUACA_DG_120401.pdf

NEW QUESTION 11
Which two SSO features are true? (Choose two.)

A. allows Jabber to use LDAP directory services for contact imports
B. allows LDAP user import on Cisco Unified Communications Manager
C. improves productivity by reducing time spent re-entering credentials for the same identity
D. transfers the authentication from the system that hosts the applications to a third-party system
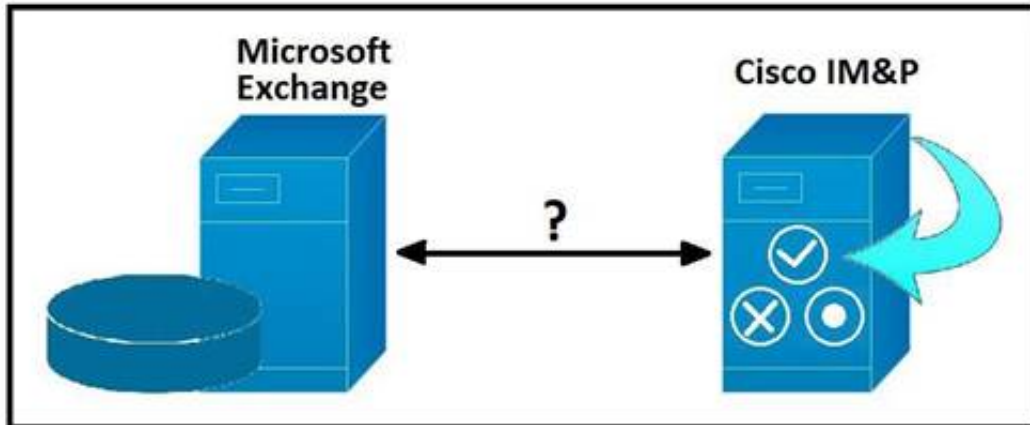E. reduces costs by decreasing the number of help calls that are made for voicemail PIN resets

Answer: CD

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/SAML_SSO_deployment_guide/11_0_1/CUCM_BK_SF9D0502_00_saml-sso-deployment-guide-1101/CUCM_BK_SF9D0502_00_saml-sso-deployment- guide11_chapter_01.html

NEW QUESTION 13
Refer to the exhibit.

Which protocol is used for communication between Cisco IM and Presence and Microsoft Exchange Server?

A. POP3
B. IMAP
C. EWS
D. XMPP

Answer: C

Explanation:
Reference: https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/srnd/collab11/collab11/presence.html

NEW QUESTION 16
Which step is the first for web-based single sign-on login?

A. Authenticate.
B. Redirect to IdP to get authenticated.
C. Present authentication assertion.
D. Request access to protected service.

Answer: D

NEW QUESTION 21
......

Thank You for Trying Our Product

* 100% Pass or Money Back

    All our products come with a 90-day Money Back Guarantee.

* One year free update

    You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

    We currently serve more than 30,000,000 customers.

* Shop Securely

    All transactions are protected by VeriSign!

100% Pass Your 300-810 Exam with Our Prep Materials Via below:

https://www.certleader.com/300-810-dumps.html