Free Questions for 350-801

Shared by Melendez on 24-05-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

The chief officer at a company must reduce collaboration infrastructure costs by onbording all on-permises equipment to the cloud by using CISCO Webex Control Hub. Administrators need the ability to manage upgrades and set up hot desking for on-premises devices.

Which action must be taken before on boardng devices by using the Control Hub?

Options:

A- Configure tie Control Hub organization ID on the devices
B- Acquire a license for each device.
C- Allow HTTP traffic from each device to Control Hub.
D- Upgrade all the devices to software version CE9.15 or later

Answer:

D

Explanation:

This is a prerequisite for using the Device Connector tool, which allows you to onboard and register several devices simultaneously to the Webex Control Hub1. The Device Connector tool creates a workspace, an activation code, and activates all of your devices in one go1. This way you don't need to be physically present in the same room to activate the devices.

The other options are not required before onboarding devices by using the Control Hub:

Configuring the Control Hub organization ID on the devices is not necessary, as the Device Connector tool will send the device information to your Webex organization and generate activation codes for them1.

Acquiring a license for each device is not necessary, as you can assign licenses to users and devices after they are registered to the Webex Control Hub2.

Allowing HTTP traffic from each device to Control Hub is not necessary, as HTTPS connectivity is required for the Device Connector tool to communicate with the devices1.

Question 2

Question Type: MultipleChoice

How many minutes does it take for automatic fallback to occur in a Presence Redundancy Group if the primary node lost a critical service?

Options:

A- 5 min
B- 10 min
C- 30 min
D- 60 min

Answer:

C

Question 3

Question Type: MultipleChoice

Which actions required for a firewall configuration on a Mobile and Remote Access

through Cisco Expressway deployment?

Options:

A- The traversal zone on Expressway-c points to Expressway-e through the peer address field on the traversal zone, which specifies the Expressway-e server address. For dual NIC deployments, set the Expressway-e address using an FQDN that resolves the IP address of the internal interface
B- The external firewall must allow these inbound connections to Expressway: SIP: TCP 5061; HTTPS: TCP 8443; XMPP TCP 5222; media: UDP 36002 to 59999
C- Do not use a shared address for Expressway-e and Expressway-c, as the firewall cannot distinguish between them. If static NAT for IP addressing on Expressway-e is used, ensure that any NAT operation on expressway-c does not resolve the same traffic IP address. Shared NAT IS not supported
D- The internal firewall must allow these inbound and outbound connections between expressway - c and Expressway-e :sip;HTTPS(tunneled over SSH between C and E. TCP 2222: TCP 7001: Traversal Media: UDP 2776 to 2777(or 36000 to 36011 for large VM/appliance); XMPP:TCP 7400

Answer:

B

Question 4

Question Type: MultipleChoice

Which Cisco IM and Presence service handles failover and state changes in the cluster?

Options:

A- XCP Sync Agent
B- Cisco Server Recovery Manager
C- Cisco XCP Connection Manager
D- XCP router

Answer:

B

Question 5

Question Type: MultipleChoice

What is the major difference between the two possible Cisco IM and Presence high-availability modes?

Options:

A- Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standbynode in the event of an outage, and it also provides load balancing.
B- Balanced mode provides user load balancing and user failover only for manually generated failovers. Active/standby mode provides anunconfigured standby node in the event of an outage, but it does not provide load balancing.
C- Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standbynode in the event of an outage, but it does not provide load balancing.
D- Balanced mode does not provide user load balancing, but it provides user failover in the event of an outage. Active/standby mode provides analways on standby node in the event of an outage,

but it does not provide load balancing.

Answer:

C

Explanation:

Balanced mode provides user load balancing and user failover in the event of an outage. Active/standby mode provides an always on standby node in the event of an outage, but it does not provide load balancing.

Here is a more detailed explanation of the two modes:

Balanced mode:In balanced mode, the IM and Presence Service nodes are configured to work together to provide high availability. The nodes are configured in a redundancy group, and the system automatically balances the load of users across the nodes in the group. If one of the nodes fails, the system automatically fails over the users to the other nodes in the group.

Active/standby mode:In active/standby mode, one of the IM and Presence Service nodes is designated as the active node, and the other nodes are designated as standby nodes. The active node handles all of the user traffic, and the standby nodes are only used if the active node fails. If the active node fails, the system automatically fails over to one of the standby nodes.

Question 6

Question Type: MultipleChoice

Exhibit.

```
admin:utils ntp status
ntpd (pid 14550) is running...

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*192.168.1.1     17.253.14.125    2 u   39   64    3    0.456   -0.236   0.116
*192.168.1.2     17.253.14.125    2 u   38   64    3    0.817   -0.695   0.395
```

Refer the exhibit. A collaboration engineer needs to replace the original, single NTP

server that was configured during the inital install of a Cisco UCM server. What is the first

step to accomplish this task?

Options:

A- Restart the NTP service on Cisco UCM
B- Delete the original NTP server from Cisco UCM
C- Stop the NTP service on Cisco UCM
D- Enable NTP authentication for the new NTP server on Cisco UCM

Answer:

B

Question 7

Question Type: MultipleChoice

An administrator must implement toll fraud prevention on Cisco UCM using these parameters:

* Enable Forced Authorization Code 112211.

* Set an authorization level of 3 for the route pattern 8005551212.

* Require no access code to dial 10-digit numbers.

How must the route pattern be implemented?

Options:

A- Pattern = 1122113.8005551212
B- Pattern = 8005551212.1122113
C- Pattern = 8005xxxxxx
D- Pattern = 3.800xxxxxxx

Answer:

A

Explanation:

To implement toll fraud prevention on Cisco UCM, an administrator can use the following parameters:

Enable Forced Authorization Code 112211.

Set an authorization level of 3 for the route pattern 8005551212.

Require no access code to dial 10-digit numbers.

The route pattern must be implemented as follows:

Pattern = 1122113.8005551212

This will require users to enter the authorization code 112211 followed by the number 8005551212 to dial this number. The authorization level of 3 will prevent users from transferring calls to this number.