



Free Questions for 350-601 by certsinside

Shared by Gallegos on 24-05-2024

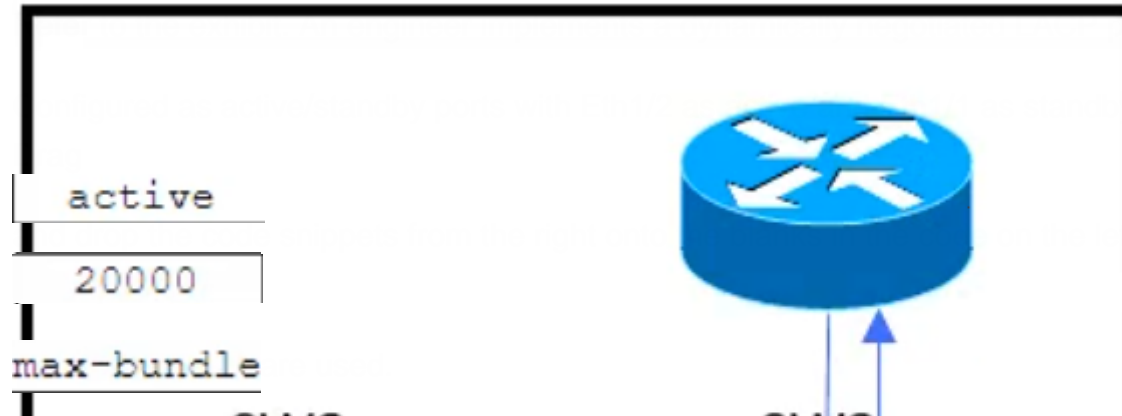
For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: DragDrop

- Refer to the exhibit.



port channel on SW1. The port channel members must be
 The Eth1/1 interface is Configured with default priority.
 to complete the Eth1/2 interface configuration for SW1.

Answer Area

```

; SW1 configuration
interface ethernet 1/2
  active
  lacp group 5 mode
  lacp port priority
  max-bundle
interface port-channel 5
  lacp
  
```

active	min-links
20000	40000
lacp	max-bundle

Question 2

Question Type: MultipleChoice



An engineer must Configure a new Cisco UCS B-Series infrastructure with a Cisco 5108 chassis. The configuration must meet these requirements:

- * The setup must use aggregation between Cisco UCS Fabric Interconnects and I/O modules.
- * The implementation requires four 10 GbE connections per I/O module.

* The Cisco UCS Fabric Interconnects must support uplinks of different speeds for future expansion.

Which two steps must be taken to meet these requirements? (Choose two.)

Options:

- A- Reacknowledge the chassis after the initial discovery.
- B- Set IOM link pinning in Global Policies.
- C- Configure unified ports for the chassis.
- D- Set Link Group Preference to Port Channel.
- E- Disable Auto Configure Server Port.

Answer:

B, C

Question 3

Question Type: MultipleChoice

An engineer must replace a defective fabric interconnect with the same model. The system must be restored, including the database of

locally created users. The equivalent Cisco UCS Manager software version must be used. Which backup type must be used to meet these requirements?

Options:

- A- Full State
- B- All Configuration
- C- System Configuration
- D- Logical Configuration

Answer:

A

Question 4

Question Type: MultipleChoice

Which Cisco UCS firmware reboot policy must be used in the maintenance policy to prevent the server firmware from upgrading automatically and wait for user input before proceeding?

Options:

- A- scheduled
- B- timer-automatic
- C- immediate
- D- user-ack

Answer:

D

Question 5

Question Type: MultipleChoice

An engineer configures user authentication on Cisco UCS Manager to ensure that the user and roles can be saved on the external server and

secured using authentication. Which set of actions meets these requirements?

Options:

- A- Implement a logical configuration backup and configure the HTTPS protocol.
- B- Configure a full state backup and implement an FTP protocol.
- C- Perform a system configuration backup and use the SCP protocol.
- D- Deploy an all configuration backup and implement a TFTP protocol.

Answer:

C

Question 6

Question Type: MultipleChoice

An engineer must upgrade the server firmware for which the service profile is configured with a host firmware package. Which action must be taken to accomplish this goal?

Options:

- A- Disassociate the service profile from the server and upgrade.
- B- Change the maintenance policy to user-ack and upgrade.
- C- Upgrade the server through the host firmware package.
- D- Perform a direct upgrade on the server using Auto Install.

Answer:

C

Explanation:

You can use firmware packages in service profiles to upgrade the server and adapter firmware, including the BIOS on the server, by defining a host firmware policy and including it in the service profile associated with a server.

Question 7

Question Type: MultipleChoice

A Cisco IMC on the Cisco UCS C-Series Server must be configured with VLAN ID 110 and a priority value of 20. Which command set meets these requirements?

Options:

A- Server# scope cimc -

Server /cimc # scope vlan -

Server /cimc/network # enable vlan

Server /cimc/network *# set vlan-id 110

Server /cimc/network *# set vlan-priority 20

Server /cimc/network *# commit

B- Server# scope cimc -

Server /cimc # scope network -

Server /cimc/network # set vlan-enabled yes

Server /cimc/network *# set vlan-id 110

Server /cimc/network *# set vlan-priority 20

Server /cimc/network *# commit

C- Server# scope cimc -

Server /cimc # scope network -

Server /cimc/network # switchport mode trunk

Server /cimc/network *# switchport trunk native vlan 110

```
Server /cimc/network *# spanning-tree portfast
```

```
Server /cimc/network *# copy run start
```

D- Server# scope cimc -

```
Server /cimc # scope network -
```

```
Server /cimc/network # switchport mode access
```

```
Server /cimc/network *# switchport access 110
```

```
Server /cimc/network *# spanning-tree portfast
```

```
Server /cimc/network *# copy run start
```

Answer:

B

Explanation:

```
Server# scope cimc
```

```
Server /cimc # scope network
```

```
Server /cimc/network # set vlan-enabled yes
```

```
Server /cimc/network *# set vlan-id 10
```

```
Server /cimc/network *# set vlan-priority 32
```

```
Server /cimc/network *# commit
```

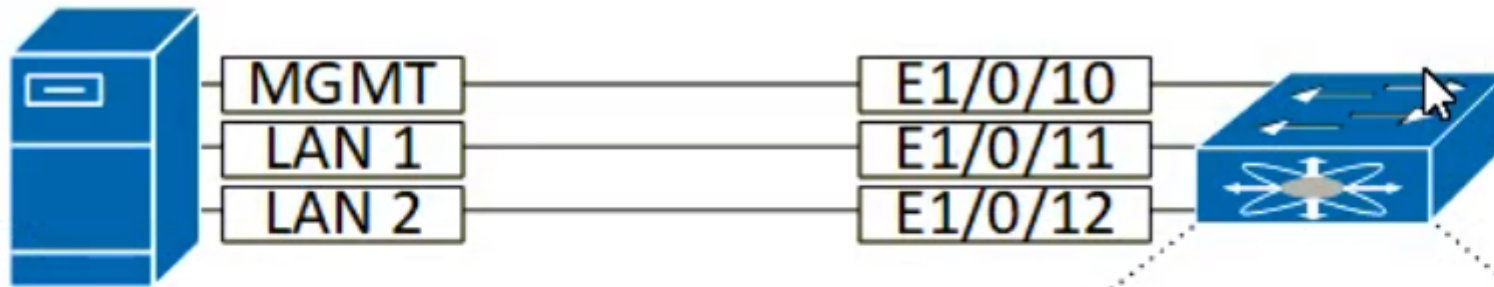
Server /cimc/network # show detail

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/cli/config/guide/1-4-1/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_141/b_Cisco_UCS_C-Series_CLI_Configuration_Guide_141_chapter_01000.html#task_F1A505AA52BE41C2A0CE089FCAE4F9D2

Question 8

Question Type: MultipleChoice

Refer to the exhibit.



```
interface Ethernet1/0/10
  switchport mode access
  switchport access vlan 100
interface Ethernet1/0/11
  switchport mode access
  switchport access vlan 101
interface Ethernet1/0/12
  switchport mode access
  switchport access vlan 102
```

An engineer must access a Cisco UCS C-Series server KVM from a remote location. The engineer must use the out-of-band interface to access the KVM. Which configuration set meets these requirements?

Options:

A- NIC mode: Shared LOM -

VLAN ID: 100

B- NIC mode: Dedicated -

VLAN ID: 101

C- NIC mode: Dedicated -

VLAN state: Disabled

D- NIC mode: Shared LOM -

VLAN state: Disabled

Answer:

C

Explanation:

Dedicated---A connection to the CIMC is available through the management Ethernet port or ports.

Shared LOM---A connection to the CIMC is available only through the LAN On Motherboard (LOM) Ethernet host ports.

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/sw/gui/config/guide/1-1-1/b_Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_1/Cisco_UCS_C-Series_Servers_Integrated_Management_Controller_Configuration_Guide_1_1_1_chapter1.html

Question 9

Question Type: MultipleChoice

The Cisco TACACS+ on a Cisco Nexus Series Switch must authenticate any user attempting to access the device and fail over to the local account

if the TACACS+ sever becomes unavailable.

Which command accomplishes these goals?

Options:

A- aaa authentication login default fallback error local

- B- aaa authentication login console group local
- C- aaa authentication login default local
- D- aaa authentication login default group ISE local

Answer:

D

Explanation:

The command `aaa authentication login default group ISE local` configures the Cisco Nexus Series Switch to use TACACS+ for authentication by default and specifies a fallback to local authentication if the TACACS+ server becomes unavailable. This ensures that users are authenticated against the TACACS+ server when it is available, but allows them to use local switch credentials if the server cannot be reached, meeting the requirement for failover to local account 1.

Cisco documentation on configuring TACACS+ for Cisco Nexus Series Switches provides detailed steps and explanations for setting up authentication and ensuring failover to local accounts

Question 10

Question Type: MultipleChoice

Refer to the exhibit.

```
MDS# show role
```

```
Role: network-admin
```

```
Description: Predefined network admin role
```

```
-----  
Rule    Perm    Type    Scope    Entity  
-----  
rule 5 permit show feature hardware  
rule 4 permit show feature environment  
rule 3 permit config feature ntp  
rule 2 permit config feature ssh  
rule 1 permit config feature tacacs+
```

```
Role: Custom-Role-B
```

```
Description: Additional admin role
```

```
-----  
Rule    Perm    Type    Scope    Entity  
-----  
rule 6 permit config feature dpvm  
rule 1 deny config feature tacacs+
```


A Cisco MDS 9000 Series Switch is configured with RBAC. The default role applies to all users. User A is also assigned to the role Custom-Role-B. Which set of features will user A be authorized to configure?

Options:

A- NTP -
SSH -
DPVM

B- SSH -
DPVM -
TACACS+
NTP

C- DPVM -
NTP -
SSH -
hardware

D- hardware
environment
TACACS+

Answer:

A

Explanation:

User A, having both the default role and Custom-Role-B, will be authorized to configure NTP, SSH, and DPVM. The default role allows configuration of NTP and SSH, while Custom-Role-B specifically permits DPVM configuration and denies TACACS+.

Question 11

Question Type: DragDrop

An engineer must authenticate OSPF on interfaces of the Cisco Nexus 9000 Series Switch so that:

- * eth1/1 uses clear text password.
- * eth1/2 uses encrypted md5 password.

Drag and drop the commands from the bottom onto the boxes in the code to complete the configuration. Not all commands are used.

```

1 SW1(config)# router ospf 1
2 SW1(config-router)# interface ethernet 1/1
3 SW1(config-if)# ip router ospf 1 area 0.0.0.0
4 SW1(config-if)# ip ospf [ ]
5 SW1(config-if)# ip ospf [ ] 0 P@ssW1
6 SW1(config)# interface ethernet 1/2
7 SW1(config-if)# ip router ospf 1 area 0.0.0.0
8 SW1(config-if)# ip ospf authentication [ ]
9 SW1(config-if)# ip ospf [ ] 3 md5 3 2b7cf4643b66b22

```

Answer:

Question 12

Question Type: MultipleChoice

message-digest-key :	mode	message-digest-key
authentication-key by	authentication	key

An engineer must perform a backup and restore in Cisco UCS to rebuild the system in a disaster recovery scenario. The backup file must be encrypted to prevent the passwords from being stored as clear text. Which backup configuration meets these requirements?

Options:

- A- Full state backup over TFTP
- B- Logical configuration backup over SCP
- C- System configuration backup over FTP
- D- All configuration backup over SFTP

Answer:

A

Explanation:

A full state backup is the appropriate choice when an engineer needs to perform a backup and restore in Cisco UCS for disaster recovery purposes. This type of backup includes a snapshot of the entire system and is saved as a binary file. Importantly, full state backups are encrypted, ensuring that passwords and other sensitive information are not stored as clear text¹². While TFTP (Trivial File Transfer Protocol) is not secure by itself, the encryption of the full state backup file provides the necessary security for the passwords within the backup.

Cisco documentation on "Backing Up and Restoring the Configuration" provides detailed information on the different backup types and their contents¹.

Cisco UCS Manager Administration Management Guide 4.2, which mentions the encryption of full state backups

To Get Premium Files for 350-601 Visit

<https://www.p2pexams.com/products/350-601>

For More Free Questions Visit

<https://www.p2pexams.com/cisco/pdf/350-601>

