Free Questions for 350-601 by certsinside

Shared by Cooke on 09-08-2024

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: **MultipleChoice**

Refer to the exhibit. An engineer is performing a Cisco Nexus 3000 Series Switch configuration backup with a TFTP server that is reachable in the global routing table. Which action completes the scheduler configuration?

Options:

A- Use the default VRF for the scheduler job.

B- Configure the scheduler authentication password.

C- Define the scheduler start time as required.

D- Make the size of the job output lower than the size of the log file.

Answer:

A

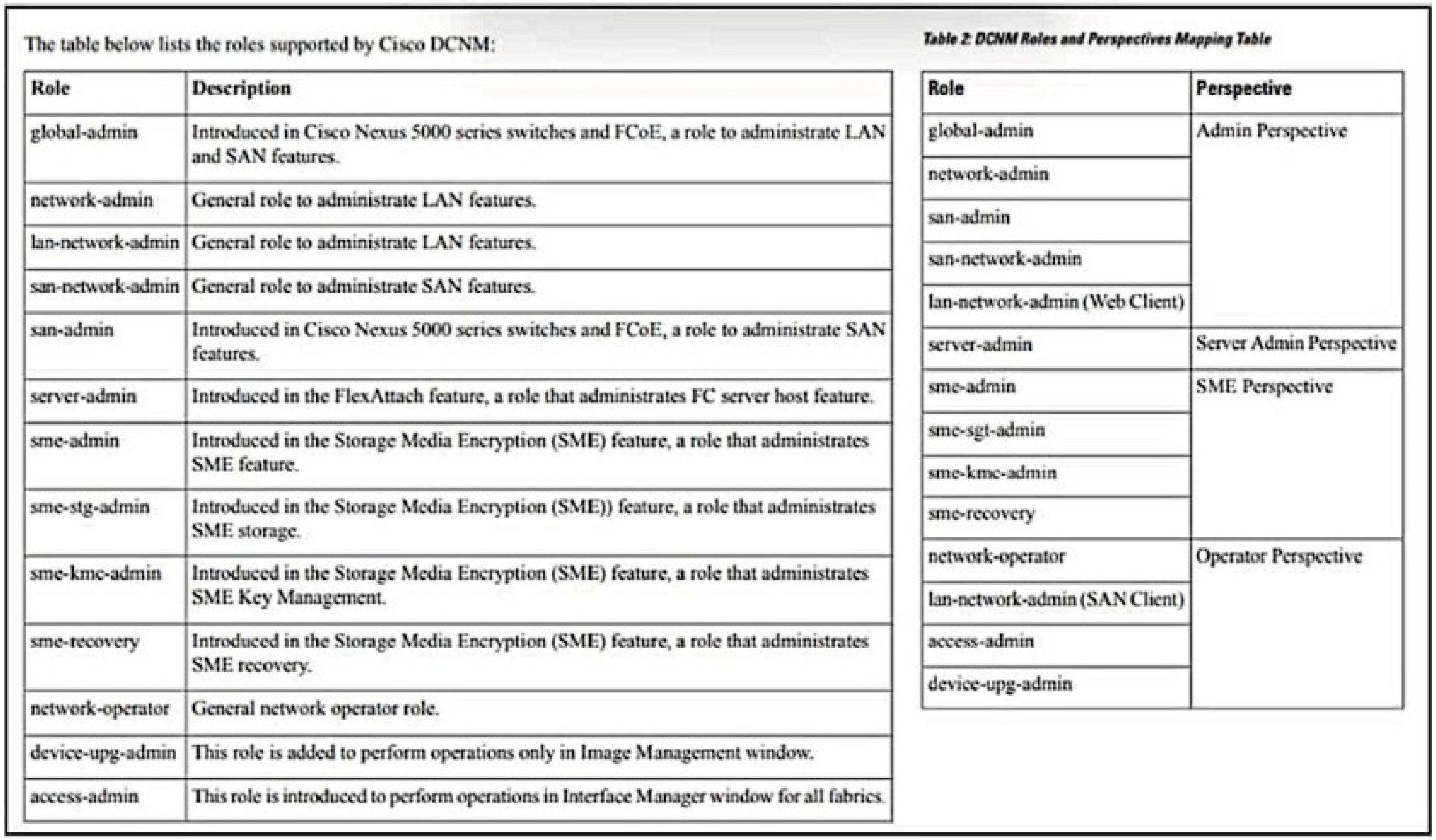
Explanation:

In the context of Cisco Nexus switches, VRF (Virtual Routing and Forwarding) is used to create multiple virtual routing tables within a single switch. By using the default VRF for the scheduler job, the engineer ensures that the TFTP server, which is reachable in the global routing table, can be accessed without the need for additional VRF configuration. This simplifies the backup process and avoids potential issues with VRF-specific routing that could prevent access to the TFTP server.

Question 2

Question Type: MultipleChoice

Refer to the exhibit.



The table below lists the roles supported by Cisco DCNM:

Role	Description
global-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate LAN and SAN features.
network-admin	General role to administrate LAN features.
lan-network-admin	General role to administrate LAN features.
san-network-admin	General role to administrate SAN features.
san-admin	Introduced in Cisco Nexus 5000 series switches and FCoE, a role to administrate SAN features.
server-admin	Introduced in the FlexAttach feature, a role that administrates FC server host feature.
sme-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME feature.
sme-stg-admin	Introduced in the Storage Media Encryption (SME)) feature, a role that administrates SME storage.
sme-kmc-admin	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME Key Management.
sme-recovery	Introduced in the Storage Media Encryption (SME) feature, a role that administrates SME recovery.
network-operator	General network operator role.
device-upg-admin	This role is added to perform operations only in Image Management window.
access-admin	This role is introduced to perform operations in Interface Manager window for all fabrics.

Table 2: DCNM Roles and Perspectives Mapping Table

Role	Perspective
global-admin	Admin Perspective
network-admin	
san-admin	
san-network-admin	
lan-network-admin (Web Client)	
server-admin	Server Admin Perspective
sme-admin	SME Perspective
sme-sgt-admin	
sme-kmc-admin	
sme-recovery	
network-operator	Operator Perspective
lan-network-admin (SAN Client)	
access-admin	
device-upg-admin	

An engineer is configuring Cisco Data Center Network Manager to automate the provisioning of Cisco Nexus 9000 Series Switches. The engineer must configure user access for network engineers to permit device operations in Interface Manager. The solution must hide Admin and Config Menu items in Interface Manager. Which two roles must be assigned to the network engineers to meet these requirements? (Choose two.)

Options:

A- network-admin

B- global-admin

C- access-admin

D- network-operator

E- san-admin

Answer:

C, D

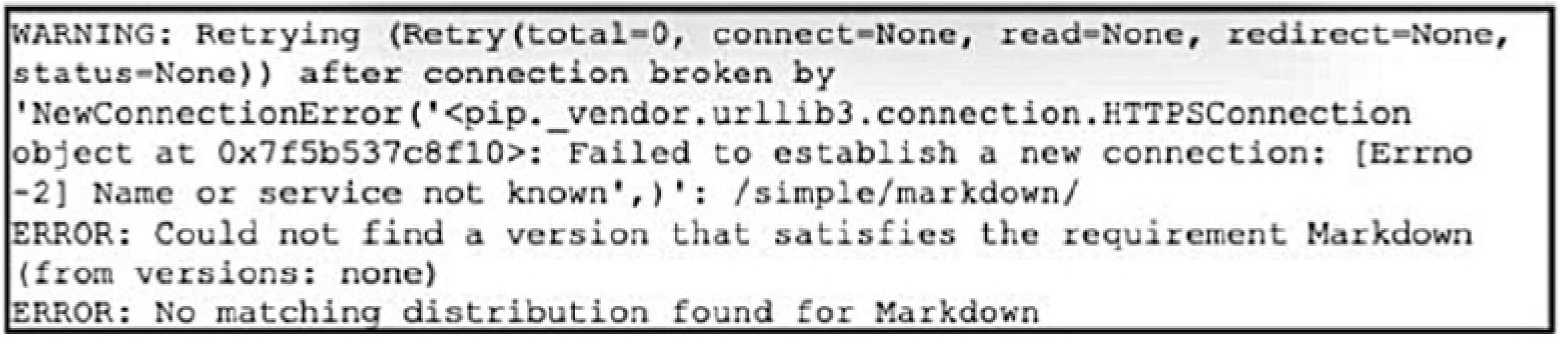
Explanation:

To meet the requirements of automating the provisioning of Cisco Nexus 9000 Series Switches while hiding Admin and Config Menu items in Interface Manager, the roles ofnetwork-operatorandaccess-adminshould be assigned. Thenetwork-operatorrole permits device operations within Interface Manager, and theaccess-adminrole is likely to have the necessary permissions to manage user access without exposing sensitive admin and configuration options.

Question 3

Question Type: MultipleChoice

Refer to the exhibit.



```
WARNING: Retrying (Retry(total=0, connect=None, read=None, redirect=None,
status=None)) after connection broken by
'NewConnectionError('<pip._vendor.urllib3.connection.HTTPSConnection
object at 0x7f5b537c8f10>: Failed to establish a new connection: [Errno
-2] Name or service not known',)': /simple/markdown/
ERROR: Could not find a version that satisfies the requirement Markdown
(from versions: none)
ERROR: No matching distribution found for Markdown
```

An engineer runs a Python script from a newly enabled guest shell on a Cisco Nexus 93108 Series Switch. The script needs an additional package called "Markdown" installed from the Python package manager. Which set of tasks must the engineer perform to install the required package?

Options:

A- Set the NAMESERVER variable in /etc/sysconfig/network. Clone the Markdown repository with the git clone command.

B- Add nameserver configuration to /etc/resolv.conf. Run sudo chvrf management pip install Markdown.

C- Enable ip domain-lookup in startup-config. Enter python install Markdown as root.

D- Configure ip name-server in configuration mode. Execute sudo yum -y install Markdown.

Answer:

B

Explanation:

To install the "Markdown" package from the Python package manager on a Cisco Nexus 93108 Series Switch, the engineer must ensure that the guest shell has internet access to reach the Python package repository. This is achieved by adding the nameserver configuration to/etc/resolv.conf, which allows the system to resolve domain names into IP addresses. After configuring the nameserver, the engineer must run the commandsudo chvrf management pip install Markdownto install the package within the management Virtual Routing and Forwarding (VRF) context, which has access to the internet.

Question 4

Question Type: **MultipleChoice**

Refer to the exhibit. A source is sending a multicast traffic stream to the receiver. How is the multicast traffic expected to flow through the network when it reaches a vPC peer?

Options:

A- * The multicast traffic is not replicated to the ports that joined a multicast group (224.0.0.13) or the peer link.
* The multicast traffic stream flows over the vPC link to ensure that orphan ports get the multicast stream in failure scenarios.

B- * The multicast traffic is replicated to the ports that joined a given multicast group and the peer link.
* The multicast traffic stream flows from Agg-1 to Agg-2 over the M1-to-M2 peer link and forwards the traffic over Layer 4 to Access-2.

C- * The multicast traffic is replicated to the ports that joined a given multicast group and the peer link.
* The multicast traffic stream flows over the peer link to ensure that orphan ports receive the multicast stream in failure scenarios.

D- * The multicast traffic is not replicated to the ports that joined a multicast group (224.0.0.13) or the peer link.
* The multicast traffic stream flows from Agg-1 to Agg-2 over the M1-to-M2 peer link and forwards the traffic over Layer 4 to Access-2.

Answer:

C

Explanation:

In a vPC (Virtual Port-Channel) environment, multicast traffic is expected to be replicated to the ports that have joined the multicast group and also across the peer link. This ensures that in case of a failure scenario, orphan ports, which are ports not part of the vPC and only connected to one of the vPC peer switches, still receive the multicast stream.Option C correctly describes this behavior, where the multicast traffic is replicated to the ports that joined a given multicast group and the peer link, and the multicast traffic stream flows over the peer link to ensure that orphan ports receive the multicast stream in failure scenarios12.

Question 5

Question Type: MultipleChoice

An engineer must create a new Cisco UCS user account to perform these actions:

* Modify systems logs, faults, and power management settings.

* View access to all other configuration in the UCS domain.

Which two roles must be assigned to the user to permit these actions? (Choose two.)

Options:

A- Server Compute

B- Read-Only

C- Operations

D- Facility Manager

E- Administrator

Answer:

C, E

Explanation:

The roles required to modify system logs, faults, and power management settings, as well as view access to all other configurations in the UCS domain, are typically those that provide broad administrative capabilities.TheOperationsrole allows for the modification of operational aspects such as logs and power management, while theAdministratorrole provides full access to all configurations and settings within the UCS domain1.

Question 6

Question Type: MultipleChoice

A QoS policy on Cisco UCS must meet these requirements:

* No-drop class must be configured.

* Jumbo frames must be enabled without fragmentation.

Which configuration must be implemented to mast these conditions?

Options:

A- Configure slow-drain timers and specify an MTU value of 9100 bytes.

B- Create a Flow Control Policy and specify an MTU value of 9000 bytes.

C- Create a QoS system class and specify an MTU value of 9216 bytes.

D- Configure Platinum system class and specify an MTU value of 9100 bytes.

Answer:

C

Explanation:

To meet the requirements of configuring a QoS policy on Cisco UCS that includes a no-drop class and enables jumbo frames without fragmentation, a QoS system class must be created with an MTU value of 9216 bytes. This MTU size is large enough to support jumbo frames, which can carry more data than standard frames, reducing the number of frames sent and improving network efficiency. The no-drop class ensures that frames are not dropped, which is crucial for certain types of traffic that require reliable delivery, such as storage traffic.

Question 7

Question Type: DragDrop

All logins to a Cisco Nexus 9000 Series Switch must pass through the TACACS+ server at IP address 192.168.10.10. The configuration must meet these requirements:

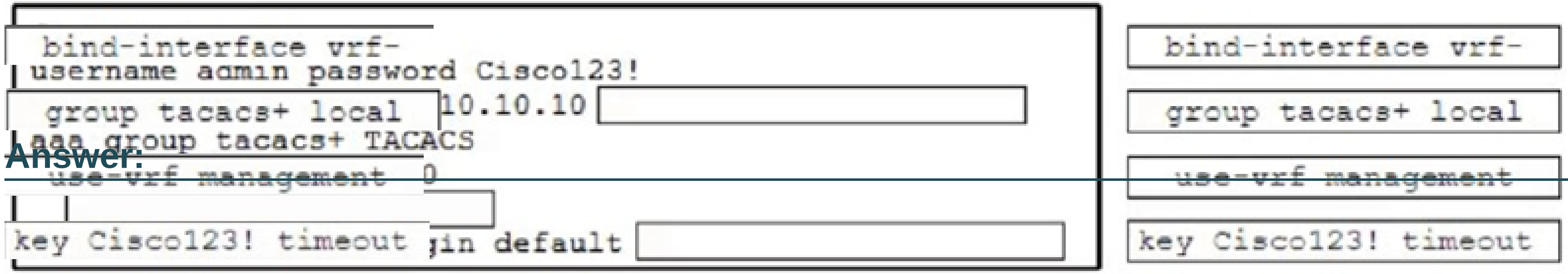
* The TACACS+ server must be used for SSH and Telnet.

* The TACACS+ server key must be Cisco123!.

* Management VRF must be used for connectivity.

* The deployment must fail back to local credentials if the TACACS+ server fails to respond within 30 seconds.

Drag and drop the code snippets from the right onto the blanks in the code on the left to complete the configuration. Not all code snippets are used.



```
bind-interface vrf-
username admin password Cisco123!
group tacacs+ local  10.10.10
aaa group tacacs+ TACACS
use-vrf management  0

key Cisco123! timeout  gin default
```

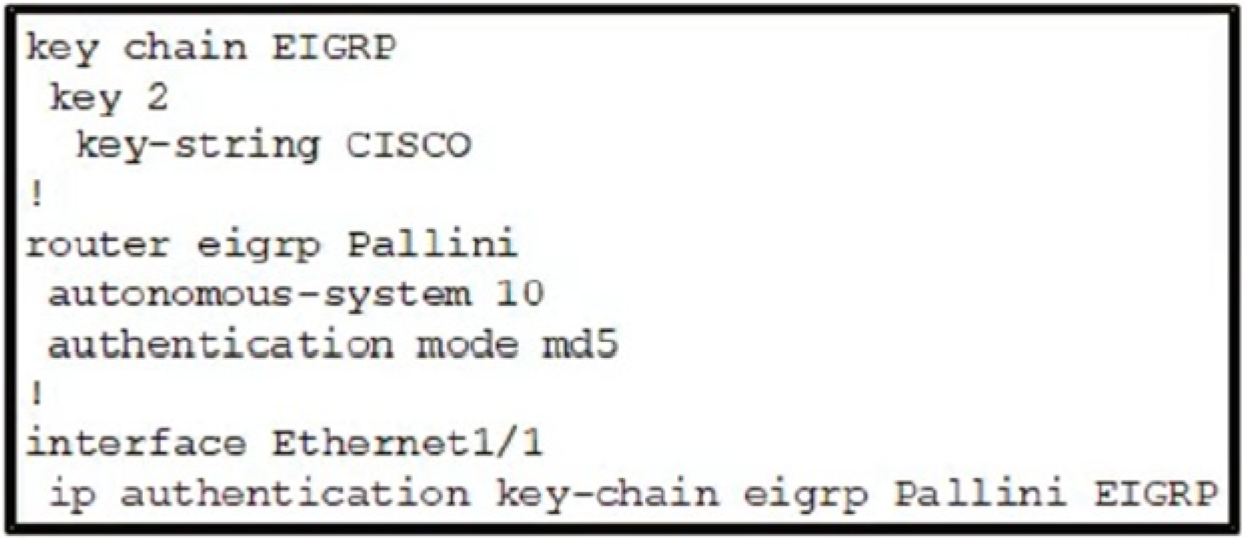
```
bind-interface vrf-
group tacacs+ local
use-vrf management
key Cisco123! timeout
```

Answer:

Question 8

Question Type: MultipleChoice

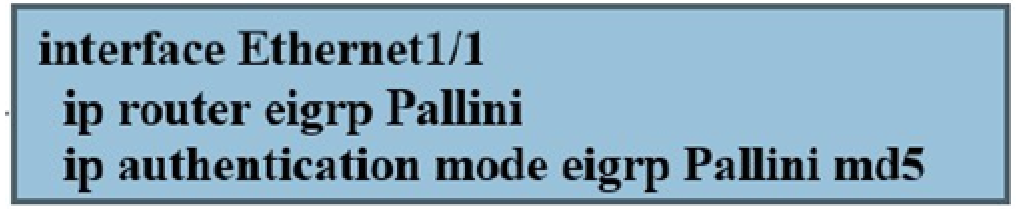
Refer to the exhibit.



```
key chain EIGRP
 key 2
  key-string CISCO
!
router eigrp Pallini
 autonomous-system 10
 authentication mode md5
!
interface Ethernet1/1
 ip authentication key-chain eigrp Pallini EIGRP
```

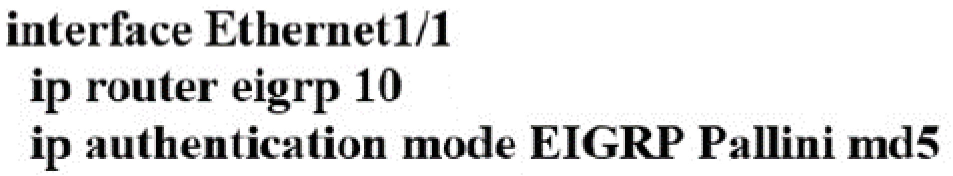
Two Cisco Nexus Series Switches use EIGRP between their Eth1/1 interfaces. The switches are configured to support EIGRP authentication. Which set of CLI commands must be used to establish EIGRP neighborship?

A)



```
interface Ethernet1/1
 ip router eigrp Pallini
 ip authentication mode eigrp Pallini md5
```

B)



```
interface Ethernet1/1
  ip router eigrp 10
  ip authentication mode EIGRP Pallini md5
```

Options:

A- Option A

B- Option B

Answer:

A

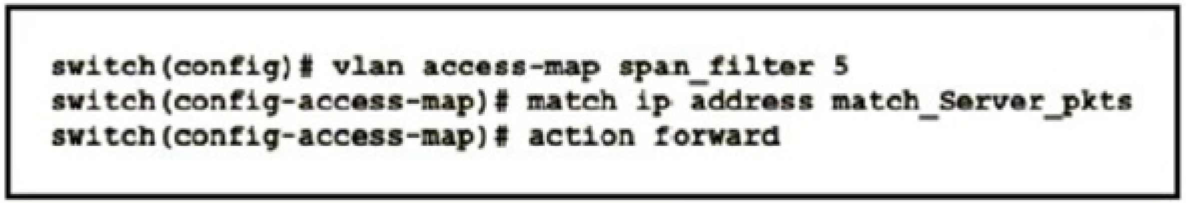
Explanation:

EIGRP authentication is used to prevent unauthorized devices from forming neighbor relationships. The correct CLI commands to establish EIGRP neighborship with authentication on Cisco Nexus switches involve configuring the interface with EIGRP, setting the EIGRP autonomous system number, and specifying the authentication key and key-chain. The commands in Option A are consistent with these requirements, hence it is the verified answer.

Question 9

Question Type: MultipleChoice

Refer to the exhibit.



```
switch(config)# vlan access-map span_filter 5
switch(config-access-map)# match ip address match_Server_pkts
switch(config-access-map)# action forward
```

An engineer reported suspicious behaviour in a server farm that is deployed on the 198.19.1.0/24 subnet. The traffic must be captured only from the server with the IP address of 198.19.1.19/24. The traffic analyzer is connected to the same switch as the server farm. Which configuration set captures the traffic?

A.

Options:

A- switch(config)# ip access-list match_Server_pkts switch(config-acl)# permit ip 198.19.1.19 0.0.0.0 any switch(config)# monitor session 1 switch {config-m on itor)# filter access-group span.filter

B- switch(config)# ip access-list match_Server_pkts Switch{config-acl)# permit ip 198.19.1.19 0.0.0.0 any switch(config)# monitor session 1 switch (config-m on itor)# filter access-group 5

C- switch(config)# ip access-lisl match_Server_pkts
switch(config-acl)# permit ip 198.19.1.19 255.255.255.255 any switch(config)# monitor session 1 switch(config-monitor)# filter access-group span.filter

D- switch(config)# ip access-list match_Server_pkts switch(config-acl)# permit ip 198.19.1.19 255.255.255.0 any switch(config)# monitor session 1 switch (config-m on itor)# filter access-group span_filter

Answer:

C

Explanation:

The correct configuration to capture traffic only from the server with the IP address of 198.19.1.19/24 is option C. This configuration uses an IP access list to match packets from the specific IP address with a subnet mask of 255.255.255.255, which indicates a single host. Themonitor sessioncommand is then used to apply this access list to a SPAN session, ensuring that only traffic from the specified server is captured.

Question 10

Question Type: MultipleChoice

A network automation engineer must configure a Cisco NX-OS REST API on a Cisco 9000 Series Switch with these requirements:

* NX-API REST and the DME database must be enabled.

* The NX-API REST must listen for HTTP traffic on port 83.

* The HTTPS certificate must be uploaded.

Which configuration set must be used to accomplish these goals?

Options:

A- feature nxapi
nxapi (tcp) port 83
nxapi certificate {httpscrt}

B- feature nxapi
nxapi (tcp) port 83
nxapi certificate {httpscrt}
nxapi certificate enable

C- feature nxapi
nxapi (http) port 83
nxapi certificate {httpscrt}

D- feature nxapi
nxapi {http} port 83

```
nxapi certificate {httpscrt | httpskey}
nxapi certificate enable
```

Answer:

B

Explanation:

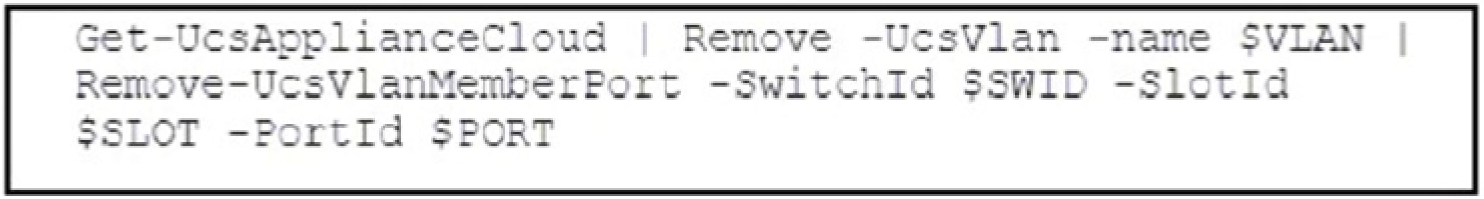
To meet the requirements for configuring Cisco NX-OS REST API on a Cisco 9000 Series Switch, the correct configuration set is option B. This set of commands enables the NX-API feature, sets the NX-API to listen for HTTP traffic on TCP port 83, uploads the HTTPS certificate, and then enables the certificate. The inclusion of thenxapi certificate enablecommand is crucial as it activates the uploaded certificate, which is necessary for establishing secure HTTPS connections.

Question 11

Question Type: MultipleChoice

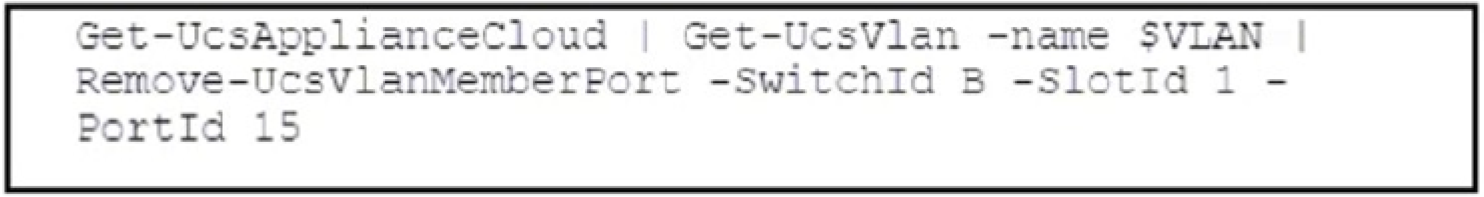
An engineer must create a PowerShell script that leverages the Cisco UCS Manager PowerShell module to submit automated requests to Cisco UCS Manager. The engineer must automate the removal of switches from VLANs. Environment variables must provide the VLAN name and switch identifiers. The VLAN must persist when it is removed from the switch port. Which command must the engineer include in the script to accomplish these goals?

A)



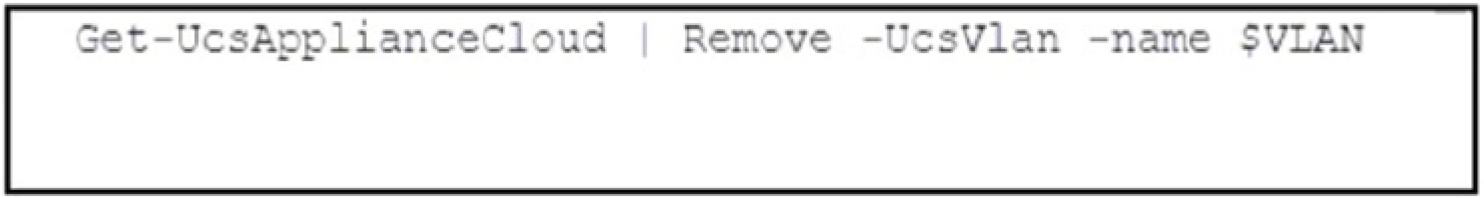
```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN |
Remove-UcsVlanMemberPort -SwitchId $SWID -SlotId
$SLOT -PortId $PORT
```

B)



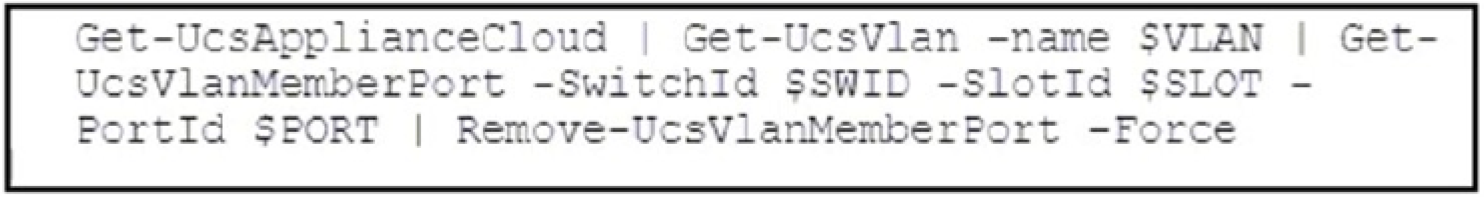
```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN |
Remove-UcsVlanMemberPort -SwitchId B -SlotId 1 -
PortId 15
```

C)



```
Get-UcsApplianceCloud | Remove -UcsVlan -name $VLAN
```

D)



```
Get-UcsApplianceCloud | Get-UcsVlan -name $VLAN | Get-
UcsVlanMemberPort -SwitchId $SWID -SlotId $SLOT -
PortId $PORT | Remove-UcsVlanMemberPort -Force
```

Options:

A- Option A

B- Option B

C- Option C

D- Option D

Answer:

D

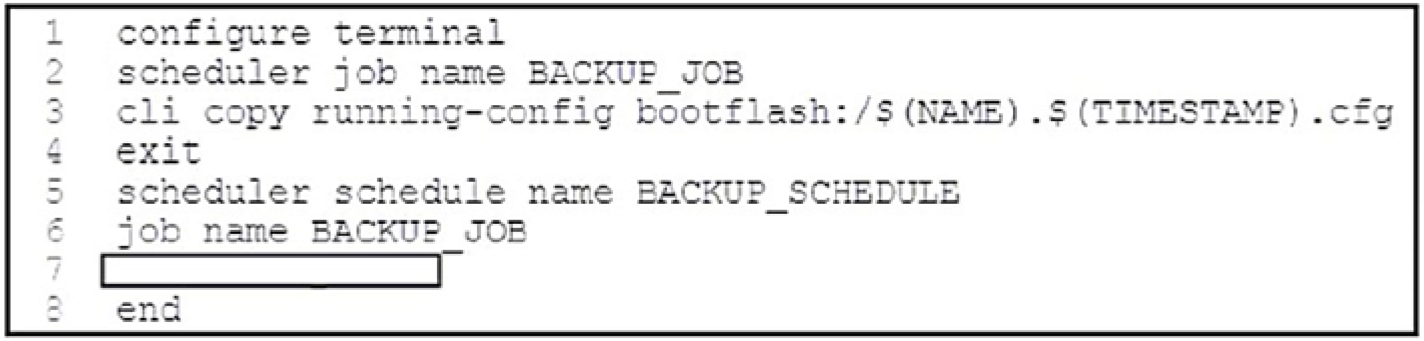
Explanation:

The PowerShell command in option D is the correct choice for automating the removal of switches from VLANs using the Cisco UCS Manager PowerShell module. This command uses environment variables to specify the VLAN name and switch identifiers, ensuring that the VLAN persists even when it is no longer associated with the switch port. The command structure allows for the removal of the VLAN association from the switch port without deleting the VLAN itself, thus maintaining the VLAN configuration for potential future use.

Question 12

Question Type: MultipleChoice

Refer to the exhibit.



```
configure terminal
scheduler job name BACKUP_JOB
cli copy running-config bootflash:/$(NAME).$(TIMESTAMP).cfg
exit
scheduler schedule name BACKUP_SCHEDULE
job name BACKUP_JOB

end
```

The Cisco NX-OS scheduler must run every day at 3:00 a.m. Which code snippet completes the script?

Options:

A- time start daily 3:00

B- time start weekly 7 3:00

C- time weekly 7 3:00

D- time daily 3:00

Answer:

D

Explanation:

The correct code snippet to ensure that the Cisco NX-OS scheduler runs every day at 3:00 a.m. is ''time daily 3:00''. This command configures the scheduler to execute the specified job daily at the given time, without the need for a 'start' keyword, which is not required in the syntax for daily repetitive tasks.