Free Questions for 350-801 by dumpshq

Shared by Suarez on 15-04-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

What is required when deploying co-resident VMs by using Cisco UCM?

Options:

A- Provide a guaranteed bandwidth of 10 Mbps.

B- Deploy the VMs to a server running Cisco UCM.

C- Avoid hardware oversubscription.

D- Ensure that applications will perform QoS.

Answer:

C

Explanation:

When deploying co-resident VMs by using Cisco UCM, it is important to avoid hardware oversubscription. This means that you should not assign more resources to the VMs than the physical hardware can provide. For example, if you have a server with 16 CPU cores, you should not assign more than 16 CPU cores to the VMs.

If you oversubscribe the hardware, the VMs will not be able to get the resources they need to run properly. This can lead to performance problems and even outages.

To avoid hardware oversubscription, you should carefully plan your VM deployments. You should also monitor the performance of the VMs to make sure that they are not overusing the resources.

Here are some additional tips for deploying co-resident VMs by using Cisco UCM:

Use a virtualization platform that supports Cisco UCM.

Make sure that the VMs have the correct operating system and software installed.

Configure the VMs to use the correct network settings.

Monitor the performance of the VMs to make sure that they are running properly.

Question 2

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.

Question 3

Question Type: MultipleChoice

An administrator is asked to implement toll fraud prevention in Cisco UCM, specifically to restrict off-net to off-net call transfers. How is this implemented?

Options:

A- Enforce ad-hoc conference restrictions.

B- Set the appropriate service parameter.

C- Implement time-of-day routing.

D- Use the correct route filters.

Answer:

B

Explanation:

To restrict off-net to off-net call transfers, an administrator can set the 'Block Offnet to Offnet Transfer' service parameter to 'On'. This will prevent users from transferring calls from one external number to another external number.

The other options are not correct because:

A) Enforce ad-hoc conference restrictions: This will prevent users from creating ad-hoc conferences, but it will not prevent them from transferring calls.

C) Implement time-of-day routing: This will allow calls to be routed to different destinations based on the time of day, but it will not prevent users from transferring calls.

D) Use the correct route filters: This will allow calls to be filtered based on the destination, but it will not prevent users from transferring calls.

Question 4

Question Type: MultipleChoice

Which wildcard must an engineer configure to match a whole domain in SIP route patterns?

Options:

A- *

B- @

C- !

D- .

Answer:

A

Explanation:

The asterisk (*) wildcard is used to match any sequence of characters, including an empty sequence. Therefore, it can be used to match any domain name in a SIP Route Pattern.

The other options are not correct because:

B) @: The @ symbol is used to separate the user name from the domain name in an email address.

C) !: The ! symbol is used to negate a character class.

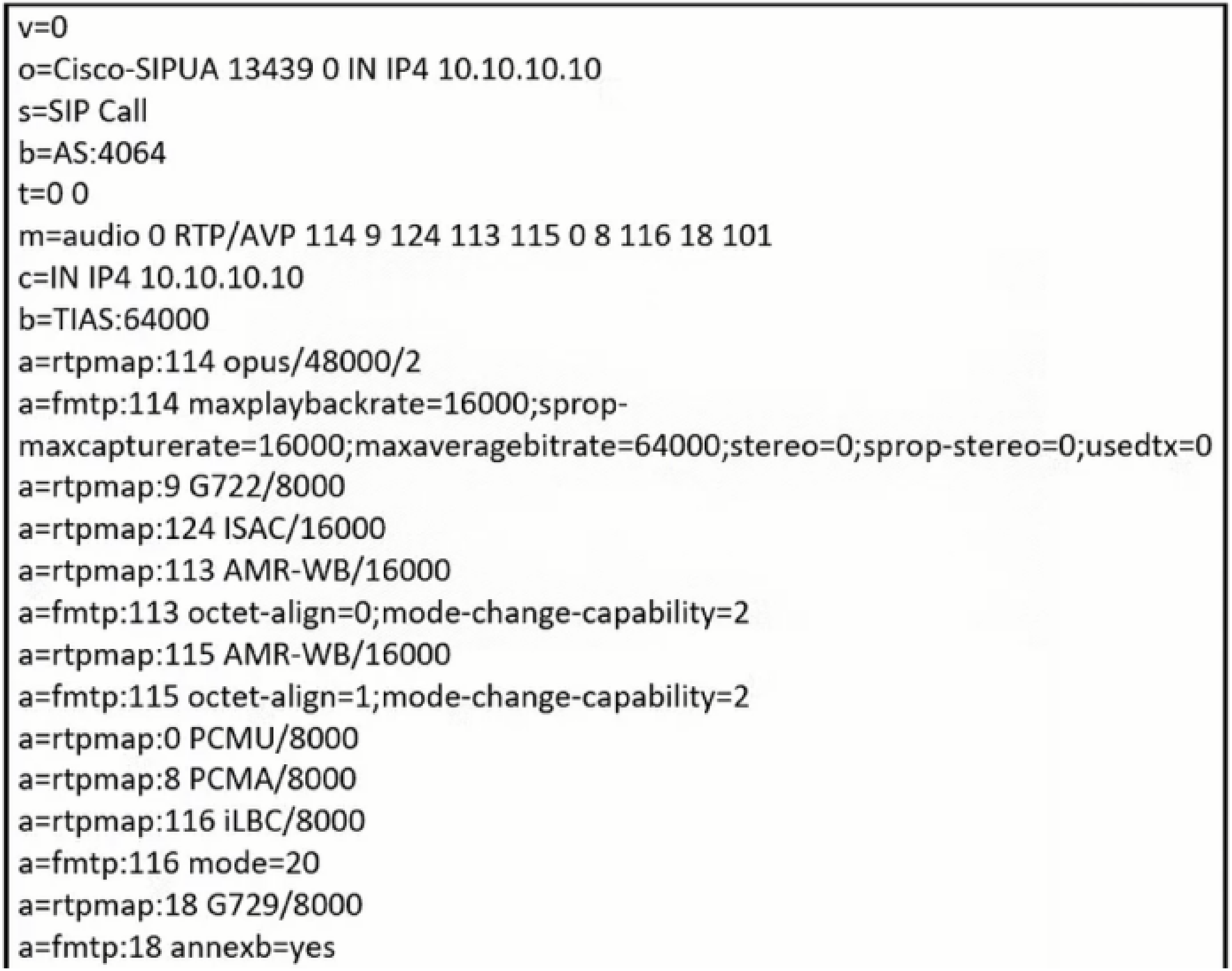
D) .: The . symbol is used to match any single character.

Question 5

Question Type: MultipleChoice

Refer to the exhibit.

https://i.postimg.cc/C57TkczG/image.png



```
v=0
o=Cisco-SIPUA 13439 0 IN IP4 10.10.10.10
s=SIP Call
b=AS:4064
t=0 0
m=audio 0 RTP/AVP 114 9 124 113 115 0 8 116 18 101
c=IN IP4 10.10.10.10
b=TIAS:64000
a=rtpmap:114 opus/48000/2
a=fmtp:114 maxplaybackrate=16000;sprop-
maxcapturerate=16000;maxaveragebitrate=64000;stereo=0;sprop-stereo=0;usedtx=0
a=rtpmap:9 G722/8000
a=rtpmap:124 ISAC/16000
a=rtpmap:113 AMR-WB/16000
a=fmtp:113 octet-align=0;mode-change-capability=2
a=rtpmap:115 AMR-WB/16000
a=fmtp:115 octet-align=1;mode-change-capability=2
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:116 iLBC/8000
a=fmtp:116 mode=20
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
```

A call is falling to establish between two SIP Devices The called device answers with these SOP Which SOP parameter causes issue?

Options:

A- The calling device did not offer a ptime value

B- The media stream is set to send only

C- The payload for G.711ulaw must be 18.

D- The RTP port is set to 0.

Answer:

D

Explanation:

The RTP port is used to send and receive media packets during a call. If the RTP port is set to 0, the called device will not be able to send or receive media packets, and the call will fail.

The other options are not correct because:

A) The calling device did not offer a ptime value: The ptime value is used to specify the amount of time between each media packet. If the calling device does not offer a ptime value, the called device will use the default value of 20 milliseconds.

B) The media stream is set to sendonly: The media stream is set to sendonly when the called device is only able to send media packets, and not receive them. This is not a problem, and the call will still succeed.

C) The payload for G.711ulaw must be 18: The payload for G.711ulaw is the type of media packet that is used. The payload must be set to 18 for G.711ulaw, but this is not a problem, and the call will still succeed.

Question 6

Question Type: MultipleChoice

Which two configuration elements are part of the Cisco UCM toll-fraud prevention?(Choose two.)

Options:

A- feature control policy

B- partition

C- SIP trunk security profile

D- SUBSCRIBE Calling Search Space

E- Calling Search Space

Answer:

A, E

Explanation:

The following are the configuration elements that are part of the Cisco UCM toll-fraud prevention:

Feature control policy- This policy controls the features that are available to users. For example, you can use this policy to prevent users from making international calls.

Calling Search Space- This space defines the numbers that users can call. For example, you can use this space to prevent users from calling premium-rate numbers.

Question 7

Question Type: MultipleChoice

An administrator installs a new Cisco TelePresence video endpoint and receives this error:"AOR is not permitted by Allow/Deny list. Which action should be taken to resolve this problem?

Options:

A- Reboot the VCS server and attempt reregistration.

B- Change the SIP trunk configuration.

C- Correct the restriction policy settings.

D- Upload a new policy in VCS.

Answer:

C

Explanation:

The error message 'AOR is not permitted by Allow/Deny list' indicates that the endpoint is not allowed to register with the VCS server because it is not on the Allow List or it is on the Deny List. To resolve this problem, you must correct the restriction policy settings.

Question 8

Question Type: MultipleChoice

Which call flow matches traffic from a Mobile and Remote Access registered endpoint to central call control?

Options:

A- Endpoint>Expressway-C>Expressway-E>Cisco UCM

B- Endpoint>Expressway-E>Expressway-C> Cisco UCM

C- Endpoint>Expressway-E> Cisco UCM

D- Endpoint>Expressway-C> Cisco UCM

Answer:

A

Explanation:

The call flow for a Mobile and Remote Access registered endpoint to central call control is as follows:

The endpoint registers with the Expressway-C.

The Expressway-C forwards the registration request to the Expressway-E.

The Expressway-E forwards the registration request to the Cisco UCM.

The Cisco UCM registers the endpoint.

When the endpoint places a call, the call flow is as follows:

The endpoint sends the call request to the Expressway-C.

The Expressway-C forwards the call request to the Expressway-E.

The Expressway-E forwards the call request to the Cisco UCM.

The Cisco UCM places the call.

The Expressway-C and Expressway-E are used to provide secure access to the Cisco UCM for endpoints that are not located on the corporate network. The Expressway-C is located on the corporate network, and the Expressway-E is located in the DMZ.

Question 9

Question Type: MultipleChoice

An engineer encounters third-party devices that do not support Cisco Discovery Protocol. What must be configured on the network to allow device discovery?

Options:

A- LLDP

B- TFTP

C- LACP

D- SNMP

Answer:

A

Explanation:

LLDP (Link Layer Discovery Protocol) is a vendor-neutral network discovery protocol that is used to discover the topology of a network. LLDP is similar to CDP (Cisco Discovery Protocol), but it is not proprietary to Cisco. LLDP is supported by a wide range of network devices, including switches, routers, and firewalls.

To configure LLDP on a network, you must enable LLDP on the devices that you want to discover. You can then use a network management tool, such as Cisco Network Assistant, to view the topology of the network.

The other options are incorrect. TFTP (Trivial File Transfer Protocol) is a network protocol that is used to transfer files between devices. LACP (Link Aggregation Control Protocol) is a network protocol that is used to aggregate multiple network links into a single logical link. SNMP (Simple Network Management Protocol) is a network protocol that is used to manage network devices.

Question 10

Question Type: **MultipleChoice**

An administrator must configure the Local Route Group feature on Cisco UCM. Which step will enable this feature?

Options:

A- For each route group, check the box for the Local Route Group feature.

B- For each route pattern, select the Local Route Group as the destination.

C- For each device pool, configure a route group to use as a Local Route Group for that device pool

D- For each route list, configure a route group to use as a Local Route Group.

Answer:

C

Explanation:

The Local Route Group feature allows you to use a route group as the destination for calls that are placed from a device pool. The route group that you use as the destination for calls from a device pool is called the Local Route Group for that device pool.

To configure the Local Route Group feature, you must first create a route group. You can then configure the Local Route Group feature for a device pool by selecting the route group that you want to use as the Local Route Group for that device pool.

Question 11

Question Type: **MultipleChoice**

How is bandwidth allocated to traffic flows in a flow-based WFQ solution?

Options:

A- All the bandwidth is divided based on the QoS marking of the packets.

B- Each type of traffic flow has equal bandwidth.

C- Bandwidth is divided among traffic flows. Voice has priority.

D- Voice has priority and the other types of traffic share the remaining bandwidth.

Answer:

D

Explanation:

In a flow-based WFQ solution, bandwidth is allocated to traffic flows based on the following criteria:

The priority of the traffic flow

The amount of bandwidth that is available

The number of traffic flows that are competing for bandwidth

Voice traffic is typically given a higher priority than other types of traffic, such as data traffic. This is because voice traffic is more sensitive to latency and jitter than data traffic.

When there is not enough bandwidth to accommodate all of the traffic flows, the WFQ algorithm will prioritize the traffic flows based on their priority. The traffic flows with the highest priority will be given the most bandwidth, and the traffic flows with the lowest priority will be given the least bandwidth.

If there is still not enough bandwidth to accommodate all of the traffic flows, the WFQ algorithm will start to drop packets. The packets that are dropped will be the packets from the traffic flows with the lowest priority.