ATMIC NETWORKS
YOUR GUIDE TO GLOBAL CERTIFIATION

"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

www.atmicnetworks .com

Warning: Keep connected with our support team for latest updates

Question: 1

An engineer is implementing OTV on a transport that supports multicast. The solution needs to meet the following requirements:

- Establish adjacency to the remote peer by using multicast.
- Enable OTV advertisements for VLAN 100 to the other site.

Which two commands should be configured to meet these requirements? (Choose two.)

A. otv site-vlan 100

B. otv data-group 232.2.2.0/28

C. otv use-adjacency-server 172.27.255.94

D. otv extend-vlan 100

E. otv control-group 232.1.1.1

Answer: B. D

Explanation:

To establish adjacency to the remote peer by using multicast, the engineer needs to configure the otv data-group command with a multicast address range that is unique for each site. This command specifies the multicast group that is used to send and receive OTV data traffic. To enable OTV advertisements for VLAN 100 to the other site, the engineer needs to configure the otv extend-vlan command with the VLAN number. This command specifies which VLANs are extended across the overlay network. Reference:

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) - Cisco, Module 3: Data Center Network Connectivity Design, Lesson 3: Implementing Cisco Overlay Transport Virtualization

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 6.x - Configuring Basic OTV [Cisco Nexus 7000 Series Switches], Configuring Basic OTV, Configuring the OTV Data Group

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 6.x - Configuring Basic OTV [Cisco Nexus 7000 Series Switches], Configuring Basic OTV, Configuring VLANs to Be Extended over the OTV Overlay Network

Question: 2

An engineer updated firmware on Fabric Interconnects and activates it. However, the endpoint fails to boot from the new firmware image. What is expected to occur in this case?

A. The system defaults to the backup image version

B. The system defaults to and boots into the GOLD firmware image

C. The system defaults to the GOLD firmware image

D. The system defaults to and boots into the kickstart image

Answer: A

Explanation:

The system will automatically revert to the backup image version if the endpoint fails to boot from the new firmware image. This is a feature of the Fabric Interconnects that ensures high availability

and reliability. The GOLD firmware image is used for diagnostics and troubleshooting, not for normal operation. The kickstart image is used for booting the Nexus switches, not the Fabric Interconnects. Reference:

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Firmware Auto Install [Cisco UCS Manager], Firmware Auto Install, Firmware Auto Install Process

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Firmware Auto Install [Cisco UCS Manager], Firmware Auto Install, Firmware Auto Install Failure Scenarios

Cisco Nexus 7000 Series NX-OS System Management Configuration Guide, Release 6.x - Upgrading the Cisco NX-OS Software [Cisco Nexus 7000 Series Switches], Upgrading the Cisco NX-OS Software, Upgrading the Cisco NX-OS Software Using the CLI

Question: 3

Which configuration statically assigns VSAN membership to a virtual Fibre Channel interface?

A. switch(config-vsan-cb>)# vsan 100 bind interface fc 3/1

B. switch<config-vsan-db)# vsan 100 bind interface vfc 31

C. switch(config-vsan-db>)# vsan 100 fc 3/1

D. switch(config-vsan-db)# vsan 100 interface vfc 31

Answer: B

Explanation:

The vsan bind interface command is used to statically assign VSAN membership to a virtual Fibre Channel interface. This command overrides the VSAN membership that is derived from the physical interface or the default VSAN. The other commands are either invalid or do not apply to virtual Fibre Channel interfaces. Reference:

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring Virtual Fibre Channel Interfaces [Cisco Nexus 9000 Series Switches], Configuring Virtual Fibre Channel Interfaces, Configuring VSAN Membership for Virtual Fibre Channel Interfaces

Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 9.3(x) - Configuring VSANs [Cisco Nexus 9000 Series Switches], Configuring VSANs, Configuring Static VSAN Membership

Question: 4

An engineer must configure OSPF routing on Cisco Nexus 9000 Series Switches. The IP subnet of the Eth 1/2 interface for both switches must be advertised via OSPF. However, these interfaces must not establish OSPF adjacency or send routing updates. The current OSPF adjacency over the interface Eth1/1 on SW1 and Eth1/1 on SW2 must remain unaffected. Which configuration must be applied to both Nexus switches to meet these requirements?

A. interface ethernet 1/2 passive-interface default

B. Interface ethernet 1/2

Ip ospf network point-to-point

C. interface ethernet 1/2
ip ospf passive-interface

D. interface ethernet 1/2

no ip ospf passive-Interface

Answer: C

Explanation:

The ip ospf passive-interface command is used to prevent OSPF adjacency and routing updates from being sent or received on a specific interface, while still advertising the interface subnet via OSPF. This command is useful for stub networks or loopback interfaces that do not need to form OSPF neighbor relationships. The other commands either

enable OSPF adjacency by default, change the OSPF network type, or disable OSPF passive mode. Reference:

Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x) - Configuring OSPF [Cisco Nexus 9000 Series Switches], Configuring OSPF, Configuring OSPF Interfaces

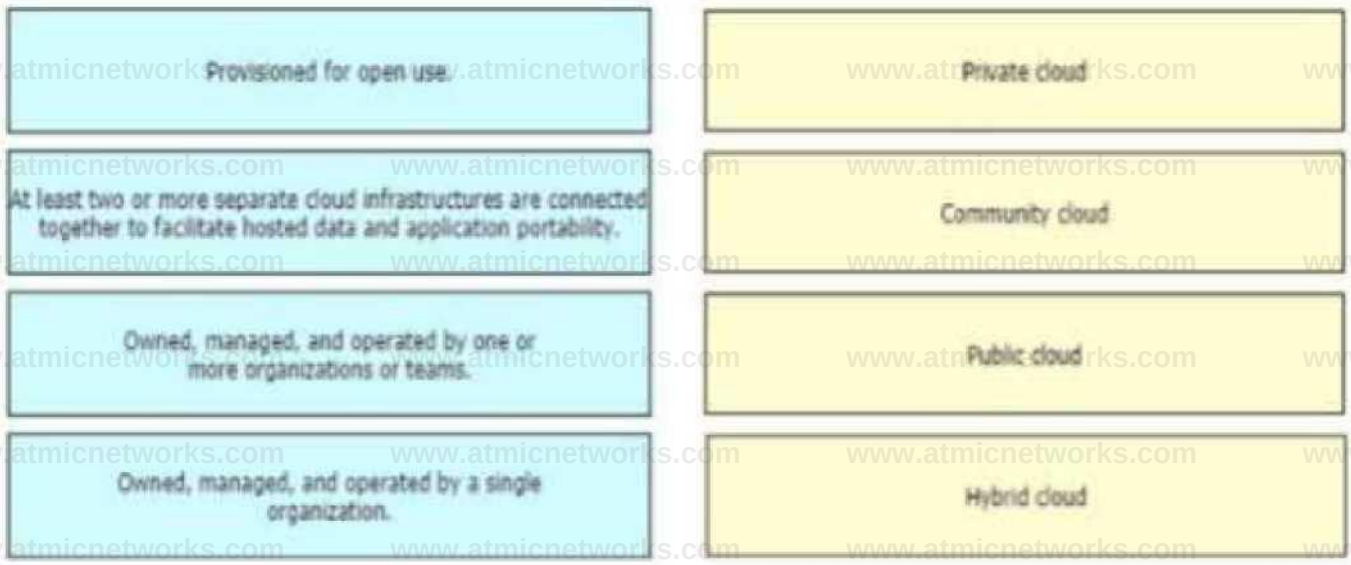
Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x) - Configuring OSPF [Cisco Nexus 9000 Series Switches], Configuring OSPF, Configuring OSPF Passive Interfaces

Cisco Nexus 9000 Series NX-OS Unicast Routing Configuration Guide, Release 9.3(x) - Configuring OSPF [Cisco Nexus 9000 Series Switches], Configuring OSPF, Configuring OSPF Network Types

Question: 5

DRAG DROP

A network engineer is asked to describe the cloud infrastructure models from the perspective of their operation and access to resources. Drag and drop the descriptions from the left onto the appropriate.



Answer:

Explanation:

Private Cloud: owned, managed, and operated by a single organization.

Community Cloud: Owned, managed, and operated by one or more organizations or teams.

Public Cloud: Provisioned for open use.

Hybrid Cloud: At least two or more separate cloud infrastructures are connected together to facilitate hosted data

and application portability.

Question: 6

An engineer needs to perform a backup of user roles and locales from Cisco UCS Manager to replicate the setting to a different fabric interconnect. The engineer wants to review the file before importing it to a target fabric interconnect. Which backup type must be selected to meet these requirements?

A. all configuration

B. system configuration

C. logical configuration

D. full state

Answer: C

Explanation:

A logical configuration backup is needed to back up user roles and locales from Cisco UCS Manager. This type of backup allows the engineer to replicate settings, including user roles and locales, to a different fabric interconnect. The file can be reviewed before importing it to the target fabric interconnect. Reference:

E. isco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager]], Backup and Restore Overview, Backup Types

F. isco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager]], Backup and Restore Overview, Logical Configuration Backup

Question: 7

An engineer must configure HTTPS secure management for Cisco UCS Manager using a key ring named kr2016 and a key size of 1024 bits. The environment consists of a primary fabric interconnect named UCS-A and a secondary fabric interconnect named UCS-B. Which command sequence must be used to accomplish this goal?

UC S-W scop* security
UCS-B security ft keyring kr2016

UCS-B secunty/keynng'ft set mod mod 1024
UCS-A 'security/keyring* ft commit-buffer

UC S-Aft scope security
UCS-A /security * create keyring kr2016
UCS-A /security/keyring' ft set modulus mod 1024
UCS-A 'security/keyring* ft commit-buffer

UC S-Bft scope security
UCS-B /security ft create keyring kr2016
UCS-B /security/keyring* ft set size modi024
UCS-A /security/keyring* ft commit-buffer

UC S-Aft scope security
UCS-A /security ft keyring name kr2016
UCS-A /security/keyring* ft set size 1024
UCS-A /security/keyring* ft commit-buffer

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A is the correct command sequence to configure HTTPS secure management for Cisco UCS Manager using a key ring named kr2016 and a key size of 1024 bits. The other options have incorrect commands or syntax errors. For example, option B uses the wrong command to set the modulus size, option C uses the wrong command to create the key ring, and option D uses the wrong command to name the key ring. Reference:

[Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Security [Cisco UCS Manager]], Configuring Security, Configuring Key Rings

[Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Security [Cisco UCS Manager]], Configuring Security, Configuring HTTPS Secure Management

[Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Security [Cisco UCS Manager]], Configuring Security, Configuring the Modulus Size for the Key Ring

Question: 8

Which server policy is used to install new Cisco IMC software on a server?

A. host firmware policy

B. hypervisor firmware policy

C. BIOS software policy

D. Cisco IMC software policy

Answer: D

Explanation:

Cisco IMC software policy is used to install new Cisco IMC software on a server. This policy allows the administrator to specify the desired Cisco IMC software version and the schedule for the installation.

The other policies are used to manage different aspects of the server firmware, such as the host firmware, the hypervisor firmware, and the BIOS software. Reference:

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Managing Firmware with Cisco UCS Manager [Cisco UCS Manager], Managing Firmware with Cisco UCS Manager, Cisco IMC Software Policy

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Managing Firmware with Cisco UCS Manager [Cisco UCS Manager], Managing Firmware with Cisco UCS Manager, Host Firmware Policy

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Managing Firmware with Cisco UCS Manager [Cisco UCS Manager], Managing Firmware with Cisco UCS Manager, Hypervisor Firmware Policy

Cisco UCS Manager Firmware Management Guide, Release 4.0 - Managing Firmware with Cisco UCS Manager [Cisco UCS Manager], Managing Firmware with Cisco UCS Manager, BIOS Software Policy

Question: 9

A network engineer must perform a backup and restore of the Cisco Nexus 5000 Series Switch configuration. The backup must be made to an external backup server. The only protocol permitted between the Cisco Nexus switch and the backup server is UDP. The backup must be used when the current working configuration of the switch gets corrupted. Which set of steps must be taken to meet these requirements?

A. 1 Perform a startup-config backup to an FTP server.

2 Copy startup-config in the boot flash to the running-config file

B. 1 Perform a running-config backup to an SFTP server

2 Copy backup-config from the SFTP server to the running-config file

C. 1 Perform a running-config backup to an SCP server

2 Copy running-config in the boot flash to the running-config file

D. 1 Perform a startup-config backup to a TFTP server

2 Copy backup-config from the backup server to the running-config file

Answer: D

Explanation:

Option D is the correct set of steps to perform a backup and restore of the Cisco Nexus 5000 Series Switch configuration using UDP as the only protocol. TFTP is a UDP-based protocol that can be used to transfer files between the switch and the backup server. The startup-config file contains the configuration that is applied when the switch boots up, while the running-config file contains the configuration that is currently active on the switch. To restore the configuration from the backup, the backup-config file needs to be copied from the backup server to the running-config file on the switch.

Reference:

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 7.x - Configuring File Systems, Directories, and Images [Cisco Nexus 5000 Series Switches], Configuring File Systems, Directories, and Images, Copying a Configuration File to a Remote Server

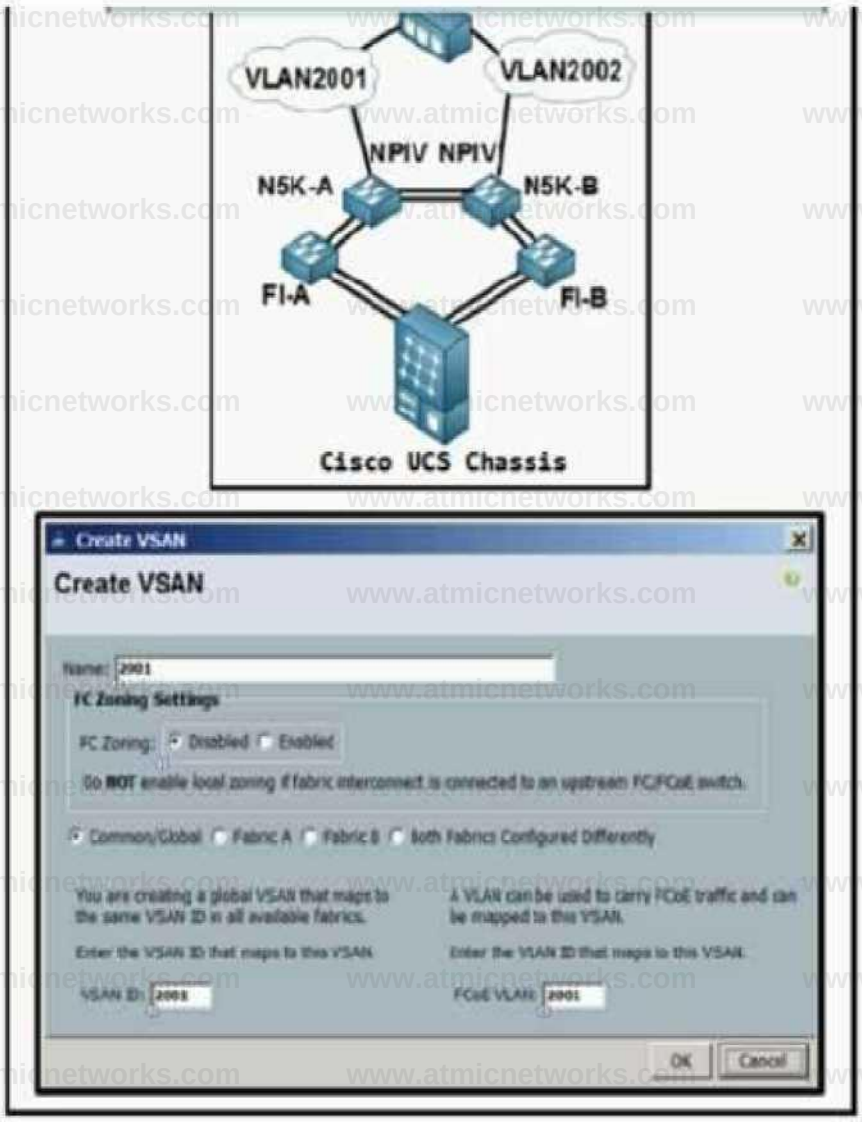
Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 7.x - Configuring File Systems, Directories, and Images [Cisco Nexus 5000 Series Switches], Configuring File Systems, Directories, and Images, Copying a Configuration File from a Remote Server

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 7.x - Configuring File Systems, Directories, and Images [Cisco Nexus 5000 Series Switches], Configuring File Systems, Directories, and Images, Copying the Running Configuration to the Startup Configuration

Cisco Nexus 5000 Series NX-OS System Management Configuration Guide, Release 7.x - Configuring File Systems, Directories, and Images [Cisco Nexus 5000 Series Switches], Configuring File Systems, Directories, and Images, Copying the Startup Configuration to the Running Configuration

Question: 10

Refer to the exhibit.



An engineer is configuring a VSAN on the network Which option must be selected to create the VSAN?

A. Fabric B

B. FC Zoning Enabled

C. Fabric A

D. Common/Global

Answer: C

Explanation:

To create a VSAN on the network, the engineer needs to select Fabric A from the drop-down menu. This will allow the engineer to assign a VSAN ID and a name to the new VSAN, and to add members to the VSAN. The other options are not relevant for creating a VSAN. Fabric B is the other fabric interconnect, FC Zoning Enabled is a feature that allows traffic isolation within a VSAN, and Common/Global is a default VSAN that cannot be modified. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring SAN Connectivity [Cisco UCS Manager], Configuring SAN Connectivity, Creating a VSAN

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring SAN Connectivity [Cisco UCS Manager], Configuring SAN Connectivity, Configuring FC Zoning

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring SAN Connectivity [Cisco UCS Manager], Configuring SAN Connectivity, Default VSANs

Question: 11

A customer wants to offload some of its order processing to a public cloud environment. The customer environment is based on Cisco ACI and uses Puppet with containenzed applications. The operations team requires a solution to orchestrate and optimize the cost of the new solution. Which product must be used to meet these requirements?

A. Cisco Intersight

B. Cisco Workload Optimization Manager

C. Cisco CloudCenter

D. Cisco Data Center Network Manager

Answer: C

Explanation:

Cisco CloudCenter is the best product to meet the requirements of the customer who wants to offload some of its order processing to a public cloud environment. Cisco CloudCenter allows the customer to deploy and manage applications in different cloud environments, including public cloud, while ensuring cost optimization and automation. Cisco CloudCenter also integrates with Cisco ACI and Puppet to provide consistent networking and configuration management across hybrid cloud deployments. The other products are not suitable for this scenario. Cisco Intersight is a cloud-based

management platform for Cisco UCS and HyperFlex systems, Cisco Workload Optimization Manager is a software solution that automates workload placement and scaling across private and public cloud environments, and Cisco Data Center Network Manager is a network management tool for Cisco Nexus and MDS switches. Reference:

Cisco CloudCenter Solution Overview - Cisco, Cisco CloudCenter Solution Overview

Cisco CloudCenter and Cisco ACI - Cisco, Cisco CloudCenter and Cisco ACI

Cisco CloudCenter and Puppet - Cisco, Cisco CloudCenter and Puppet

Cisco Intersight Overview - Cisco, Cisco Intersight Overview

[Cisco Workload Optimization Manager Overview - Cisco], Cisco Workload Optimization Manager Overview

[Cisco Data Center Network Manager Overview - Cisco], Cisco Data Center Network Manager Overview

Question: 12

A DNS server with IP address 192.168.1.1 is deployed in a data center A network engineer must configure a Cisco UCS Fabric Interconnect to use this DNS. Which configuration should be applied?

ficl-mgmt-Al scope system
ficl-mgmt-A /system * create dns 192.168.1.1
ficl-mgmt-A /system* * commit-buffer

ficl-mgmt-A* scope fabric-interconnect a
ficl-mgmt-A /fabric-interconnect« set name 192.168.1.1
ficl-mgmt-A /fabric-interconnect * scope system
ficl-mgmt-A /system * commit-buffer

ficl-mgmt-A* scope fabric-interconnect a
ficl-mgmt-A /fabric-interconnect * set name 192.168.1.1
ficl-mgmt-A /fabric-interconnect* * commit-buffer

ficl-mgmt-A* scope system
ficl-mgmt-A /system * scope services
ficl-mgmt-A /system/services * create dns 192.168.1.1
ficl-mgmt-A /system/services* * commit-buffer

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A is the correct configuration to use the DNS server with IP address 192.168.1.1 on a Cisco UCS Fabric Interconnect. The engineer needs to scope the system settings, create a DNS entry with the IP address, and commit the buffer. The other options have incorrect commands or syntax errors. For example, option B uses the wrong command to set the name of the fabric interconnect, option C uses the wrong command to create the DNS entry, and option D uses the wrong command to scope the system settings. Reference:

[Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring System Settings [Cisco UCS Manager]], Configuring System Settings, Configuring DNS

[Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring System Settings [Cisco UCS Manager]], Configuring System Settings, Configuring the Fabric Interconnect Name

Question: 13

What is a feature of NFS?

A. role-based access control

B. Kerberos-based security model

C. block-based file access

D. zone-based access control

Answer: B

Explanation:

NFS (Network File System) is a distributed file system protocol that allows users on client computers to access files over a network in a manner similar to how local storage is accessed. NFS uses a Kerberos-based security model to provide authentication, integrity, and confidentiality of dat

a. It ensures that unauthorized users do not have access and protects the data from eavesdropping and tampering as it moves across the network. The other options are not features of NFS. Role-based access control is a method of restricting access to resources based on the roles of users. Block-based file access is a type of storage access that transfers data in fixed-sized blocks. Zone-based access control is a feature of Fibre Channel SANs that allows traffic isolation within a VSAN. Reference:

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring NFS [Cisco Nexus 9000 Series Switches], Configuring NFS, NFS Overview

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring NFS [Cisco Nexus 9000 Series Switches], Configuring NFS, Configuring NFS Security

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring iSCSI [Cisco Nexus 9000 Series Switches], Configuring iSCSI, iSCSI Overview

Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, Release 9.3(x) - Configuring VSANs [Cisco Nexus 9000 Series Switches], Configuring VSANs, Configuring Zone-Based Access Control

Question: 14

Refer to the exhibit.

```
Enter the configuration method, (console/gux) ? console

Enter the setup mode; setup newly or restore from backup, (setup/restore) ?
restore

NOTE:
  To configure Fabric interconnect using a backup file on a remote server, you
will need to setup management interface.
           The management interface will be re-configured (if
necessary), based on information stored in the backup file

Continue to restore this Fabric interconnect from a backup file (yes/no) ? yes

Physical Switch MgmtO IPv4 address : 192.168.10.10
Physical Switch MgintO IPv4 netmask : 255.255.255.0
IPv4 address of the default gateway : 192.168.10.1
Enter the protocol to get backup file (scp/ftp/tftp/sftp) ? scp
```

```
Enter the IP address of backup server: 20.10.20.10
Enter fully qualified backup file name: Backup.bak
Enter user ID: user
Enter password:
  Retrieved backup configuration file.
Configuration file - Ok
```

Which type of backup is required to restore a Cisco UCS configuration?

A. system configuration

B. all configuration

C. logical configuration

D. full state

Answer: A

Explanation:

The exhibit shows a process of restoring the configuration of Cisco UCS using a backup file. In this context, the system configuration backup is required to restore the Cisco UCS configuration. The system configuration includes all setup information, policies, pools, templates, service profiles, VLANs/Fabric interconnect configurations etc., which are essential for the operational restoration of Cisco UCS. The other backup types are not suitable for this scenario. The all configuration backup includes the system configuration and the logical configuration, but it also includes the statistics and the faults, which are not needed for the restoration. The logical configuration backup includes the policies, pools, templates, and service profiles, but it does not include the setup information and the VLANs/Fabric interconnect configurations, which are also needed for the restoration. The full state backup includes the entire state of the system, including the firmware versions and the BIOS settings, but it is only used for disaster recovery, not for configuration restoration. Reference:

Cisco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager], Backup and Restore Overview, Backup Types

Cisco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager], Backup and Restore Overview, System Configuration Backup

Cisco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager], Backup and Restore Overview, All Configuration Backup

Cisco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager], Backup and Restore Overview, Logical Configuration Backup

Cisco UCS Manager Backup and Restore Management Guide, Release 4.0 - Backup and Restore Overview [Cisco UCS Manager], Backup and Restore Overview, Full State Backup

Question: 15

A network engineer must create an EEM script that saves a copy of the running configuration on bootflash and writes a message to syslog when a user saves the configuration to a Cisco Nexus

switch. Which configuration set should be applied to complete this task?

```
event manager applet local- backup
  event cli match "copy running-config startup-config"
  action 1 cli copy running-config bootflash:/current_config.txt
  action 2 syslog msg Configuration saved and copied to bootflash

event manager applet local- backup
  event cli match "write memory”
  action 1 cli copy running-config bootflash:/current_config.txt
  action 2 snmp-trap strdata "Configuration saved and copied to bootflash’’

event manager applet local- backup
  event cli match "copy running-config startup-config"
  action 1 cli copy running-config bootflash:/current_config.txt
  action 2 syslog msg Configuration saved and copied to bootflash
  action 3 event-default

event manager applet local- backup
  event cli match "write memory"
  action 1 cli copy running-config bootflash:/current_config.txt
  action 2 syslog msg Configuration saved and copied to bootflash
  action 3 event-default
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A is the correct configuration set to create an EEM script that saves a copy of the running configuration on bootflash and writes a message to syslog when a user saves the configuration to a Cisco Nexus switch. The EEM script uses the event manager applet command to define the applet name and the event that triggers the script. In this case, the event is the CLI pattern “copy runningconfig startup-config” which matches the command that a user would use to save the configuration. The action commands specify the commands that the script will execute when the event occurs. In this case, the script will copy the running configuration to bootflash, write a message to syslog, and exit. The other options have incorrect commands or syntax errors. For example, option B uses the wrong event keyword, option C uses the wrong action keyword, and option D uses the wrong file

name. Reference:

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring Embedded Event Manager [Cisco Nexus 9000 Series Switches], Configuring Embedded Event Manager, Configuring EEM Policies Using the CLI

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring Embedded Event Manager [Cisco Nexus 9000 Series Switches], Configuring Embedded Event Manager, Configuring EEM Event Statements

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring Embedded Event Manager [Cisco Nexus 9000 Series Switches], Configuring Embedded Event Manager, Configuring EEM Action Statements

Question: 16

Which adjacency server configuration makes two OTV edge devices located in the same site bring up the dual-site adjacency?

A)

Nexus-1:

interface Ethernetl/2 ip address 20.1.1.1/24

interface Overlav200
otv use-adjacency-server 20.1.1.2 unicast-only
otv join-interface Ethernetl/2

Nexus-2:

interface Ethernetl/2 ip address 20.1.1.2/24

interface Overlav200
otv use-adjacency-server 20.1.1.1 unicast-only
otv join-interface Ethernetl/2

B)

Nexus-1:

interface Ethernetl/2 ip address 20.1.1.1/24

interface Overlav200
otv adjacency-server unicast-only
otv join-interface Ethernetl/2

Nexus-2:

interface Ethernetl/2 ip address 20.1.1.2/24

interface Overlav200
oh join-interface Ethernetl/2
otv adjacency-server unicast-only
otv use-adjacency-server 20.1.1.1 unicast-only

C)

Nexus-1:

interface Ethernetl/2 ip address 20.1.1.1/24

interface Overlav200
otv adjacency-server unicast-only
otv join-interface Ethernetl/2

Nexus-2:

interface Ethernetl/2 ip address 20.1.1.2/24

intevrface Overlav200 oh' adjacency-server unicast-only oh' join-interface Ethernetl/2

D)

Nexus-1:

interface Ethernetl/2 ip address 20.1.1.1/24

interface Overlav200
otv adjacency-sen-er unicast-only
otv join-interface Ethernetl/2

Nexus-2:

interface Ethernetl/2 ip address 20.1.1.2/24

intevrface Overlav200 oh adjacency-server unicast-only oh' join-interface Ethernetl/2

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C is the correct adjacency server configuration to make two OTV edge devices located in the same site bring up the dual-site adjacency. The adjacency server is a logical entity that maintains the control plane information for the OTV overlay network. The adjacency server can be configured in unicast-only mode, which means that the OTV edge devices use unicast packets to exchange control plane information. To enable dual-site adjacency, which means that the OTV edge devices can form

adjacencies with devices in the same site as well as devices in different sites, the adjacency server must be configured with the same IP address on both devices in the same site. The other options have incorrect configurations or IP addresses. For example, option A uses different IP addresses for the adjacency server on the same site, option B uses the same IP address for the adjacency server on different sites, and option D uses an invalid IP address for the adjacency

server. Reference:

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 6.x - Configuring Basic OTV [Cisco Nexus 7000 Series Switches], Configuring Basic OTV, Configuring the OTV Adjacency Server

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 6.x - Configuring Basic OTV [Cisco Nexus 7000 Series Switches], Configuring Basic OTV, Configuring Dual-Site Adjacency

Cisco Nexus 7000 Series NX-OS OTV Configuration Guide, Release 6.x - Configuring Basic OTV [Cisco Nexus 7000 Series Switches], Configuring Basic OTV, Configuring the OTV Adjacency Server IP Address

Question: 17

An engineer must configure multiple EPGs on a single access port in a large Cisco ACI fabric without using VMM integration. The relevant access policies and tenant policies have been created. A single AAEP is used to configure the access port in the fabric. Which two additional steps must be taken to complete the configuration? (Choose two.)

A. A contract must be defined between the EPGs

B. The EPGs must be linked to the correct physical domain

C. The EPGs must link directly to the corresponding AAEP

D. The corresponding bridge domains must be configured in legacy mode

E. The EPGs must be configured as static ports

Answer: B, E

Explanation:

To configure multiple EPGs on a single access port in a large Cisco ACI fabric without using VMM integration, the EPGs must be linked to the correct physical domain (Option B) and configured as static ports (Option E). The physical domain is associated with VLAN namespaces and determines the VLAN encapsulation at the interface level. The static ports are used to manually assign the EPGs to the access port. The other options are not required for this configuration. A contract is used to define the communication policy between EPGs, but it is not necessary to create one for this scenario. The EPGs do not link directly to the AAEP, but rather to the interface policy group that is associated with the AAEP. The bridge domains do not need to be configured in legacy mode, which is a mode that allows communication with non-ACI networks. Reference:

Cisco Application Centric Infrastructure Fundamentals, Release 4.x - Endpoint Groups (EPGs) [Cisco Application Centric Infrastructure], Endpoint Groups (EPGs), Physical Domain

Cisco Application Centric Infrastructure Fundamentals, Release 4.x - Endpoint Groups (EPGs) [Cisco Application Centric Infrastructure], Endpoint Groups (EPGs), Static Ports

Cisco Application Centric Infrastructure Fundamentals, Release 4.x - Endpoint Groups (EPGs) [Cisco Application Centric Infrastructure], Endpoint Groups (EPGs), Contracts

Cisco Application Centric Infrastructure Fundamentals, Release 4.x - Endpoint Groups (EPGs) [Cisco Application Centric Infrastructure], Endpoint Groups (EPGs), Attachable Access Entity Profile

Cisco Application Centric Infrastructure Fundamentals, Release 4.x - Bridge Domains [Cisco Application Centric Infrastructure], Bridge Domains, Legacy Mode

Question: 18

A network engineer must configure a power redundancy policy on a Cisco UCS C-Series Rack Server. The power redundancy must support two power sources being used to power the server. Which configuration should be applied to meet the requirement?

```
server# scope org /
server /org # scope psu-policy
server /org psu-policy # set redundancy N+1
server/org psu-policy' # commit-buffer
```

```
server# scope org /
server /org # scope psu-policy
server /org/psu-policy # set psu-redundancy-policy gnd
server/org/psu-redundancy-policy* # commit-buffer
```

```
server# scope org /
server /org # scope psu-policy
server/org/psu-policy # set psu-redundancy-policy N+1
server/org/psu-redundancy-policy* # commit-buffer
```

```
server# scope org /
server/org # scope psu-policy
server/org/psu-policy # set redundancy grid
server/org/psu-policy' # commit-buffer
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C is the correct configuration to apply a power redundancy policy on a Cisco UCS C-Series Rack Server that supports two power sources. The power redundancy policy determines how the server uses the available power supplies to optimize power usage. The grid option means that the server uses power from both power supplies simultaneously. If one power supply fails, the server continues to operate with the remaining power supply. The other options are not suitable for this requirement. The n+1 option means that the server uses one fewer power supply than the number of power supplies that are installed. If a power supply fails, the server uses the extra power supply. The non-redundant option means that the server uses only one power supply, regardless of the number of power supplies that are installed. If the power supply fails, the server shuts down. The ps- redundant option means that the server uses power from the most efficient power supply. If the power supply fails, the server switches to another power supply. Reference: Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 4.0 - Configuring Server Power [Cisco Integrated Management Controller], Configuring Server Power, Configuring the Power Policy Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 4.0 - Configuring Server Power [Cisco Integrated Management Controller], Configuring Server Power, Power Redundancy Modes

Question: 19

Refer to the exhibit.

```
MDSSWITCH# config terminal
MDSSWITCH(config)# fcip profile 1
MDSSWITCH(config-profile)# ip address 192.0.1.10
MDSSWITCH(config-profile)# port 5000
MDSSWITCH(config-profile)# tcp max-bandwidth-mbps 5000
min-available-bandwidth-mbps 4000 round-trip-time-ms 1
MDSSWITCH(config-profile)# exit
MDSSWITCH(config)# interface fcip 1
MDSSWITCH(config-if)# use-profile 1
MDSSWITCH(config-if)# peer-info ipaddr 192.0.1.11
MDSSWITCH(config-if)# tcp-connections 1
MDSSWITCH(config-if)# ip-compression mode2
MDSSWITCH(config-if)# no shutdown
MDSSWITCH(config-if)# exit
MDSSWITCH(config)# interface ipStorage 1/1
MDSSWITCH(config-if)# ip address 192.0.1.10 255.255.255.0
MDSSWITCH(config-if)# switchport mtu 2500
MDSSWITCH(config-if)# no shutdown
MDSSWITCH(config-if)# end
```

An engineer configures FCIP on a Cisco MDS 9000 Series switch. What is the result of implementing the configuration?

A. The switch attempts to make two TCP connections

B. Compression is performed by using hardware

C. Mode2 is enabled by default.

D. Compression is performed by using software.

Answer: D

Explanation:

The configuration shown in the exhibit indicates that FCIP (Fibre Channel over IP) is configured with ip-compression mode2 enabled on a Cisco MDS 9000 Series switch. This means compression is performed by using software (Option D), as mode2 refers to software-based compression in FCIP configurations. The other options are not correct based on the configuration. The switch does not attempt to make two TCP connections, as there is no tcp-connections command in the configuration. Compression is not performed by using hardware, as mode1 refers to hardware-based compression in FCIP configurations. Mode2 is not enabled by default, as the default mode for FCIP compression is none. Reference:

Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide, Release 8.x - Configuring FCIP [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring FCIP, Configuring FCIP Compression

Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide, Release 8.x - Configuring FCIP [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring FCIP, Configuring the Number of TCP Connections for an FCIP Interface

Question: 20

Where is the witness deployed in a two-node Cisco HyperFlex Edge deployment?

A. to the HyperFlex Edge two-node cluster

B. to an additional server with network access to HyperFlex Edge

C. to a third-party cloud provider

D. to Cisco Intersight

Answer: D

Explanation:

In a two-node Cisco HyperFlex Edge deployment, the witness is deployed to Cisco Intersight. This cloud-based management platform provides intelligent insights and automation that scales with the business. It aids in managing all HyperFlex Edge deployments globally from a single cloud-based interface. Reference:

Cisco HyperFlex Edge Data Sheet - Cisco, Cisco HyperFlex Edge Data Sheet, Cisco HyperFlex Edge Deployment Options

Cisco HyperFlex Edge Installation Guide, Release 4.0 - Deploying HyperFlex Edge Clusters [Cisco HyperFlex HX Data Platform], Deploying HyperFlex Edge Clusters, Deploying a Two-Node HyperFlex Edge Cluster

Question: 21

Which storage protocol reduces file locks by using leasing?

A. CIFS

B. NFS 4

C. NFS 3

D. SMB

Answer: B

Explanation:

NFS 4 reduces file locks by using leasing, which is an improvement over the locking mechanisms used in previous versions of NFS like NFS 3 or CIFS/SMB. Leasing allows clients to cache file data locally, reducing the need for frequent and potentially costly network operations. Reference:

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring NFS

[Cisco Nexus 9000 Series Switches], Configuring NFS, NFS Overview

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring NFS [Cisco Nexus 9000 Series Switches], Configuring NFS, Configuring NFSv4 Leasing

Question: 22

Refer to the exhibit.

```
UCS-At scope eth-traffic-nor.
UCS-A /eth-traffic-mon $ scope fabric a
UCS-A /eth-traffic-mon/fabric # create eth-mon-session Monitor33
UCS-A /eth—traffic-mon/fabric/eth-mon-session/dest-interface* ♦ commit-buffer
UCS-A /eth-traffic-mon/fabric/eth-mon-session/dest-interface ♦
```

```
UCS-At scope service-profile org / serviceprofilel
UCS-A /org/service-profile ♦ scope vnic ethex-dynamic-prot-008
UCS-A /org/service-profile/vnic ♦ create mon-src Monitor23
UCS-A /org/service-profile/vnic/mon-src* ♦ commit-buffer
UCS-A /org/service-profile/vnic/mon-src I
```

```
UCS-Al scope eth-traffic-mon
UCS-A /eth-traffic-mon I scope fabric a
UCS-A /eth-traffic-mon/fabric ♦ scope eth-mon-session Monitors3
UCS-A /eth-traffic-mon/fabric/eth-mon-session ♦ enable
UCS-A /eth-traffic-mon/fabric/eth-mon-session* I commit-buffer
```

Service degradation is reported on a VM that is deployed on a Cisco UCS blade server. The traffic from the vNIC is required

to SPAN in both directions to a packet analyzer that is connected to UCS-A slot 2 port 12. Which two commands are needed to complete the configuration? (Choose two.)

A. UCS-A /org/service-profile/vnic/mon-src* # set direction both

B. UCS-A /eth-traffic-mon/fabric/eth-mon-session' # create dest-interface 2 12

C. UCS-A /org/service-profile/vnic/mon-src* # set direction receive transmit

D. UCS-A /eth-traffic-mon/fabric/eth-mon-session # activate

E. UCS-A /eth-traffic-mon/fabric/eth-mon-session* # create eth-mon-session/dest-interface 2 12

Answer: A, D

Explanation:

To SPAN traffic in both directions from a vNIC on a VM deployed on a Cisco UCS blade server to a packet analyzer connected to UCS-A slot 2 port 12, commands A and D are required. Command A sets the direction of traffic monitoring to both receive and transmit directions, while command D activates the Ethernet traffic monitoring session. The other commands are not needed or incorrect for this configuration. Command B uses the wrong syntax for creating the destination interface, command C uses the wrong keyword for setting the direction, and command E uses the wrong syntax for creating the Ethernet traffic monitoring session. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring Ethernet Traffic Monitoring [Cisco UCS Manager], Configuring Ethernet Traffic Monitoring, Configuring Ethernet Traffic Monitoring

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Ethernet Traffic Monitoring [Cisco UCS Manager], Configuring Ethernet Traffic Monitoring, Configuring Ethernet Traffic Monitoring

Question: 23

An engineer must build a lab replica of a Cisco UCS production environment. The file must be imported into a new Cisco UCS cluster using a Cisco UCS manager GUI. The file must be in XML format and be exported from Cisco UCS Manager using encrypted method. Which two configuration parameters should be selected to meet these requirements?. (Choose two.)

A. Type: Logical configuration

B. Protocol SCP

C. Type Full state

D. Protocol TFTP

E. Type All configuration

Answer: B, C

Explanation:

To meet the requirements of building a lab replica of a Cisco UCS production environment, the file must be exported in XML format using an encrypted method. Option B, Protocol SCP (Secure Copy Protocol), is used for securely transferring computer files between a local and a remote host or between two remote hosts. Option C, Type Full state, ensures that the complete configuration and state are included in the exported file. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Exporting the System Configuration

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Exporting the System Configuration

Question: 24

A new employee must be granted access to add VLANs into an existing Cisco UCS Manager and configure NTP synchronization with date and time zone settings. Which two privileges must be granted to the employee to complete the task? (Choose two.)

A. Service Profile Compute (Is-compute)

B. Ext LAN Config (ext-lan-security)

C. Service Profile Network Policy (Is-network-policy)

D. Service Profile Config (Is-config)

E. Ext LAN Policy (ext-lan-policy)

Answer: B, D

Explanation:

The new employee needs to add VLANs into an existing Cisco UCS Manager and configure NTP synchronization with date and time zone settings. Option B, Ext LAN Config (ext-lan-security), grants privileges to configure external LAN connectivity settings including VLANs. Option D, Service Profile Config (Is-config), allows for configuring service profiles including NTP synchronization settings. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring User Accounts and Organizations [Cisco UCS Manager], Configuring User Accounts and Organizations, Configuring Roles

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring User Accounts and Organizations [Cisco UCS Manager], Configuring User Accounts and Organizations, Configuring Roles

Question: 25

A Cisco MDS 9000 Series Switch is configured for SAN Analytics and SAN Telemetry Streaming. An engineer must enable analytics for NVMe on interfaces in the range of fc1/1-12. Due to a large amount of traffic generated in the SAN environment, the data must be collected at regular intervals of 60 seconds from ports fc 1-12 and then for ports fc13-24 for the next 60 seconds. Ports in the range fc4/13-14 were already enabled for analytics. Which set of commands must be used to meet these requirements?

```
interface fd/1-12
   port-sampling module 4 size 12 interval 60
   analytics nvme

interface fc1/1-12
   port-sampling module 4 size 12 interval 60000
   analytics type fc-scsi

analytics port-sampling module 4 size 12 interval 60000

interface fc1/1-12
   analytics fc-scsi
   analytics fc-nvme

analytics port-sampling module 4 size 12 interval 60

interface fc1/1-12
   analytics type fc-nvme
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

The commands under option A enable analytics for NVMe on interfaces in the range of fc1/1-12 with port-sampling module 4 size 12 interval 60 analytics nvme. This meets the requirement of collecting data at regular intervals of 60 seconds from ports fc1/1-12. Reference:

Cisco MDS 9000 Series NX-OS Interfaces Configuration Guide, Release 8.x - Configuring SAN Analytics and Telemetry Streaming [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring SAN Analytics and Telemetry Streaming, Configuring SAN Analytics

Cisco MDS 9000 Series NX-OS Interfaces Configuration Guide, Release 8.x - Configuring SAN Analytics and Telemetry Streaming [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring SAN Analytics and Telemetry Streaming, Configuring Port Sampling

Question: 26

Refer to Exhibit:

```
n9k2# guestshell
Cguestshell^guestshell ~]$ python
Python 2.7,5 (default, Jun 17 2014, 18:11:42)
[GCC 4.8.2 20140120 (Red Hat 4.8.2-16)] on linux2
Type "help", "copyright", "credits" or "license" for more information.
»>
```

An engineer must use the python module in the guest shell of the Cisco Nexus 9000 Series switch to shutdown port Ethernet 1/4 Which command set will accomplish this?

```
from cli import •
cli("conf tM)
cli("interface eth 1 /4”)
clif'shutdown")

from cli import *
cli(”conf t; interface eth1/4 ; shut")

from cisco import cli
cli("conf t; interface eth 1/4’*)
clif'shutdown")

from cisco import cli
clifconf t" ; ‘ interface eth1/4” ; "shut”)
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A is the correct command set to use the python module in the guest shell of the Cisco Nexus 9000 Series switch to shutdown port Ethernet 1/4. The commands import the cli module, which allows executing CLI commands from Python scripts, and then use the cli function to enter the configuration mode, specify the interface, and issue the shutdown command. Reference:

Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x) - Python [Cisco Nexus 9000 Series Switches], Python, Using the CLI Module

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring Interfaces

[Cisco Nexus 9000 Series Switches], Configuring Interfaces, Shutting Down and Restarting an

Interface

Question: 27

A Cisco UCS C-Series server is installed at a data center. The server should be managed by the Cisco UCS Manager by using a single cable for management and data traffic. Which configuration should be applied after the Physical connection is established?

A. UCS-A# scope server 1

UCS-A /server# scope cimc

UCS-A /server/cimc # scope mgmt-conn sideband

UCS-A /server/cimc # mgmt-conn-state enabled

UCS-A /server/cimc/mgmt-conn* # commit-buffer

B. UCS-A# scope chassis 1

UCS-A /chassis# scope cimc

UCS-A /chassis/cimc # scope mgmt-conn sideband

UCS-A /chassis/cimc/mgmt-conn # mgmt-conn-state enabled

UCS-A /chassis/cimc/mgmt-conn* # commit-buffer

C. UCS-A# scope chassis 1

UCS-A /chassis# scope cimc

UCS-A /chassis /cimc # set mgmt-conn-state enabled

UCS-A /chassis /cimc/mgmt-conn* # commit-buffer

D. UCS-A# scope server 1

UCS-A /server# scope cimc

UCS-A /server/cimc # scope mgmt-conn sideband

UCS-A /server/cimc/mgmt-conn #set mgmt-conn-state enabled

UCS-A /server/cimc/mgmt-conn* # commit-buffer

Answer: D

Explanation:

Option D is the correct configuration to enable the Cisco UCS Manager to manage a Cisco UCS C- Series server by using a single cable for management and data traffic. The commands enter the server scope, then the cimc scope, then the mgmt-conn scope with the sideband option, which enables the management connection through the sideband interface. Then, the mgmt-conn-state is set to enabled and the changes are committed to the buffer. Reference:

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Cisco UCS C-Series Servers [Cisco UCS Manager], Configuring Cisco UCS C-Series Servers, Configuring the Management Connection

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Cisco UCS C-Series Servers [Cisco UCS Manager], Configuring Cisco UCS C-Series Servers, Enabling the Management Connection Through the Sideband Interface

Question: 28

A network engineer needs to upgrade the EPLDs of the fabric modules for a Cisco MDS director-class switch. In which order are components reloaded during the process?

A. one fabric module at the time

B. all fabric modules followed by the entire switching platform

C. all fabric modules in parallel

D. one module and one supervisor at the time

Answer: A

Explanation:

Option A is the correct order of reloading components during the process of upgrading the EPLDs of the fabric modules for a Cisco MDS director-class switch. The EPLD upgrade is performed on one fabric module at a time, and the fabric module is reloaded after the upgrade. The other fabric modules and the switching platform are not reloaded during the process. Reference:

Cisco MDS 9000 Family NX-OS Upgrade and Downgrade Guide, Release 8.x - Upgrading the EPLDs [Cisco MDS 9000 NX-OS and SAN-OS Software], Upgrading the EPLDs, Upgrading the EPLDs on a Cisco MDS 9700 Series Switch

Cisco MDS 9000 Family NX-OS Upgrade and Downgrade Guide, Release 8.x - Upgrading the EPLDs [Cisco MDS 9000 NX-OS and SAN-OS Software], Upgrading the EPLDs, Guidelines and Limitations for Upgrading the EPLDs

Question: 29

DRAG DROP

An engineer must shut down the Ethernet 1/2 interface when the Ethernet 4/5 interface state is down. Drag and drop the CLI commands from the bottom onto the blanks in the exhibit to implement this EEM. Not all commands are used.

switch# configure terminal switch(config)# track. 1 switch(config-track)# end switch(config)# event manager applet track_4_5_doi switch(config-applet)# event track 1 state down switch(config-applet)# action 1 syslog msg EEM ap] track_4 5_down shutting down port et being hl/2 due to e1 down switch(config-applet)# action 2 cli conf term switch(config-applet)# action 3 cli switch(config-applet)# action 4 cli switch(config-applet)# end		m slet th4/5

interface ethemet 1/2 interface ethemet 4/5 no shut shut

Answer:

Explanation:

```
switch# configure terminal
switch(config)# track 1 interface ethernet 4/5
switch(config-track)# end

switch(config)# event manager applet track_4_5_down
switch(config-applet)# event track 1 state down
switch(config-applet)# action 1 syslog msg EEM applet
track_4_5_down shutting down port eth1/2 due to eth4/5
being down
switch(config-applet)# action 2 cli conf term
switch(config-applet)# action 3 cli interface ethernet 1/2
switch(config-applet)# action 4 cli shut
switch(config-applet)# end
```

Question: 30

APIC EPG Resolution Immediacy is set to "Immediate" Which statement is true about the Deployment Immediacy for VMM domains associated to EPGs?

A. The "Immediate" and "On demand" options require a port group to be created on the VDS.

B. If "On demand" is selected, the policy is programmed in the hardware only when the APIC detects a VM created in the EPG.

C. If “On demand” is selected the policy is programmed in the hardware only when the first packet is received through the data path.

D. If “immediate” is selected the policy is programmed in the hardware as soon as the leaf is booted.

Answer: D

Explanation:

Option D is the correct statement about the Deployment Immediacy for VMM domains associated to EPGs when the APIC EPG Resolution Immediacy is set to “Immediate”. This means that the policy is pushed to the hardware as soon as the leaf switch is booted, regardless of whether there are any VMs in the EPG or not. This ensures that the policy is ready to be enforced as soon as a VM is created or moved into the EPG. Reference:

Cisco APIC Basic Configuration Guide, Release 4.2(x) - Configuring VMM Domains [Cisco Application Policy Infrastructure Controller (APIC)], Configuring VMM Domains, Configuring the Deployment Immediacy for VMM Domains

Cisco APIC Basic Configuration Guide, Release 4.2(x) - Configuring VMM Domains [Cisco Application Policy Infrastructure Controller (APIC)], Configuring VMM Domains, Configuring the Resolution Immediacy for EPGs

Question: 31

Which statement describes monitoring Fibre Channel traffic on a Cisco UCS 6332 Fabric Interconnect?

A. Fibre Channel traffic is monitored only on one vHBA per server.

B. The destination port for monitoring must be an unassigned Fibre Channel port.

C. The monitoring of Fibre Channel traffic is limited to the default VSAN.

D. Fibre Channel traffic is capable to be monitored as it is encapsulated as FCoE.

Answer: D

Explanation:

Option D is the correct statement about monitoring Fibre Channel traffic on a Cisco UCS 6332 Fabric Interconnect. Fibre Channel traffic can be monitored even when it is encapsulated as FCoE (Fibre Channel over Ethernet) by using the SPAN (Switched Port Analyzer) feature. This allows network administrators to capture and analyze the Fibre Channel traffic flow and performance on any port or vHBA on the fabric interconnect. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring Fibre Channel Traffic Monitoring [Cisco UCS Manager], Configuring Fibre Channel Traffic Monitoring, Configuring Fibre Channel Traffic Monitoring

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Fibre Channel Traffic Monitoring [Cisco UCS Manager], Configuring Fibre Channel Traffic Monitoring, Configuring Fibre Channel Traffic Monitoring

Question: 32

Several production and development database servers exist in the same EPG and IP subnet. The IT security policy is to prevent connections between production and development. Which attribute must be used to assign the servers to different microsegments?

A. Data center

B. VMM domain

C. VM name

D. IP address

Answer: C

Explanation:
Option C is the correct attribute to use to assign the servers to different microsegments based on their VM names. By doing this, IT security can enforce policies that isolate production from development database servers existing in the same EPG and IP subnet. This can be achieved by using the microsegmentation feature of Cisco ACI, which allows granular control over the communication between endpoints within an EPG. Reference:

Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.2(x) - Microsegmentation [Cisco Application Policy Infrastructure Controller (APIC)], Microsegmentation, Microsegmentation Overview

Cisco APIC Layer 4 to Layer 7 Services Deployment Guide, Release 4.2(x) - Microsegmentation [Cisco Application Policy Infrastructure Controller (APIC)], Microsegmentation, Configuring Microsegmentation

Question: 33

A network engineer needs to configure system logging on the MDS switch. The messages must be displayed with the severity level of "warning" and above. For security reasons the users must be logged out of the console after 5 minutes of inactivity Which configuration must be applied to meet these requirements?

MDS-A|config)« logging consol* 5 MDS-A(config-consol*)d *x*c-tim*out 300

MDS-A(config)! line consol*
MDS-A(config<onsol*)# speed 38400
MDS-A|config-consolei# exec-timeout 5
MDS-A(config)! logging consol* 4

MDS-A(config)! consol*
MDS-A| config-consol*# speed 38400
MDS-A(config-console # session-limit 5
MDS-A(configi# logging consol* 5

MDS-A(config# logging line 4
MDS-A|config-console# session-limit 300

A. Option A
B. Option B
C. Option C
D. Option D

Answer: A

Explanation:

Option A is the correct configuration to meet the requirements of configuring system logging on the MDS switch. The commands set the console logging level to 5, which corresponds to the severity level of "warning" and above, and set the exec-timeout to 300 seconds, which means that the users will be logged out of the console after 5 minutes of inactivity.

The other options are either incorrect or incomplete for the task. Reference:

Cisco MDS 9000 Family NX-OS System Management Configuration Guide, Release 8.x - Configuring System Message Logging [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring System Message Logging, Configuring Console Logging

Cisco MDS 9000 Family NX-OS System Management Configuration Guide, Release 8.x - Configuring the Command-Line Interface [Cisco MDS 9000 NX-OS and SAN-OS Software], Configuring the Command-Line Interface, Configuring the CLI Timeout Value

Question: 34

A network administrator must configure an extra keyring in Cisco UCS Manager. The key must provide a high level of encryption and secure authentication when users use the web interface. Which configuration command set must be applied to meet these requirements?

E. set https keyring kring7984 set https cipher-suite-mode secure set https ssl-protocol tis1-2 commit-buffer

set https keyring kring7984 set https cipher-suite-mode secure set https tis-protocol tlsl-2 commit-buffer

set https keyring kring7984 set https cipher-suite-mode high set https ssl-protocol tls1-2# commit-buffer

set https keyring kring7984 set https cipher-suite-mode high set https tis-protocol tlsl-2 commit-buffer

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A is the correct command set to configure an extra keyring in Cisco UCS Manager. The commands create a keyring named “extra” with a modulus of 4096 bits, which provides a high level of encryption. The commands also generate a self-signed certificate for the keyring, which enables secure authentication when users use the web interface. Reference:

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Key Management [Cisco UCS Manager], Configuring Key Management, Configuring Key Rings

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Key Management [Cisco UCS Manager], Configuring Key Management, Configuring Certificates

Question: 35

An engineer needs to make an XML backup of Cisco UCS Manager The backup should be transferred using an authenticated and encrypted tunnel and it should contain all system and service profiles configuration Which command must be implemented to meet these requirements?

create file scp:/ userghost35 backups all-config9.bak all-configuration

copy startup-config scp:> user@host35'backups all-config9 bak all-configuration

create jackup scp:'.userghost35'backupsall-config9.bak all*configuration

copy running-config scp usera,host35 backups all-config9 bak all-configuration

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C is the correct command to make an XML backup of Cisco UCS Manager. The command creates a backup file named “all-config9.bak” that contains all system and service profiles configuration. The command also specifies the protocol as SCP (Secure Copy Protocol), which transfers the backup file using an authenticated and encrypted tunnel.

Reference:

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Exporting the System Configuration

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Exporting

the System Configuration Using SCP

Question: 36

DRAG DROP

An engineer is implementing NetFlow on a Cisco Nexus 7000 Series Switch. Drag and drop the NetFlow commands from the left into the correct order they must be entered on the right.

NK-I (config)# interface <interface> N7K-l(config-if> ip flow monitor NetflowMonitor input	Step 1
N7K-1 (config)# feature netflow	Step 2
N7K-l(config>## flow exporter NetflowMonitor N7K4(config)# flow record NetflowMonitor	Step 3
N"K4 (contig)# flow monitor NetflowMonitor	Step 4

Answer:

Explanation:

1- feature netflow

2- flow exporter

3- flow monitor

4- interface<interface>

Question: 37

An engineer is configuring a backup operation on the existing Cisco UCS environment using a logical configuration. Which configuration is expected to be saved by using this backup type?

A. systems

B. roles

C. service profiles

D. servers

Answer: C

Explanation:

Option C is the correct configuration that is expected to be saved by using a logical configuration backup. A logical configuration backup includes the service profiles, service profile templates, policies, pools, and logical LAN and SAN connectivity configuration. It does not include the systems, roles, or servers configuration, which are part of the full state or all configuration backups. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Backup Types

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Backing Up and Restoring the System Configuration [Cisco UCS Manager], Backing Up and Restoring the System Configuration, Backup Types

Question: 38

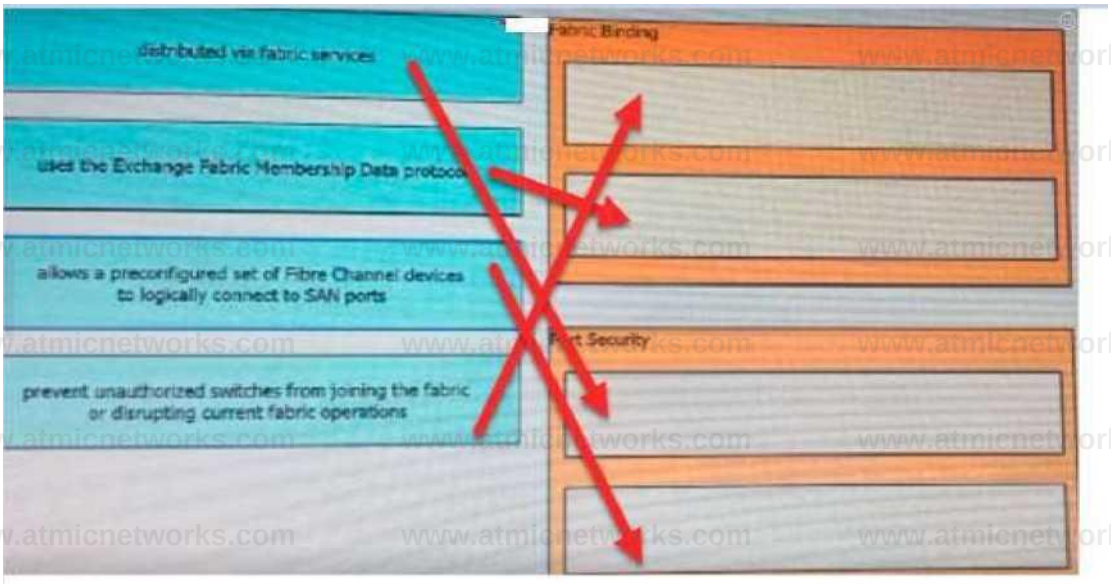
DRAG DROP

An engineer is implementing security on the Cisco MDS 9000 switch. Drag drop the descriptions from the left onto the correct security features on the right.

can be distributed via fabric services	Fabric Binding
uses the Exchange Fabric Membership Data protocol	Target 1
allows a preconfigured set of Fibre Channel des ices to logically connect to SAN ports	Target!
pres ent unauthorized switches front joining the fabric or disrupting current fabric operations	Port Security
	Target 3
	Target 4

Answer:

Explanation:



Reference: https://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/

san_switching/7x/b_5500_SAN_Switching_Config_7x_chapter_010010.html#con_1170967

Question: 39

Which two components should be checked when a Cisco Nexus 9000 Series Switch fails to boot using POAP? (Choose two.)

A. image noted in the script file against switch bootflash

B. DHCP server to bootstrap IP information

C. script signed with security key

D. TFTP server that contains the configuration script

E. POAP feature license

Answer: B, D

Explanation:

Options B and D are the correct components that should be checked when a Cisco Nexus 9000 Series Switch fails to boot using POAP (Power On Auto Provisioning). POAP requires a DHCP server to bootstrap IP information for the switch, and a TFTP server that contains the configuration script and the image file for the switch. The other options are either irrelevant or incorrect for POAP. Reference:

Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x) - Configuring Power On Auto Provisioning [Cisco Nexus 9000 Series Switches], Configuring Power On Auto Provisioning, POAP Overview

Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, Release 9.3(x) - Configuring Power On Auto Provisioning [Cisco Nexus 9000 Series Switches], Configuring Power On Auto Provisioning, POAP Process

Question: 40

Which two firmware packages are included in the Cisco UCS C-Series Rack-Mount UCS-Managed Server Software bundle? (Choose two.)

A. system

B. third-party

C. PSU

D. CIMC

E. BIOS

Answer: D, E

Explanation:

Options D and E are the correct firmware packages that are included in the Cisco UCS C-Series RackMount UCS-Managed Server Software bundle. The bundle contains the firmware for the CIMC (Cisco Integrated Management Controller) and the BIOS (Basic Input/Output System) of the server. The other options are either not part of the bundle or not applicable for the server. Reference:

Cisco UCS C-Series Rack-Mount Server Software and Firmware Compatibility Matrix for Cisco UCS Manager, Release 4.0 [Cisco UCS Manager], Cisco UCS C-Series Rack-Mount Server Software and Firmware Compatibility Matrix for Cisco UCS Manager, Release 4.0, Cisco UCS C-Series Rack-Mount UCS-Managed Server Software Bundle

Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.0 [Cisco Integrated Management Controller], Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.0, Firmware Management

Question: 41

An engineer performs a set of configuration changes for the vPC domain using Session Manager. Which two commands are used to verify the configuration and apply the device changes when no errors are returned? (Choose two)

A. write

B. verify

C. commit

D. checkpoint

E. apply

Answer: C, E

Explanation:

Option C and E are the correct commands to verify the configuration and apply the device changes when no errors are returned using Session Manager. The verify command checks the syntax and validity of the configuration commands, and the apply command applies the configuration changes to the device. The other options are either not related to Session Manager or not required for the task. Reference:

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring Session Manager

[Cisco Nexus 9000 Series Switches], Configuring Session Manager, Using Session Manager

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring Session Manager
[Cisco Nexus 9000 Series Switches], Configuring Session Manager, Session Manager Commands

Question: 42

What are two requirements when planning a Cisco HyperFlex All Flash standard cluster installation using three HX240c M5 servers? (Choose Two)

A. If the Jumbo MTU option in the HyperFlex installer is enabled, then jumbo frames do not have to be enabled on the upstream switches.

B. The hypervisors must be installed to Cisco FlexFlash SD cards.

C. If the Jumbo MTU option in the HyperFlex installer is enabled, then jumbo frames must also be enabled on the upstream switches.

D. The cluster deployment type must support a mix of HDD and SSD.

E. The servers must be discovered, unassociated, and connected to each fabric interconnect.

Answer: C, E

Explanation:

Option C and E are the correct requirements when planning a Cisco HyperFlex All Flash standard cluster installation using three HX240c M5 servers. Option C states that if the Jumbo MTU option in the HyperFlex installer is enabled, then jumbo frames must also be enabled on the upstream switches, which is true for optimal performance and compatibility. Option E states that the servers must be discovered, unassociated, and connected to each fabric interconnect, which is also true for the cluster installation process. The other options are either false or not applicable for the scenario. Reference:

Cisco HyperFlex Systems Installation Guide for Cisco Intersight, Release 4.0 - Cisco HyperFlex Cluster Installation with Cisco Intersight [Cisco HyperFlex HX Data Platform], Cisco HyperFlex Cluster Installation with Cisco Intersight, Before You Begin

Cisco HyperFlex Systems Installation Guide for Cisco Intersight, Release 4.0 - Cisco HyperFlex Cluster Installation with Cisco Intersight [Cisco HyperFlex HX Data Platform], Cisco HyperFlex Cluster Installation with Cisco Intersight, Install a Cisco HyperFlex Cluster

https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoft ware/

AdminGuide/3_5/

b_HyperFlexSystems_AdministrationGuide_3_5/b_HyperFlexSystems_AdministrationGuide_3_5_chapter_01111.html

Question: 43

An engineer must implement a Cisco UCS system at a customer site. One of the requirements is to implement SAN boot. The storage system maps the source WWPN to a unique LUN. Which method does Cisco recommend to configure the SAN boot?

A. Create a SAN boot policy in which every initiator is mapped to the same target LUN.

B. Define the vHBAs as bootable and leave the default values on the target definition.

C. Define the vHBAs as bootable and leave the boot target definition empty.

D. Create a SAN boot policy in which every initiator is mapped to a different target LUN.

Answer: D

Explanation:

Option D is the recommended method to configure the SAN boot when the storage system maps the source WWPN to a unique LUN. This method creates a SAN boot policy in which every initiator is mapped to a different target LUN, which ensures that each server boots from its own LUN and avoids any conflicts or errors. The other options are either incorrect or incomplete for the task. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring SAN Boot [Cisco UCS Manager], Configuring SAN Boot, Configuring SAN Boot

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring SAN Boot [Cisco UCS Manager], Configuring SAN Boot, Configuring SAN Boot

Question: 44

An engineer creates a service profile in Cisco UCS Manager and must assign a policy that reboots blades when changes are applied. The changes must be applied only after user acknowledgment. Which two policies must be configured to

meet these requirements? (Choose two.)

A. Boot Policy

B. Global Policy

C. Power Control Policy

D. Maintenance Policy

E. Reboot Policy

Answer: D, C

Explanation:

Option D and C are the correct policies that must be configured to meet the requirements. A Maintenance Policy specifies how the changes are applied when a service profile is associated or disassociated with a server or when an updated service profile is applied to a server. A Power Control Policy allows users to select how Cisco UCS Manager should restore power to the servers in a chassis after the chassis loses power. Reference:

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring Maintenance Policies [Cisco UCS Manager], Configuring Maintenance Policies, Configuring Maintenance Policies

Cisco UCS Manager GUI Configuration Guide, Release 4.0 - Configuring Power Control Policies [Cisco UCS Manager], Configuring Power Control Policies, Configuring Power Control Policies

Question: 45

A customer data center is configured for distribution of user roles, call home, and NTP. The data center was split into two geographically separate locations called DC1 and DC2. The requirement is for the user role configurations to be distributed in DC1 and for NTP and call home features to be constrained to DC2. Which two configuration sets must be used to meet these requirements? (Choose two.)

A.

I On Data Center 1 **configure terminal cfs 1 roles aaa**

I On Data Center 1 **configure terminal cfs region 1 ntp callhome**

I On Data Center 1 **configure terminal cfs 1 ntp callhome**

c I On Data Center 2 **configure terminal cfs region 2 roles**

E.

! On Data Center 2 **configure terminal cfs 2 roles aaa**

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: B, E

Explanation:

Option B and E are the correct configuration sets that must be used to meet the requirements.

Option B enables the user role distribution in DC1 by setting the role distribution policy to enabled and the role distribution scope to global. Option E constrains the NTP and call home features to DC2 by setting the NTP and call home policies to local and assigning them to the DC2 fabric interconnects. Reference:

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring User Role Distribution [Cisco UCS Manager], Configuring User Role Distribution, Configuring User Role Distribution

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring NTP [Cisco UCS Manager], Configuring NTP, Configuring NTP

Cisco UCS Manager CLI Configuration Guide, Release 4.0 - Configuring Call Home [Cisco UCS Manager], Configuring Call Home, Configuring Call Home

Question: 46

Refer to the exhibit.

```
■nt,sl com flour* tenlul
■CXUBt locator-led tai 100
MXXCSIccnfig)I feature fax
UTOi(coatis I fas 100
MXXCflean!ig-f«x|I type X22J21M
NtXOI (coat i fl-fail* aerial JAnimgiA
MXW(CMfifl)I inUtface etharaet 1/24 12
KTX73|can f i g -1 f | I sw 1tofapor t
MIXV31 con C i J lll I ewltcAport node fe* fabric
M1XUBleantxg-ifJI fax associate 100
KIXV1leantifl*if)I no shutdown

KXXfS I show fax 100 detail
HIX 100 Description HUO 100 alate. Online HLM V«»IM> SOIJINKII (switch VMXM> s.oiiiMliin ra 1 atari® varaion: 4 0(2)111(0 205) Mrtok Intatin varaloh: 5,0(2)N1 (0,205)
  extender Wxlel: M9K-C22121W, Extender Serial: J%rl<27BQLC cart Ho; 7)-1 Jan oi
  Card Id. IM, Mac Addr ««:«(:bd;02.2ai42, Nun Mao. (4 Module Sv Gen 21 (Switch Sv Gear 211 post level: couplets
pnmlag cede static Has-Unis. 1
  Fabric port for control traffic: Bthl/29 Fabric Intwtfsca state.
    Bthl/2^ -      Interface   lip.   State*    Active
    ttM/2*         XBtexUoe    <p     State     Active
    Bthl/2?        Interface   up     State:    Active
    Bthl/26        Interface   up     State     Active
    Ctbl/29        Interface   Up.    State.    Active
    it th 1/10 -    later face  Up.    State:    Active
    Sthl/31        Interface   Up     state:    Active
    Bthl/32        later fa#*  up.    State     Active
```

An engineer must distribute all the host ports to use all eight configured FEX uplinks. The solution must minimize disruption if an uplink fails Which action accomplishes this objective?

A. Set the pinning max-links value to 8

B. Statically assign each host interface to a fabric uplink

C. Change the supported FEX type

D. Configure the eight uplinks in a port channel

Answer: A

Explanation:

Option A is the correct action that accomplishes the objective. Setting the pinning max-links value to 8 ensures that all host ports are distributed across all eight configured FEX uplinks, providing optimal bandwidth utilization and redundancy. If an uplink fails, this configuration minimizes disruption by automatically redistributing host ports among the remaining active uplinks. Reference:

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring Fabric Extenders [Cisco Nexus 9000 Series Switches], Configuring Fabric Extenders, Configuring Fabric Extender Pinning

Cisco Nexus 9000 Series NX-OS Interfaces Configuration Guide, Release 9.3(x) - Configuring Fabric Extenders [Cisco Nexus 9000 Series Switches], Configuring Fabric Extenders, Configuring Fabric Extender Pinning Max-Links

Question: 47

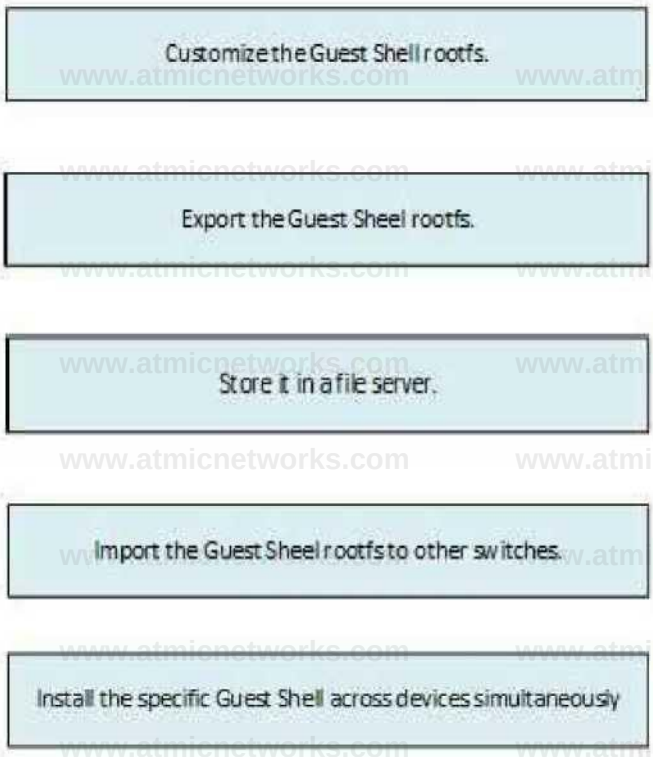
DRAG DROP

An engineer deploys a custom Guest Shell rootfs on a Nexus 9000 Series Switch. Drag and drop the steps from the left into the order required to deploy the solution on the right. Not all options are used.

Customize the guest shell rootfs.	Step 1
Export the Guest Shell rootfs.	Step 2
Store it in a file server.	Step 3
Import the Guest Shell rootfs to other switches.	Step 4
Install the specific Guest Shell across devices simultaneously.	Step 5

Answer:

Explanation:



https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/progammability/g uide/b-cisco-nexus-9000-series-nx-os-programmability-guide-93x/b-cisco-nexus-9000-series-nx-os- programmability-guide-93x_chapter_0100.html

Replicating the Guest Shell

Question: 48

A customer has a requirement for an automation solution that supports periodically acquiring configuration from a centralized server and aligning UCS servers to their desired state. Which opensource tool meets these requirements?

A. SaltStack

B. Terraform

C. Puppet

D. Kubemetes

Answer: C

Explanation:

Option C is the correct answer. Puppet is an open-source software configuration management tool that is used for deploying, configuring, and managing servers. It allows for the centralized management of various system configurations and aligns UCS servers to their desired state by periodically acquiring configurations from a centralized server. Reference:

Cisco Data Center Core Technologies, Module 5: Data Center Automation and Orchestration, Lesson 5.1: Describe Automation and Orchestration Concepts, Topic 5.1.1: Configuration Management Tools

Cisco Data Center Core Technologies, Module 5: Data Center Automation and Orchestration, Lesson 5.2: Implement Automation and Orchestration, Topic 5.2.2: Implement Puppet

Question: 49

An engineer is implementing Cisco Intersight in a secure environment. The environment must use LDAP directory service and ensure information integrity and confidentiality. Which two steps must be taken to implement the solution? (Choose two.)

A. Enable Encryption for LDAP

B. Add a self-signed LDAP certificate to Cisco Intersight.

C. Enable Certificate Signing Request in Cisco Intersight.

D. Add a trusted root LDAP certificate to Cisco Intersight

E. Add a trusted OAuth token to Cisco Intersight

Answer: A, D

Explanation:

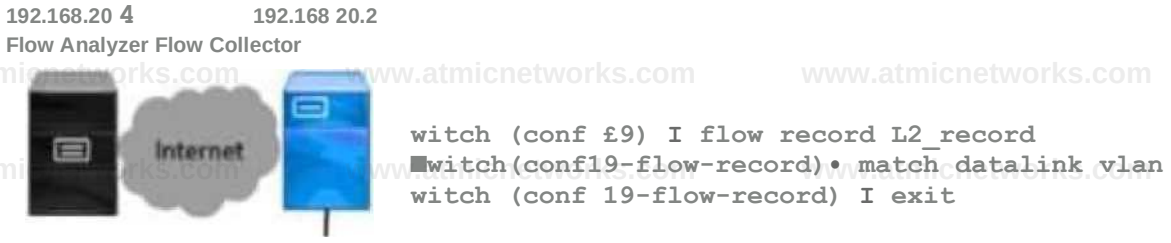
Option A and D are the correct steps to implement the solution. Enabling encryption for LDAP ensures information integrity and confidentiality during data transmission between systems. Adding a trusted root LDAP certificate to Cisco Intersight establishes a secure connection by validating the authenticity of the LDAP server. Reference:

Cisco Intersight User Guide, Release 1.0 - Configuring Cisco Intersight [Cisco Intersight], Configuring Cisco Intersight, Configuring LDAP Settings

Cisco Intersight User Guide, Release 1.0 - Configuring Cisco Intersight [Cisco Intersight], Configuring Cisco Intersight, Configuring Certificates

Question: 50

Refer to the exhibit.



Refer to the exhibit. VLAN 10 Is experiencing delays and packet drops when the traffic is forwarded through the switch.

The destination flow analyzer accepts traffic captures of not more than 30 seconds. Which configuration implements the traffic capture that meets the requirements?

swltch(config}9 How timeout 30000
switch(config}# Interface ethernet 1/1
swltch(config*if)# switchport
swltch(config-if)# switchport access vlan 10
switch(config.if)# ip flow monitor L2_monitor output

switch(config)# flow timeout 30
swltch(config}# Interface ethernet 1/1
swltch(config-if)# switchport
swltch(config*if|# switchport access vlan 10
switch(config-if)# mac packet classify
switch(config-if)# layer2*switched flow monitor L2_monitor input

swltch(config)# Interface ethernet 1/1
swltch(conflg*if)# flow timeout 30
swltch(config-if)# switchport access vlan 10
switch(config-if)# mac packet classify
swltch(config-if)# ip flow monitor L2_monitor Input

swltch(config)# Interface ethernet 1/1
swltch(config)# flow timeout 30000
switch(config-if)# switchport
swltch(config*if)# layer2-switched flow monitor L2_monitor output
switch(config.if)# switchport access vlan 10

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Option B is the correct configuration that implements the traffic capture that meets the requirements. The configuration sets the flow timeout to 30 seconds, which matches the destination flow analyzer's limit. The configuration also enables MAC packet classification and layer 2-switched flow monitoring on the interface ethernet 1/1, which belongs to VLAN 10. This allows the switch to capture the traffic from VLAN 10 and send it to the flow analyzer for troubleshooting.

Reference:

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring NetFlow [Cisco Nexus 9000 Series Switches], Configuring NetFlow, Configuring NetFlow

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x) - Configuring NetFlow [Cisco Nexus 9000 Series Switches], Configuring NetFlow, Configuring Layer 2- Switched NetFlow

Question: 51

Port security is statically configured on a Cisco Nexus 7700 Series switch and F3 line card. The switch is configured with an Advanced Services license. Which two actions delete secured MAC addresses from the interface? (Choose Two)

A. The address must be removed from the configuration.

B. The address must reach the age limit that is configured for the interface.

C. The interface must be converted to a routed port.

D. The device must be restarted manually.

E. Shutdown and then no shutdown must be run on the interface.

Answer: A, B

Explanation:

On a Cisco Nexus 7700 Series switch, secured MAC addresses can be removed by either manually deleting the address from the configuration or when the address ages out, which is determined by the age limit set for the interface. The other options do not apply to the deletion of secured MAC addresses.

Question: 52

A network engineer repeatedly saves a configuration on Catalyst switches to NVRAM using the write memory command.

What action should be taken to implement the same action on Nexus switches?

A. Use the write memory command to save the configuration.

B. Use the alias command to use the write memory command.

C. Use the exit command to leave the configuration mode and save the configuration automatically.

D. Use the wri command to use the copy running-config startup-config command.

Answer: D

Explanation:

On Nexus switches, the equivalent command to save the configuration to NVRAM is 'copy runningconfig startup-config'.

The 'write memory' command is specific to Catalyst switches and is not used on Nexus switches.

Reference:

https://community.cisco.com/t5/switching/write-command-on-nexus-switchs/td-p/1958386

Question: 53

Which data interchange format is presented in this output?

```
"totalCount" "l",
 imdata": [
   "fabricNode": {
      "attributes": {
         "address": "10.0 40.65".
         "apicType" "apic",
         "dn" "topology pod-1 node-201".
         "Id": "201",
         "I a st Sta teMod Ts": "2020-09-07T10:20:57.236*00:00" "modTs": "2020-O9-O7T10
         21:18.912*00:00",
         "model": "N9K-C9336PQ"
         "monPolDn": "uni'fabric monfab-default".
         "role": "spine",
         "serial": "FDO39106329J",
         "uld": "0".
         "vendor": "Cisco Systems. Inc".
```

1

A. XML

B. YAML

C. JSON

D. CSS

Answer: C

Explanation:

The data interchange format presented in the output is JSON (JavaScript Object Notation), which is commonly used for transmitting data in web applications and for configuration files. It is easily readable both by humans and machines.

For detailed explanations and references, it's best to consult the official Cisco documentation or the Cisco Data Center Core Technologies study guide.

Question: 54

Refer to the exhibit.

```
switch* (how tidlui-Hrvu Global RADIUS (harod secret ••••••• re transudes ion count 5 tlaeout value:10 following RADIUS servers are configured
ay radius elaeo users cat available for authentication on port.1*12 available for accounting on port 181J 172 22 81 37 available for authentication
on port 1812 available for accounting on port:181J RADIUS shared secret:•••••• 10.10.0.0:
                available for authentication on port 1812 available for accounting on port:101J RADIUS shared secret:

switch* show radius-server groups total nuaber of groups:4 following RADIUS server groups are configured group radius:
                server: all configured radius servers group Groupl-
                server: Server! on auth-port 1*12. acct-port 1*1 J server: Server! on auth-port 1812, acct-port 1813 group Group!
```

A network engineer requires remote access via SSH to a Cisco MDS 9000 Series Switch. The solution must support secure access using the local user database when the RADIUS servers are unreachable from the switches. Which command meets these requirements?

A. aaa authentication none

B. aaa authentication login default group radius

C. aaa authentication login default group local

D. aaa authentication login default fallback error local

Answer: D

Explanation:

The command 'aaa authentication login default fallback error local' is used to ensure that if RADIUS servers are unreachable, the system will fall back to using the local user database for SSH access to the Cisco MDS 9000 Series Switch.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guide s/security/nx-os/sec_cli_6-x/cradtac1.html

Question: 55

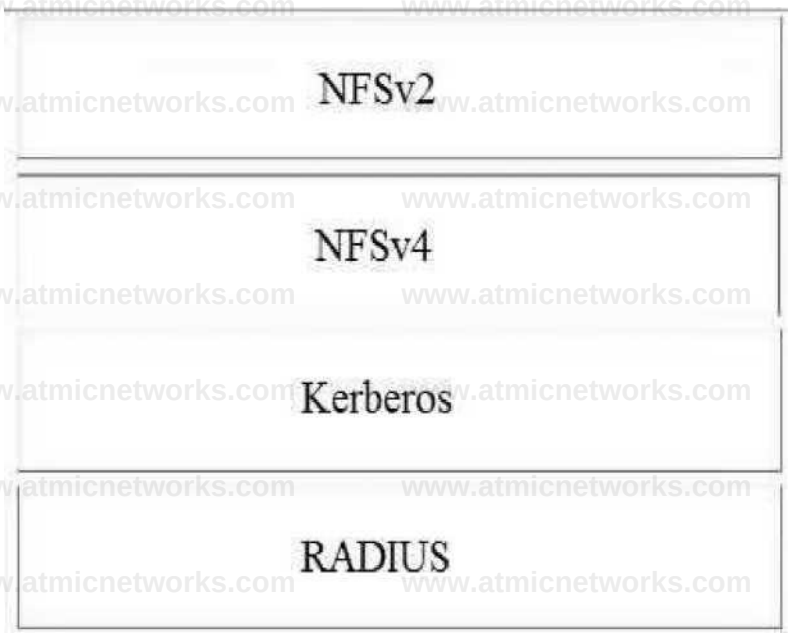
DRAG DROP

Drag and drop the storage technologies from the left onto the correct descriptions on the right.

NFSv2	uses client machine authentication
Kerberos	uses users authentication
NFSv4	authenticates clients and sewers in NFSv4
RADIUS	authenticates clients to corporate directory systems

Answer:

Explanation:

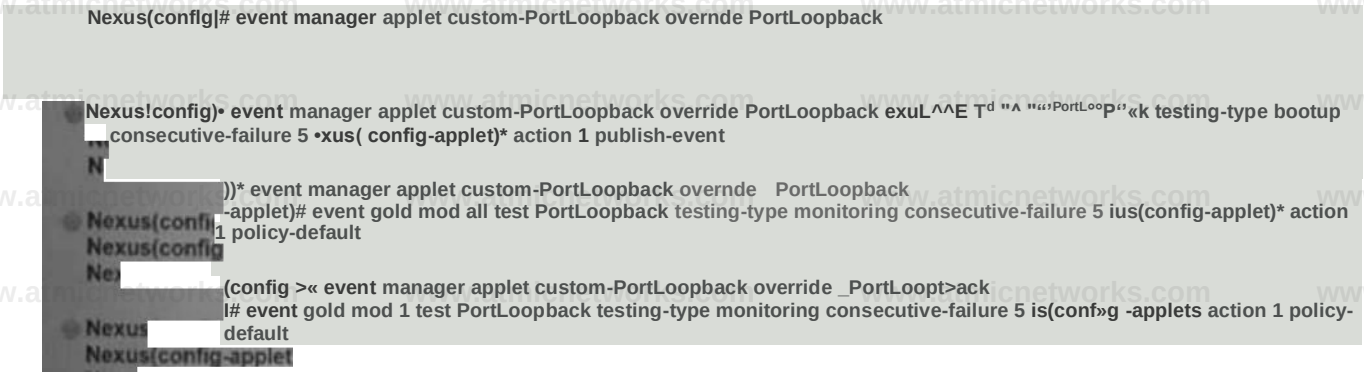


The release of NFSv4 brought a revolution to authentication and security to NFS exports. NFSv4 mandates the implementation of the RPCSEC_GSS kernel module, the Kerberos version 5 GSS-API mechanism, SPKM-3, and LIPKEY. With NFSv4, the mandatory security mechanisms are oriented towards authenticating individual users, and not client machines as used in NFSv2 and NFSv3.

https://web.mit.edu/rhel-doc/5/RHEL-5-manual/Deployment_Guide-en-US/s1-nfs-security.html

Question: 56

The Cisco Nexus switch Generic Online Diagnostics policy for a PortLoopback test requires 10 consecutive failures to error disable the port. The customer wants to change it to 5 consecutive failures. Which configuration applies the changes for module 1 only?



A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The configuration that applies the changes for module 1 only, setting the Generic Online Diagnostics policy for a PortLoopback test to error disable the port after 5 consecutive failures, would be Option C based on the provided options.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/system- management/guide/b_Cisco_Nexus_7000_Series_NX-OS_System_Management_Configuration_Guide-RI/configuring_online_diagnostics.html

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system- management/bcisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b-cisco-nexus-9000-seriesnx-os-system-management-configuration-guide-93x_chapter_011010.html

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKDCN-3234.pdf

Question: 57

An engineer must start a software upgrade on a Cisco Nexus 5000 Series Switch during a zone merge. What is the result of this action?

A. The zone merge stops.

B. The zone merge pauses until the upgrade completes

C. The upgrade stops

D. The zone merge executes and then the upgrade completes.

Answer: A

Explanation:

Starting a software upgrade on a Cisco Nexus 5000 Series Switch during a zone merge will result in the zone merge process stopping. This is to prevent any conflicts or issues that may arise from performing two significant operations simultaneously.

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/upgrade/602_N2_2/n5500_upgrade_downgrade_602_n2_2.html

Question: 58

An engineer must configure a Nexus 7000 series switch for HSRP on VLAN 100. When fully functional, the router must be the active master. Which set of commands must be used to implement the scenario?

```
feature harp interface vlanlOO
ip address 10.1 1 2 255 255 255 0
priority 120
hsrp version 2 hsrp 1000 ip 10.1.1.1
```

```
feature hsrp
interface vlanlOO ip address 10.1 1.2 255.255.255.0 priority 100
hsrp version 2
```

hsrp 1000 ip 10.1.1.1

feature-set hsrp interlace vlanlOO
ip address 10.1.1.2 255 255.255 0
priority 110
hsrp version 2
hsrp 1000 ip 10.1.1.1

feature-set hsrp
interlace vlanlOO ip address 10.1.1.2 255.255.255.0 priority 80
hsrp version 2
hsrp 1000 ip 10.1.1.1

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To configure HSRP on a Nexus 7000 series switch for VLAN 100 and ensure the router is the active master, you would typically use the hsrp command within the VLAN configuration mode, set the priority higher than the default to make it the preferred active router, and use the preempt command to allow the router to take over as the active router if it has a higher priority.

Reference:

https://www.google.com/search?q=hsrp+priority&oq=hsrp+priority&aqs=chrome..69i57j0l2j0i20i263i395j0i395l6.5307j1j4&sourceid=chrome&ie=UTF-8

Question: 59

An engineer is configuring a vHBA template in UCS Manager. The engineer needs to specify the logical addresses used by the vHBA and the path through which the SAN traffic flows. Which two resources must be specified in the vHBA template? (Choose two.)

A. MAC addresses

B. WWPNPool

C. WWNN

D. VLAN ID

E. Fabric ID

Answer: B, E

Explanation:

When configuring a vHBA template in UCS Manager, you need to specify the WWPN (World Wide Port Name) from a WWPN pool (B) to uniquely identify the port in the fabric, and the Fabric ID (E) to define the path through which the SAN traffic will flow.

https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-manager/whitepaper_c11-697337.html

Question: 60

Which data structure results from running this Python code?

```
>» import json
»> f = openffnamt.json', Y)
»> varl «json load(f)
```

```
»> varl
{nW: u'bdl', u'ap': (u'epgs* Ku'namt': u'app'}, {u'namt': u'web*). (u'name'
u'db')J. u'nama*: u'Onli nt Store'), u'name : u'39106329' u'pvn': u'pvnl}
```

A. Set

B. Tuple

C. Dictionary

D. List

Answer: C

Explanation:

he Python code provided suggests that it is reading a JSON file and storing its contents in a variable. JSON files are typically represented as dictionaries in Python, so the resulting data structure would be a Dictionary ©

Question: 61

An engineer needs to monitor ingress traffic that arrives at interface Ethernet 1/3 that belongs to a Cisco Nexus 5600 Series Switch. The traffic analyzer machine located at interface Ethernet 1/5 is already monitoring other production, and the traffic analyzer must not be impacted by the traffic captured from the interface Eth1/3. The operations team allocated a traffic budget for the new

monitoring session of 1 Gbps to meet this requirement Which set of commands configures the SPAN session?

```
interface Ethernet 1/3
  switchport monitor rate-limit 1G

monitor session 2
  destination interface ethernet 1/5
  source interface Eth 1/3

interface Ethernet 1/3 rx
   switchport mode SD
   switchport monitor rate-limit 1G
monitor session2
   destination interface ethernet 1/5

interface Ethernet 1/3
  monitor rate-limit 1G
  destination interface ethernet 1/5
  source interface rx

interface Ethernet 1/5
```

```
monitor session 2
destination interface tx

interface Ethernet 1/3
 monitor session 2
  destination interface ethernet 1/5
 source interface rx

interface Ethernet 1/5
 monitor rate-limit 1G
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To configure a SPAN session on a Cisco Nexus 5600 Series Switch that monitors ingress traffic on

interface Ethernet 1/3 without impacting the traffic analyzer on Ethernet 1/5, you would typically use the monitor session command to create a new session, specify the source interface with the source keyword, and the destination interface with the destination keyword. Additionally, you would apply a rate limit to the session to adhere to the traffic budget of 1 Gbps.

Q, Find Matches in This Book

	' bwiiuii^uiinyjH iiiieiiave ethernet *slot/port*	cincis Hiiciidbc cuiniyuiduuii uiuuc ıuı me spebiiicu Ethernet interface selected by the slot and port values.
Step 3	switch(config-if)# switchport monitor rate-limit 1G	Specifies that the rate limit is 1 Gbps.
Step 4	switch(config-if)# exit	Reverts to global configuration mode

Example

This example shows how to limit the bandwidth on Ethernet interfa

e 1/2 to 1 Gbps:

switch(config)# **interface ethernet 1/2**
switch(config-if)# **switchport monitor rate-limit 1G** witch(config-if)#

Configuring Source Ports

Procedure

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters global configuration mode.
Step 2	switch(config) # monitor session *session-number*	Enters monitor configuration mode for the specified monitoring session
Step 3	switch(config-monitor) # source interface *type slot/port* [rx | tx I both]	Adds an Ethernet SPAN source port and specifies the traffic direction in which to duplicate packets. You can enter a range of Ethernet, Fibre Channel, or virtual Fibre Channel ports. You can specify the traffic direction to duplicate as ingress (Rx), egrej^ (Tx), or both. By default, the direction is both. Q

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5600/sw/system_management/7x/

b_5600_System_Mgmt_Config_7x/configuring_span.html

Question: 62

What are two types of FC/FCoE oversubscription ratios? (Choose two.)

A. server storage to end-node count

B. port bandwidth to uplink bandwidth

C. edge ISL bandwidth to core ISL bandwidth

D. host bandwidth to storage bandwidth

E. switch processing power to end-node processing power

Answer: B, D

Explanation:

FC/FCoE oversubscription ratios refer to the relationship between the bandwidth provided and the bandwidth required. Common types of oversubscription ratios include port bandwidth to uplink bandwidth (B), which measures the bandwidth available at the access layer compared to the uplink, and host bandwidth to storage bandwidth (D), which relates to the bandwidth demand from servers compared to the available storage bandwidth.

https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/BRKDCN-1121.pdf

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/operations/n5k_fcoe ops.html

Question: 63

Due to a domain name change at a customer site, a Cisco UCS cluster must be renamed. An engineer must recommend a solution to ensure that the Cisco UCS Manager is available over HTTPS. Which action accomplishes this goal?

A. Reinstall the cluster to generate the default key ring certificate

B. Generate a new default key ring certificate from the Cisco UCS Manager

C. Reboot the SSO component of the Cisco UCS Manager

D. Regenerate the default key ring certificate manually

Answer: B

Explanation:

When there is a domain name change, and the Cisco UCS Manager needs to be available over HTTPS, generating a new default key ring certificate from the Cisco UCS Manager (B) is typically the recommended action. This ensures that the HTTPS service has a valid certificate that matches the new domain name.

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1_chapter_0110.html

The default key nng certificate must be manually regenerated if the cluster name changes or the certificate expires

Question: 64

An environment consists of a Cisco MDS 9000 Series Switch that uses port channels. An engineer must ensure that frames between the source and the destination follow the same links for a specific flow. Subsequent flows are allowed to use a different link Which load balancing method should be used to accomplish this goal?

A. src-id/dst-id

B. src-dst-oui

C. src-dst-port

D. src-id/dst-id/oxid

Answer: C

Explanation:

The src-dst-port load balancing method ensures that frames in the same flow (identified by the source and destination ports) follow the same links in a port channel. This method is effective in environments with Cisco MDS 9000 Series Switches because it maintains the order of frame delivery within a flow, which is crucial for storage traffic. Subsequent flows can use different links, allowing for efficient utilization of the port channel bandwidth. Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials.

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guide s/fabric/nx-os/nx_os_fabric/vsan.html?bookSearch=true

https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_1_x/1_3/san-os/configuration/guide/PortChnl.pdf

Question: 65

A customer needs a tool to take advantage of the CI/CD model to streamline its operation and optimize cost. The customer wants to integrate the solution with the cisco products it currently it currently uses, Including Cisco ACI networking and Cisco UCS servers. The solution should also provide on-premises Kubernetes and AppDynamics performance monitoring. Because of the security requirements, the solution not install a local client on products under management. which orchestration solution meets these requirements?

A. Cisco APIC

B. CISCO UCS director

C. Cisco DCNM

D. Cisco CloudCenter

Answer: D

Explanation:

Cisco CloudCenter is the appropriate orchestration solution for the customer's requirements. It supports the CI/CD model, which is essential for streamlining operations and optimizing costs. Cisco CloudCenter can integrate with Cisco ACI networking and Cisco UCS servers, providing a unified

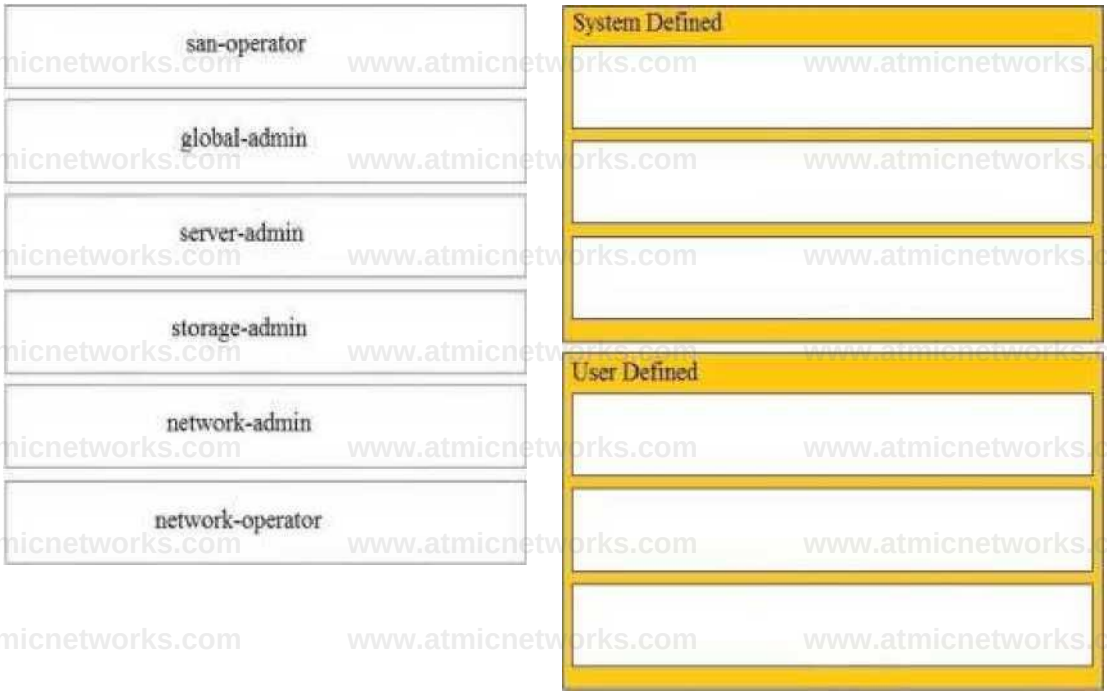
management platform. It also offers on-premises Kubernetes support and AppDynamics performance monitoring without the need to install local clients on managed products, aligning with the customer's security requirements.
Reference: Cisco CloudCenter documentation and Cisco Data Center Core Technologies study guide.

Question: 66

DRAG DROP

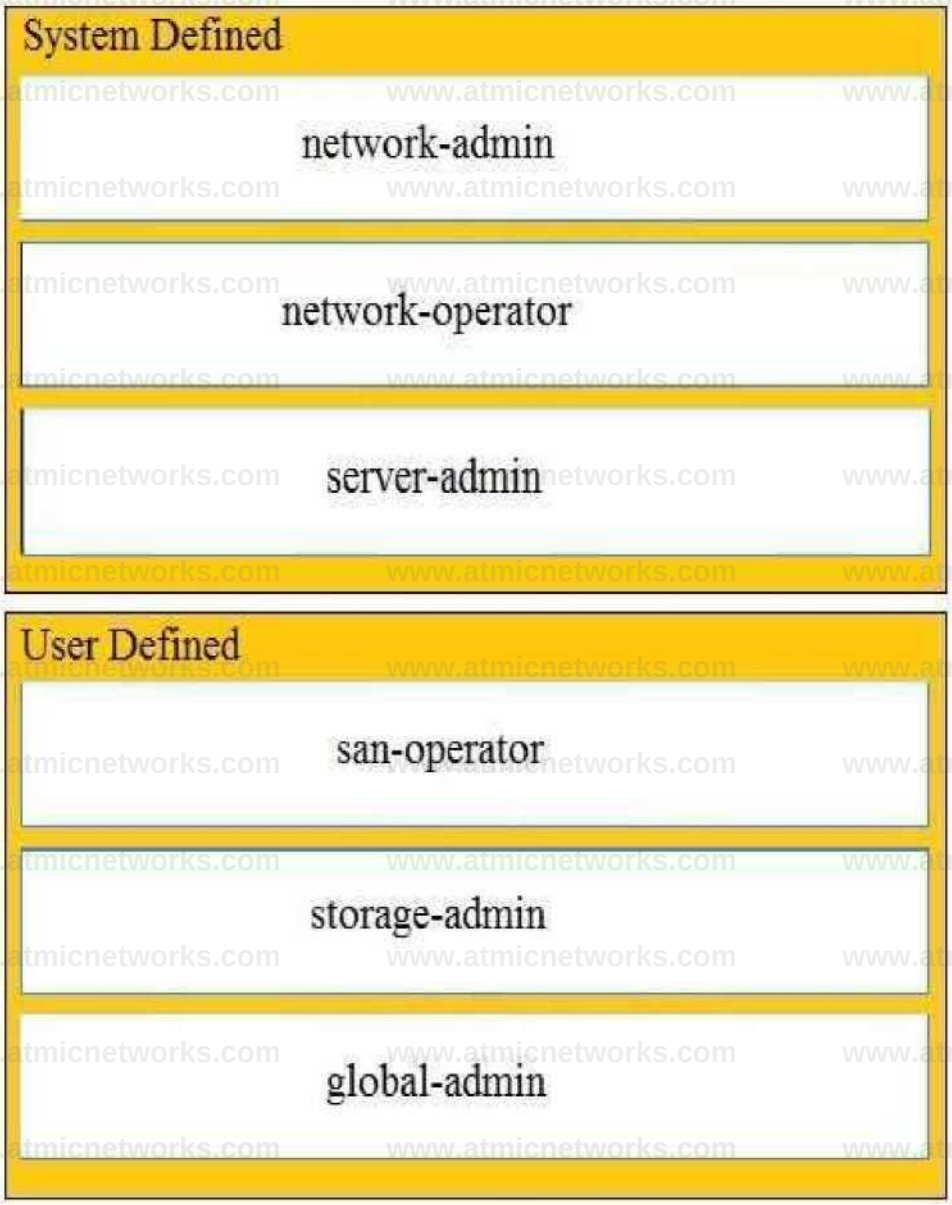
A network engineer must implement RBAC on Cisco MDS 9000 Series Multilayer Switches.

Drag and drop the Cisco MDS 9000 Series roles from the left onto the correct categories on the right.



Answer:

Explanation:



https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_UCSM_Admin_Mgmt_Guide_chapter_01.html

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/security/cisco_mds9000_security_config_guide_8x/configuring_users_and_common_roles.html#con_1422305

Question: 67

Which configuration generates a syslog message when CPU utilization is higher than 60%?

A. event manager applet HIGH-CPU

event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

B. event manager applet HIGH-CPU

event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type exact entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

C. event manager applet HIGH-CPU

event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op gt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

D. event manager applet HIGH-CPU

event snmp oid 1.3.6.1.4.1.9.9.109.1.1.1.1.6.1 get-type next entry-op lt 60 poll-interval 5 action 1.0 syslog priority notifications msg "cpu high"

Answer: A

Explanation:

The correct configuration to generate a syslog message when CPU utilization is higher than 60% is option

A. This configuration uses the Event Manager Applet feature of Cisco IOS to monitor the CPU utilization via SNMP. When the CPU utilization exceeds 60%, the specified action is triggered, which in this case is to send a syslog message with a priority of notifications and the message “cpu high”. The event snmp oid command specifies the OID to be monitored, and the entry-op gt 60 part of the command sets the condition for triggering the action when the value is greater than 60. The pollinterval 5 specifies that the SNMP OID will be polled every 5 seconds.

https://www.cisco.com/c/en/us/support/docs/ip/internet-protocol-ip/200931-EEM-Subsystem-in- Order-to-Monitor-CPU-Tr.pdf

https://blog.ipspace.net/2008/06/generate-snmp-trap-on-high-cpu-load.html

Question: 68

Host 1 is in VLAN 100 located is DataCenter 1 and Host2 is in VLAN200 located in DataCenter2. Which OTV VLAN mapping configuration allows Layer 2 connectivity between these two hosts?

DC1:

interface Overlayl otv extend-vlan 100
otv vlan mapping 100 to 200

DC2:

interface Overlavl ft
otv extend-vlan 100
otv vlan mapping 100 to 200

B DC1:

interface Overlavl oh extend-vlan 100 otv vlan mapping 100 to 200

DC2:

interface Overlavl otv extend-vlan 200

c DC1:

interface Overlavl otv extend-vlan 100

DC2:

interface Overlav2
oh' extend-vlan 200

0 DC1:

interface Overlavl oh extend-vlan 100

DC2:

interface Overlavl oh' extend-vlan 200

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To allow Layer 2 connectivity between Host 1 in VLAN 100 located in DataCenter 1 and Host 2 in VLAN 200 located in DataCenter 2, the correct OTV VLAN mapping configuration is option C. This configuration involves mapping VLAN 100 to VLAN 200 across the OTV overlay so that hosts in these separate VLANs can communicate as if they were in the same Layer 2 domain. The VLAN mapping is achieved by configuring the OTV edge devices in both data centers to associate the VLANs with each other.

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/200998-Nexus- 7000-OTV-VLAN-Mapping-on-Overlay.html?dtid=osscdc000283

https://www.cisco.com/c/en/us/support/docs/switches/nexus-7000-series-switches/200998-Nexus-7000-OTV-VLAN-Mapping-on-Overlay.html

Question: 69

A host EPG Client wants to talk to a webserver in EGP Web. A contract with default settings is defined between EPG Client and EPG Web, which allows TCP communication initiated by the client toward the webserver with TCP destination port 80. Which statement is true?

A. If EPG Web is made a preferred group member, a contract between EPG Client and EPG Web is no longer required for the host in EPG Client to reach the webserver in EPG Web.

B. If vzAny is configured to consume and provide a "deny all" contract, traffic between EPG Client and EPG Web is no longer allowed.

C. The host in EPG Client is allowed to connect to TCP destination port 80 on the webserver in EPG Web.

The webserver will not be allowed to initiate a separate TCP connection to a host port with TCP source port 80.

D. The host in EPG Client is allowed to connect to TCP destination port 80 on the webserver in EPG Web.

The webserver is allowed to initiate a separate TCP connection to a host port with TCP source port 80.

Answer: C

Explanation:

The contract between EPG Client and EPG Web allows TCP communication initiated by the client toward the webserver with TCP destination port 80. This means that the host in EPG Client can establish a connection to the webserver in EPG Web on TCP port 80. However, the contract does not allow the webserver to initiate a connection back to the host on the same port, which is typically used for HTTP traffic.

Reference: The explanation is based on the understanding of Cisco Application Centric Infrastructure (ACI) contracts, which are used to define the communication between EPGs (Endpoint Groups). For more detailed information, refer to the Cisco Data Center Core Technologies source book and the ACI documentation available on Cisco's official website.

Question: 70

A network engineer plans to upgrade the firmware of a Cisco UCS B-Series chassis by using the Auto Install feature. Which component is upgraded during the infrastructure firmware upgrade stage?

A. Cisco IMC

B. Adapter

C. I/O module

D. BIOS

Answer: C

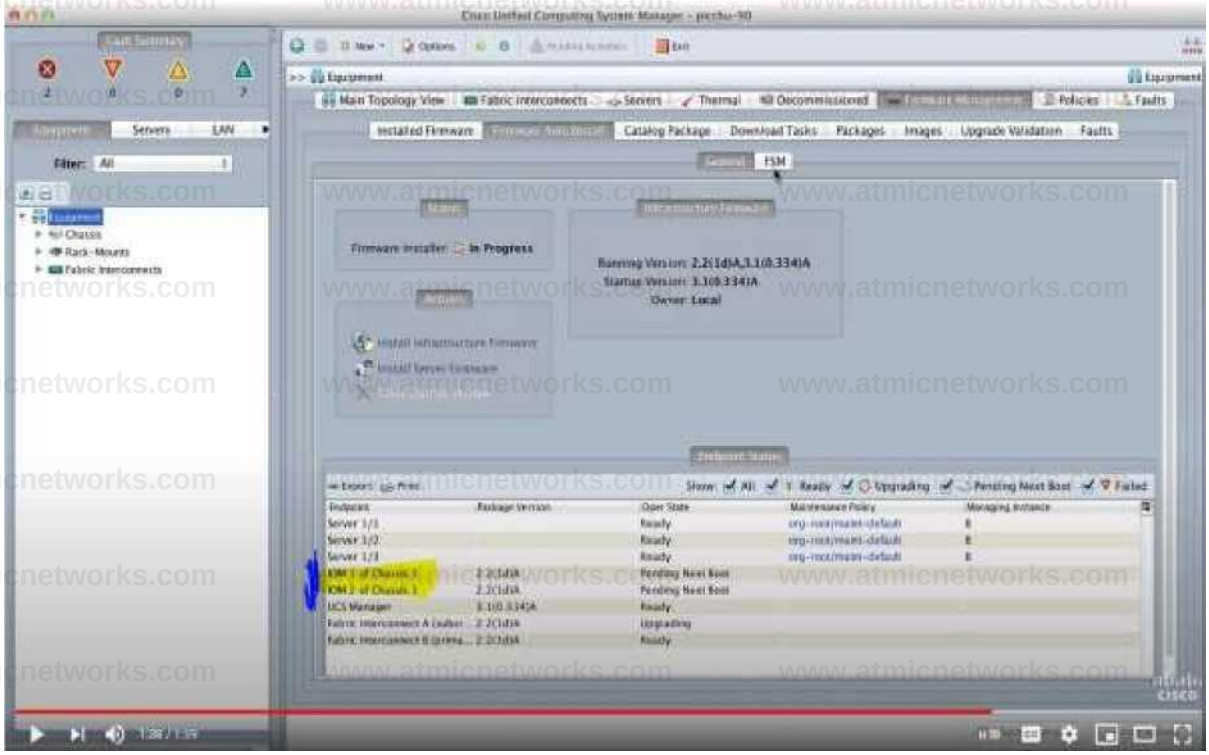
Explanation:

: During the infrastructure firmware upgrade stage using the Auto Install feature, the I/O module is upgraded. The infrastructure firmware upgrade includes updates to the fabric interconnects and I/O modules, which are essential components of the UCS B-Series chassis network connectivity.

Reference: This information can be found in the Cisco UCS Manager Firmware Management Guide, which details the process and components involved in the firmware upgrade of Cisco UCS B-Series chassis.

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Firmware-Mgmt/4-0/b_UCSM_GUI_Firmware_Management_Guide_4-0/b_UCSM_GUI_Firmware_Management_Guide_4-0_chapter_0100.html

https://www.youtube.com/watch?v=g-4OgYigvRI



Question: 71

What is required for using puppet in a Cisco NX-OS environment?

A. Open Agent Container

B. XML management interface

C. NX-API

D. OpenNP

Answer: A

Explanation:

Puppet, an open-source configuration management tool, requires the Open Agent Container (OAC) to run on Cisco NX-OS. The OAC provides a contained environment where third-party agents like Puppet can run without affecting the host NX-OS system.

Reference: The requirement for OAC when using Puppet in a Cisco NX-OS environment is outlined in the Cisco NX-OS Puppet Configuration Guide, which explains the integration of Puppet with Cisco NX- OS and the necessary components.

Question: 72

An engineer is enabling port security on a Cisco MDS 9000 Series Switch. Which feature of enabling port security on a Cisco MDS 9000 Series Switch must be considered?

A. It always learns about switches that are logging in.

B. It can be distributed by using Cisco Fabric services.

C. It authorizes only the configured sWWN to participate in the fabric.

D. It binds the fabric at the switch level.

Answer: C

Explanation:

Port security on Cisco MDS 9000 Series Switches is designed to prevent unauthorized devices from accessing the fabric. When port security is enabled, only the configured sWWN (switch World Wide Name) is authorized to participate in the fabric. This ensures that unauthorized switches or devices cannot log in or access the network, enhancing security within the data center. Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR v1.2)

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/configuration/guide s/security/nx-os/sec_cli_6-x/psec.html#92130

Question: 73

Which behavior defines streaming telemetry as a push model in Cisco devices?

A. Monitoring clients are pulling data from the network to see real-time statistics

B. JSON encoded telemetry data is transported using the gRPC protocol

C. The network devices send data in JSON or GPB format to configured endpoints

D. Events and network changes generate telemetry data

Answer: C

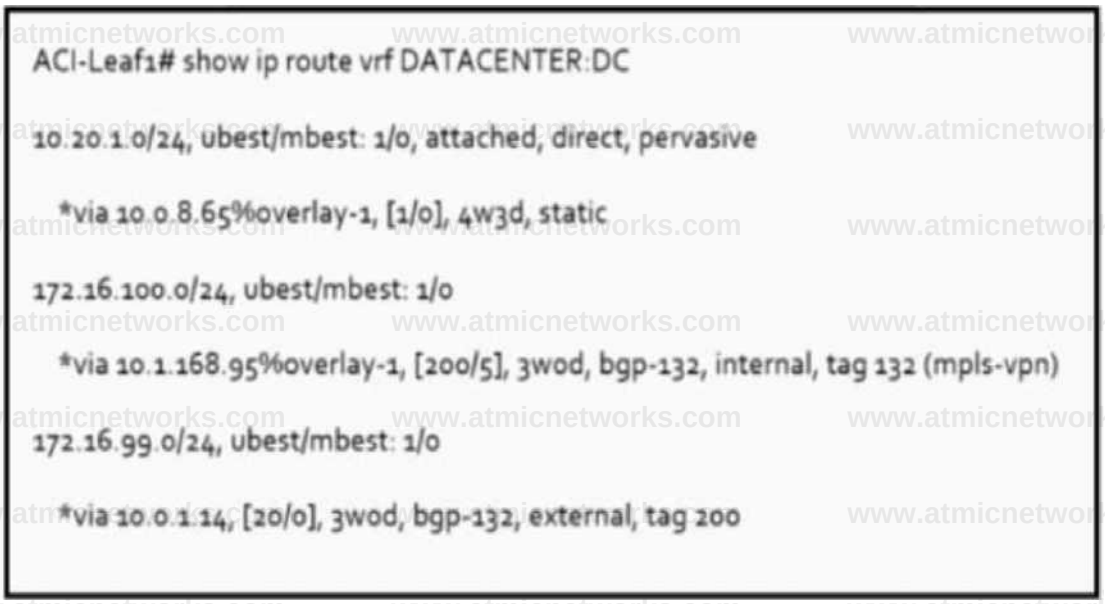
Explanation:

Streaming telemetry as a push model in Cisco devices refers to the mechanism where network devices send data in JSON or GPB format to configured endpoints without being requested for such data. This contrasts with traditional pull models where monitoring clients request data from network devices. Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR v1.2)

https://developer.cisco.com/docs/ios-xe/#!streaming-telemetry-quick-start-guide/streaming- telemetry

Question: 74

Refer to the exhibit.



Which two statements describe the routing table of the leaf switch? (Choose two.)

A. The next hop 10.0.8.65 for route 10.20.1.0724 is the TEP address of a border leaf in ACI.

B. The next hop 10.0.1.14 for route 172.16.99.0/24 is the TEP address of a border leaf in ACI.

C. The next hop 10.1.168.95 for route 172.16.100 0/24 is the TEP address of a border leaf in ACI.

D. 172.16.100.0/24 is a BD subnet in ACI.

E. 10.20.1.0/24 is a BD subnet in ACI.

Answer: CE

Explanation:

Question: 75

Which two statements about the process of upgrading an EPLD on a Cisco MDS 9000 series Switch are correct? (Choose two.)

A. The EPLDs for all the modules on a switch must be upgraded at the same time.

B. EPLD upgrades can be completed without powering down the module during the upgrade.

C. EPLDs can be upgraded only to the latest EPLD image.

D. EPLDs can be upgraded without replacing the hardware.

E. An upgrade verification identifies the impact of each EPLD upgrade.

Answer: B, D

Explanation:

EPLD upgrades on Cisco MDS 9000 series switches can be done without powering down the module during the upgrade (Option B), which allows for continuous operation and no downtime.
Additionally, EPLDs can be upgraded without replacing the hardware (Option D), making the process more cost-effective and less resource-intensive. Reference := Cisco Data Center Core Technologies

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/7_3/upgrade/upgrade.h tml

Question: 76

Refer to the exhibit.

```
FI-1# scope org /
FI-1 /org # create maint-policy maintenance
FI-1 /org/maint-policy* # set reboot-policy timer-automatic
FI-1 /org/maint-policy* # set soft-shutdown-timer never
```

Which action must be taken before the maintenance policy can be committed?

A. Set the soft shutdown timer to a specific time.

B. Associate a service profile to the maintenance policy.

C. Set the policy to apply the change on the next reboot.

D. Specify a maintenance time by selecting a schedule.

Answer: C

Explanation:

Before a maintenance policy can be committed, it is essential to set the policy to apply the change on the next reboot (Option C). This ensures that the changes are applied in a controlled manner, avoiding any immediate disruptions.

Reference := Cisco Data Center Core Technologies

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/CLI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Manager_CLI_Administration_Mgmt_Guide_3_1/b_Cisco_UCS_Manager_CLI_Administration_Mgmt_Guide_3_1_chapter_01100.html

Question: 77

What is a characteristic of EPLD updates on Cisco MDS 9000 Series Switches?

A. EPLD updates are installed only via the Cisco DCNM GUI

B. EPLD packages update hardware functionality on a device

C. EPLD bundles are released separately from a Cisco MDS NX-OS release

D. EPLD updates are nondisruptive to traffic flow

Answer: B

Explanation:

EPLD updates on Cisco MDS 9000 Series Switches are characterized by updating hardware functionality on a device (Option B). This means that the updates can enhance device capabilities or address issues without the need for physical hardware changes. Reference := Cisco Data Center Core Technologies

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/release/notes/epld/epld_rn.html

Question: 78

DRAG DROP

A storage engineer must configure zoning on a Cisco MDS 9000 Series switch. Drag and drop actions from the left into the order on right

Answer:

Explanation:

```
Switch1# configure terminal
Enter configuration commands, one per line. End with CNTL/Z

Switch1#(config)# vsan database
Switch1#(config-vsan-db)# vsan 100
Switch1#(config-vsan-db)# exit

Switch1#(config)# zone name zone1 vsan 100
Switch1#(config-zone)# member pwwn 11:11:11:11:11:11:11:1a
Switch1#(config-zone)# member pwwn 11:11:11:11:11:11:11:1b
Switch1#(config-zone)# exit

Switch1#(config)# zoneset name setA vsan 100
Switch1#(config-zoneset)# member zone1
Switch1#(config-zoneset)# exit

Switch1#(config)# zoneset activate name setA vsan 100
Zoneset activation initiated, check zone status
Switch1#(config)# exit

Switch1# sh zoneset active vsan 100
zoneset name setA vsan 100
zone name zone1 vsan 100
pwwn 11:11:11:11:11:11:11:1a
pwwn 11:11:11:11:11:11:11:1b
Switch1#
```

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/6_2/

configuration/guides/fabric/nx-os/nx_os_fabric/zone.html

Question: 79

The Cisco Nexus 5600 Series Switch experiences occasional packet drops on interface ethernet 1/16.

An engineer wants to implement a SPAN session to investigate the issue further. The network analyzer to which the packets must be directed is located on interface 1/3. The analyzer is limited on disk space available for traffic capture, so the Nexus switch should send only the relevant dat

a. Which two command sets configure the SPAN session that meets these requirements? (Choose two.)

interface ethernet 1/3 switchport monitor

monitor session 2
destination interface ethernet 1/3 span interface ethernet 1/16

interface ethernet 1/3 switchport span

span session 2
type SPAN-on-DROP
destination interface ethernet 1/3 source interface ethernet 1/16

monitor session 2 type SPAN-on-DROP destination interface ethernet 1/3 source interface ethernet 1/16

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: C, D

Explanation:

Option C and Option D are correct because they configure the SPAN session to monitor the source interface ethernet 1/16 and send the traffic to the destination interface ethernet 1/3. These options also include the use of the type SPAN-on-DROP command, which ensures that only dropped packets are sent to the analyzer, thus conserving disk space.

https://www.cisco.com/c/en/us/products/collateral/switches/nexus-5000-series-switches/white- paper-c11-733022.html

Question: 80

An engineer requires a solution to automate the configuration and deployment of remote network devices for a customer. The engineer must keep these considerations in mind:

- The customer's environment is based on industry-accepted standards and requires a solution that meets these standards.
- The security requirements mandate the use of a secure transport mechanism between the automation software and target devices such as SSH or TLS.
- The solution must be based on a human-readable and easy to parse format such as XML or JSON.

Which solution must be used to meet these requirements?

A. SNMP

B. REST API

C. Ansible

D. NETCONF

Answer: D

Explanation:

NETCONF is the ideal solution for this scenario for the following reasons:

Standards-based: NETCONF is built upon industry-standard protocols (XML, SSH, TLS) ensuring compatibility and adherence to open standards.

Secure transport: NETCONF mandates secure transport mechanisms like SSH or TLS for communication between the automation software and managed devices, aligning with security requirements.

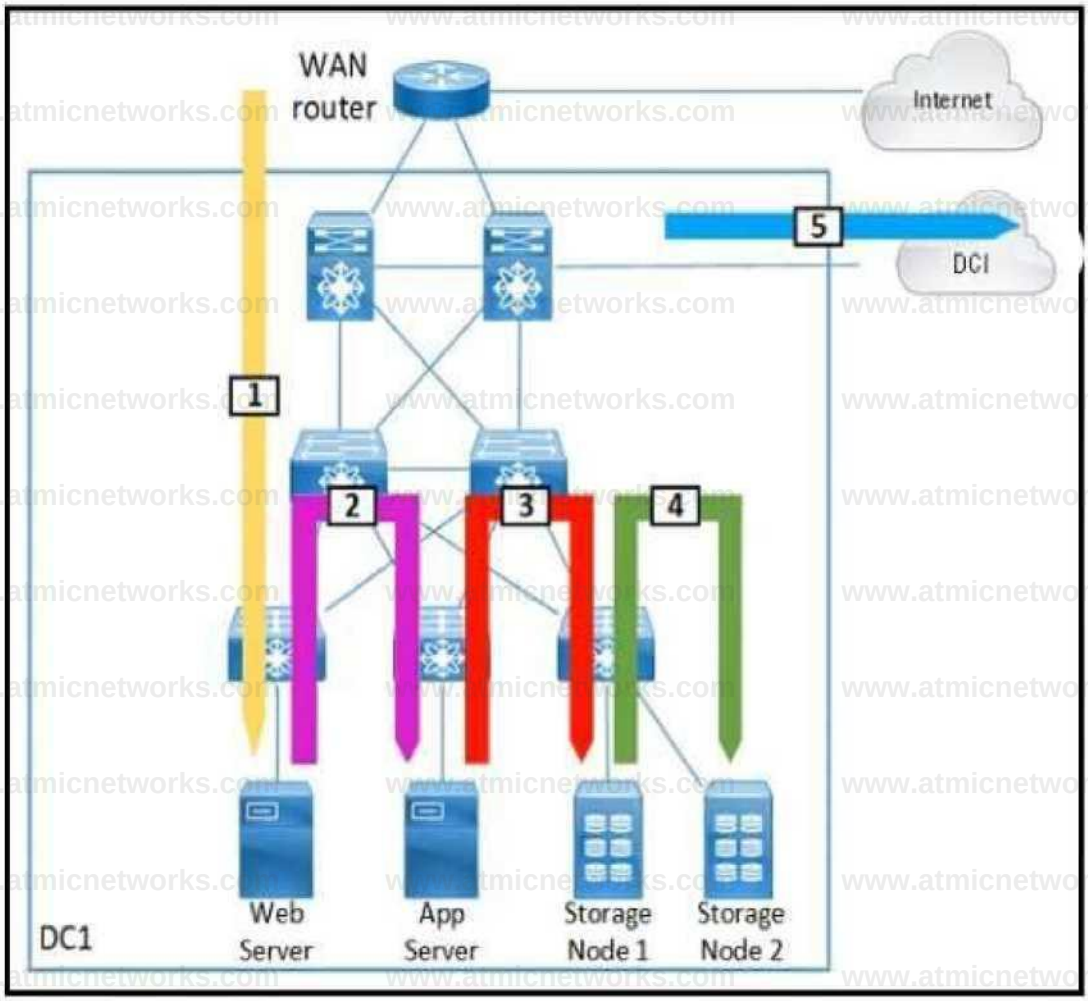
Data Format: NETCONF utilizes XML for data encoding and transport, providing a human-readable and machine-parsable format that is easy to work with.

Remote Device Automation: NETCONF is designed specifically for remote configuration and management of network devices, making it perfect for the task of automating remote device deployments.

Question: 81

DRAG DROP

Refer to the exhibit.



Drag and drop each traffic flow type from the left onto the corresponding number on the right Not all traffic flow types are used

Answer:

Explanation:

North-South

East-Wes

StorageTraffic

Storage Replication

Inter-Data Center

Question: 82

The engineer must configure SPAN on a cisco Nexus 5000 Series switch to get a capture of the traffic from these applications for an in-depth packet analysis. Which two characteristics must be considered? (Choose two.)

A. The Ethernet, FC, vFC, port channel, SAN port channel can be used as SPAN source ports.

B. The rx/tx option is available for VLAN or VSAN SPAN sessions.

C. SPAN source port can be monitored in multiple SPAN sessions.

D. Only Ethernet, FC, vFC, port channel port types can be a destination SPAN port.

E. A SPAN source port cannot be a destination SPAN port.

Answer: C, E

Explanation:

SPAN (Switched Port Analyzer) is a feature that allows network traffic from one or more source ports to be mirrored to a destination port for analysis. When configuring SPAN on a Cisco Nexus 5000 Series switch, two characteristics must be considered:

A SPAN source port can be monitored in multiple SPAN sessions. This means that the same port can send traffic to different destination ports for different purposes or applications.

A SPAN source port cannot be a destination SPAN port. This means that a port cannot receive traffic from another port that it is already monitoring. This prevents loops and conflicts in the SPAN configuration.

Reference := Configuring SPAN

https://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/configuration/guide/cli_rel_4_1/Cisco_Nexus_5000_Series_Switch_CLI_Software_Configuration_Guide_chapter50.html

Question: 83

Which solution provides remote and direct file-level access to users and systems?

A. direct-attached storage

B. Fibre Channel over Ethernet

C. storage area network

D. network-attached storage

Answer: D

Explanation:

Network-attached storage (NAS) is a solution that provides remote and direct file-level access to users and systems. NAS devices are connected to the network and offer shared storage space for files and data. Users and systems can access the files using standard protocols such as NFS or SMB. NAS devices can also offer features such as backup, replication, and security.

Reference := Cisco Data Center Core Technologies

Question: 84

The FCoE technology is used in a data center and the MDS switches are configured as Fibre Channel Forwarders. What configuration should be applied to an MDS switch in order to be used as the best switch to connect by the CNAs in the fabric?

A. fcoe fcf-priority 1024

B. fcoe fcf-priority 512

C. fcoe fcf-priority 0

D. no fcoe fcf-priority

Answer: A

Explanation:

FCoE (Fibre Channel over Ethernet) is a technology that allows Fibre Channel traffic to be encapsulated and transported

over Ethernet networks. FCoE requires the use of FCFs (Fibre Channel Forwarders), which are devices that act as bridges between the FCoE and Fibre Channel domains. FCFs can be configured with a priority value that determines their preference for connecting to CNAs (Converged Network Adapters), which are devices that support both Ethernet and Fibre Channel protocols. The priority value ranges from 0 to 1024, with 0 being the lowest and 1024 being the highest. To configure an MDS switch as the best switch to connect by the CNAs in the fabric, the fcoe fcf-priority 1024 command should be applied. This gives the switch the highest priority and makes it the most preferred FCF for the CNAs.

Reference := Configuring FCoE

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/fcoe/521n11/b_5k_FC oE_Config_521N11/b_5k_FCoE_Config_521N11_chapter_011.pdf

Question: 85

Due to a major version change, an engineer must perform a software upgrade on a Cisco Nexus Series switch. Which two technologies can be implemented to reduce disruptions to the network during the upgrade? (Choose two.)

A. MLAG
B. HSRP
C. PAgP
D. VDC
E. vPC

Answer: D, E

Explanation:

To reduce disruptions during a major software upgrade on a Cisco Nexus Series switch, technologies like VDC (Virtual Device Contexts) and vPC (Virtual Port Channels) can be implemented. VDC allows for the partitioning of a single physical device into multiple logical devices, which can be managed and operated independently. This means that one VDC can be upgraded while others remain

operational, minimizing downtime. vPC enables the linking of two switches to create a single logical switch, providing redundancy and allowing for one switch to be upgraded while the other maintains the network operations1.

Question: 86

Refer to the exhibit.

Python Code:

```
import requests
import json

url='http://lab-9318Obdlf-swl/ins'
switchuser='dazfre'
switchpassword='ClscoroxO'

myheaders={'content-type * 'application/json')
payload={
  "ins_api": {
    "version": "1.0",
    "type": "cli_show",
    "chunk": "0",
    "aid": "1",
    "input": "configure terminal : feature hsrp", "output_format": "json"
  }
}
response = requests post(url,data=json.dumps(payload), headers = myheaders, auth=
(switchuser, switchpassword))

print(response.text)
```

ERROR MESSAGE
I

```
      "ins_api" [
            "type": "cli show"
            "version":     "1.0",
            "sid" "eoc", "outputs", [ "output" [{
                                  "clierror" "% invalid command\n", "input"
                                  "configure terminal" "msg" "input CLI command
                                  error", "code" "400"
                            }/{ "clierror" "% invalid command\n", "input"
                                        "feature hsrp",
                                  "msg" "input CLI command error", "code"      "400"
                            }]
            }
       }
```

Why does the python code for Cisco NX-API print an error message?

A. The “type” is wrong in the header of the request and should be “cli_ conf”.

B. NX-API does not allow configuration for features via the requests module.

C. The “type” is wrong is the body of the request and should be “cli_ conf”.

D. The JSON is not a supported format for the NX-API.

Answer: C

Explanation:

"Commands that belong to different message types should not be mixed. For example, show commands are cli_show message type and are not supported in cli_conf mode."
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus7000/sw/programmability/guide e/ cisco_nexus7000_programmability_guide_8x/b-cisco-nexus7000-programmability-guide-8x_chapter_011.html

the payload "type" value is wrong in the body of the request. For the request to be successful, it should be changes to "cli_conf".

For example, if we run the same request with the updated payload:

```
{
"ins_api": {
"version": "1.0",
"type": "cli_conf",
"chunk": "0",
"sid": "1",
"input": "configure terminal ;feature hsrp",
"output_format": "json"
}
}
```

We get a 200 response:

```
{
```

"ins_api": {

"sid": "eoc",

"type": "cli_conf",

"version": "1.0",

"outputs": {

"output": [

{

"code": "200",

"msg": "Success",

"body": {}

},

{

"code": "200",

"msg": "Success", "body": {}

}

]

}

}

}

CLI verification:

nxos9kv# sh run | inc hsrp

feature hsrp

Question: 87

A server engineer wants to control power uses on a Cisco UCS C-series rack server down to the component level. Which

two components support specific power limits? (Choose two.)

A. memory

B. graphic card

C. processor

D. network controller

E. storage controller

Answer: A, C

Explanation:

Question: 88

What occurs when running the command install deactivate <filename> while a software maintenance upgrade is performed on a Cisco Nexus 9000 Series switch?

A. The current set of packages is committed.

B. The package is removed from the switch.

C. The package features for the line card are disabled.

D. The current upgrade stops.

Answer: C

Explanation:

Reference:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/6-x/system_management/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_System_Management_Configuration_Guide/sm_smu.html#task_B8B0F5BA80BE41AEA93197F56 0665648

Question: 89

A network architect wants to propose a scalable network monitoring solution in which data is repeatedly acquired from network devices. The solution must use a push model and provide close to realtime access to operational dat

a. Which technology must be used to meet these requirements?

A. streaming telemetry

B. logging

C. SNMPv3

D. CLI-based scripting

Answer: A

Explanation:

https://blogs.cisco.com/developer/its-time-to-move-away-from-snmp-and-cli-and-use-model-driven-telemetry

Streaming telemetry is a technology that enables scalable network monitoring by repeatedly acquiring data from network devices and sending it to configured endpoints. Streaming telemetry uses a push model, meaning that the network devices initiate the data transmission without being polled by the monitoring clients. Streaming telemetry also provides close to real-time access to operational data, allowing for more dynamic and responsive network analysis and

troubleshooting12.

Reference := 1: Cisco Data Center Core Technologies 2: Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x)

Question: 90

A network engineer is adding a Cisco HyperFlex data platform to the Cisco intersight management portal. Which two components are required for Intersight to claim the Cisco HyperFlex data platform? (Choose two.)

A. device FQDN

B. device public IP address

C. device claim code

D. device ID

E. device serial number

Answer: C, E

Explanation:

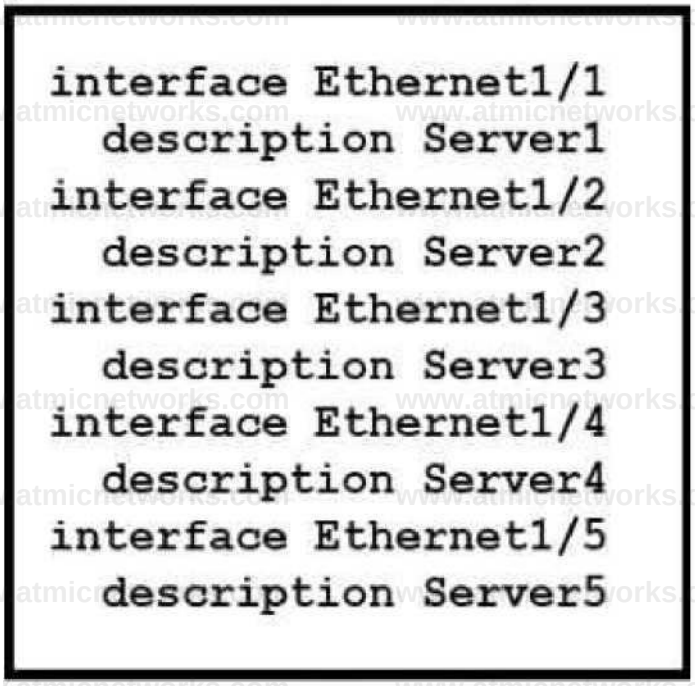
To add a Cisco HyperFlex data platform to the Cisco Intersight management portal, two components are required for Intersight to claim the Cisco HyperFlex data platform: the device claim code and the device serial number. The device claim code is a unique identifier that is generated by the Cisco HyperFlex installer and is used to register the device with Intersight. The device serial number is the serial number of the Cisco HyperFlex controller node and is used to verify the device ownership and entitlement3.

Reference := 3: [Cisco HyperFlex Systems Installation Guide for Cisco Intersight, Release 4.0] : [Cisco

Intersight Device Connector Installation and Reference Guide]

Question: 91

Refer to the exhibit.



Which command is run from the Guest Shell to set the description on the first five interfaces of the Cisco Nexus switch?

```
[guestshellgguestshell ~]S for x in (1..5); do dohost "conf t" ; "interface ethVSx" ; "description ServerSx" ; done

[guestshellgguestshell ~]S for x in (1..5); dohost "conf t: interface ethl/Sx : description ServerSx";

[guestshellgguestshell -JS for x in {1. 5}: dohost "conf t: interface ethVSx : description ServerSx" ;

[guestshellgguestshell -]$ for x in (1. 5): do dohost "conf t: interface ethl/Sx ; description ServerSx" ; done
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The command in Option D correctly uses a loop to iterate over the range {1…5}, which represents the first five interfaces. The dohost command is used to send commands to the host Cisco Nexus switch from the Guest Shell. The syntax interface eth1/$x and description Server$x within the loop sets the description for each interface eth1/1 to eth1/5 to "Server1" to "Server5" respectively.

Here's the command from Option D formatted for clarity:

```
[guestshell@guestshell ~]$ for x in {1..5}; do
  dohost "conf t" ;
interface eth1/$x;
description Server$x;
done
```

This command will configure the description for each of the first five Ethernet interfaces with the respective server number as part of the description.

Question: 92

A Cisco UCS user called "Employee1" accidentally changed the boot policy of the Cisco UCS server at the Cisco UCS Manager root level. This change impacted all service profiles and their storage connectivity was lost. The system administrator wants to prevent this issue from recurring in the future. The new security policy mandates that access must be restricted up to the organization level and prevent other users from modifying root policies. Which action must be taken to meet these requirements?

A. Modify the privilege level assigned to the user

B. Define a custom user role and assign it to users

C. Assign the user "Employee1" the network-operator role

D. Assign users to a specific Cisco UCS locale

Answer:B

To prevent users from modifying root policies, the system administrator can define a custom user role and assign it to users. A custom user role can have specific privileges and scope of access that are different from the predefined user roles. For example, a custom user role can have read-only access to the root policies, but full access to the organization policies. By assigning this custom user role to users, the system administrator can ensure that only authorized users can

modify the root policies, while still allowing users to manage their own organization policies. This way, the system administrator can avoid accidental changes to the boot policy or other root policies that can impact all service profiles and their storage connectivity. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.2: Cisco UCS Manager Administration

[Cisco UCS Manager Administration Management Guide, Release 4.1], Chapter: User Management, Section: Creating a Custom User Role

[Cisco UCS Manager GUI Configuration Guide, Release 4.1], Chapter: Managing Organizations and Locales, Section: Creating an Organization

Question: 93

An engineer is running an ACI fabric, has VMM integration with VMware vCenter, and wants to enable microsegmentation based on vCenter VM attributes. Which statement about microsegmentation is true?

A. ACI does not support microsegmentation based on vCenter VM attributes. You should use network attributes for mircosegmentation.

B. An ACI microsegmented EPG automatically creates a port group with a private VLAN configured on a VMware vCenter distributed virtual switch.

C. When enabled, microsegmentation performs distributed switching and routing on the ESXi hosts.

D. Microsegmentation is supported only using AVE or AVS.

Answer: C

Explanation:

Microsegmentation is a feature of ACI that allows granular control of traffic between endpoints based on vCenter VM attributes, such as name, guest OS, or network adapter type.

Microsegmentation works by creating a micro-EPG for each VM and applying contracts and policies to the micro-EPGs. When microsegmentation is enabled, ACI performs distributed switching and routing on the ESXi hosts using the Cisco Application Virtual Switch (AVS) or the Cisco Application Virtual Edge (AVE). This allows ACI to enforce policies at the hypervisor level, without requiring any changes to the physical network or the VM configuration. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 6: Cisco ACI, Lesson 6.3: Cisco ACI Integration

Cisco ACI Virtualization Guide, Release 4.2(x), Chapter: Configuring Microsegmentation

Question: 94

A network architect considers a Cisco HyperFlex design solution for a company. The proposed solution is for a virtual environment that is not performance-sensitive, but the solution must have high storage capacity and a low cost. Which Cisco HyperFlex storage configuration should be used?

A. All-Flash

B. Hybrid

C. All-SAN

D. All-NVMe

Answer: B

Explanation:

A hybrid Cisco HyperFlex storage configuration is the best option for a virtual environment that is not performance-sensitive, but requires high storage capacity and a low cost. A hybrid configuration consists of a mix of solid-state drives (SSDs) and hard disk drives (HDDs) in each node. The SSDs are used for caching and metadata, while the HDDs are used for data storage. This allows for a balance

between performance and capacity, as well as a lower cost per gigabyte than an all-flash configuration. A hybrid configuration also provides data deduplication and compression features to optimize storage efficiency and reduce the storage footprint. A hybrid configuration is suitable for general-purpose workloads, such as virtual desktop infrastructure (VDI), databases, and file servers. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 4: Cisco HyperFlex, Lesson 4.1: Cisco HyperFlex Overview

Cisco HyperFlex Systems Design Guide, Chapter: Cisco HyperFlex Storage Configurations

Question: 95

Refer to the exhibit.

```
show install all impact epld bootflash:n9000-epld.6.1.2.I3.1.img
```

What is the outcome of this command when the ELPD is updated on a Cisco Nexus 9000 series switch?

A. displays the compatibility of the EPLD upgrade and the image in the bootflash

B. shows a simulated upgrade of the EPLD

C. upgrades the EPLD on the switch disruptively

D. displays the impact of the upgrade on the operation of the switch

Answer: D

Explanation:

The command “show install all impact epld bootflash:n9000-epld.6.1.2.13.1.img” is used to display the impact of the EPLD (Electronic Programmable Logic Device) upgrade on the operation of the Cisco Nexus 9000 series switch. This command does not perform the upgrade; instead, it provides a report that shows what the upgrade would affect if it were to be executed. This is useful for planning and ensuring that the upgrade will not disrupt critical services or operations on the switch. Reference :=

Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide, Chapter: Managing EPLD Images

Question: 96

DRAG DROP

Refer to the exhibit.

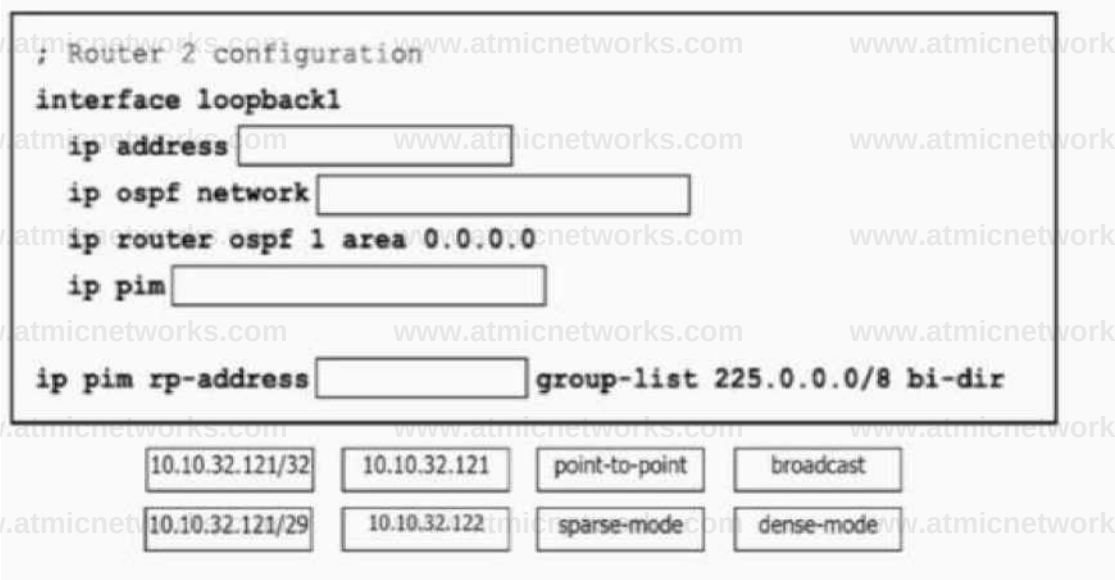
```
; Router 1 configuration
interface loopback1
  ip address 10.10.32.121/30
  ip ospf network point-to-point
  ip router ospf 1 area 0.0.0.0
  ip pin sparse-mode

ip pin rp-address 10.10.32.122 group-list 225.0.0.0/8 bi-dir
```

In a bidirectional PIM network using Phantom RP as an RP redundancy mechanism, two Cisco NX-OS routers have these requirements:

- R1 must be the active RP.
- R2 must be the backup RP that is used only if R1 is not reachable

Drag and drop the configuration steps to complete the configuration for Router 2. Not all

configuration steps are used.



Answer:

Explanation:

Answer:

ipaddress 10.10.32.121/29

ip ospf network point-to-point

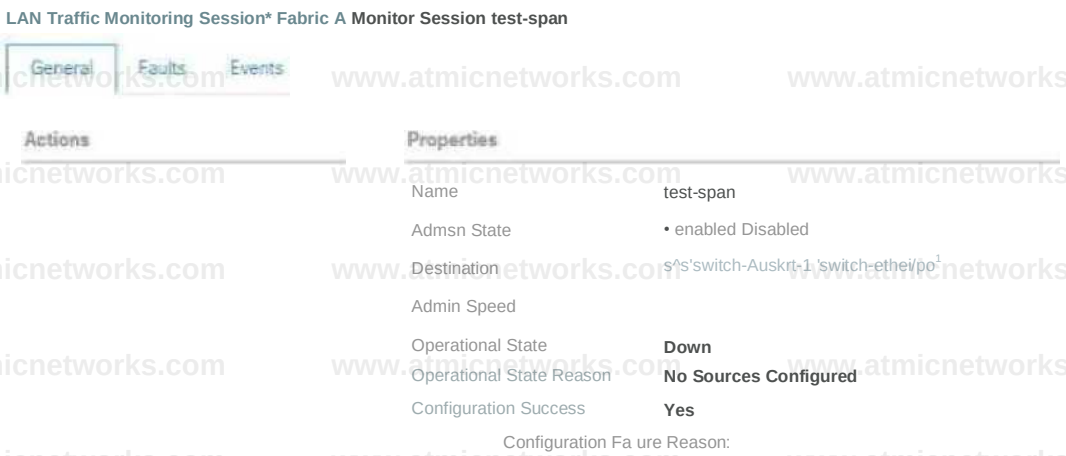
router ospf 1 area 0.0.0.0

ip pirn sparse-mode

ip pirn rp-address 10.10.32.122 group-list 255.0.0.0/8 bi-dir

Question: 97

Refer to the exhibit.



An engineer must monitor all LAN traffic on Fabric A from a blade server. Which source should be configured in the test-span monitor session to complete this task?

A. all vHBAs from the service profile that correspond to this server

B. all uplink FCoE ports

C. all uplink Ethernet ports

D. all vNICs from the service profile that correspond to this server

Answer: C

Explanation:

To monitor all LAN traffic on Fabric A from a blade server, the source should be configured as all uplink Ethernet ports in the test-span monitor session. This configuration allows the engineer to capture all LAN traffic that traverses the uplink Ethernet ports, providing a comprehensive view of the network activity related to Fabric A. By monitoring these ports, the engineer can analyze traffic patterns, detect anomalies, and ensure the proper functioning of the network.

Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, which covers the necessary concepts for monitoring and managing traffic within a Cisco data center network.

Cisco Data Center Network Manager (DCNM) Guide, which provides detailed instructions on setting

up and configuring monitoring sessions for traffic analysis.

Question: 98

After a Cisco Nexus 7000 Series Switch chassis replacement, the administrator discovers that all vPC- enabled LACP port channels are reinitialized. The administrator wants to prevent this issue the next time the chassis is replaced. Which two actions must be taken to meet this requirement before the isolated device is reloaded'? (Choose two)

A. Set the vPC MAC address to a tower value than the peer

B. Change the vPC system-priority of the replacement chassis to a higher value than the peer if.

C. Change the vPC system-priority of the replacement chassis to a lower value than the peer.

D. Set the vPC MAC address to a higher value than the peer

E. Configure auto-recovery to the disable state on both peers

Answer: A, C

Explanation:

Question: 99

Which feature must be enabled to support the use of JSON and XML encoding when a Cisco Nexus 7000 series switch is deployed?

A. NX-API

B. LLDP

C. Open Agent Container

D. Bash shell

Answer: A

Explanation:

NX-API is a feature that enables the use of JSON and XML encoding when a Cisco Nexus 7000 series switch is deployed.

NX-API is a RESTful API that allows external applications to communicate with the switch using HTTP/HTTPS requests and responses. NX-API supports JSON and XML as the data formats for encoding and decoding the requests and responses. By using NX-API, external applications can access and configure the switch features and functions without using the CLI or SNMP. NX-API also provides a sandbox mode that allows users to test and validate their API calls before applying them to the switch. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.4: Cisco Nexus 9000 Series Switches

Cisco Nexus 7000 Series NX-OS Programmability Guide, Release 8.x, Chapter: Using NX-API

Question: 100

A network architect is asked to design and manage geographically distributed data centers across cities and decides to use a Multi-Site Orchestrator deployment. How many orchestrators should be deployed?

A. 3

B. 5

C. 4

D. 2

Answer: D

Explanation:

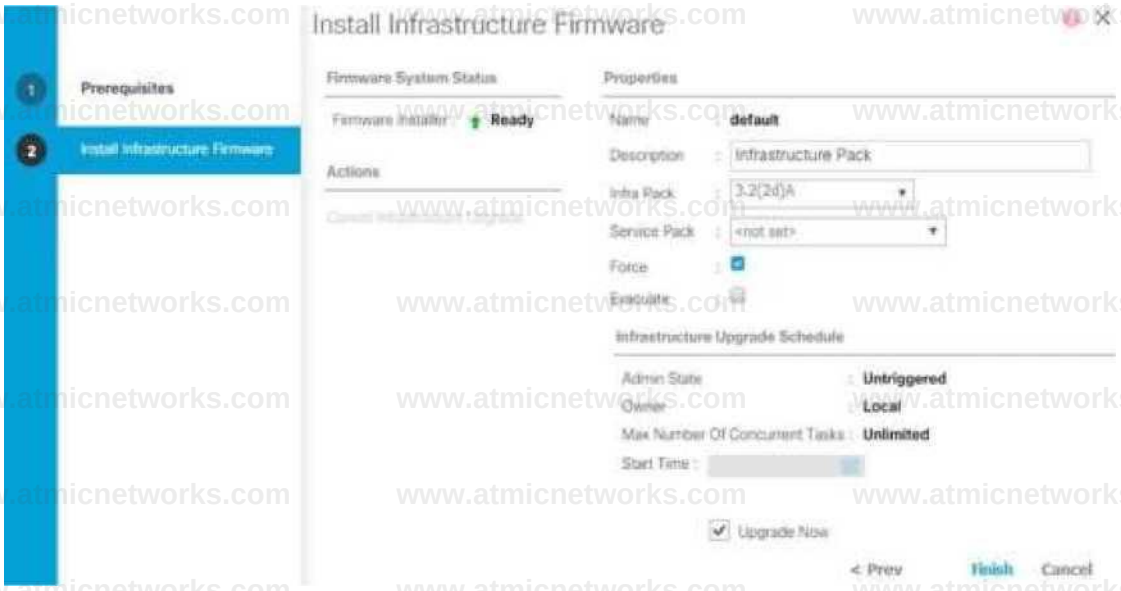
A Multi-Site Orchestrator deployment requires two orchestrators to be deployed, one in each of the two main data center sites. The Multi-Site Orchestrator is a software component that enables the management and orchestration of multiple Cisco Application Centric Infrastructure (ACI) fabrics that are geographically distributed across different locations. The Multi-Site Orchestrator provides a single pane of glass for configuring, monitoring, and troubleshooting the ACI fabrics, as well as synchronizing policies and tenants across the sites. The Multi-Site Orchestrator also supports disaster recovery and high availability scenarios by allowing the replication of data and services between the sites. The Multi-Site Orchestrator deployment consists of two orchestrators that form a cluster and communicate with each other using a secure channel. Each orchestrator is connected to one or more ACI fabrics in the same site, and acts as a proxy for the other orchestrator to access the ACI fabrics in the remote site. The orchestrators use a leader-election algorithm to determine which one is the active orchestrator and which one is the standby orchestrator. The active orchestrator handles all the requests from the users and the applications, while the standby orchestrator monitors the health and status of the active orchestrator and takes over in case of a failure. The orchestrators also perform periodic data synchronization to ensure consistency and reliability. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 6: Cisco ACI, Lesson 6.4: Cisco ACI Multi-Site

Cisco ACI Multi-Site Orchestrator User Guide, Chapter: Cisco ACI Multi-Site Orchestrator Overview

Question: 101

Refer to the exhibit.



Which two Cisco UCS components are upgraded as a result of the configuration? (Choose two.)

A. adapters

B. board controller

C. IOMs

D. BIOS

E. Cisco UCS Manager

Answer: A, D

Explanation:

The configuration shown in the exhibit is related to the infrastructure firmware upgrade process in a Cisco UCS environment. When an infrastructure firmware upgrade is initiated, it typically includes updates to various components such as the adapters and the BIOS. The adapters require firmware updates to ensure compatibility with new features and fixes, while the BIOS update is crucial for system stability and to support new hardware and software enhancements. The infrastructure firmware package, also known as the 'A bundle', contains the necessary firmware images for these components1.

Reference :=

Cisco UCS Manager Firmware Management Guide, Release 4.0, which provides detailed information on firmware upgrades for Cisco UCS components.

System Configuration - Managing Firmware, which outlines the guidelines and procedures for firmware upgrades in Cisco UCS Manager.

Question: 102

Which data structure results from running this Python code?

```
»> import json
»> f = openffname.json'. 'r')
>» varl = json.load(f)
»> varl
(u'bd': ubdT. u'ap': {u'epgs': [(u'name': u'app'}, (u'name': u'web'}. (u'name'
u'db*}], u'name': u'OnlineStore'}, u'name*: u'39233259'. u'pvn*: u'pvnl*)
```

A. tuple

B. dictionary

C. set

D. list

Answer: B

Explanation:

The Python code snippet provided imports the json module and loads a JSON file into a variable named var1. Since JSON files inherently represent object data as dictionaries in Python, the resulting data structure is a dictionary. This is evident from the output shown, which displays a dictionary with nested dictionaries and lists, containing keys like 'bd', 'ap', 'name', etc., and corresponding values.

Reference := The explanation is based on standard Python data structures and JSON file handling as described in Python documentation and typical Python programming resources. JSON objects are represented as dictionaries in Python, which is a fundamental concept in working with JSON data in the language.

Question: 103

A network engineer configures a converged network adapter (CNA) and must associate a virtual fiber Channel 7 interface to VSAN 7. The CAN connected to the interface Eth1/7, and VLAN 700 is mapped to the VSN

A. Which configuration must be applied to create the virtual Fiber Channel interface and associate it with the Ethernet physical interface?

A)

fMc'HCorflg)# vlan 700 swit ch(config-vlan }#fcoe vsan 7

B)

L swfchfcorfig# vsan database sw:tch(conh^vsan]« vsan 7 Interface vfc 7

C)

swWi(conflj)* Interface ethemet 1(7 swilcMconbg lb# vfc 7 attach vlan 1,700

D)

swlch(conflg)* Interface vfc 7
swi!ch(eonflg.lbe bind interface ethemet 1/7

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To create a virtual Fiber Channel interface and associate it with an Ethernet physical interface, the correct configuration commands would be:

Enter the interface configuration mode for the virtual Fiber Channel interface using the command interface vfc7.

Bind the virtual Fiber Channel to the Ethernet interface using the command bind interface ethernet 1/7.

This configuration associates the virtual Fiber Channel interface with VSAN 7 and maps VLAN 700 to the VSAN, as required by the converged network adapter (CNA).

Reference := The explanation is based on standard practices for configuring virtual Fiber Channel interfaces in a Cisco

environment, as detailed in Cisco's data center configuration guides and technical documentation.

Question: 104

An engineer must use the Embedded Event Manager to monitor events that occur on a cisco Nexus 9000 series switch. An environment variable needs to be created so that several policies use the

monitored events in in their actions. The external email server is represented by IP address 10.10.10.10. which command sets the environment variable?

A. N9k2(config)# event manager policy environment mallserver ''10.10.10.10''

B. N9k2# event manager environment mallserver ''10.10.10.10''

C. N9k2 (config-apple1)# environment mallserver ''10.10.10.10''

D. N9k2 (config)# event manager environment mallserver ''10.10.10.10''

Answer: D

Explanation:

To create an environment variable that can be used by several policies in the Embedded Event Manager, the engineer should use the command N9k2 (config)# event manager environment mailserver "10.10.10.10''. This command defines a global environment variable named mailserver with the value of 10.10.10.10, which represents the external email server. The environment variable can then be referenced by any policy that needs to use the email server in its actions, such as sending notifications or alerts. The environment variable can also be modified or deleted as needed. The other commands are incorrect because they either use the wrong mode, the wrong keyword, or the wrong syntax.

Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.4: Cisco Nexus 9000 Series Switches

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x), Chapter: Configuring Embedded Event Manager

Question: 105

Which communication method does NFS use for requests between servers and clients?

A. XDR

B. SSC

C. PRC

D. SMB

Answer: A

Explanation:

NFS uses XDR (External Data Representation) as the communication method for requests between servers and clients. XDR is a standard format for encoding and decoding data that is exchanged between different systems. XDR allows NFS to handle data with different byte orders, word sizes, and data types. XDR is also used by ONC RPC, which is the underlying protocol for NFS. XDR ensures that the data is represented consistently and correctly across different platforms and architectures. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 7: Data Center Storage Connectivity, Lesson 7.2: Network File System

Network File System (NFS) - GeeksforGeeks, which explains the basics of NFS and its architecture.

RFC 4506 - XDR: External Data Representation Standard, which defines the XDR standard and its specifications.

Question: 106

A customer reports Fibre Channel login requests to a cisco MDS 9000 series Switch from an unauthorized source. The customer requires a feature that will allow all devices already logged in and learned in and learned to be added to the Fibre channel active database. Which two features must be enabled to accomplish this goal? (Choose two.)

A. Auto-learning

B. Port security

C. Enhanced zoning

D. Device aliases

E. Smart aliases

Answer: B, D

Explanation:

To accomplish the goal of adding all devices already logged in and learned to the Fibre Channel active database, the customer should enable port security and device aliases on the Cisco MDS 9000 series switch. Port security is a feature that allows the switch to restrict the number and type of devices that can log in to a Fibre Channel port. Port security can be configured to automatically add the devices that are already logged in and learned to the active database, and prevent any unauthorized devices from logging in. Device aliases are user-friendly names that can be assigned to devices based on their World Wide Names (WWNs). Device aliases can be used to simplify the management and configuration of devices, as well as to enhance the security and visibility of the Fibre Channel network. Device aliases can also be automatically added to the active database along with the port security information, and can be used for zoning and other operations. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 7: Data Center Storage Connectivity, Lesson 7.3: Fibre Channel Protocol

Cisco MDS 9000 Family NX-OS Security Configuration Guide, Chapter: Configuring Port Security

Cisco MDS 9000 Family NX-OS Interfaces Configuration Guide, Chapter: Configuring Device Aliases

Question: 107

An engineer evaluates a UI-based infrastructure management system capable of monitoring and deploying standardize VXLAN BGP EVPN deployments. The storage administrator else need the solution to manage the cisco MDS 9090 series Switches. Which solution meets these requirements?

A. Intersight

B. UCSD

C. Tetration

D. DCNM

Answer: D

Explanation:

DCNM (Data Center Network Manager) is a UI-based infrastructure management system that meets the requirements of the question. DCNM can monitor and deploy standardized VXLAN BGP EVPN deployments across multiple Cisco Nexus switches, using predefined templates and workflows.

DCNM can also manage Cisco MDS 9000 series switches, providing visibility and control over the storage network. DCNM supports various features and functions for both LAN and SAN environments, such as configuration, provisioning, monitoring, troubleshooting, automation, and security. DCNM is a comprehensive and scalable solution for data center network management.

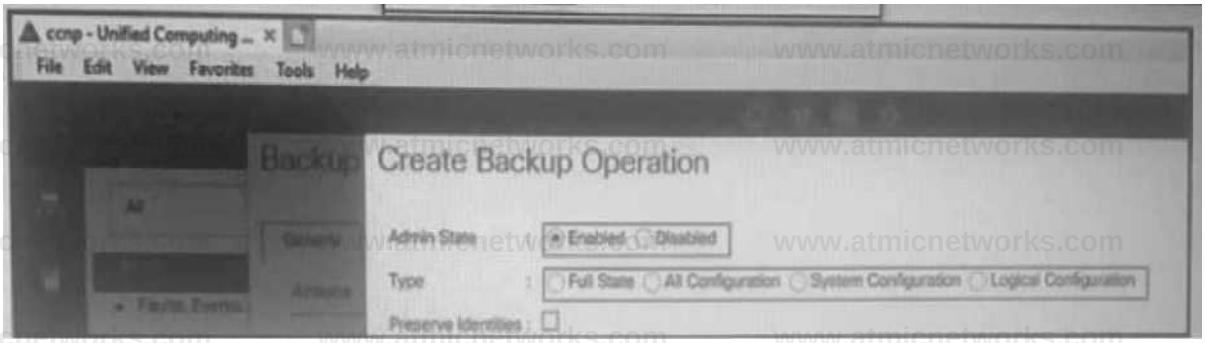
Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 8: Data Center Automation and Orchestration, Lesson 8.1: Cisco Data Center Network Manager

[Cisco Data Center Network Manager 11.x Data Sheet], which provides an overview of DCNM features and benefits.

Question: 108

Refer to the exhibit.



Refer to the exhibit. Which backup operation type not include the preserve identities feature?

A. Full state
B. Logical configuration
C. System configuration
D. All configuration

Answer: B

Explanation:

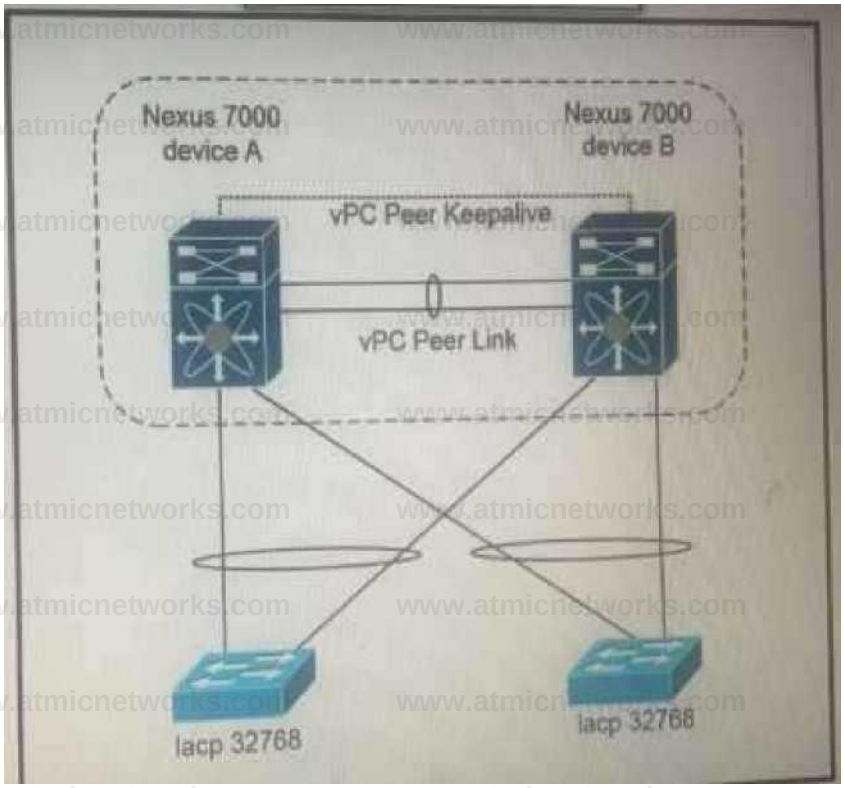
The preserve identities feature is not included in the logical configuration backup operation type. This type of backup

includes the configuration settings that are logically grouped, such as service profiles, policies, and pools, but does not include the unique identifiers or configurations that are specific to a particular system or setup, which are preserved in a full state or system configuration backup.

Reference := For detailed information on the different backup operation types and their characteristics, please refer to the official Cisco documentation on Implementing and Operating Cisco Data Center Core Technologies (DCCOR), specifically the sections related to backup and restore operations within the Cisco Unified Computing System (UCS) Manager1.

Question: 109

Refer to the exhibit.



Refer to the exhibit. Which configuration ensure that the cisco Nexus 7000 series switches are the primary devices for LACP?

A)

```
N7K_A(corf g^c-domains iyst#m~pnorit N7K Blconfig vpc domalni# systom-prlortt
```

B)

```
N7K_A(COCflp"Vpc* domain)^ jyitoni-prior*
MYK R^onfio-voc-domaini# svstem-orlortt
```

C)

```
N7K A(confio-vpc-domain)# lyitom-prlorl^
N7IVB?config-vpc-doma»n>* lystem-priori
```

D)

```
N7K_A(config-vpc-domain)# role priority 1
N7K_B(config-vpc-domain)# role priority 2
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To ensure that the Cisco Nexus 7000 series switches are the primary devices for LACP, the configuration must use the lacp system-priority command to assign a lower priority value to the switches. This command determines which device is the active partner in an LACP negotiation. The lower the priority value, the higher the preference. In option A, the switches have a priority value of 1, which is the lowest possible value and the highest preference. Therefore, option A is the correct configuration to make the switches the primary devices for LACP.

Reference := The explanation is based on the official Cisco documentation on Configuring Link Aggregation Control Protocol (LACP) 1, specifically the section on Configuring LACP System Priority.

Question: 110

A network engineer must enable port security on all cisco MDS series switches in the fabric. The requirement is to avoid the extensive manual configuration of the switch ports. Which action must be taken to meet these requirements?

A. Activate CFS distribution and the auto-learning port security feature.

B. Activate CFS distribution and file auto-learning port security feature on a per-VSAN basis.

C. Enable the auto-learning port security feature on a per-VSAN basis.

D. Enable the auto-learning port security feature.

Answer: B

Explanation:

To enable port security on all Cisco MDS series switches in the fabric and avoid the extensive manual configuration of the switch ports, the network engineer must activate the CFS (Cisco Fabric Services) distribution and enable the auto-learning port security feature on a per-VSAN basis. CFS is a protocol that allows the switches to distribute and synchronize configuration information across the fabric. By activating the CFS distribution for port security, the network engineer can propagate the port security configuration to all the switches in the fabric automatically, without having to configure each switch individually. The auto-learning port security feature allows the switches to learn and store the port security information of the devices that are already logged in and authorized on the ports, and prevent any unauthorized devices from logging in. The auto-learning port security feature can be enabled on a per-VSAN basis, which means that the port security information is specific to each VSAN and does not affect other VSANs. This provides more flexibility and granularity for the port security configuration. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 7: Data Center Storage Connectivity, Lesson 7.3: Fibre Channel Protocol

Cisco MDS 9000 Family NX-OS Security Configuration Guide, Chapter: Configuring Port Security

Question: 111

A network engineer is deploying a cisco ALL-flash hyperflex solution. Which local storage configuration is required for the operating system and persistent logging?

A. Two solid state drives

B. Two SATA drives

C. One SATA drive

D. One solid state drive

Answer: A

Explanation:

A Cisco All-Flash HyperFlex solution requires two solid state drives (SSDs) for the local storage configuration of the operating system and persistent logging. The SSDs are used to store the hypervisor, the HyperFlex controller VM, and the system logs. The SSDs also provide high performance and reliability for the system operations. The SSDs are configured in a RAID 1 mirror mode, which provides redundancy and fault tolerance. The SSDs are separate from the data storage drives, which are also SSDs in an All-Flash HyperFlex solution. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 4: Cisco HyperFlex, Lesson 4.1: Cisco HyperFlex Overview

Cisco HyperFlex Systems Installation Guide for Cisco Intersight, Chapter: Cisco HyperFlex System Requirements

Question: 112

An engineer configures the properties of a cisco UCS cisco integrated Management controller network adapter for a standalone cisco C-Series server. The Fallback Timeout in the vNIC was set to 600. When the failure occurs. The secondary must be used and then fallback when the primary interface becomes available again. Which action be taken to meet these requirements?

A. Set default VLAN on the adapters.

B. Increase Cos to 6.

C. Disable VNTAG mode.

D. Enable Uplink failover.

Answer: D

Explanation:

To meet the requirements of using the secondary interface and then falling back to the primary interface when it becomes available again, the engineer should enable the Uplink failover option in the vNIC properties of the Cisco UCS Cisco Integrated Management Controller (CIMC) network adapter for a standalone Cisco C-Series server. The Uplink failover option allows the vNIC to switch to the secondary interface in case of a failure in the primary interface, and then switch back to the

primary interface when it recovers. The Uplink failover option also allows the engineer to configure the Fallback Timeout value, which determines how long the vNIC waits before switching back to the primary interface. In this case, the Fallback Timeout value is set to 600 seconds, which means the vNIC will wait for 10 minutes before falling back to the primary interface. Reference :=

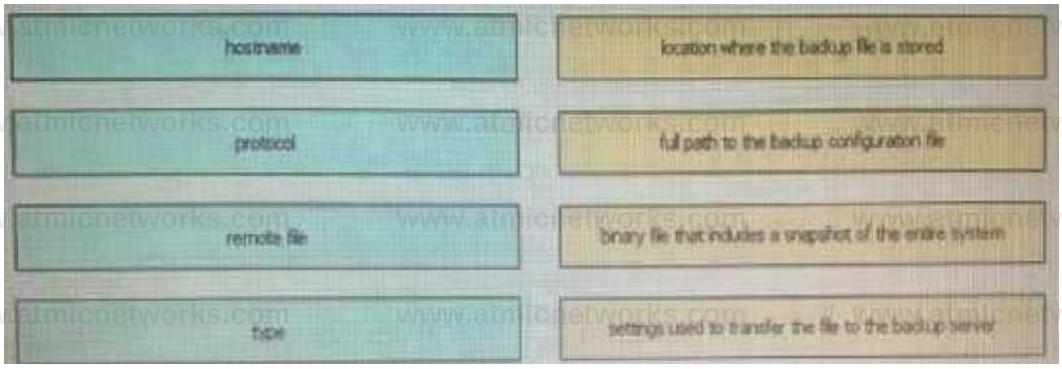
Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.3: Cisco UCS C-Series Servers

Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 4.0, Chapter: Configuring Network-Related Settings and Features, Section: Configuring vNICs

Question: 113

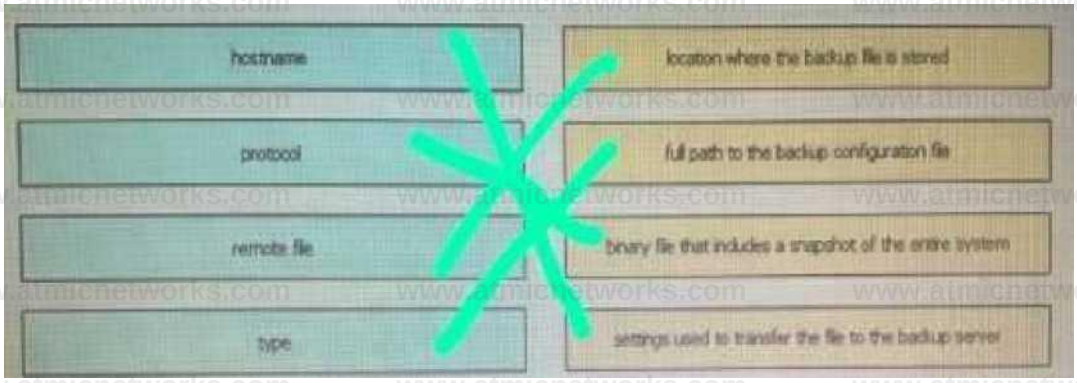
DRAG DROP

Drag and drop the fields for configuring a full state backup file of the Cisco UCS Manager from the left onto the descriptions on the right.



Answer:

Explanation:



Question: 114

A network engineer must prevent data comuption due to cross fabric communication in an FCoE environment. Which configuration must be applied to the Cisco Nexus Unified Switches to achieve this objective?

A. Switch(config)#fcoe fcmap 0e,fc,2a

B. Switch(config-if)# no fcoe fcf-priority 0

C. Switch(config-if) # shutdown lan

D. Switch(config) # no fcoe fcf-priority

Answer: A

Explanation:

To prevent data corruption due to cross fabric communication in an FCoE environment, the network engineer must apply the configuration Switch(config)#fcoe fcmap 0e,fc,2a to the Cisco Nexus Unified Switches. This configuration sets the FCoE MAC address prefix (fcmap) to a custom value of 0e,fc,2a, which is different from the default value of 0e,fc,00. The fcmap is used to identify the FCoE traffic and map it to the corresponding Fibre Channel ID (FCID). By using a custom fcmap, the network engineer can avoid the possibility of FCID conflicts or overlaps between different FCoE fabrics, which can cause data corruption or loss. The custom fcmap must be configured on all the switches in the same FCoE fabric, and must be unique across different FCoE fabrics. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 7: Data Center Storage Connectivity, Lesson 7.4: FCoE Protocol

Cisco Nexus 9000 Series NX-OS FCoE Configuration Guide, Release 9.3(x), Chapter: Configuring FCoE, Section: Configuring the FCoE MAC Address Prefix

2. switch(config)# fcoe fcmap *fabric-map*
3. (Optional) switch(config)# no fcoe fcmap *fabnc-map*

DETAILED STEPS

	Command or Action	Purpose
Step 1	switch# configure terminal	Enters configuration mode.
Step 2	switch(config)# fcoe fcmap *fabric-map*	Configures the global FC-Map The default value is OE.FC.OO. The range is from OE.FC 00 to OE.FC FF.
Step 3	switch(config)# no fcoe fcmap *fabric-map*	(Optional) Resets the global FC-Map to the default value of OE.FC.OO

This example shows how to configure the global FC-Map

switch# **configure terminal**

switch(config)# **fcoe fcmap 0e.fc.2a**

Question: 115

Which component is disrupted when the cisco integrated Management controller is upgraded on a cisco UCS series server?

A. Cisco UCS Manager

B. SAN traffic

C. KVM sessions

D. Data traffic

Answer: C

Explanation:

The Cisco Integrated Management Controller (IMC) is a system management component built into Cisco UCS C-Series servers. When the IMC is upgraded, it disrupts the Keyboard, Video, Mouse (KVM) sessions that are used for remote server management. This is because the IMC upgrade process requires a reboot of the controller, which temporarily disconnects any active KVM sessions. However, it does not affect Cisco UCS Manager, SAN traffic, or data traffic, as these

components operate independently of the IMC.

Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials and the Cisco Data Center Core Technologies source book.

Question: 116

A company is investigating different options for IT automation tools. The IT team has experience with python programming language and scripting using a declarative language. The proposed tool should be easy to set up and should not require installing an agent on target devices. The team will also need to build custom modules based on the python programming language to extend the tools functionality. Which automation tool should be used to meet these requirements?

A. Puppet

B. Ansible

C. NX-API

D. Chef

Answer: B

Explanation:

Ansible is an open-source IT automation tool that is easy to set up and does not require an agent to be installed on target devices. It uses a declarative language and can be extended with custom modules written in Python, which aligns well with the IT team's experience. Ansible's agentless architecture and support for Python make it an ideal choice for the company's requirements.

Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course

materials and the Cisco Data Center Core Technologies source book.

Question: 117

```
switch(config-dest)# sensor-group 100
switch(conf-tm-sensor)# path show_stats_fc3/1
switch(conf-tm-sensor)# subscription 100
switch(conf-tm-sub)#
switch(conf-tm-sub)# dst-grp 100
```

Refer to the exhibit. An engineer needs to implement streaming telemetry on a cisco MDS 9000 series switch. The requirement is for the show command data to be collected every 30 seconds and sent to receivers. Which command must be added to the configuration meet this requirement?

A. Sensor-grp 200 sample-period 30000

B. Snsr-grp 200 sample-interval 30

C. Sensor-grp 200 sample-period 30

D. Snsr-grp 200 sample-interval 30000

Answer: D

Explanation:

To meet the requirement of collecting show command data every 30 seconds and sending it to receivers, the command must specify the sample interval in milliseconds. Therefore, the correct command is Snsr-grp 200 sample-interval 30000, which sets the sample interval to 30,000 milliseconds (equivalent to 30 seconds).

Reference := The configuration details for streaming telemetry on a Cisco MDS 9000 series switch can be found in the Cisco MDS 9000 Series SAN Analytics and SAN Telemetry Streaming Configuration Guide1.

Question: 118

A cisco Nexus 9000 series switch experiences a startup configuration comuption. The engineer must implement a procedure to recover configuration file from the switch. Which command set must be used?

A.

1. Copy the running-configuration to the startup configuration.
2. Clear the current configuration of the switch.
3. Restart the device.
4. Copy a previously saved configuration file to the running configuration.

B.

1. Clear the current configuration of the switch
2. Restart the device.
3. Copy the running configuration to the startup configuration
4. Copy a previously saved configuration file to the running configuration

C.

1. Clear the current configuration of the switch
2. Restart the device.
3. Copy a previously saved configuration file to the running-configuration
4. Copy the running-configuration to the startup configuration.

D.

1. Restarting device.
2. Copy the running-configuration file to a remote server.
3. Clear the current configuration of the switch.
4. Copy the running configuration to the startup configuration

Answer: C

Explanation:

When a Cisco Nexus 9000 series switch encounters a startup configuration corruption, the recovery process involves clearing the current configuration, restarting the device, and then restoring the configuration from a previously saved

file. The correct sequence is to first clear the configuration to prevent the corrupted startup configuration from loading upon restart. After restarting the device, the previously saved configuration file should be copied to the running configuration. Finally, to ensure the switch starts with the correct configuration in future restarts, the running configuration should be saved to the startup configuration.

Reference: The recovery process is detailed in the Cisco community documentation, where it outlines the steps for recovering the configuration in UCS by importing the configuration from a previously saved location

Question: 119

An engineer must configure OSPF in the data center. The external routes have already been redistributed OSPF. The network must meet these criteria:

* The data centre servers must reach services in the cloud and the services behind the redistributed routes.

* The exit point toward the internet should be propagated only when there is a dynamically learned default route from the upstream router.

Which feature is required?

A. Default-information originate

B. Stubby area

C. Totally stubby area

D. Default-information originate always

Answer: A

Explanation:

The requirement for the data center servers to reach services in the cloud and services behind redistributed routes, along with the condition that the exit point toward the internet should only be propagated when there is a dynamically learned default route, necessitates the use of the 'defaultinformation originate' OSPF feature. This feature allows the advertisement of the default route in OSPF when it is present in the routing table, which is the case when it is dynamically learned from the upstream router.

Reference: The 'default-information originate' feature is part of OSPF configuration and is used to control the advertisement of default routes in an OSPF environment. This is further explained in the Cisco OSPF Configuration Guide, which details the use of this command to propagate default routes under certain conditions

https://learningnetwork.cisco.com/s/question/0D53i00000Kt544/defaultinformationoriginate- always

Question: 120

What is a characteristic of the install all command on the cisco Nexus series switch?

A. Upgrades only certain modules

B. Automatically checks the image integrity

C. Impact data plan traffic

D. Continues the upgrade process if any step in the sequence fails

Answer: B

Explanation:

A characteristic of the install all command on the Cisco Nexus series switch is that it automatically checks the image integrity before performing the installation. The install all command is used to install a system image and kickstart image on the switch, as well as to upgrade the BIOS and other
firmware components. The install all command performs a series of checks and validations before installing the images, such as verifying the compatibility, checksum, and signature of the images. This ensures that the images are not corrupted or tampered with, and that they match the hardware and software requirements of the switch. The install all command also performs a backup of the current configuration and images, and allows the user to abort the installation process if needed. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.4: Cisco Nexus 9000 Series Switches

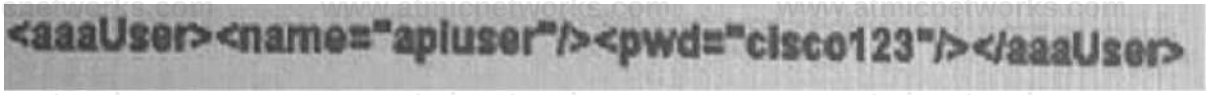
Cisco Nexus 9000 Series NX-OS System Management Configuration Guide, Release 9.3(x), Chapter: Installing Software Images and EPLDs, Section: Installing System and Kickstart Images

Question: 121

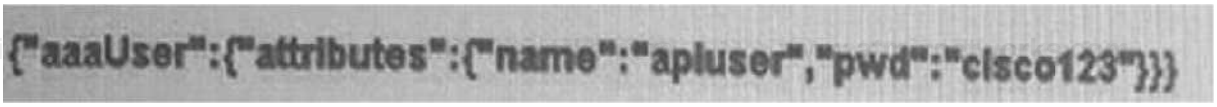
An engineer is using REST API calls to configure the cisco APIC. Which data structure must be used within a post message to receive a login token?

A)

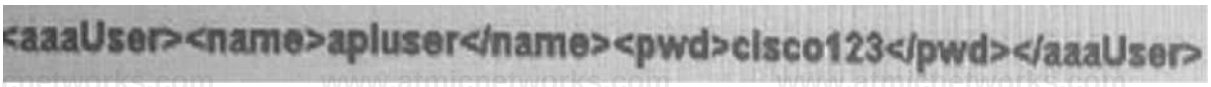
B)



C)



D)



A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

The correct data structure to use within a POST message to receive a login token when configuring the Cisco APIC via REST API calls is an XML payload that includes the <aaaUser> tags with nested <name> and <pwd> tags for the username and password. This structure is shown in Option A, which is the standard format for authentication requests to the Cisco APIC.

Reference := For more detailed information, please refer to the Cisco APIC REST API Configuration Guide, which provides comprehensive instructions on using REST API for system configuration, including authentication and token retrieval processes.

Question: 122

The EPLD update of the supervisor module has been scheduled for several cisco MDS 9000 switches. What will be the

impact of the update?

A. All control plane traffic is stopped for the duration of the EPLD update and the switch remain operational for the duration of the upgrade.

B. The redundant supervisor lakes over while the EPLD update is in progress and there is no service disruption.

C. All traffic is stopped for the duration of the EPLD update and the switch is rebooted after the upgrade is completed.

D. The redundant supervisor lakes while the EPLD update is in progress and the switch is rebooted after the upgrade is completed.

Answer: B

Explanation:

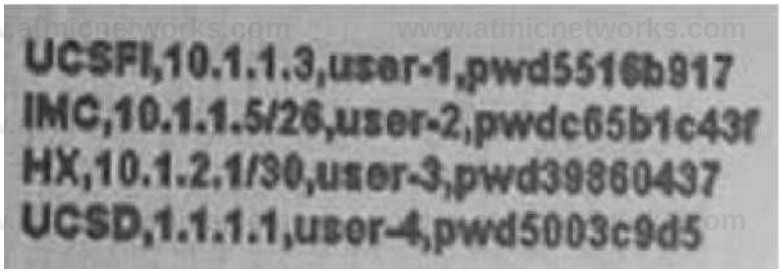
The impact of the EPLD update of the supervisor module on the Cisco MDS 9000 switches is that the redundant supervisor takes over while the EPLD update is in progress and there is no service disruption. EPLD (Electronic Programmable Logic Device) is a firmware component that controls the functionality of various hardware modules on the switch, such as the supervisor, line cards, and fabric modules. The EPLD update is performed to enhance the performance and features of the hardware modules, and to fix any bugs or issues. The EPLD update process requires a reload of the affected module, which can cause a temporary loss of connectivity and traffic. However, if the switch has a redundant supervisor module configured in high availability mode, the EPLD update can be performed without any service disruption. This is because the redundant supervisor takes over the control plane functions while the active supervisor is being updated, and then switches back to the active supervisor when the update is completed. The EPLD update does not affect the data plane traffic, as the line cards and fabric modules continue to forward packets during the update process.
Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 7: Data Center Storage Connectivity, Lesson 7.3: Fibre Channel Protocol

Cisco MDS 9000 Family NX-OS System Management Configuration Guide, Chapter: Installing Software Images and EPLDs, Section: Updating EPLDs

Question: 123

An engineer configures an intersight virtual application and must claim over 200 targets. The engineer starts the Claim target procedure. The engineer has prepared this initial comma- separated value file to provision the targets:



Which Information must be included In the comma-separated value flit to provision the targets?

A. FQON, AD name, IP address, email

B. location, address, name. password

C. certificate, user name, password. email

D. target type, hostname or P address, user name, password

Answer: D

Explanation:

When configuring an Intersight virtual application and claiming targets, the information required in the comma-separated value (CSV) file for provisioning includes the target type, hostname or IP address, user name, and password. This set of information is necessary to uniquely identify and authenticate each target for the claim process.

Reference := The requirements for the CSV file format for claiming targets in Cisco Intersight can be found in the official Cisco documentation on the Intersight Virtual Appliance and Intersight Assist Getting Started Guide

Question: 124

What is an advantage of NFSv4 over Fibre Channel protocol?

A. Improved security

B. Lossless throughout

C. Congestion management

D. Uses IP transport

Answer: A

Explanation:

NFSv4 offers several advantages over Fibre Channel protocol, one of which is improved security.
NFSv4 is designed to be more secure than its predecessors, providing strong security features that are not inherent in Fibre Channel. It includes mechanisms for authentication, integrity, and privacy, which are part of its standard protocol suite. NFSv4 also integrates well with security infrastructures like Kerberos, allowing for secure, authenticated access to file systems over a network.

Reference := Newer Is Sometimes Better: An Evaluation of NFSv4 - Stony Brook University, The Advantages of NFSv4.1 - SNIA on Network Storage

Question: 125

Which two configuration settings are available in the in the cisco UCS flmware Auto sync server policy?

A. User Notification

B. User Acknowledge

C. No Action

D. Delayed Action

E. Immediate Action

Answer: B, C

Explanation:

The Cisco UCS firmware Auto Sync Server policy includes several configuration settings that determine how and when firmware on servers is synchronized. The two available settings from the options provided are 'User Acknowledge' and 'No Action'. 'User Acknowledge' requires an administrator to manually acknowledge firmware upgrades in the Pending Activities dialog box before they are applied. 'No Action' means no firmware upgrade is initiated on the server. These settings allow administrators to control the firmware synchronization process according to their operational policies and procedures.

Reference := Using Firmware Automatic Synchronization Server Policy - Cisco, Cisco UCS B-Series CLI Firmware Management Guide, Release 2.2

Question: 126

An administrator is implementing DCNM so that events are triggered when monitored traffic exceeds the configured present utili zation threshold. The requirement is to configuration a maximum limit of 39860437 bytes that applies directly to the statistics collected as a ratio of the total link capacity. Which DCNM performance monitoring configuration parameter must be implemented to achieve this result?

A. Absolution Values

B. Baseline

C. Utill%

D. Per port Monitoring

Answer: C

Explanation:

The DCNM performance monitoring configuration parameter that must be implemented to achieve the result of triggering events when monitored traffic exceeds the configured percent utilization threshold is the Util% parameter. This parameter allows the administrator to set a utilization threshold as a percentage, which, when exceeded, triggers an event. The requirement to configure a maximum limit of 39860437 bytes directly relates to the statistics collected as a ratio of the total link capacity, which is effectively managed by setting the Util% parameter. This parameter is part of the Performance Manager Configuration Wizard in DCNM, which provides the ability to set up two thresholds that trigger events when the monitored traffic exceeds the percent utilization configured. These thresholds can be set as either Critical or Warning events that are reported on the DCNM-SAN web client Events browser page1.

Reference := Cisco DCNM Fundamentals Guide, Release 11.x

Question: 127

A network architect must redesign a data center on OSPFv2. The network must perform fast reconvergence between directly connected switches. Which two actions must be taken to meet the requirement? (Choose two)

A. Configure all links on AREA 0.

B. Implement a virtual link between the switches.

C. Use OSPF point-to-point links only.

D. Set low OSPF hello and DEAD timers.

E. Enable BFD for failure detection.

Answer: D, E

Explanation:

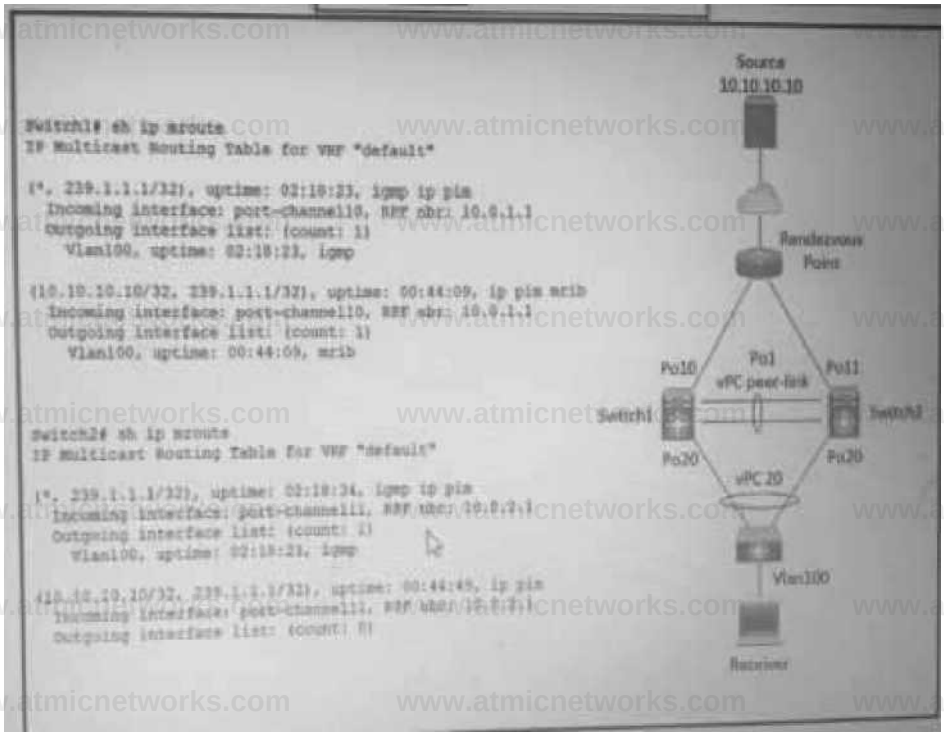
To achieve fast reconvergence between directly connected switches in a data center using OSPFv2, two critical actions must be taken. First, setting low OSPF hello and DEAD timers can significantly reduce the time it takes for OSPF to detect a link failure and start the reconvergence process. This is because OSPF hello packets are used to maintain neighbor relationships, and the DEAD timer determines how long a router will wait without receiving a hello packet before declaring the neighbor down. By reducing these timers, OSPF can detect failures more quickly and initiate a faster reconvergence.

Second, enabling Bidirectional Forwarding Detection (BFD) for failure detection is essential. BFD is a network protocol that provides fast failure detection times for all media types, encapsulations, topologies, and routing protocols. By implementing BFD, OSPF can be notified of link failures almost immediately, allowing for a rapid response to changes in the network topology and ensuring minimal disruption to data flows2.

Reference := IP Routing: OSPF Configuration Guide - OSPFv3 Fast Convergence

Question: 128

Refer to the exhibit.



Refer to the exhibit. A host with source address 10.10.10.10. sends traffic to multicast group 239.1.1.1. how do the vPC switches forward the multicast traffic?

A. If multicast traffic is received on Po11 Switch2, the traffic is forwarded out only one Po20.

B. If multicast traffic is received on Po10 Switch1, the traffic is forwarded out on Po1 and Po20.

C. If multicast traffic is received on Po11 and Switch2, the traffic is dropped.

D. If multicast traffic is received on Switch over the vPC peer-link, the traffic is dropped.

Answer: B

Explanation:

In a vPC (Virtual Port Channel) configuration, multicast traffic is handled based on the IGMP (Internet Group Management Protocol) and PIM (Protocol Independent Multicast) configurations. When a host sends traffic to a multicast group, the vPC switches determine the forwarding path based on the multicast routing table and the RPF (Reverse Path Forwarding) check.

Option B is correct because when multicast traffic with source address 10.10.10.10 targeting group 239.1.1.1 is received on Po10 Switch1, the switch will perform an RPF check and forward the traffic out of the interfaces that lead to the Rendezvous Point (RP) and the receivers. This ensures that the multicast traffic is efficiently distributed to all receivers that are part of the multicast group. The

traffic would be forwarded out on Po1, which is typically connected to the RP, and Po20, which connects to other receivers in the network.

Reference := For more detailed information on multicast traffic forwarding in a vPC environment, please refer to Cisco's official documentation on Implementing Cisco Data Center Core Technologies (DCCOR), specifically the sections discussing multicast routing and vPC configurations.

Question: 129

An engineer configured an environment that contains the vPC and non-vPC switches. However, it was noticed that the downstream non-vPC switches do not receive the upstream vPC switch peers. Which vPC feature must be implement to ensure that vPC and non-vPC switches receive same STP bridge ID from the upstream vPC switch peers?

A. vpc local role-priority 4000

B. peer-switch

C. system-mac 0123.4567.89ab

D. peer-gateway

Answer: B

Explanation:

To ensure that vPC and non-vPC switches receive the same STP bridge ID from the upstream vPC switch peers, the engineer must implement the peer-switch feature on the vPC domain. The peerswitch feature allows the two vPC peer switches to act as a single logical switch for STP purposes, and to use the same bridge ID and priority. This way, the downstream switches will see the vPC peer switches as a single STP root, and will not have any STP loops or inconsistencies. The peer-switch feature also improves the convergence time and reduces the number of STP instances required in the network.

Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.5: Cisco Nexus 7000 Series Switches

Cisco Nexus 7000 Series NX-OS Interfaces Configuration Guide, Release 6.x, Chapter: Configuring vPCs, Section: Configuring the Peer Switch Feature

Question: 130

A company is running a pair of cisco Nexus 7706 series switches as part of a data center segment. All network engineers have restricted read-Write access to the core switches. A network engineer must a new FCoE VLAN to allow traffic from services toward FCoE storage. Which set of actions must be taken to meet these requirements?

A.

1. Create a user defined role and add the required privileges.
2. Assign a role to a user.

B.

1. Add the required privilege to the VDC-admin role.
8. Commit the changes to the active user database.

C.

1. Modify a network-operator role and add the required privileges.
2. Assign a VDC-operator role to a user.

D.

1. Assign the network-admin role to a user.
2. Commit the role to the switch to the active user database

Answer: A

Explanation:

Create a user defined role and add the required privileges.

Assign a role to a user. Comprehensive and Detailed Explanation: = To meet the requirements of adding a new FCoE VLAN to the core switches with restricted read-write access, the network engineer must create a user defined role and assign it to a user. A user defined role is a custom role that can be created to grant specific privileges and permissions to a user, based on the tasks and functions they need to perform. A user defined role can be created using the role command, and then the required privileges can be added using the rule command. For example, to create a role

named FCoE-admin and add the privilege to configure FCoE VLANs, the following commands can be used:

role FCoE-admin rule 1 permit read-write feature fcoe rule 2 permit read-write feature vlan

After creating the user defined role, it can be assigned to a user using the username command. For example, to assign the FCoE-admin role to a user named John, the following command can be used:

username John role FCoE-admin

By creating and assigning a user defined role, the network engineer can ensure that the user has the minimum required privileges to perform the FCoE VLAN configuration, without granting them full network-admin access or modifying the existing roles. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.5: Cisco Nexus 7000 Series Switches

Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 6.x, Chapter: Configuring User Accounts and RBAC, Section: Configuring User-Defined Roles

Question: 131

Refer to the exhibit.

Refer to the exhibit. Esxi-server is associated to the blade server. A VLAN added to trunk-

a. the VLAN is missing on the vNIC of ESXI-server. Which action should be taken to add the VLAN to the cNIC?

A. Change the template type of ESXI-Server to an updating template.

B. Change the template type of Trunk-A to an updating template.

C. Remove both template and recreate them as updating templates.

D. Remove the VLAN from the Trunk-A template and add the VLAN again.

Answer: B

Explanation:

When a VLAN is added to a trunk and it does not appear on the vNIC of an associated server, it typically indicates that the vNIC template is not updating as it should to reflect changes. By changing the template type of Trunk-A to an updating template, any changes made to the trunk configuration, such as adding a new VLAN, will be dynamically applied to all vNICs associated with that template. This action will allow the newly added VLAN to be included in the vNIC configuration without the need to manually update each vNIC or recreate the templates.

Reference := This recommendation aligns with best practices for managing vNIC templates in Cisco UCS environments, where updating templates are used to ensure changes propagate automatically to all associated instances

Question: 132

An engineer must implement an automation solution to allow the backup of the configuration of cisco Nexus series switches to a centralized location. The solution must:

* Support the team-developed custom monitoring scripts that are packaged using RPM packaging that the framework must support.

* Be developed from the underlying cisco Nexus operating system.

* Have no impact on the operating system of the underlying switch if the resource contention occurs.

* Use Python to expand the existing automation framework.

Which solution meets these requirements?

A. Guest Shell

B. Bash Shell

C. TCL Shell

D. Vegas Shell

Answer: A

Explanation:

The solution that meets the requirements for implementing an automation solution to allow the backup of the configuration of Cisco Nexus series switches to a centralized location is the Guest Shell. The Guest Shell is a Linux-based container that runs on the Cisco Nexus operating system and provides a secure environment for running Python scripts and custom applications. The Guest Shell supports the RPM packaging format, which allows the team-developed custom monitoring scripts to be easily installed and managed. The Guest Shell is isolated from the underlying Cisco Nexus operating system, which means that it has no impact on the operating system if the resource contention occurs. The Guest Shell also allows the use of Python to expand the existing automation framework, such as using the NX-API or the Cisco Nexus Python SDK to interact with the switch configuration and state. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 8: Data Center Automation and Orchestration, Lesson 8.2: Cisco NX-OS Programmability

Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x), Chapter: Using Guest Shell

Question: 133

Refer to the exhibit.

Refer to the exhibit. What is the result of executing this python code?

A. It backs up Cisco switches to Cisco Prime infrastructure.

B. It sends the switch configuration to Cisco TAC.

C. It sends a Cisco device backup to a remote destination.

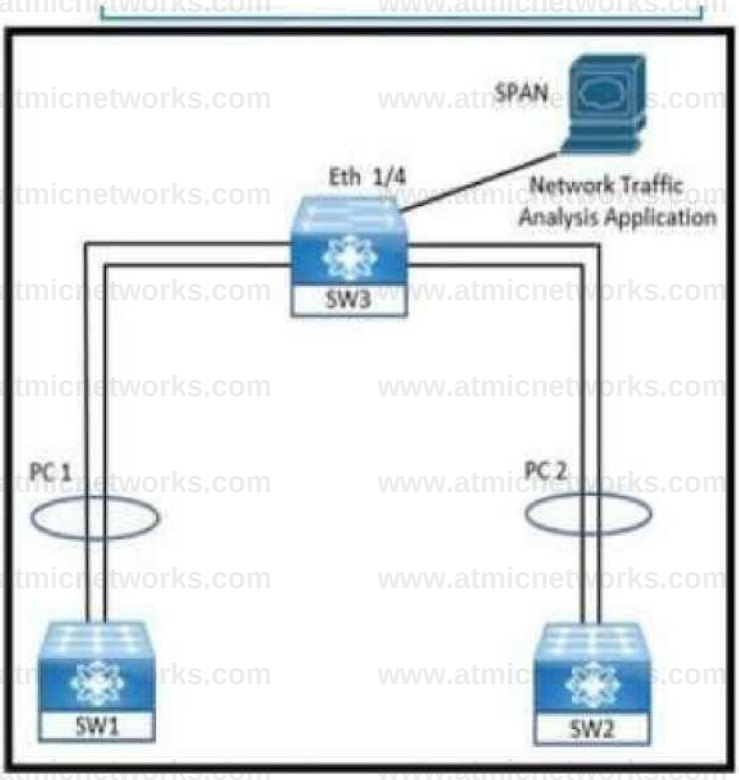
D. It schedules a backup on a Cisco switch using EEM.

Answer: C

Explanation:

Question: 134

Refer to the exhibit.



Refer to the exhibit. An engineer must monitor ingress traffic from SW1 and SW2 port-channel interfaces from SW3. Which configuration must be implemented to accomplish this goal?

A)

```
SW3» configure terminal
SW3tcorf>j;s tource interface port-channel 1 rx SM(caft) I* source Interface port-channel 2 u

SW^tCOnftjp interface ethornet IM
SW3(cor*g-if)I destination interface ethornet IM
§WXcor*sj-rfj* exit

$A?(corf :^ interface Pert-channel 1-2
SW3(confiQ-if j* twitch port monitor
SW3(COr*9if )# exit
```

B)

```
SW?4 configure terminal
$w3(cQMQ)* monitor eettion 2
SW^confiQ-r • ' 'XI source interface port-channel 1 Ct SW^config-monitorx* source interface port-channel 2 Ct

5WJicvfig)a Interface Port-channel 1 SWXconiiQ-il)P twitchport monitor SWXcortv if)* exit

$WK< ,<;X interface Port-channel 2 SWJfCOnfig if)* twitchport monitor $W]|ctrtiglp exit
```

C)

```
SW3# configure terminal
SW^egrdtg)* monitor session 2
SWAcorr^-mantorXt source interface port-channel 1 tx Sw3lcor*9 moMixxt source interface port-channel 2 n

SWXconfig)* Interface port-channel 1
$W3icort»j.if)* switchport monitor
$W3(cor*9 if )• exit

SWx:." ;;»interface port-channel 2 SWStcanhg if)* switchport monitor ^.-W3(corf g-if )* exit
```

D)

```
$W3# configure terminal
SW^corik ,x monitor session 2
SW^confi-j-mcrutrir.i; source interface port-channel 1 rx $WJ(COnf»}-monitor a source interface port-channel 2 rx

$W3(conhgi* Interface ethornet IM 5WJJ : W^-#)» twitchport monitor $WJ(cor*9-<)* exit

SW3( config)* monitor tettion 2
SW3(conf^moncor o destination Interface ethornet IM
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

To monitor ingress traffic from SW1 and SW2 port-channel interfaces from SW3, the engineer must implement a configuration that specifies the source interfaces for monitoring and the destination interface where the monitored traffic will be sent. The correct configuration is found in Option D, which includes the commands to create a monitor session, specify the source interfaces as portchannel 1 and port-channel 2 with the 'rx' option to indicate ingress traffic, and set the destination interface to Ethernet 1/4 where the traffic can be analyzed. This setup uses a Switched Port Analyzer (SPAN) or Remote SPAN (RSPAN) to capture and forward the traffic for monitoring purposes.

Reference := The configuration aligns with Cisco's best practices for setting up SPAN or RSPAN sessions for traffic monitoring as detailed in the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials and Cisco's official documentation

Question: 135

An engineer implements an ACI fabric and must implement microsegmentation of endpoints within the same IP subnet using a network-based attribute. The attribute mapping must allow IP subnet independence. Which attribute must be selected?

A. MAC address

B. Custom

C. Tag

D. IP

Answer: C

Explanation:

The attribute that must be selected to implement microsegmentation of endpoints within the same IP subnet using a

network-based attribute that allows IP subnet independence is the Tag attribute. The Tag attribute is a user-defined attribute that can be assigned to endpoints based on any criteria, such as location, function, or security level. The Tag attribute can be used to create microsegmentation policies in ACI, which define the rules for communication between endpoints within the same or different bridge domains. The Tag attribute enables IP subnet independence, which means that the microsegmentation policies are not tied to the IP subnet of the endpoints, and can be applied across different subnets or even different fabrics. The Tag attribute also simplifies the management and scalability of microsegmentation policies, as it does not require the use of IP addresses or MAC addresses to identify endpoints. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 6: Data Center Network Connectivity Design, Lesson 6.2: Cisco ACI Overview and Concepts

Cisco Application Centric Infrastructure Fundamentals, Chapter: Endpoint Groups and Microsegmentation, Section: Microsegmentation Using Tags

Question: 136

An engineer is configuring a vHBA template in Cisco UCS Manager. The engineer needs to specify the logical addresses used by the vHBA and the path through which the SAU Traffic flows. Which two resources must be specified in the vHBA template? (Choose two)

A. WWIN
B. VLAN ID
C. Fabric ID
D. MAC addresses
E. WWVPN Pool

Answer: A, C

Explanation:

When configuring a vHBA template in Cisco UCS Manager, the engineer needs to specify the logical addresses used by the vHBA and the path through which the SAN traffic flows. The two resources that must be specified in the vHBA template are the WWN (World Wide Name) and the Fabric ID. The WWN is a unique identifier for the vHBA that is used for zoning and LUN masking in the SAN environment. The WWN can be assigned manually or automatically from a

WWN pool. The Fabric ID is a parameter that determines which fabric interconnect (A or B) the vHBA is associated with. The Fabric ID can be set to a specific value or to 'default', which allows the system to choose the best available fabric interconnect based on the availability and load balancing policies. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.2: Cisco UCS B-Series Connectivity

Cisco UCS Manager GUI Configuration Guide, Release 4.0, Chapter: Configuring SAN Connectivity, Section: Creating vHBA Templates

Question: 137

An engineer must configure a VXLAN routing on a cisco Nexus 9000 series Switch. The engineer requires a solution where all the leaf switches have the same gateway MAC and IP address. Which configuration set accomplishes this task?

A)

```
NX9K(cortg)* fabric forwarding anycaat-gataway-mac AABBMBBAABB
NX9K(corif>gp interfact VLAN jrtttrfact-namtNxSKJconhg-rfp fabric forwarding moda anycast-gateway
```

B)

```
NX$K(cortigP fabric forwarding anycast-gateway-mac AA BB AA BB AABB Nx9K(coci6g)#
interface VLAN-tnterf ace-name
Nx9»qconfig-''J# vrf momber vrf-namo
Nx9K|cofrf>g- ')* fabric forwarding mode anycast-gateway
```

C)

```
NXdKJcortgp instill foaturo-sot fabric
NX9K(c0fd)g)* foaturo-sot fabric
MX9K(co^g)# fabric forwarding anycast-gatoway-mac AA BBAA BBAABB
Mx9K|cor* g)® intorfaco VLAN-intorfaco-n am o
NXSKiconfig^)# vrf mombor vrf-namo
NXSK(COnf)g*<f)* fabric forwarding mode anycast-gatoway
```

D)

```
Nx9K(configp install foaturo-sot fabric
NXBK(coflftgP foaturo «st fabric
```

NX9K(C0flhgP**fabric forwarding anycast gatoway-mac AA BB AA BB AABB**
NX9K(corf)g)d **intorfaco VLAN-intorfaco-namo**
N <9K(conf>g-'i# **fabric forwarding modo anycast-gatoway**

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

For VXLAN routing on a Cisco Nexus 9000 series switch where all leaf switches share the same gateway MAC and IP address, the configuration must enable the anycast gateway feature. This is achieved by setting the fabric forwarding anycast-gateway-mac to a common MAC address across all leaf switches and configuring the VLAN interface with the fabric forwarding mode anycastgateway command. Option D provides the correct set of commands to accomplish this task, ensuring that the leaf switches can route traffic using the same gateway MAC and IP address, which simplifies the network design and eases the management of the VXLAN overlay.

Reference := The configuration steps are aligned with Cisco's best practices for VXLAN routing as described in the Cisco documentation and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials, which detail the process of setting up VXLAN and using anycast gateways

Question: 138

Which virtual MAC address is the default for HSRP version 2 group 10?

A. 0000.5E00.0110

B. 0000.0C9F.F00A

C. 3716.1350.1C0A

D. 0000.0C9F.F010

Answer: B

Explanation:

The virtual MAC address that is the default for HSRP version 2 group 10 is 0000.0C9F.F00A. HSRP (Hot Standby Router Protocol) is a protocol that provides redundancy and load balancing for IP networks by allowing multiple routers to share a virtual IP address and MAC address. HSRP version 2 supports up to 4096 groups, and uses a different MAC address format than HSRP version 1. The MAC address format for HSRP version 2 is 0000.0C9F.FXXX, where XXX is the hexadecimal value of the group number. For group 10, the hexadecimal value is 0A, so the MAC address is 0000.0C9F.F00A. Reference := Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.6: Cisco Nexus 5000 Series Switches

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide, Release 5.2(1)N1(1), Chapter: Configuring HSRP, Section: HSRP Version 2 edge browser The user has the page open in a Microsoft Edge browser window whose metadata is:

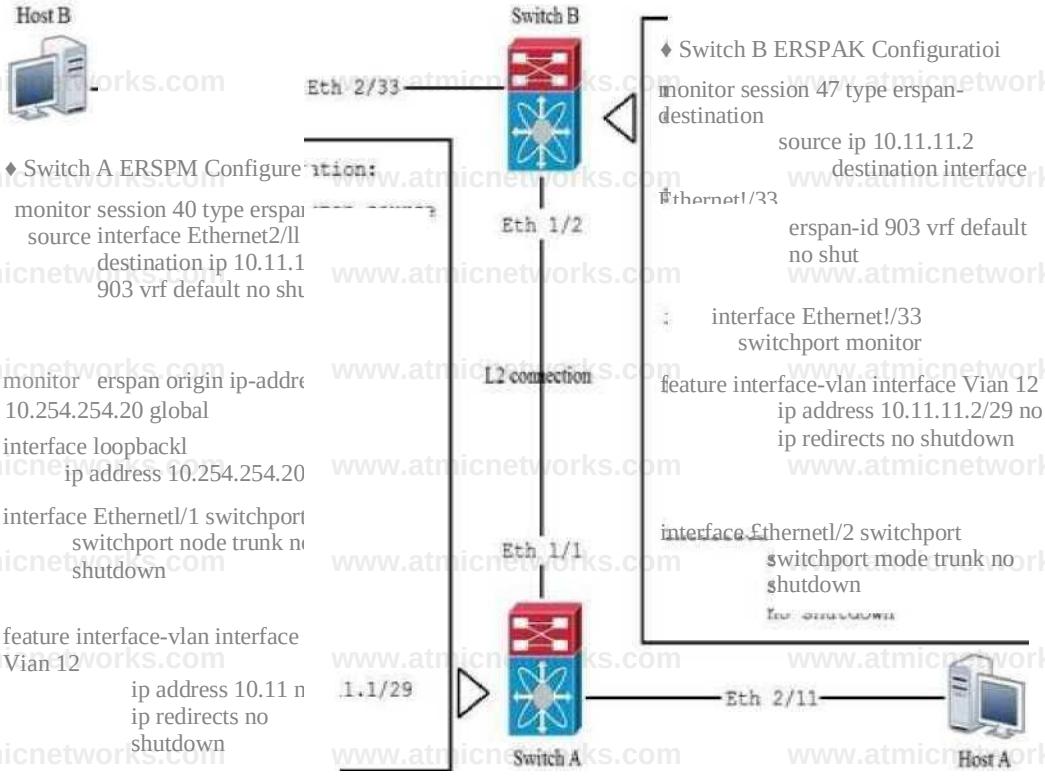
JSON 0

<EWPTY>

A jenerat^code. Re-. ^ a'-z js&caf^ More nfo on FAQ

Question: 139

Refer to the exhibit.



Which statement about the ERSPAN configuration in this environment is true.

A. Host A is the source of ERSPAN spanned traffic and host B is the traffic analyzer.

B. Host B is the source of ERSPAN spanned traffic and host A is the traffic analyzer.

C. The session number of the source of ERSPAN spanned traffic must have a session ID of 48 for the traffic analyzer to receive the traffic.

D. The session number of the source of ERSPAN spanned traffic must have a session ID of 47 for the traffic analyzer to receive the traffic.

Answer: B

Explanation:

In the ERSPAN configuration provided, Host B is connected to Switch A and is configured as the source of the ERSPAN spanned traffic. This is indicated by the configuration on Switch A, which includes the command monitor session 48 type erspan-source, specifying that it is sending ERSPAN traffic to a destination. The destination IP address for this traffic is set to 10.11.11.2, which corresponds to Host A's interface VLAN12 IP address. Therefore, Host A, connected to Switch B, is the traffic analyzer, receiving the spanned traffic from Host B.

Reference := The explanation is based on the standard ERSPAN configuration practices where the source switch is configured with a session type of 'erspan-source' and the destination switch with 'erspan-destination'. This information is typically covered in Cisco's documentation on ERSPAN configurations and the Cisco Data Center Core Technologies (DCCOR) course materials.

Question: 140

Refer to the exhibit.

```
ACI-Leafl# show ip route vrf DATACENTER:DC
A.  .20.1.0/24, ubest/mbest: 1/0, attached, direct, pervasive
    *via 10.0.8.65%overlay-l, [1/0], 4w3d, static
B.  2.16.100.0/24, ubest/mbest: 1/0
    *via 10.1.168.95%overlav-l, [200/5], 3wod, bgp-132, internal, tag 132 (mpls-vpn)
C.  2.16.99.0/24, ubest/mbest: 1/0
    *via 10.0.1.14, [20/0], 3wod, bgp-132, external, tag 200
```

Which two statements about the routing table of the leaf switch are true? (Choose two.)

A. The next hop 10.0.1.14 for route 172.16.99.0/24 is the TEP address of a border leaf in ACI.

B. 172.16.100.0/24 is a BD subnet in ACI.

C. The next hop 10.0.8.65 for route 10.20.1.0./24 is the TEP address of a border leaf in ACI.

D. The next hop 10.1.168.95 for route 172.16.100.0/24 is the TEP address of a border leaf in ACI.

E. 10.20.1.0./24 is a BD subnet in ACI.

Answer: A, D

Explanation:

In the context of Cisco ACI (Application Centric Infrastructure), TEP (Tunnel Endpoint) addresses are used for encapsulating and forwarding traffic within the fabric. The next hop addresses mentioned in options A and D are indicative of TEP addresses, which are typically assigned to border leaf switches within the ACI fabric. These border leaf switches are responsible for routing traffic between the ACI fabric and external networks.

Option A is correct because the next hop 10.0.1.14 for the route 172.16.99.0/24 is consistent with the TEP address format used in ACI, suggesting it is the TEP address of a border leaf.

Option D is also correct as the next hop 10.1.168.95 for the route 172.16.100.0/24 follows the TEP address pattern, indicating it is the TEP address of another border leaf in ACI.

Question: 141

Which mroute state is created when Bidirectional PIM is deployed at a site?

A. MVPN Type-6

B. *,G

C. MVPN Type-7

D. S,G

Answer: B

Explanation:

Bidirectional PIM is designed for scenarios where there are many sources and receivers that need to communicate with each other, such as in videoconferencing. Unlike traditional PIM sparse mode, which creates both (,G) and (S,G) entries, Bidirectional PIM only allows the (*,G) entry for the shared tree and does not build an (S,G) entry. This approach reduces the number of mroute state entries, conserving resources. Traffic can flow up and down the shared tree in Bidirectional PIM, and there is no RPF check; instead, a Designated Forwarder (DF) is used to prevent loops. Reference := Multicast Bidirectional PIM - NetworkLessons.com

Question: 142

Refer to the exhibit.

```
N7K-1 interface Vlan165 no shutdown no ip redirects ip address
10.16.165.2/27 no ipv6 redirects hsrp version 2 hsrp 165 preempt priority
150 ip 10.16.165.1

vpc domain 100 role priority 100 peer-keepalive destination 10.1.1.2
source 10.1.1.1 vrf default
  delay restore 60 peer-gateway auto-recovery ip arp synchronize
```

```
N7K-2 interface Vlan165 no shutdown no ip redirects ip address
10.16.165.3/27 no ipv6 redirects hsrp version 2 hsrp 165 priority 50 ip
10.16.165.1

vpc domain 100
  role priority 200 peer-keepalive destination 10.1.1.1 source 10.1.1 2
vrf default
  delay restore 60 peer-gateway auto-recovery ip arp synchronize
```

Which statement describes the default gateway configuration of the vPC?

A. N7K-1 acts as the default gateway for all traffic.

B. N7K-2 forwards traffic that is destined for the default gateway by using the peer link.

C. N7K-2 acts as the default gateway for all traffic.

D. Either switch can act as the active default gateway.

Answer: D

Explanation:

https://community.cisco.com/t5/networking-documents/peer-gateway-feature-on-the-nexus- 7000/ta-p/3113290

Question: 143

Refer to the exhibit.

```
Start time: Mon Apr 15 09:23:01 2019
Last election time: Mon Apr 15 09:24:24 2019
A: UP, PRIMARY
B: UP, SUBORDINATE
A: memb state UP, lead state PRIMARY, mgmt services state: UP
B: memb state UP, lead state SUBORDINATE, mgmt services state: UP heartbeat state PRIMARY_OK
INTERNAL NETWORK INTERFACES:
eth1, UP
eth2, UP
HA NOT READY
No device connected to this Fabric Interconnect
```

What be connected to clear the HA NOT READY status?

A. server chassis

B. network uplinks

C. management ports

D. Layer 1-Layer 2 ports

Answer: C

Explanation:

The HA NOT READY status on a Cisco Fabric Interconnect typically indicates that the system is not in a state to provide High Availability due to certain connectivity issues. In this case, the status message "No device connected to this Fabric Interconnect" suggests that there is no connectivity through the management ports. Establishing a connection through these ports is essential for the Fabric Interconnect to communicate with other devices in the network and form a High Availability cluster. Once the management ports are connected and properly configured, the HA NOT READY status should be resolved.

Reference := This explanation is based on standard procedures for addressing High Availability issues in Cisco Data Center environments, as outlined in Cisco's technical documentation and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials

Question: 144

A small remote office is set to connect to the regional hub site via NSSA ASBR. Which type of LSA is sent to the remote office OSPF area?

A. type 7 LSA

B. type 3 LSA

C. type 1 LSA

D. type 5 LSA

Answer: A

Explanation:

In an OSPF Not-So-Stubby Area (NSSA), external routes can be introduced into the area by an NSSA Autonomous System Boundary Router (ASBR) as type 7 LSAs. These LSAs are unique to NSSA areas and allow for the injection of external routes in a limited fashion. An NSSA Area Border Router (ABR) then translates these type 7 LSAs into type 5 LSAs, which are propagated throughout the OSPF domain. Reference := Configure the OSPF Not-So-Stubby Area (NSSA) - Cisco

Question: 145

Refer to the exhibit.

```
N7K-1 spanning-tree vlan 1-10 priority 8192

vpc domain 100
  role priority 100
  peer-keepalive destination 10.1.1.2 source 10.1.1.1 vrf default
  delay restore 60
  peer-switch auto-recovery ip arp synchronize

N7K-2
spanning-tree vlan 1-10 priority 8192

vpc domain 100
  role priority 200
  peer-keepalive destination 10.1.1.1 source 10.1.1.2 vrf default
  delay restore 60
  peer-switch auto-recovery ip arp synchronize
```

The STP priority of N7K-1 and N7K-2 are the lowest in the network. Which statement describes STP on the vPC?

A. N7K-1 appears as the STP root.

B. N7K-2 appears as the STP root.

C. N7K-1 and N7K-2 appear as a single STP root.

D. N7K-1 preempts N7K-2 as the STP root.

Answer: C

Explanation:

In a vPC configuration, both Nexus switches (N7K-1 and N7K-2) are designed to work together to present themselves as a single logical entity to downstream devices. This design allows for a loop- free topology without the need for Spanning Tree Protocol (STP) to block any of the ports to prevent

loops. As a result, both N7K-1 and N7K-2 share the same STP priority, making them appear as a single STP root to the rest of the network. This approach enhances the use of available bandwidth and provides redundancy without relying on STP to resolve loops.

Reference := The principles of vPC and its interaction with STP are well documented in Cisco's technical literature, including the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials1. For a more detailed explanation, please refer to these resources.

Question: 146

Refer to the exhibit.

```
switch(config)# interface Ethernet 2/2
switch(config)# ip address 172.23.231.240/23
switch(config)# ip verify unicast source reachable-via rx
```

What is configured as a result of running these commands?

A. reverse lookup for outbound packets

B. strict unicast RPF

C. loose unicast RPF

D. IP Source Guard

Answer: C

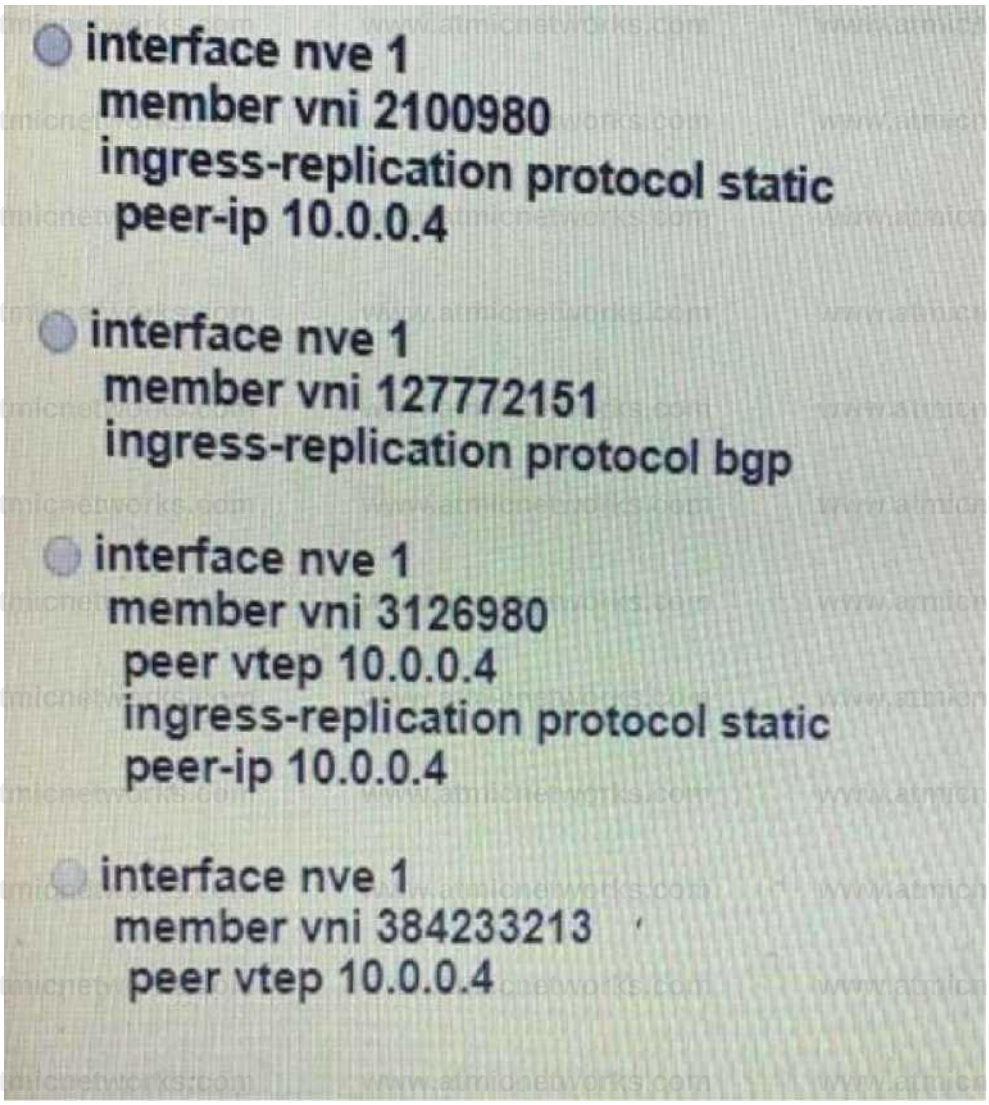
Explanation:

The commands shown in the exhibit configure Unicast Reverse Path Forwarding (uRPF) in loose mode on the interface Ethernet 2/2. The ip verify unicast source reachable-via rx command enables uRPF to check that the source address of a received packet has a route in the routing table and that the packet has been received from a valid interface that aligns with the routing table. This helps prevent IP spoofing by ensuring that packets are received from the expected interface.

Reference := This explanation is based on the principles of uRPF as described in Cisco's security configuration guides and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials. For more detailed information, please refer to these resources.

Question: 147

Which configuration implements static ingress replication?



A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Static ingress replication is a method used in VXLAN environments where the replication of multicast, broadcast, and unknown unicast traffic is manually defined. In the context of Cisco Data Center Core Technologies, Option A implements static ingress replication by explicitly specifying peers for replication using the ingress-replication protocol static command followed by the peer- ip command to define the IP address of the replication peer. This configuration is necessary when multicast routing is not an option in the underlay network.

Reference := For further details, one would typically refer to Cisco's official documentation on VXLAN configurations and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) study materials, which provide in-depth explanations on the setup and management of network overlays including static ingress replication.

Question: 148

Refer to the exhibit.

```
OTV-Sitel# show otv
OTA[7] Overlay Information
Site Identifier 0000.0000.0111
Overlav interface Overlay200
VPN name: Overlay200
VPN state: UP
Extended vlans: 178 2500-2563 (Total:65)
Join interface(s): Ethl/2 (20.1.1.1)
Site vlan: 1999 (up)
AED-Capable: Yes
Capability: Unicast-Only
Is Adjacency Server: Yes
Adjacency Server(s): 20.1.1.1 / 20.2.1.1
```

A network engineer is setting up a multihomed OTV network. The first site has been set up with a primary and secondary adjacency server. Which configuration must be added on the remote OTV AEDs site?

A. interface Overlay200

otv join-interface Ethernet1/2

otv extend-vlan 178, 2500-2563

otv use-adjacency-server 20.1.1.1 unicast-only

B. interface Overlay200

otv join-interface Ethernet1/2

otv extand-vlan 178, 2500-2563

otv adjacency-server unicast-only

C. interface Overlay200

otv join-interface Ethernet1/2

otv extend-vlan 178, 2500-2563

D. interface Overlay200

otv join-interface Ethernet1/2

otv extend-vlan 178, 2500-2563

otv use-adjacency-server 20.1.1.1 20.2.1.1 unicast-only

Answer: D

Explanation:

In a multihomed OTV network, it is essential to configure the remote OTV AEDs (Authoritative Edge Devices) to use both the primary and secondary adjacency servers for redundancy and resiliency. The correct configuration, Option D, includes the otv use-adjacency-server command with both IP addresses of the primary and secondary servers followed by unicast-only, which indicates that the AEDs should use unicast connections to the adjacency servers instead of multicast.

Reference := This configuration aligns with best practices for setting up OTV networks as described in Cisco's Data Center Core Technologies documentation. For a more comprehensive understanding, refer to the study materials related to OTV configurations in the Cisco Data Center Core Technologies (DCCOR) course.

Question: 149

A customer has a requirement to deploy a cloud service and needs to have full control over the underlying OS, data and application. Which cloud model meets this requirement?

A. PaaS

B. MaaS

C. IaaS

D. SaaS

Answer: C

Explanation:

The cloud model that meets the requirement of having full control over the underlying OS, data and application is Infrastructure as a Service (IaaS). IaaS is a cloud service model that provides the customer with access to virtualized computing resources, such as servers, storage, and networks, over the internet. The customer can install, configure, and manage the OS, data, and application of their choice on the rented infrastructure, without having to worry about the maintenance or security of the physical hardware. IaaS offers the customer the highest level of flexibility and control over their cloud environment, compared to other cloud models such as Platform as a Service (PaaS) or Software as a Service (SaaS). Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 8: Data Center Automation and Orchestration, Lesson 8.3: Cisco Cloud Services

Cisco Cloud Computing - IaaS

Question: 150

Refer to the exhibit.

```
Nexus- show vpc peer keeper | i Keepaks e
-Keepalive interval: 1000 msec
—Keepalive timeout: 5 seconds
-Keepalive hold timeout 3 seconds
-Keepalive vrf: nianapetnent
-Keepalive udp pan ; 3'00
-Keepalive Ms; 192

Senna ethanals rrr local Interface mput kmit captured frames 1000

Capninny on niptrtu
2019-06-15 I2:O1:51J42S97 192.168 254.11 -> 192.168.254.3ICMP Echo(p«ig)request
2019-06-15 12:01:51 242860 192.168 254.3 ■> 192.168 2 54 ]| ICMP Echo I print ireph
2019-06-15 11:50:15.9'54'4 192.168 254.1 -> 192.168 254.3 TCP 47540 - bootps [SYN] SopO Win* 1024 LenO MSS 1460
2019-06-15 11:50:15.9'554' 192.168254.3-> 192.168254 1 TCP 29 > 4'540 (RST A CK] Seq=I Ack=I Win-0LCB=0
2019-06-15 11:50:15.9'5564 192.168 254.1 -> 192 168.2543 TCP 47540 >44 |SYN] Seq=0 Wtn=1024 Len=0 MSS=14<0
2019-06-15 11:50:15.9*5924 192.168 254.1 -> 192 168 254 3 TCP 4'540 > discard JSYTq Seq=0 Wm=1024 Leu=0 MSSM460
2019-06-15 11:50:15.9'602' 192.168.251.1 -> 192 168.2543 TCP 17540>97 [SYN] Seq=O Wtn=1024 Len=0 MSS=I 160
2019416-15 11:50:15.9'6381 192.168.254.1 -> 192 168254 3 TCP 175 to >35 |SYN] Seq=4) Wrii=1024 I.en=0 MSS--116O
2019416-15 11:50 16 661845 1 92,168,254.3 ■> 192 168254 4 UDP Source port 3200 Destination port 3200
2019-06-15 11:50:16 '61147 OO.8e '3:a2 41:13 ->01:80x2 00:00.00 SI? Conf Root - 819210 ec:el4i9:df:6c:S0CoH " 22 Port 0x8013
2019-06-15 11:50:16.853248 192.168.254.4 •> 192 1682543 UDP Source port: 3200 Destination port: 3200
2019-06-15 11:50:17326253 192.168 254.1 -> 192.168254 3 SSHEncnplcd request packet len 52
2019-06-15 11:50:17.32'313 192.1682 543 - • 192.168254 1 SSHEncnpfed response packet len= 1348
2019-06-15 11:50:1'3''246 192.168.254.4 - • 239.255 70.83 UDP Source port: 7546 Destination port; 7546
20)94)6-15 11:50:17.552215 192.168.254.1 -> 192.168254.3 TCP 14139 >ssh [ACK] Seq=365 Ack=I 1277 Win=63546L«=0
20194)6-15 11:50:17 661764 192.168254.3 -> 19'168254 4 UDP Source port: 3200 Destination port: 3200
```

2019-06-15 11:50 17 653212 192.168 254.4 ■> 192.1682543 UDP Source port. 3200 Destination port 3200
20194)6-15 11:50 17 8'263 7 8c 60 4f:aac2:e! ->01 80 e*:00:00 OeLIDP Chassis d = 8c 60.4l ;u c2 el Port Id = msmtO HI = 120
20194)6-15 11:50:08.173056 192.168 256.3 ■> 192 168 254 2 NT? NTP client
20194)6-15 11:50:03 1'3256 192 168 2562 -> 192.168254.3 NT? NTP server

A flapping link issue has been reported on the vPC keepalive link. A packet capture has been activated on the Cisco Nexus switch. What is the destination IP address of the vPC keepalive packets that are sent by the switch?

A. 192.168.254.4

B. 239.255.70.83

C. 192.168.254.1

D. 192.168.254.2

Answer: C

Explanation:

The destination IP address for the vPC keepalive packets sent by the switch is 192.168.254.1. This is indicated in the packet capture output, where ICMP Echo (ping) requests are being sent to this address as part of the keepalive mechanism to ensure the vPC peer link is operational.

Reference := For more detailed information on vPC keepalive configuration and troubleshooting, the Cisco Data Center Core Technologies study materials and official Cisco documentation should be consulted. These resources provide comprehensive guidance on managing and maintaining vPC connections.

Question: 151

Refer to the exhibit.

```
restart pirn
```

Which result of running the command is true?

A. The PIM database is deleted.

B. Multicast traffic forwarding is suspended.

C. PIM join messages are suspended.

D. MRIB is flushed

Answer: C

Explanation:

The command in question is likely to temporarily suspend the Protocol Independent Multicast (PIM) join messages. This

action does not delete the PIM database or flush the Multicast Routing Information Base (MRIB), nor does it suspend multicast traffic forwarding. Instead, it interrupts the PIM join messages, which are used to build and maintain the multicast distribution tree.

Reference := For an in-depth explanation, one should refer to the Cisco Data Center Core Technologies study materials, which cover the PIM protocol and its behaviors in detail.

Question: 152

Refer to the exhibit.

```
Nexus(config)# show checkpoint summary
User Checkpoint Summary

1)  BeforeL3:
Created by admin
Created at Mon, 15:25:08 31 Dec 2018
Size is 9,345 bytes
Description: None

System Checkpoint Summary

2)  system-fm-vrrp:
Created by admin
Created at Fri, 09:57:02 14 Jun 2019
Size is 20,865 bytes
Description: Created by Feature Manager.

3)  system-fm-hsrp_engine:
Created by admin
Created at Fri, 09:57:28 14 Jun 2019
Size is 20,852 bytes
Description: Created by Feature Manager.
```

What is the reason the system-fm-vrrp checkpoint was created?

A. The VRRP service restarted and the checkpoint was automatically created.

B. The network administrator manually created it.

C. The VRRP process crashed and the checkpoint was automatically created.

D. The VRRP-enable feature has been disabled.

Answer: B

Explanation:

The checkpoint named “system-fm-vrrp” was created by an admin, as indicated by the description “Created by Feature Manager.” This suggests that it was a deliberate action rather than an automatic response to a service restart or crash. Checkpoints in Cisco systems can be manually created for various reasons, such as before making significant changes to the configuration, which allows for a rollback to a known good state if necessary.

Reference := For more information on the creation and management of checkpoints in Cisco systems, one should refer to the Cisco Data Center Core Technologies documentation and study materials, which provide detailed procedures and best practices.

Question: 153

What are two capabilities of the Cisco Network Assurance Engine? (Choose two.)

A. It verifies the speed of network packet flows by using telemetry.

B. It predicts the network load on a data center.

C. It validates that devices comply with network security policies.

D. It ensures that network performance meets an SLA.

E. It predicts the impact of changes to the network.

Answer: C, E

Explanation:

Two capabilities of the Cisco Network Assurance Engine are that it validates that devices comply with network security policies and that it predicts the impact of changes to the network. The Cisco Network Assurance Engine is a software solution that uses mathematical modeling and verification techniques to continuously analyze the state and configuration of the data center network. It can validate that the network devices are compliant with the intended security policies, such as access control lists, firewall rules, and encryption standards. It can also predict the impact of planned or unplanned changes to the network, such as software upgrades, configuration changes, or device failures, and provide proactive recommendations to avoid or resolve issues. The Cisco Network Assurance Engine helps to ensure that the network is always operating as intended and aligned with the business objectives. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 8: Data Center Automation and Orchestration, Lesson 8.4: Cisco Data Center Network Assurance and Insights

Cisco Network Assurance Engine

Question: 154

What is an advantage of streaming telemetry over SNMP?

A. on-change traps sent to a receiver

B. periodic push-based subscription messages

C. periodic polling of the device status

D. MD5-based authentication on polling

Answer: B

Explanation:

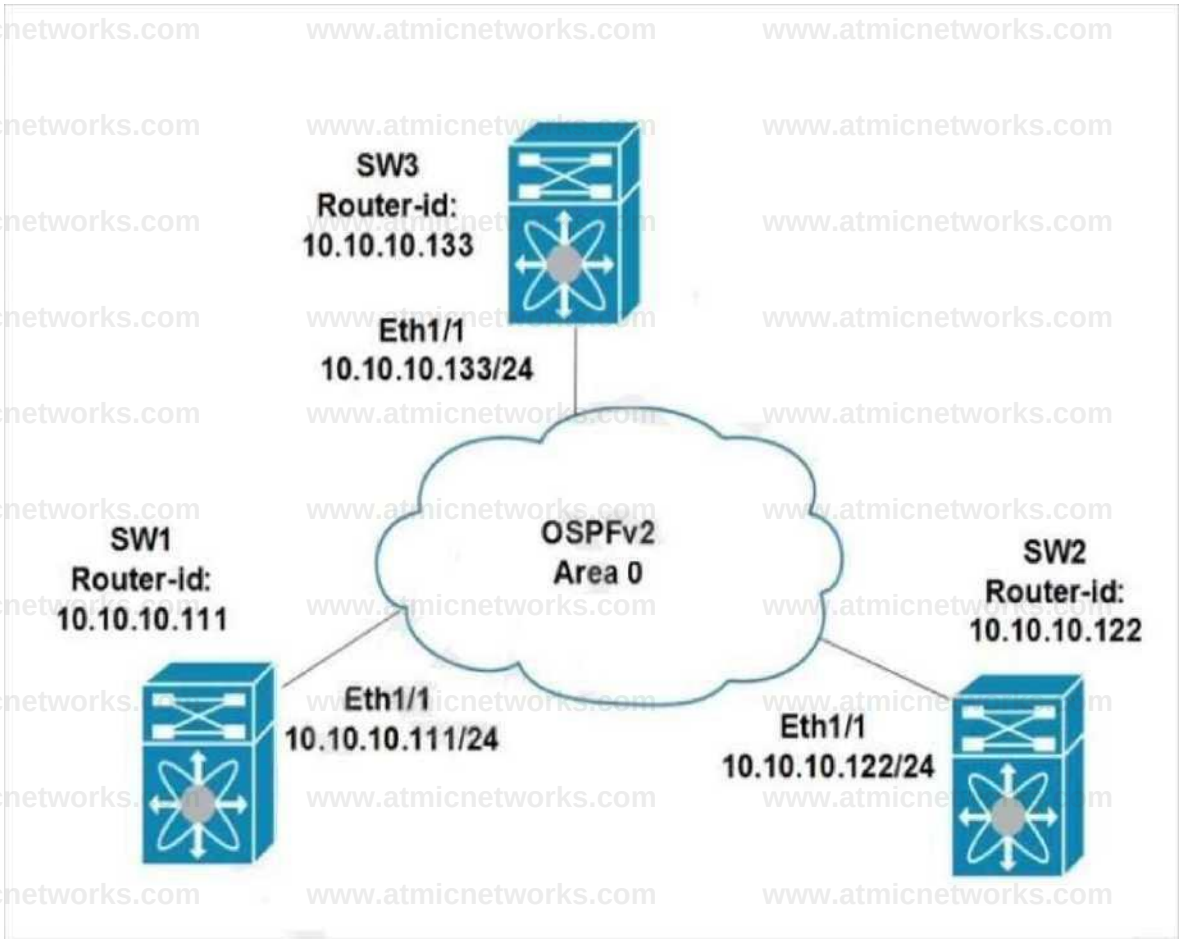
An advantage of streaming telemetry over SNMP is that it supports periodic push-based subscription messages. Streaming telemetry is a method of collecting and transporting network data from devices to a receiver, such as a collector or a dashboard. Streaming telemetry allows the devices to send data periodically or on-demand, based on a subscription model. The receiver can subscribe to specific data sets or events that it is interested in, and the device will push the data to the receiver as it becomes available. This reduces the overhead and latency of polling the device status using SNMP, and provides more granular and real-time visibility into the network state and performance. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 8: Data Center Automation and Orchestration, Lesson 8.2: Cisco NX-OS Programmability

Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x), Chapter: Configuring Streaming Telemetry

Question: 155

Refer to the exhibit.



All switches are configured with the default OSPF priority. Which configuration should be applied to ensure that the SW2 Cisco Nexus switch controls the LSA floods and advertises the network to the remaining nodes in the OSPFv2 area?

A. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 255

B. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 1

C. SW2# configure terminal SW2 (config)# router ospf 1 SW2 (config-router)# router-id 10.10.10.22

D. SW2# configure terminal SW2 (config)# interface ethernet 1/1 SW2 (config-if)# ip ospf priority 0

Answer: A

Explanation:

In OSPF, the router with the highest priority on a network becomes the Designated Router (DR), responsible for generating LSAs for the network. By default, all Cisco routers have an OSPF priority of

1. To ensure that SW2 becomes the DR and controls the LSA floods, its priority needs to be the

highest in the OSPFv2 area. The command in option A sets the OSPF priority to the maximum value of 255, which will make SW2 the most likely candidate to be elected as the DR, provided that no other router has a higher priority or a higher router ID if priorities are equal.

Reference := This explanation is based on the OSPF election process as described in Cisco's OSPF design guide and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials. For detailed information, please refer to these resources.

Question: 156

Which MAC address is an HSRP version 2?

A. 0100.5E7F.FFFF

B. 3799.9943 3000

C. 0000.0C9F.F0C8

D. 0000.OC07.AC1H

Answer: C

Explanation:

The MAC address that is an HSRP version 2 address is 0000.0C9F.F0C8. HSRP (Hot Standby Router Protocol) is a protocol that provides redundancy and load balancing for IP networks by allowing multiple routers to share a virtual IP address and MAC address. HSRP version 2 supports up to 4096 groups, and uses a different MAC address format than HSRP version 1. The MAC address format for HSRP version 2 is 0000.0C9F.FXXX, where XXX is the hexadecimal value of the group number. For group 200, the hexadecimal value is C8, so the MAC address is 0000.0C9F.F0C8. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.6: Cisco Nexus 5000 Series Switches

Cisco Nexus 5000 Series NX-OS Unicast Routing Configuration Guide, Release 5.2(1)N1(1), Chapter: Configuring HSRP, Section: HSRP Version 2

Question: 157

Refer to the exhibit.

```
switch? show vpc brief Legend:
                  (•) - local VPC is down.  forwarding via VPC peer-link

  vPC domain id                     : 10
  Peer status                       : peer adjacency formed  ok
  vPC keep-alive status             : peer is alive
  Configuration consistency status:  success
  Typ*-2 consistency status         : success
  VPC role                          : primary
  Number of vECs configured         : 1
  Peer Gateway                      : Enabled
  Dual-active excluded VLANs        : -

  vPC Peer-link status
```

```
  id Port Status Active vians

  1    Po20 up       100-105

  vPC status

  id Port Status Consistency Reason                     Active vians

  7     Pel    up     success     success                100-104 100-102
  8     Po8    up     success     success                100-103
  9     Po9    up     success     success
```

Which VLANs are capable to be assigned on vPC interfaces?

A. 100-103

B. 100-104

C. 100-102

D. 100-105

Answer: B

Explanation:

The VLANs capable of being assigned on vPC interfaces are those that are active on the vPC peer-link. According to the exhibit, the active VLANs on the vPC peer-link range from 100 to 105. However, VLAN 105 is not listed under the individual port statuses for Po7 and Po8, which indicates that VLAN 105 is not actively participating in the vPC. Therefore,

the VLANs that can be assigned to vPC interfaces are 100-104.

Reference := For a detailed understanding of vPC configurations and VLAN assignments, one should refer to the Cisco Data Center Core Technologies study materials, which provide comprehensive coverage of vPC operations and best practices.

Question: 158

An engineer needs to Implement a solution that prevents loops from occurring accidentally by connecting a switch to interface Ethemet1/1. The port Is designated to be used tor host connectivity. What configuration should be implemented?

switch# configure terminal
swrtch(config># interface Ethernet1/1 switch(config-if)# spanning-tree guard loop

switch# configure terminal
switch! config)# interface Ethernet 1/1
switch(config-if)# spanning-tree bpdu filter enable

switch# configure terminal
$witch(config)# interface Ethernet 1/1
switch(config-if)# spanning-tree bpduguard enable

switch# configure terminal
switch(config)# interface Ethernet1/1
switch(config-if)# spanning-tree loopguard default

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To prevent loops from occurring accidentally on a switch interface designated for host connectivity, the best practice is to enable Spanning Tree Protocol (STP) protections. Option A, which includes the command spanning-tree guard loop, is the correct configuration to apply. This command enables Loop Guard, a feature that prevents alternate or root ports from becoming designated ports due to a failure that leads to a unidirectional link. If a port stops receiving Bridge Protocol Data Units (BPDUs), Loop Guard puts the port into an STP loop-inconsistent state, effectively preventing potential loops.

Reference := This information is aligned with the best practices for loop prevention as described in Cisco's Data Center Core Technologies materials. For further details, refer to the study guide or source documents related to STP and its security features within the Cisco Data Center Core Technologies curriculum.

Question: 159

An engineer installed a new Nexus switch with the mgm0interface in vrf management. Connectivity to the rest of the network needs to be tested from the guest shell of the NX-OS. Which command tests connectivity from the shell of the NX-OS?

[guestshell@guestshell -]$ ping 173.37.145.84 vrf management

[guesUhellggUMtshell -]$ chvrf management ping 173.37.145.84

[guestshell@guestshell -]$ iping vrf management Ip 173.37.145.84

[guesUhell@guestshell -]S dohost "ping vrf management 173.37.145.84'

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To test connectivity from the guest shell of the NX-OS, the command that should be used is ping vrf management [IP address]. This command sends ICMP Echo requests to the specified IP address within the management VRF, which is useful for verifying network connectivity from the guest shell environment.

Reference := For more detailed procedures and explanations, one would refer to the Cisco Data Center Core Technologies (DCCOR) study materials, which provide in-depth knowledge on managing and operating Cisco Nexus switches and their features, including the use of the guest shell for network connectivity tests.

Question: 160

Refer to the exhibit.

```
BOTH tor fabric aoaeion ayleaaion description 'Tin la ay fabric WPM MMIM* destination tanant tl application app! apq apgl destination-ip IN.0.10 123 source-ip-pref la 10
0 20 1 erspan-Id 100 Ip deep 42 Ip ttl 10 atu WK wait
  source Interface sth 1/1 switch 101 direction ta filter tenant tl bd bdl filter tenant tl vrf vrfl
  no abut
```

An engineer needs to implement a monitoring session that should meet the following requirements:

- Monitor traffic from leaf to leaf switches on a Cisco ACI network
- Support filtering traffic from Bridge Domain or VRF

Which configuration must be added to meet these requirements?

A. interface eth 1/2 switch 101

B. interface eth 1/2 leaf 101

C. filter tenant t1 application app1 epg epg1

D. application epg epg1 app1

Answer: C

Explanation:

To monitor traffic between leaf switches in a Cisco ACI network and support filtering traffic from a Bridge Domain or VRF, the configuration must allow for specifying the traffic of interest based on tenant, application, and EPG. Option C, filter tenant t1 application app1 epg epg1, meets these requirements by defining a filter that targets traffic from a specific EPG within an application profile in the tenant 't1'. This filter can be applied to the monitoring session to capture the relevant traffic.

Reference := For detailed procedures on implementing monitoring sessions in Cisco ACI, refer to the Cisco Data Center Core Technologies documentation, particularly sections covering ACI traffic monitoring and filtering.

Question: 161

An engineer needs to create a new user in the local user database on Cisco UCS Fabric Interconnect. The user needs permissions to change the following configuration inside UCS Manager version 3.1:

- vNIC and vHBA profiles
- Fan speed and power redundancy profile of UCS Manager

Which two roles must be assigned to a user to achieve this goal? (Choose two.)

A. server-compute

B. facility-manager

C. operations

D. server-equipment

E. server-profile

Answer: A, E

Explanation:

To achieve the goal of creating a new user in the local user database on Cisco UCS Fabric Interconnect that can change the vNIC and vHBA profiles and the fan speed and power redundancy profile of UCS Manager, the engineer needs to assign two roles to the user: server-compute and server-profile. The server-compute role allows the user to configure and manage the compute resources, such as servers, service profiles, pools, and policies. The server-profile role allows the user to configure and manage the network resources, such as vNICs, vHBAs, VLANs, VSANs, and LAN and SAN connectivity policies. These two roles provide the user with the necessary permissions to change the configuration inside UCS Manager version 3.1, as required by the goal. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.3: Cisco UCS Fabric Interconnect and Unified Port Feature

Cisco UCS Manager GUI Configuration Guide, Release 3.1, Chapter: Managing User Accounts, Roles, and Passwords, Section: Creating User Accounts

Reference:

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-1/b_Cisco_UCS_Admin_Mgmt_Guide_3_1/b_UCSM_Admin_Mgmt_Guide_chapter_01.html

Question: 162

Refer to the exhibit.

```
1.13 0 5 99 1 92.160.259.1 -> 192.163.251.13 TCP 60 29652 > ash [ACK] 5eq-l Ack-53 Xin-32449 Len=O
1.136261 00:Ge: 73: a2:41: Ge -> Spanning-tree-(for-bridge#) 00 5TP 60 Conf. Root ⁹ B192/10/ec:el:a9:df:6c:80 Coat - 22 Fort = OxBOOe
1.30 3417 192.160.2 54.13 -> 192.168.254.1 SSI 106 Encrypted response packet len=52
1.570377 192.160.254.1 -> 192.163.254.13 TCP 60 29652 > ash JACK] Seq«l Ack-105 Nln=32786 Len=0
1.815550 192.168.254.13 -> 192.168.254.1 SSI 106 Encrypted response packet len=52
2.021840 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ash (ACK) Seq~l Aek>3S7 Win®32773 L«a=0
2.325173 192.168.254.13 -> 192.168.254.1 SSI 106 Encrypted response packet len=52
2.731382 192.168.254.1 -> 192.168.254.13 TCP 60 29652 > ash [ACK] Seq-1 Ack-209 Win-32760 Leo-0
2.947365 192.168.254.13 -> 192.168.254.1 NT? 90 NTP Version 2, client
2.947623 192.168.254.1 -> 192.168.254.13 NTP 90 NTP Version 2, server
3.138157 00:8e:73:a2:41:0e -> Spanning-tree - (foi-br idgea) _00 SIP 60 Conf. Root • 6192/10/ec:el:a9:df: 6c;80 Cost - 22 Port * OxBOOe
3.139400 192.168.254.13 -> 192.168.254.1 SSK 106 Encrypted response packet lea-52
3.270720 192.160.254.4 -> 239.255.70.03 OOP 166 Source port: cfs Destination port cfs
3.341123 192.168.254.1 -> 192.169.254.13 TCP 60 29652 > ash [ACK] Seq-1 Ack>261 Win-32747 len-0
3.035409 1 92.160.254.13 -> 192.160.254.1 SSK 106 Encrypted response packet leu-52
4.041411 192.168.2 54.1 -> 192.168.254.13 TCP 60 29652 > ash [ACK] Seq-1 Ack-313 Wia-32734 Len-0
4.535204 192.160.254.13 -> 192.168.254.1 SSK 106 Encrypted response packet lea-32
4.74 1 072 1 92.168.2 54.1 -> 192.168.254.13 TCP 60 29652 > ash [ACK] Seq«l Act=365 Win-32721 Len-0
4.947300 192.168.254.13 -> 192.168.254.1 FTP 90 NTP Version 2, client
4.94 7 5 1 9 1 92.168.2 54.1 -> 192.168.254.13 NTP 90 NTP version 2, server
5.13 9627 00:Ge:73:a2:41:0e -> Soanning-tree-(fcr-bridgas) _00 STP 60 Conf. Root ⁹ 0192/lO/ec:el:a9:df:6c:8O Cost - 22 Port ■ OxBOOe
5.140867 192.160.254.13 -> 192.168.254.1 SSK 106 Encrypted response packet lt»«52
```

Cisco Fabric Services is enabled in the network. Which type of IP address is used by the Cisco Fabric Services protocol?

A. IPv4 unicast address

B. IPv4 multicast address

C. IPv4 gateway address

D. IPv4 anycast address

Answer: B

Explanation:

Cisco Fabric Services (CFS) utilizes IPv4 multicast addresses to disseminate configuration information across network devices. This ensures that all devices within the network have consistent and synchronized configuration data, which is crucial for maintaining the integrity and stability of the network.

Reference: For a detailed understanding, please refer to the Cisco Data Center Core Technologies (DCCOR) study materials, specifically the sections discussing CFS and its operational mechanisms within the network infrastructure.

Question: 163

Refer to the exhibit.

```
switch# show install all inpact epld n9000-epld.9.2.1.img
Compatibility check:
Module Type Upgradable Impact Reason

     1       SUP      YES disruptive Module Upgradable

Retrieving EPLD versions... Please wait.

Inages will be upgraded according to following table:
Module Type EPLD              Running-Version New-Version Upg-Required

1     SUP     MI PPGA              0x23           0x23          No
1     SUP     IO FPGA              0x06           0x06          No
1     SUP     MI FPGA2             0x23           0x23          No
```

A network engineer plans to upgrade the current software images of a Cisco Nexus switch. What is the impact of starting the EPLD upgrade?

A. The switch reboots one time for the new EPLD versions to take effect.

B. The switch reboots multiple times for the new EPLD versions to take effect.

C. The switch skips the EPLD upgrade for each EPLD device of the switch.

D. The switch skips the EPLD upgrade for MIFPGA and proceeds with the other EPLD devices.

Answer: B

Explanation:

Upgrading the EPLD on a Cisco Nexus switch is a disruptive process that requires the switch to reboot multiple times. Each EPLD device on the switch must be upgraded individually, and the switch must reboot to initialize the new EPLD version for each device. This process ensures that all hardware components are properly updated and can operate with the new firmware, but it does cause temporary disruptions to network traffic as each module reboots.

Reference: For more detailed information, please refer to the Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes, where it discusses the impact of EPLD upgrades and the necessity of multiple reboots during the process1. Additionally, the Cisco Nexus 9000 Series NX-OS Software

Upgrade and Downgrade Guide provides guidelines on the upgrade process, including the disruptive nature of EPLD

upgrades

Question: 164

A network engineer must perform a backup and restore of the Cisco Nexus 5000 Series Switch configuration. The backup must be made to an external backup server. The only protocol permitted between the Cisco Nexus Series switch and the backup server is UDP. The backup must be used when the current working configuration of the switch gets corrupted. Which set of steps must be taken to meet these requirements?

A. 1. Perform a running-config backup to an SFTP server. 2. Copy backup-config from the SFTP server to the running-config file.

B. 1. Perform a startup-config backup to a TFTP server. 2. Copy backup-config from the backup server to the running-config file.

C. 1. Perform a running-config backup to an SCP server. 2. Copy running-config in the boot flash to the running-config file.

D. 1. Perform a startup-config backup to an FTP server. 2. Copy startup-config in the boot flash to the running-config file.

Answer: B

Explanation:

To meet the requirements of performing a backup and restore of the Cisco Nexus 5000 Series Switch configuration using UDP as the only protocol, the network engineer must follow these steps:

Perform a startup-config backup to a TFTP server. The startup-config file contains the configuration that is applied when the switch boots up. To backup this file to a TFTP server, the engineer can use the copy startup-config tftp: command, and specify the IP address or hostname of the TFTP server and the destination filename. For example:

switch# copy startup-config tftp: Enter hostname for the tftp server: 10.10.10.10 Enter destination

filename: backup-config

Copy backup-config from the backup server to the running-config file. The running-config file contains the configuration that is currently active on the switch. To restore this file from the backupconfig file on the TFTP server, the engineer can use the copy tftp: running-config command, and specify the IP address or hostname of the TFTP server and the source filename. For example:

switch# copy tftp: running-config Enter hostname for the tftp server: 10.10.10.10 Enter source filename: backup-config

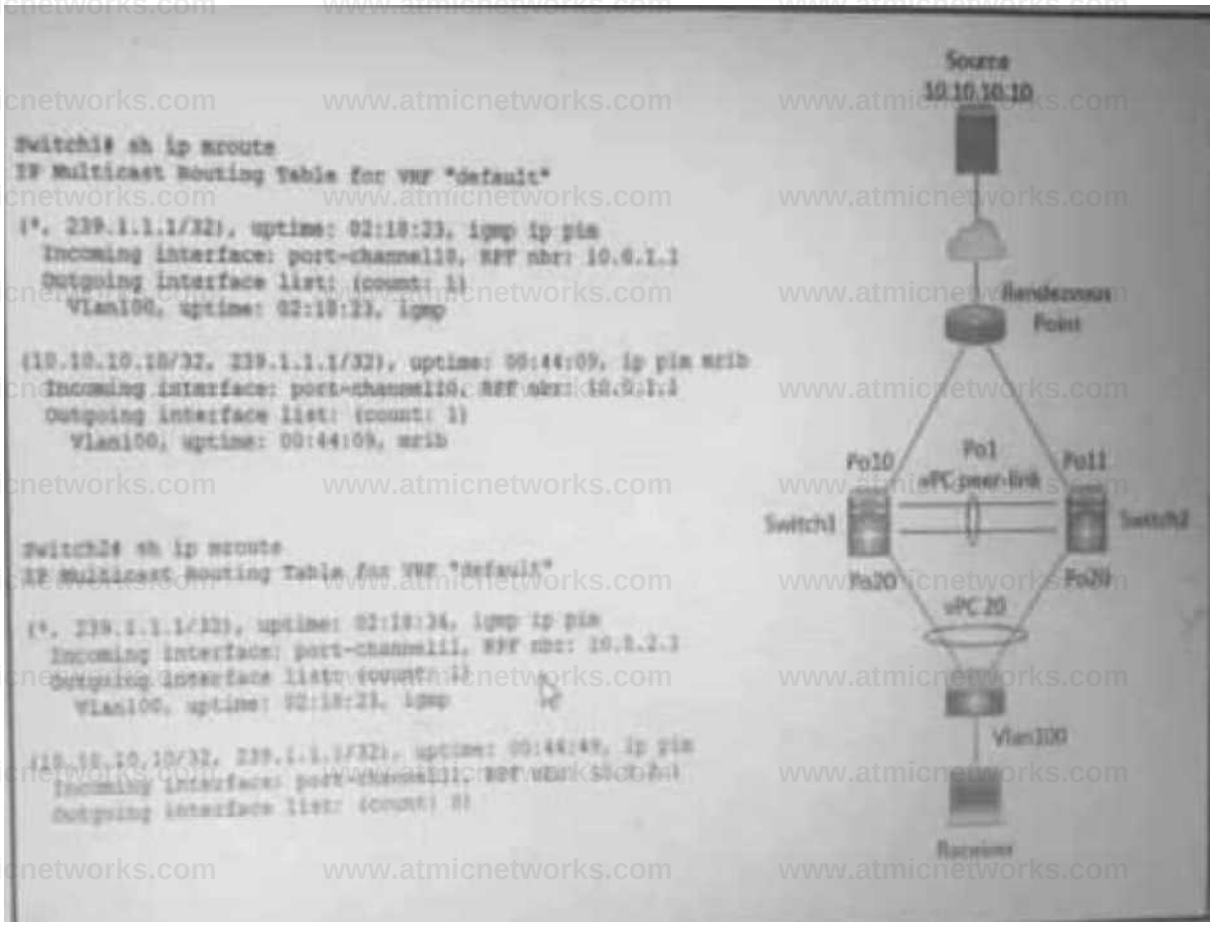
These steps will allow the engineer to backup and restore the switch configuration using UDP as the only protocol, as TFTP is a UDP-based protocol. The backup-config file can be used when the current working configuration of the switch gets corrupted, as required by the goal. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 3: Data Center LAN Network Connectivity, Lesson 3.6: Cisco Nexus 5000 Series Switches

Cisco Nexus 5000 Series NX-OS Fundamentals Configuration Guide, Release 5.2(1)N1(1), Chapter: Configuring System Files, Section: Copying a Configuration File to a Remote Server Using TFTP, FTP, SFTP, or SCP

Question: 165

Refer to the exhibit.



A host with a source address 10.10.10.10 sends traffic to multicast group 239.1.1.1. How do the vPC switches forward the multicast traffic?

A. If multicast traffic isreceived on Switch1 over the vPC peer-link, the traffic is dropped

B. If multicast traffic isreceived on Po10 Switch1, the traffic is forwarded out on Po1 andPo20

C. If multicast traffic isreceived on Po11 Switch2, the traffic is forwarded out only on Po20

D. If multicast traffic isreceived on Po11 Switch2, the traffic is dropped.

Answer: B

Explanation:

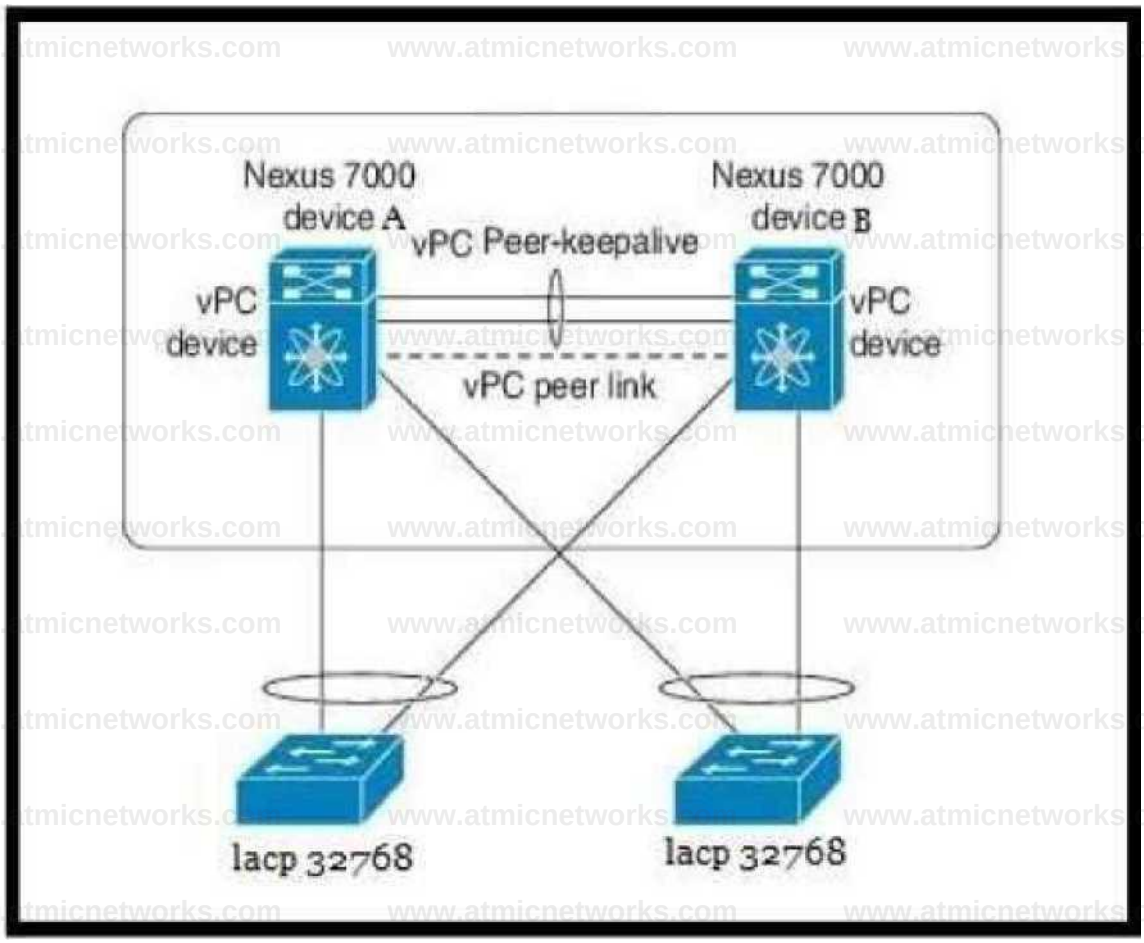
In a vPC (Virtual Port-Channel) configuration, multicast traffic is handled based on the vPC design and operational rules. When a host sends traffic to a multicast group, the vPC switches determine the forwarding path based on the source and the vPC domain configuration. If multicast traffic is received

on a vPC member port, such as Po10 on Switch1, the traffic is typically forwarded out on all ports that are part of the same VLAN and have receivers interested in the multicast group, which includes Po1 and Po20 in this case. This ensures that the multicast traffic reaches all intended recipients across the vPC domain.

Reference: For a comprehensive understanding, the Cisco documentation on "Multicast forwarding in vPC based on location of the source" provides detailed scenarios and explanations on how multicast traffic is forwarded in a vPC environment1. Additionally, the "Cisco Nexus 9000 Series NX-OS Multicast Routing Configuration Guide" offers insights into the configuration and behavior of multicast routing on Nexus switches, which can be applied to understand the vPC behavior with multicast traffic

Question: 166

Refer to the exhibit.



Which configuration ensure that the cisco Nexus 7000 series switches are the primary devices for LACP?

A. N7K_A(config-vpc-domain)# role priority 1

N7K_B(config-vpc-domain)# role priority 2

B. N7K_A(config-vpc-domain)# system-priority 32768

N7K_B(config-vpc-domain)# system-priority 32768

C. N7K_A(config-vpc-domain)# system-priority 100

N7K_B(config-vpc-domain)# system-priority 200

D. N7K_A(config-vpc-domain)# system-priority 4000

N7K_B(config-vpc-domain)# system-priority 4000

Answer: C

Explanation:

To ensure that the Cisco Nexus 7000 series switches are the primary devices for LACP, the system priority needs to be configured with lower values indicating higher priority. In this case, setting N7K_A with a system priority of 100 and N7K_B with a system priority of 200 ensures that N7K_A has a higher priority and becomes the primary device for LACP. The system priority is used in the LACP system ID which determines the LACP priority; the lower the value, the higher the priority.

Reference: The configuration guidelines for LACP on Cisco devices can be found in the Cisco documentation, which explains the role of system priority in determining the primary device in an LACP setup1. Additionally, the Cisco Data Center Core Technologies study materials provide detailed information on configuring LACP and vPC domain parameters.

Question: 167

Which method must a network engineer use to upgrade the BIOS firmware of a Cisco UCS standalone C-Series reck-mount server?

A. Use the Cisco host upgrade utility.

B. Use the Cisco hardware upgrade utility.

C. Use the Cisco host firmware policy.

D. Use the U-ACPI Interface.

Answer: A

Explanation:

The method that a network engineer must use to upgrade the BIOS firmware of a Cisco UCS standalone C-Series rack-mount server is to use the Cisco host upgrade utility. The Cisco host upgrade utility is a tool that allows the network engineer to upgrade the firmware of various components of the server, such as the BIOS, the CIMC, the RAID controller, and the network adapter. The Cisco host upgrade utility can be downloaded from the Cisco website and run from a bootable USB drive or CD- ROM. The Cisco host upgrade utility provides a graphical user interface that guides the network engineer through the firmware upgrade process, and allows the network engineer to select the firmware versions and the components to be upgraded. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.4: Cisco UCS C-Series Servers

Cisco Host Upgrade Utility User Guide, Chapter: Overview of the Cisco Host Upgrade Utility

Question: 168

Which action must be performed before renumbering a Cisco UCS chassis?

A. Move the chassis to new ports on fibric interconnect.

B. Re-acknowledge the chassis.

C. Decommission the chassis.

D. Run the shut and no shut command on the connected ports.

Answer: B

Explanation:

The action that must be performed before renumbering a Cisco UCS chassis is to re-acknowledge the chassis. Re-acknowledging the chassis is a process that forces the Cisco UCS Manager to rediscover the chassis and its components, such as the I/O modules, the power supplies, and the fans. Reacknowledging the chassis is necessary before renumbering the chassis, because it ensures that the Cisco UCS Manager has the latest information about the chassis and its configuration. Reacknowledging the chassis also allows the network engineer to apply any pending configuration changes or policies to the chassis and its components. Re-acknowledging the chassis can be done from the Cisco UCS Manager GUI or CLI, by selecting the chassis and choosing the Re-Acknowledge option. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.1: Cisco UCS Architecture

Cisco UCS Manager GUI Configuration Guide, Release 4.0, Chapter: Managing Chassis, Section: ReAcknowledging a Chassis

Question: 169

A server engineer wants to control power usage on a Cisco UCS C-Series rack server down to the component level.

Which two components support specific power limits? (Choose two.)

A. storage controller
B. network controller
C. processor
D. graphic card
E. memory

Answer: C, D

Explanation:

The two components that support specific power limits on a Cisco UCS C-Series rack server are the processor and the graphic card. The processor and the graphic card are the two components that consume the most power on a server, and they can be configured to have specific power limits to control the power usage and performance of the server. The power limits can be set using the Cisco Integrated Management Controller (CIMC) web interface or CLI, or using the Cisco UCS Manager if the server is integrated with a Cisco UCS domain. The power limits can be applied to individual processors or graphic cards, or to the entire server. The power limits can help to optimize the power efficiency

and thermal management of the server, as well as to prevent power capping or throttling issues. Reference :=

Implementing and Operating Cisco Data Center Core Technologies (DCCOR) v1.2, Module 5: Cisco Unified Computing System, Lesson 5.4: Cisco UCS C-Series Servers

Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide, Release 4.0, Chapter: Configuring Server Power, Section: Configuring Processor Power Limits

Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide, Release 4.0, Chapter: Configuring Server Power, Section: Configuring Processor Power Limits

Question: 170

An engineer is implementing an import operation in Cisco UCS Manager. What is the impact of performing this operation?

A. A configuration can be imported from a higher release to a lower release.

B. Information can be modified on the management plane only.

C. Only a configuration file that was exported from the same Cisco UCS Manager can be imported.

D. An import operation can be scheduled.

Answer: B

Explanation:
The import function is available for all configuration, system configuration, and logical configuration files. You can perform an import while the system is up and running. An import operation modifies information on the management plane only. Some modifications caused by an import operation, such as a change to a vNIC assigned to a server, can cause a server reboot or other operations that disrupt traffic.

https://www.cisco.com/en/US/docs/unified_computing/ucs/sw/gui/config/guide/141/UCSM_GUI_Configuration_Guide_141_chapter43.html#concept_D789E16C90724AEFB99D565574E45AD5

Question: 171

An engineer wants to create a backup of Cisco UCS Manager for disaster recovery purposes. What are two characteristics of a full state backup of a Cisco UCS Manager database? (Choose two.)

A. performs a complete binary dump of the database as a .txz file

B. contains all of the configurations

C. performs a complete binary dump of the database as a bin file

D. performs a complete binary dump of the databases as a sql file

E. contains all of the runtime states and statuses but not the configurations

Answer: B, E

Explanation:

A full state backup of a Cisco UCS Manager database performs a complete binary dump of the database as a .bin file, not a .txz or a .sql file. A full state backup contains all of the configurations and all of the runtime states and statuses of the Cisco UCS domain, but not the passwords. A full state backup can be used to restore the Cisco UCS Manager database to the same or a different fabric interconnect, as long as the hardware configuration is identical. Reference := Implementing and Operating Cisco Data Center Core Technologies (DCCOR) - Cisco, Chapter 5: Implementing Cisco Unified Computing System Rack Servers, Section: Back Up and Restore the Cisco UCS Manager Database

Question: 172

What happens to the default host firmware policy after a Cisco UCS Manager upgrade?

A. It is updated to contain the firmware entries of all the components

B. It is replaced by a new default policy without any firmware entries.

C. It is assigned to all the service profiles that include a host firmware policy.

D. It is set to match the host firmware policy.

Answer: A

Explanation:

The default host firmware policy is a system-defined policy that contains the firmware entries of all the components that are supported by the Cisco UCS Manager version. When a Cisco UCS Manager upgrade occurs, the default host firmware policy is updated to contain the firmware entries of all the components that are supported by the new Cisco UCS Manager version. The default host firmware policy is not replaced, assigned, or matched by any other policy after a Cisco UCS Manager upgrade. Reference := Implementing and Operating Cisco Data Center Core Technologies (DCCOR) - Cisco, Chapter 5: Implementing Cisco Unified Computing System Rack Servers, Section: Manage Firmware Versions in Cisco UCS Manager

Question: 173

An engineer is asked to use SaaS to manage Cisco computing. Which two items are needed to accomplish the task? (Choose two.)

A. UCS Manager

B. Node name/Serial Number

C. Device/Claim ID

D. UCS Central

E. Intersight

Answer: C, E

Explanation:

To use SaaS to manage Cisco computing, you need to have a Cisco Intersight account and a device/claim ID for each device that you want to manage. Cisco Intersight is a cloud-based platform that provides unified management, automation, and analytics for Cisco data center products. A device/claim ID is a unique identifier that is generated when you register a device with Cisco Intersight. You can use the device/claim ID to claim the device and add it to your Intersight account. Once you claim the device, you can monitor, configure, and troubleshoot it from the Intersight dashboard. Reference: For more information on how to use SaaS to manage Cisco computing, please refer to the following resources:

Cisco Intersight Overview

Cisco Intersight Getting Started Guide

Cisco Intersight Device Connector

Question: 174

An engineer is seeking the most optimal on demand CPU performance while configuring the BIOS settings of a UCS C-series rack mount server.

What setting will accomplish this goal?

A. C0/C1 state

B. C6 Retention

C. C2 state

D. C6 non-Retention

Answer: A

Explanation:

To achieve the most optimal on demand CPU performance while configuring the BIOS settings of a UCS C-series rack mount server, you should set the CPU Performance option to C0/C1 state. This option enables the CPU to operate in the highest performance state (C0) or the lowest power state (C1) depending on the workload demand. This allows the CPU to maximize its performance and efficiency without compromising its thermal and power limits. The other options (C6 Retention, C2

state, and C6 non-Retention) reduce the CPU performance by putting the CPU into deeper sleep states (C2 or C6) when idle, which can increase the latency and power consumption when resuming the CPU activity.

Reference: For more details on how to configure the BIOS settings of a UCS C-series rack mount server, please refer to the following resources:

Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide

Cisco UCS C-Series Rack-Mount Server BIOS Settings

Question: 175

An engineer is duplicating an existing Cisco UCS setup at a new site. What are two characteristics of a logical configuration backup of a Cisco UCS Manager database? (Choose two.)

A. contains the AAA and RBAC configurations

B. contains a file with an extension.tgz that stores all of the configurations

C. contains the configuration organizations and locales

D. contains all of the configurations

E. contains the VLAN and VSAN configurations

Answer: B, C

Explanation:

A logical configuration backup of a Cisco UCS Manager database is a file that contains all of the configurations that are stored in the Cisco UCS Manager database, such as policies, pools, service profiles, templates, and firmware versions. The file has an extension .tgz and can be created and restored using the Cisco UCS Manager GUI or CLI. A logical configuration backup also contains the configuration organizations and locales, which are logical entities that group and isolate resources within a Cisco UCS domain. Organizations and locales can be used to delegate administrative tasks and privileges to different users or groups. The other options (AAA and RBAC configurations, VLAN and VSAN configurations) are not part of a logical configuration backup, but rather a full state backup, which is a different type of backup that includes the operational state and statistics of the Cisco UCS domain. Reference: For more information on how to create and restore a logical configuration backup of a Cisco UCS Manager database, please refer to the following resources:

Cisco UCS Manager Backup and Restore Management Guide

Cisco UCS Manager Configuration Common Practices and Quick Start Guide

Question: 176

Which two settings must be configured before enabling a Cisco UCS Manager domain for Cisco Intersight connectivity? (Choose two.)

A. syslog redirection

B. DNS servers

C. SMTP servers

D. NTP servers

E. SMTP reply-to-address

Answer: B, D

Explanation:

Before enabling a Cisco UCS Manager domain for Cisco Intersight connectivity, you must configure the DNS servers and the NTP servers for the domain. The DNS servers are required to resolve the hostname of the Cisco Intersight service (svc.intersight.com) and the NTP servers are required to synchronize the time between the Cisco UCS Manager and the Cisco Intersight service. These settings ensure that the Cisco UCS Manager can establish a secure and reliable connection with the Cisco Intersight service and register the domain with the Cisco Intersight account.

Reference: For more information on how to configure a Cisco UCS Manager domain for Cisco Intersight connectivity, please refer to the following resources:

Cisco UCS Manager Configuration Guide for Intersight Device Connector

Cisco Intersight Getting Started Guide

Question: 177

An engineer must configure Cisco IMC server management NIC for autonegotiation. Which setting should be selected?

A. Cisco card

B. shared LOM

C. dedicated

D. shared LOM EXT

Answer: B

Explanation:

To configure the Cisco IMC server management NIC for autonegotiation, you should select the shared LOM setting. This setting allows the Cisco IMC to share the LAN on motherboard (LOM) ports with the host operating system and negotiate the speed and duplex settings automatically. The shared LOM setting also provides redundancy and failover capabilities for the Cisco IMC management access. The other settings (Cisco card, dedicated, and shared LOM EXT) do not enable autonegotiation for the Cisco IMC server management NIC.

Reference: For more details on how to configure the Cisco IMC server management NIC, please refer to the following resources:

Cisco Integrated Management Controller Configuration Guide

Cisco Integrated Management Controller (IMC) Data Sheet

Question: 178

Refer to the exhibit.

```
UCS-A# scope adapter 1/1/1
UCS-A# /chassis/server/adapter # show image
Name                                Type        Version        State

ucs-m81kr-vic.2.2.lb.bin Adapter 2.2(lb)                       Active


UCS-A# /chassis/server/adapter # update firmware 2.2 (lb)
UCS-A# /chassis/server/adapter* # activate firmware 2.2(lb) set-startup-only
UCS-A# /chassis/server/adapter* # commit-buffer
UCS-A# /chassis/server/adapter #
```

What is the result of this series of commands?

A. It reboots the server immediately.

B. It verifies the firmware update on the server.

C. It activates the firmware on the next adapter boot.

D. It updates the firmware on adapter 1/1/1 immediately.

Answer: C

Explanation:

The series of commands provided in the exhibit are part of the process to update and activate firmware on a Cisco UCS server adapter. The update firmware command is used to update the firmware, while the activate firmware command, combined with the set-startup-only option, schedules the activation of the firmware upon the next reboot of the adapter. This means that the new firmware will not be active immediately but will take effect after the adapter is rebooted, ensuring that the current operations are not disrupted.

Reference: For further details on firmware management commands and their effects in Cisco Data Center Core Technologies, you can refer to the Cisco UCS Manager Firmware Management Guide, which provides comprehensive instructions on updating and activating firmware on UCS components1. Additionally, the Cisco UCS Manager CLI Configuration Guide offers insights into the CLI commands used for managing firmware

Question: 179

What is the benefit of adding Cisco HyperFlex Hardware Acceleration Cards to a HyperFlex deployment?

A. offline encryption acceleration

B. increased network throughput

C. GPU acceleration

D. Increased compression efficiency

Answer: D

Explanation:

The benefit of adding Cisco HyperFlex Hardware Acceleration Cards to a HyperFlex deployment is increased compression efficiency. These cards are PCIe devices that offload the compression and decompression operations from the CPU, resulting in higher performance and lower latency for most storage workloads. The cards also reduce the CPU utilization and power consumption of the HyperFlex nodes, enabling more resources for other applications. The other options (offline encryption acceleration, increased network throughput, and GPU acceleration) are not benefits of the HyperFlex Hardware Acceleration Cards. Reference: For more information on the HyperFlex Hardware Acceleration Cards, please refer to the following resources:

Configure HyperFlex Hardware Acceleration Cards

Cisco HyperFlex Systems Installation Guide for VMware ESXi, Release 4.0

Cisco HyperFlex HX240c M5 Data Sheet

• Additional Information on HyperHex Hardware Acceleration Cards

Overview of HyperFlex Hardware Acceleration Cards

This chapter provides details for installation, post-installation, and troubleshooting of HyperFlex Hardware Acceleration Cards (PID HX-PCIE-OFFLOAD-1) on HyperFlex nodes and for configuring your initial cluster These cards provide improved performance and compression efficiency for most storage workloads.

An HXDP-P Enterprise license is required for installing and configuring HyperFlex Hardware N°te Acceleration Cards

https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoft ware/Installation_VMWare_ESXi/3_5/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_3_5/b_HyperFlexSystems_Installation_Guide_for_VMware_ESXi_3_5_chapter_01100.html#:~:text=Overv iew%20of%20HyperFlex%20Hardware%20Acceleration%20Cards,-

This%20chapter%20provides&text=These%

20cards%20provide%20improved%20performance%20and%20compression%20efficiency%20for%20

most

%20storage%20workloads.

Question: 180

Which two hypervisors does Cisco HyperFlex support? (Choose two.)

A. VMware vSphere

B. Microsoft Hyper-V

C. OpenStack

D. Citrix XenServer

E. RedHat KVM

Answer: A, E

Explanation:

Cisco HyperFlex is a hyperconverged infrastructure solution that combines compute, storage, and networking in a software-defined platform. Cisco HyperFlex supports two hypervisors: VMware vSphere and RedHat KVM. VMware vSphere is a widely used virtualization platform that provides enterprise-class features and performance. RedHat KVM is an open source hypervisor that is integrated with the Linux kernel and offers scalability and flexibility. Cisco HyperFlex does not support Microsoft Hyper-V, OpenStack, or Citrix XenServer as hypervisors, although it can interoperate with them through other Cisco products or solutions. Reference: For more information on Cisco HyperFlex and its supported hypervisors, please refer to the following resources:

Cisco HyperFlex Systems Solution Overview

Cisco HyperFlex Systems Installation Guide for VMware ESXi

Cisco HyperFlex Systems Installation Guide for Red Hat Enterprise Linux KVM

Question: 181

An engineer changed a configuration and must perform a rollback. Which statement applies to a Cisco Nexus 5600 Series switch?

A. Errors are skipped when an atomic rollback type is triggered.

B. A user who is assigned to the network-operator user role can perform a rollback.

C. The configuration rollback functionality is disabled when FCoE is enabled.

D. A system checkpoint is generated automatically when the running configuration is saved to NVRAM.

Answer: A

Explanation:

The statement that applies to a Cisco Nexus 5600 Series switch when performing a rollback is that errors are skipped when an atomic rollback type is triggered. An atomic rollback is a type of rollback that implements the checkpoint configuration only if no errors occur during the process. If any errors are encountered, the rollback is aborted and the running configuration is restored to its previous state. This ensures that the switch does not end up in a partially configured or inconsistent state. The other statements are not true because:

A user who is assigned to the network-operator user role cannot perform a rollback. The networkoperator user role has read-only access to the switch and cannot modify the configuration. To perform a rollback, the user must have the network-admin or vdc-admin user role.

The configuration rollback functionality is not disabled when FCoE is enabled. The rollback feature is supported on all Cisco Nexus 5600 Series switches regardless of the FCoE configuration. However, some FCoE-related commands may not be rolled back due to dependencies or conflicts with other features.

A system checkpoint is not generated automatically when the running configuration is saved to NVRAM. A system checkpoint is a predefined checkpoint that contains the last saved configuration of the switch. A system checkpoint is created or updated only when the user explicitly saves the running configuration to the startup configuration using the copy running-config startup-config command or its alias, copy run start. Reference: For more details on how to configure and use the rollback feature on a Cisco Nexus 5600 Series switch, please refer to the following resources:

Configuring Rollback

Cisco Nexus 5600 Series NX-OS System Management Configuration Guide, Release 7.x

Cisco Nexus 5600 Series NX-OS System Management Command Reference

Question: 182

Which statement about the impact of a rolling EPLD upgrade on a Cisco MDS 9000 Series Switch is true?

A. All modules on the switch are disrupted.

B. An EPLD upgrade is nondisruptive.

C. Only the modules that are being upgraded are disrupted.

D. The upgrade can be performed from the standby supervisor module.

Answer: C

Explanation:

The statement that is true about the impact of a rolling EPLD upgrade on a Cisco MDS 9000 Series Switch is that only the modules that are being upgraded are disrupted. A rolling EPLD upgrade is a type of EPLD upgrade that allows the user to upgrade one or more modules in a switch without affecting the rest of the modules. The rolling EPLD upgrade requires a module reload for each module that is being upgraded, which causes a temporary disruption of traffic and services on that module. However, the other modules in the switch continue to operate normally and do not require a reload. The other statements are not true because:

All modules on the switch are not disrupted. As explained above, only the modules that are being upgraded are disrupted, while the other modules are unaffected by the rolling EPLD upgrade.

An EPLD upgrade is not nondisruptive. An EPLD upgrade is a process that updates the firmware of the electrical programmable logic devices (EPLDs) that provide hardware functionalities in the switch modules. An EPLD upgrade always involves a module reload, which causes a disruption of traffic and services on that module. However, the disruption can be minimized by using the hitless or non- disruptive EPLD upgrade modes, which preserve the forwarding state and configuration of the module during the reload.

The upgrade cannot be performed from the standby supervisor module. The EPLD upgrade process requires the supervisor module to be in active mode before it can be upgraded. The standby supervisor module must be switched to active mode manually or automatically before the upgrade can begin. Reference: For more information on how to perform a rolling EPLD upgrade on a Cisco MDS 9000 Series Switch, please refer to the following resources:

Cisco MDS 9000 Series EPLD Release Notes, Release 8.4(1)

Cisco MDS 9000 Series NX-OS System Management Configuration Guide

Question: 183

Which command reduces the amount of time it takes to complete the ISSU on a Cisco Nexus 7000 series switch that has dual supervisor modules and two I/O modules?

A. install all kickstart <image>system<image>parallel

B. install all epld bootflash:<image>

C. install all epld bootflash:<image>

D. install all kickstart<image>system<image>

Answer: A

Explanation:

The command that reduces the amount of time it takes to complete the ISSU on a Cisco Nexus 7000 series switch that has dual supervisor modules and two I/O modules is install all kickstart <image>system<image>parallel. This command performs a parallel upgrade of the kickstart and system images on all modules, which reduces the downtime and speeds up the ISSU process. The other commands (install all epld bootflash:<image> and install all kickstart<image>system<image>) do not perform a parallel upgrade and take longer to complete the ISSU. Reference: For more information on how to perform an ISSU on a Cisco Nexus 7000 series switch, please refer to the following resources:

Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide
Cisco Nexus 7000 Series NX-OS ISSU Upgrade Guide

Question: 184

Which two statements about the process of performing an EPLD upgrade on a Cisco MDS 9000 series Switch are true? (Choose two.)

A. If an upgrade is interrupted, the upgrade continues after a connection is restored.

B. The upgrade can be performed from the standby supervisor module.

C. The active supervisor can be upgraded.

D. Modules must be online to be upgraded.

E. The Upgrade process disrupts only the module that is being upgraded.

Answer: A, B

Explanation:

F. Two statements that are true about the process of performing an EPLD upgrade on a Cisco MDS 9000 series Switch

are:

If an upgrade is interrupted, the upgrade continues after a connection is restored. This means that the EPLD upgrade process is resilient to network or power failures and can resume from where it left off once the connection is reestablished.

The upgrade can be performed from the standby supervisor module. This allows the active supervisor module to continue to provide management and control functions while the EPLD upgrade is in progress. The standby supervisor module can also take over the active role if needed during the upgrade.

The other statements are not true because:

The active supervisor cannot be upgraded. The EPLD upgrade process requires the supervisor module to be in standby mode before it can be upgraded. The active supervisor module must be switched to standby mode manually or automatically before the upgrade can begin.

Modules do not need to be online to be upgraded. The EPLD upgrade process can upgrade modules that are offline or powered down as well as modules that are online. The offline modules are upgraded when they are brought online or powered up.

The upgrade process disrupts all modules that are being upgraded. The EPLD upgrade process requires a module reload for each module that is being upgraded, which causes a temporary disruption of traffic and services on that module. The disruption can be minimized by using hitless or non-disruptive EPLD upgrade modes, which preserve the forwarding state and configuration of the module during the reload. Reference: For more details on how to perform an EPLD upgrade on a Cisco MDS 9000 series Switch, please refer to the following resources:

Cisco MDS 9000 Family NX-OS System Management Configuration Guide

Cisco MDS 9000 Family EPLD Upgrade Release Notes

Question: 185

DRAG DROP

An engineer is configuring VNTag between a virtualized server and a Cisco Nexus 5500 Series switch.
Drag and drop the configuration steps from the into the correct order on the right.

Configure support for VNTag mode on the interface that connects to the server.	Step 1
Configure the vNICs of the server.	Step 2
Configure the server to support NIV mode.	Step 3

Enable the virtualization feature set.	Step 4
Configure the port profile.	Step 5
Install the virtualization feature set.	Step 6

Answer:

Explanation:

install the virtualization feature set

Enable the virtualization feature set

Configure the port profile

Configure support for VNTag mode on the interface that connects to the server.

Configure the server to support NIV mode

Configure the vNICs of the server

https://www.cisco.com/c/en/us/support/docs/switches/nexus-5000-series-switches/117691-config-5500switch-00.html

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5500/sw/adapter-fex/6x/b_5500_Adapter_FEX_Config_6x/ b_5500_Adapter_FEX_Config_602N11_chapter_010.html

Question: 186

Multiple roles are applied to a user on the Cisco MDS 9000 Series Switch. Which statement is true?

A. Any commands that have conflicting settings between roles are denied.

B. Access to a command takes priority over being denied access to a command.

C. The first role assigned takes precedence over subsequent roles.

D. The last role assigned takes precedence over previous roles.

Answer: B

Explanation:

The statement that is true about the behavior of multiple roles applied to a user on the Cisco MDS 9000 Series Switch is that access to a command takes priority over being denied access to a command. This means that if a user has multiple roles assigned and one of the roles grants access to a command while another role denies access to the same command, the user will be able to execute the command. The access permission overrides the deny permission in case of a conflict.

The other statements are not true because:

Any commands that have conflicting settings between roles are not denied. As explained above, the access permission prevails over the deny permission in case of a conflict.

The first role assigned does not take precedence over subsequent roles. The order of role assignment does not affect the command authorization. All roles assigned to a user are evaluated together and the most permissive setting is applied.

The last role assigned does not take precedence over previous roles. The order of role assignment does not affect the command authorization. All roles assigned to a user are evaluated together and the most permissive setting is applied.

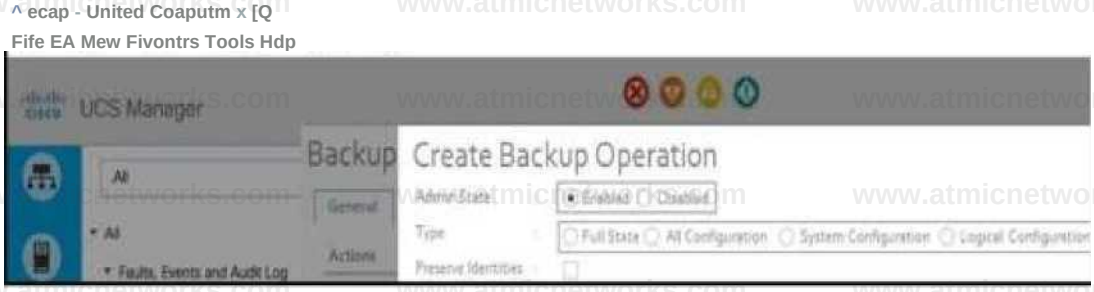
Reference: For more information on how to configure and manage roles on the Cisco MDS 9000 Series Switch, please refer to the following resources:

Cisco MDS 9000 Family NX-OS Security Configuration Guide

Cisco MDS 9000 Family NX-OS System Management Command Reference

Question: 187

Refer to the exhibit.



Which backup operation type does not include the Preserve Identities feature?

A. logical configuration

B. system configuration

C. full state

D. all configuration

Answer: A

Explanation:

The backup operation type that does not include the Preserve Identities feature is the logical configuration. This type of backup includes the settings and configurations that are logically defined within the Cisco UCS Manager, such as service profiles, policies, and management settings. However, it does not include the unique identifiers or 'identities' such as MAC addresses, WWN pools, and UUIDs, which are preserved in other types of backups like system configuration and full state.

Reference: The information about different backup operation types and the specifics of what each includes can be found in the Cisco Data Center Core Technologies documentation and the Cisco UCS Manager Backup and Restore Management Guide1.

Question: 188

Refer to the exhibit.

```
CISCO-UCS-A# scope org /
CISCO-UCS-A /org* I create service-profile Ciscol instance CISCO-UCS-A
/org/service-profile* ♦ set bios-policy biosl CISCO-UCS-A /org/service-profile*
I set boot-policy bootl CISCO-UCS-A /org/service-profile* # set ext-mgmt-ip-
state none CISCO-UCS-A /org/service-profile* # set host-fw-policy ipmi-user987
CISCO-UCS-A /org/service-profile* # set identity dynamic-uuid derived CISCO-UCS-
A /org/service-profile* ♦ set ipmi-access-profile ipmil CISCO-UCS-A
/org/service-profile* # set local-disk-policy locall CISCO-UCS-A /org/service-
profile* # set maint-policy maintl CISCO-UCS-A /org/service-profile* f set mgmt-
fw-policy mgmtl CISCO-UCS-A /org/service-profile* ♦ set power-control-policy
powerl CISCO-UCS-A /org/service-profile* ♦ set scrub-policy scrubl CISCO-UCS-A
/org/service-profile* I set sol-policy soil CISCO-UCS-A /org/service-profile* #
set stats-policy statsl CISCO-UCS-A /org/service-profile* I set user-label Cisco
CISCO-UCS-A /org/service-profile* * vcon-policy vconnpolicy CISCO-UCS-A
/org/service-profile* t commit-buffer CISCO-UCS-A /org/service-profile I
```

What is a characteristic presented in the service profile of the UUID?

A. based on the hardware

B. vendor assigned

C. unique system generated

D. allocated from a UUID pool

Answer: D

Explanation:

In Cisco Unified Computing System (UCS), a service profile's UUID (Universally Unique Identifier) can be allocated from a UUID pool. This pool is predefined within UCS Manager and allows for consistent identity assignment across different hardware, enabling stateless computing. The UUIDs are not based on the hardware, not vendor assigned, and although they are unique, they are not system

generated in this context; they are drawn from a pool created specifically for service profiles to ensure uniqueness and manageability within the UCS environment.

Reference: The concept of UUID pools and their use in service profiles is detailed in the Cisco Data Center Core Technologies documentation, particularly in sections discussing service profile creation and management within the UCS Manager. For a deeper understanding, the Cisco UCS Manager GUI Configuration Guide provides step-by-step instructions on how to create and assign UUID pools for service profiles.

Question: 189

A UCS B- Series server located in B5108 chassis 1 slot 1 is currently unavailable. The server needs to be associated with a specific service profile when it becomes available. Which associate service profile option should be selected to accomplish this goal?

A. server pool

B. server

C. custom server

D. restrict migration

Answer: B

Explanation:

The correct option to associate a UCS B-Series server with a specific service profile when it becomes available is B. server. In Cisco UCS Manager, associating a service profile with a server can be done directly by selecting the server from the list of available hardware. This direct association ensures that when the server becomes available, it will be associated with the specified service profile, which contains the settings and policies for the server's operation within the UCS environment.

Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course

Question: 190

Which service profile is affected if the default host firmware policy in Cisco UCS Manager is changed?

A. any service profile that has no host firmware policy defined

B. any service profile that uses a user-created host firmware policy

C. any service profile that is not in the root sub-org

D. any service profile that uses the global-default host firmware policy

Answer: D

Explanation:

Changing the default host firmware policy in Cisco UCS Manager affects any service profile that uses the global-default host firmware policy. This is because the global-default host firmware policy serves as a template for service profiles that do not have a specific host firmware policy defined. When changes are made to the default policy, they propagate to all service profiles that reference it, potentially affecting the firmware version and settings across multiple servers.

Reference: 350-601 DCCOR exam topics2.

Question: 191

A Cisco UCS user called “Employee1” accidentally changed the boot policy of the Cisco UCS server at the Cisco UCS Manager root level. This change impacted all service profiles, and their storage connectivity was lost. The system administrator wants to prevent this issue from recurring in the future. The new security policy mandates that access must be restricted up to the organization level and prevent other users from modifying root policies. Which action must be taken to meet these requirements?

A. Modify the privilege level assigned to the user

B. Assign users to a specific Cisco UCS locale

C. Assign the user "Employee1" the network-operator role

D. Define a custom user role and assign it to users

Answer: B

Explanation:

To prevent unauthorized changes at the root level and to restrict access up to the organization level, the appropriate action is to assign users to a specific Cisco UCS locale. A locale is a logical grouping that defines the scope of user permissions in Cisco UCS Manager. By assigning users to a locale, their access can be limited to specific organizations or service profiles, preventing them from modifying policies at the root level.

Reference: Cisco Data Center Certifications guide3.

Question: 192

What is an advantage of NFS as compared to Fibre Channel?

A. NFS enable thin provisioning for LUNs.

B. NFS provides the dynamic allocation of storage capacity.

C. NFS removes the impact of IP overhead.

D. NFS provides direct access to the underlying storage hardware.

Answer: B

Explanation:

An advantage of NFS (Network File System) as compared to Fibre Channel is that NFS provides the dynamic allocation of storage capacity. This means that NFS allows the storage space to be allocated and released on demand, depending on the needs of the applications and users. NFS also enables the sharing of files and directories across different servers and clients, simplifying the management and access of dat

a. Fibre Channel, on the other hand, is a protocol that provides high-speed and low-latency communication between storage devices and servers, but it requires fixed and pre-allocated storage capacity, which can lead to underutilization or overprovisioning of resources. Fibre Channel also requires dedicated hardware and cabling, which can increase the cost and complexity of the storage network.

Reference: For more information on NFS and Fibre Channel, please refer to the following resources:

DCCOR: Fibre Channel & Storage Networking

iSCSI vs. Fibre Channel

Question: 193

Which statement is true about upgrading the firmware on a Cisco MDS storage switch with dual supervisors?

A. The standby supervisor must be offline before the firmware upgrade begins.

B. Both supervisors load the new firmware and then the active supervisor reboots.

C. Supervisors can be upgraded independently to test the new firmware.

D. The new firmware is load on the standby supervisor first.

Answer: D

Explanation:

The statement that is true about upgrading the firmware on a Cisco MDS storage switch with dual supervisors is that the new firmware is load on the standby supervisor first. This is part of the non- disruptive upgrade process that allows the switch to continue operating while the firmware is updated. The standby supervisor receives the new firmware image and reloads with the new version, while the active supervisor remains in service with the old version. Then, a switchover occurs, making the standby supervisor the new active one, and the old active supervisor receives the new firmware image and reloads. Finally, the modules are upgraded one by one, starting from the lowest numbered module. The other statements are not true because:

The standby supervisor does not need to be offline before the firmware upgrade begins. It can be online and in standby mode, ready to receive the new firmware image and reload.

Both supervisors do not load the new firmware and then the active supervisor reboots. This would cause a disruption of service and a loss of configuration. The firmware upgrade is done in a sequential manner, with one supervisor at a time.

Supervisors cannot be upgraded independently to test the new firmware. The firmware versions on both supervisors must match, otherwise the switchover will fail and the switch will not operate properly.

Reference: For more details on how to perform a firmware upgrade on a Cisco MDS storage switch, please refer to the following resources:

How to Perform an MDS 9000 Series Switch Non-Disruptive Upgrade

Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide, Release 6.2(x)

Question: 194

A Cisco MDS 9000 series storage Switch has reloaded unexpectedly. Where does the engineer look for the latest core dump file?

A. /mnt/core

B. /mnt/pss

C. /mnt/logs

D. /mnt/recovery

Answer: A

Explanation:

The location where the engineer can look for the latest core dump file after a Cisco MDS 9000 series storage switch has reloaded unexpectedly is /mnt/core. A core dump file is a file that contains the memory state of the kernel at the time of a system failure. The core dump file can help the engineer or the Cisco technical support to analyze the cause of the problem and to fix it. The core dump file is stored in the /mnt/core directory on the switch, and it can be accessed using the CLI command 'show cores' or 'utils core active list'. The other directories (/mnt/pss, /mnt/logs, and /mnt/recovery) do not contain the core dump file, but they may contain other useful information for troubleshooting, such as process state information, log files, and recovery files.

Reference: For more information on how to troubleshoot core dumps on a Cisco MDS 9000 series storage switch, please refer to the following resources:

Troubleshooting Core Dumps

Cisco MDS 9000 Family Kernel Core Server Installation and Configuration Guide

Question: 195

In an FCoE environment, for which two sets of data must an interface that implements the PAUSE mechanism always provision sufficient ingress buffer? (Choose two)

A. frames that were sent with high credit

B. frames that were processed and transmitted by the transmitter before the PAUSE frame left the sender

C. frames that were sent on the link but not yet received.

D. frames that were sent on the link and received.

E. frames that were processed and transmitted by the transmitter after the PAUSE frame left the sender.

Answer: B, C

Explanation:

In an FCoE environment, the PAUSE mechanism is used to provide lossless behavior for Fibre Channel traffic over Ethernet. The PAUSE mechanism allows a receiver to send a PAUSE frame to a sender when its ingress buffer is full or close to full, instructing the sender to stop transmitting for a specified period of time. This prevents packet loss due to buffer overflow at the receiver. However, the PAUSE mechanism also introduces latency and jitter, which can affect the performance of FCoE applications. Therefore, the receiver must provision sufficient ingress buffer to accommodate the following two sets of data12:

Frames that were processed and transmitted by the transmitter before the PAUSE frame left the sender. These frames are already on the wire and cannot be stopped by the PAUSE frame. They will arrive at the receiver and consume ingress buffer space.

Frames that were sent on the link but not yet received. These frames are also on the wire and will arrive at the receiver after the PAUSE frame. They will also consume ingress buffer space.

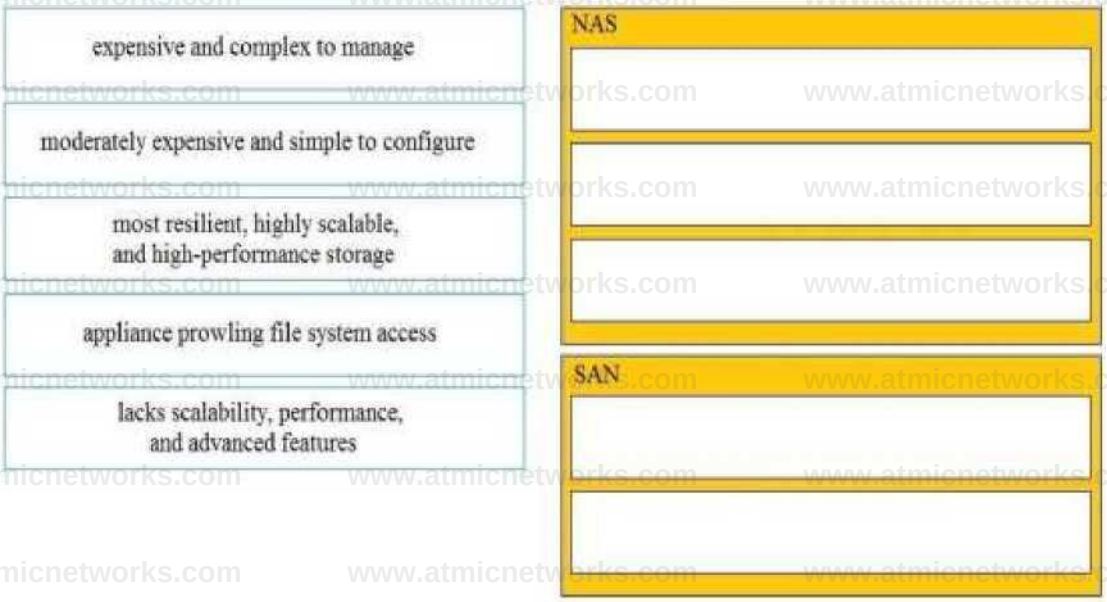
The amount of ingress buffer required depends on the link speed, the link distance, and the PAUSE duration. The receiver must ensure that the ingress buffer can hold at least twice the link distance worth of data, plus some margin for safety3. For example, if the link speed is 10 Gbps, the link distance is 10 km, and the PAUSE duration is 100 microseconds, the receiver must have at least 25 MB of ingress buffer for each FCoE virtual lane4.

Reference := 1: Nexus 7000 F2/F2e Ingress Buffer modifications for FCoE MultiHop over long distance - Cisco 2: Cisco Nexus 7000 Series FCoE Configuration Guide 3: In an FCoE environment, for which two sets of data must an interface that implements the PAUSE mechanism always provision sufficient ingress buffer? (Choose two) 4: Fibre Channel over Ethernet (FCoE) - Cisco

Question: 196

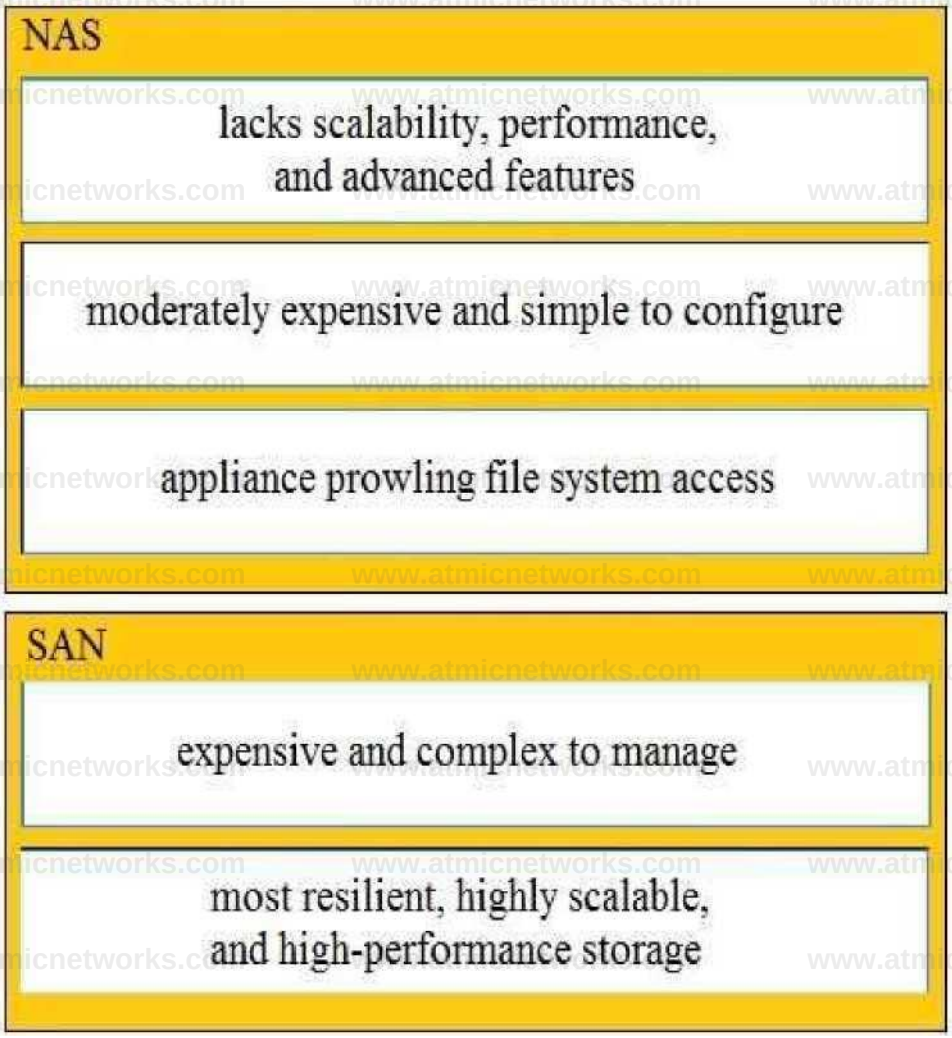
DRAG DROP

Drag and drop the characteristics from the left onto the correct storage systems on the right.



Answer:

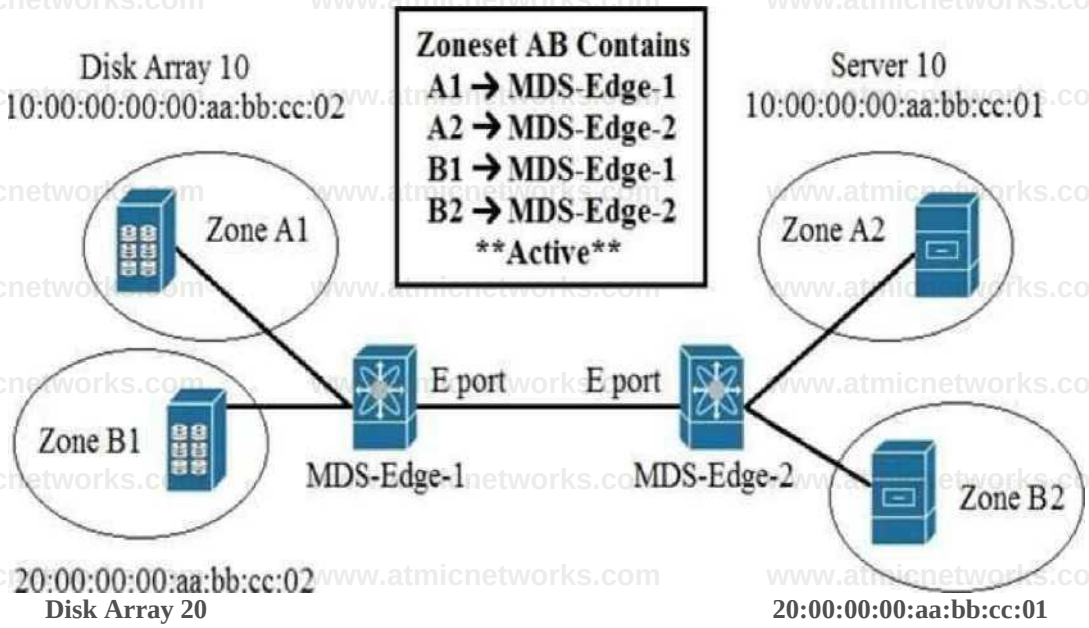
Explanation:



2,4,5 – NAS 1,3 - SAN

Question: 197

Refer to the exhibit.



An engineer is implementing zoning on two Cisco MDS switches. After the implementation is finished, E Ports that connect the two Cisco MDS switches becomes isolated. What is wrong with the implementation?

A. E Ports on both MDS switches must be configured as F ports for the zoning to function.

B. Zones are local to the MDS switch and name service must be used to activate the connection between E ports.

C. Different zone set names must be configured on both MDS switches.

D. Zones must have the same name on both MDS switches for the E ports to function.

Answer: B

Explanation:

The issue with the implementation is that zones are local to the MDS switch, and name service must be used to activate the connection between E ports. In Cisco MDS switches, zoning is enforced at the switch level. Each switch in a fabric can have a different active zone set or none at all. The name server for each switch only contains information about devices that are logged into that specific switch.

Question: 198

An engineer is implementing FCoE. Which aspect of DCBXP on a Cisco Nexus switch affects this implementation?

A. It uses the Cisco Fabric Services protocol to exchange parameters between two peer links.

B. It always is enabled on 10/100-Mbps native Ethernet ports.

C. It provides the authentication of peers on the Cisco Nexus switch.

D. It requires that LLDP transmit and LLDP receive are enabled on the FCoE interface.

Answer: D

Explanation:

FCoE (Fibre Channel over Ethernet) requires a lossless Ethernet network to ensure that no frames are dropped, which is crucial for storage traffic. DCBXP (Data Center Bridging Exchange Protocol) is part of the DCB (Data Center Bridging) suite of protocols that help to create a lossless Ethernet by providing a means to exchange parameters between peers to ensure consistent configuration across the network. For FCoE to function correctly on a Cisco Nexus switch, it is essential that LLDP (Link Layer Discovery Protocol) transmit and receive capabilities are enabled on the interface where FCoE is configured. This allows the switch to advertise and receive configuration information for parameters like priority-based flow control (PFC) and Enhanced Transmission Selection (ETS), which are critical for the lossless operation required by FCoE.

Reference: The information is based on the Cisco Data Center Core Technologies (DCCOR) course, which covers the implementation of data center technologies including network, compute, storage network, automation, and security.

More details can be found in the course material and official Cisco documentation on FCoE and DCBXP

implementation

Question: 199

Which product includes prebuilt templates that can be used to customize fabric deployments?

A. Cisco ACI

B. Cisco UCS Manger

C. Cisco data Center Network Manger

D. Cisco Tetration

Answer: C

Explanation:

Cisco Data Center Network Manager (DCNM) is designed to help manage all NX-OS network deployments, which includes LAN fabrics, SAN fabrics, and IP Fabric for Media (IPFM) networking in the data center. DCNM provides prebuilt templates that can be used to customize fabric deployments, allowing for a more streamlined and efficient setup process. These templates include best-practice policy templates for Easy Fabric Mode and support for Python scripting for more complex policy templates, facilitating the customization and automation of fabric deployments.

Reference: This information is supported by the Cisco Data Center Network Manager 11 Data Sheet, which outlines the features and benefits of DCNM, including the availability of prebuilt templates for fabric customization

Question: 200

Which statement about the MAC address that the FCoE Initialization Protocol chooses for use by an E-Node in an FCoE implementation is true?

A. The FCoE Initialization Protocol uses the burned-in MAC address of the converged network adapter for all FCoE operations.

B. The FCoE Initialization protocol uses a 24-bit FC-MAP and concatenates a 24-bit Fibre Channel ID to create a fibric-provided MAC address.

C. The FCoE Initialization Protocol uses 01.00.0C as the first 24 bits of the MAC address and appends a 24-bit Fibre Channel ID to derive a full 48-bit FCoE MAC address.

D. FCoE does not use a MAC address. The FCoE Initialization Protocol is used to acquire a Fibre Channel ID, and the address is used for all FCoE communications in the same way as Fibre Channel Protocol.

Answer: B

Explanation:

The FCoE Initialization Protocol (FIP) uses a 24-bit FC-MAP and concatenates a 24-bit Fibre Channel ID to create a fabric-provided MAC address. This is part of the FIP's role in establishing and maintaining the virtual links between an E-Node and the Fibre Channel Forwarder (FCF). The MAC address is essential for the E-Node to participate in FCoE communications within the fabric. The process ensures that each E-Node has a unique address on the Ethernet network, which encapsulates the Fibre Channel frames for transport. Reference := Cisco MDS 9000 Series FCoE Configuration Guide, Release 9.x

Question: 201

An engineer is implementing NPV mode on a Cisco MDS 9000 Series Switch. Which action must be taken?

A. The FCNS database must be disabled in the fabric.

B. A port channel must be configured to the upstream switch.

C. All switches in the fabric must be Cisco MDS switches.

D. NPIV must be enabled on the upstream switch.

Answer: D

Explanation:

When implementing NPV mode on a Cisco MDS 9000 Series Switch, it is crucial to ensure that NPIV is enabled on the upstream switch. NPV mode allows the switch to pass traffic between end devices and the core without consuming a domain ID. For NPV to function correctly, the upstream switch must support NPIV, which allows multiple virtual machines to share a single physical port without conflicts. Reference := Switch Configuration - Configuring N Port Virtualization

Question: 202

Which two statements describe modifying Cisco UCS user accounts? (Choose two.)

A. Disabling a user account maintains all of the data in the Cisco UCS Fabric Interconnect.

B. The admin account is used only to log on by using SSH.

C. The password of the user account must contain a minimum of 10 characters.

D. Local user accounts override the same account on a remote authentication server, such as TACACS, RADIUS, or LDAP.

E. The password of the user account expires in 30 days.

Answer: A, D

Explanation:

: In Cisco UCS, modifying user accounts involves several considerations. Disabling a user account does indeed maintain all the data in the Cisco UCS Fabric Interconnect, which means that the user's settings and privileges are retained even though the account is inactive (A). Local user accounts have precedence over remote authentication server accounts. This means that if a user account exists both locally and on a remote server like TACACS, RADIUS, or LDAP, the local account settings will take priority (D).

Reference := Managing User Accounts - Cisco1.

Question: 203

An engineer must ensure fabric redundancy when implementing NPV mode on a Cisco MDS 9000 Series Switch. Which action enables fabric redundancy?

A. Connect the NPV devices to multiple upstream switches.

B. Add a port channel to upstream switches.

C. Configure the NPV devices to use on external FLOGI database.

D. Use TE ports to connect to upstream switches.

Answer: A

Explanation:
For fabric redundancy in NPV mode on a Cisco MDS 9000 Series Switch, the engineer must connect the NPV devices to multiple upstream switches (A). This setup ensures that if one upstream switch fails, the NPV device can still reach the fabric through another upstream switch, maintaining fabric redundancy.

Reference := Switch Configuration - Configuring N Port Virtualization - Cisco2.

Question: 204

An engineer is converting a Cisco MDS switch to support NPIV mode. What should be considered when implementing the solution?

A. It must be enabled on VSAN 1 only.

B. It must be enabled globally on all VSANs.

C. It requires mapping of external interface traffic.

D. It requires the FLOGI database to be disabled.

Answer: B

Explanation:

When converting a Cisco MDS switch to support NPIV mode, it must be enabled globally on all VSANs (B). NPIV allows multiple virtual machines to share a single physical Fibre Channel port, which means that enabling it on all VSANs ensures that this functionality is available across the entire network.

Reference := Solved: Enabling NPIV - Cisco Community

Question: 205

DRAG DROP

An engineer must recover configuration on a Cisco MDS 9000 Series switch from a previous version that was backed up to bootflash and then verify the restoration.

Drag and drop the commands on the left to the correct order on the right.

copy boottlash:<conriguration_file> runring-config		Step 1
copy running-config startup-config		Step 2
show startup-config		Step 3
write erase		Step 4
reload		Step 5

Answer:

Explanation:

write erase

reload

copy boottlash:<conriguration_file> runring-config

copy running-config startup-config

show startup-config

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/nx- os/configuration/guides/fund/

fund_nx-os_5-x/b_Cisco_MDS_9000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_5- x/

b_Cisco_MDS_9000_Series_NX-OS_Fundamentals_Configuration_Guide_Release_5- x_chapter_01000.html

Question: 206

Refer to the exhibit.

```
N5K-1(config)#interface fc2/3
N5K-1(config-if)#switchport mode sd
N5K-1(config-if)# no shutdown
```

What is the result of implementing this configuration?

A. The Fibre Channel interface is configured for synchronization distribution.
B. The Fibre Channel interface is configured for SPAN.

C. The Fibre Channel interface is configuration for source distribution.

D. The Fibre Channel interface is configured for FSPF.

Answer: A

Explanation:

In the provided configuration, the commands are used to configure a Fibre Channel interface on a Cisco Nexus 5000 Series switch. The “interface fc2/3” command is used to enter the interface configuration mode for the specified Fibre Channel interface. The “switchport mode sd” command configures the Fibre Channel interface for synchronization distribution (SD). SD is a feature that allows the distribution of clocking information through the network to synchronize different parts of a system.

Reference: The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course provides detailed information on configuring Fibre Channel interfaces, including synchronization distribution12. Additional resources can be found in Cisco’s data center certification materials3

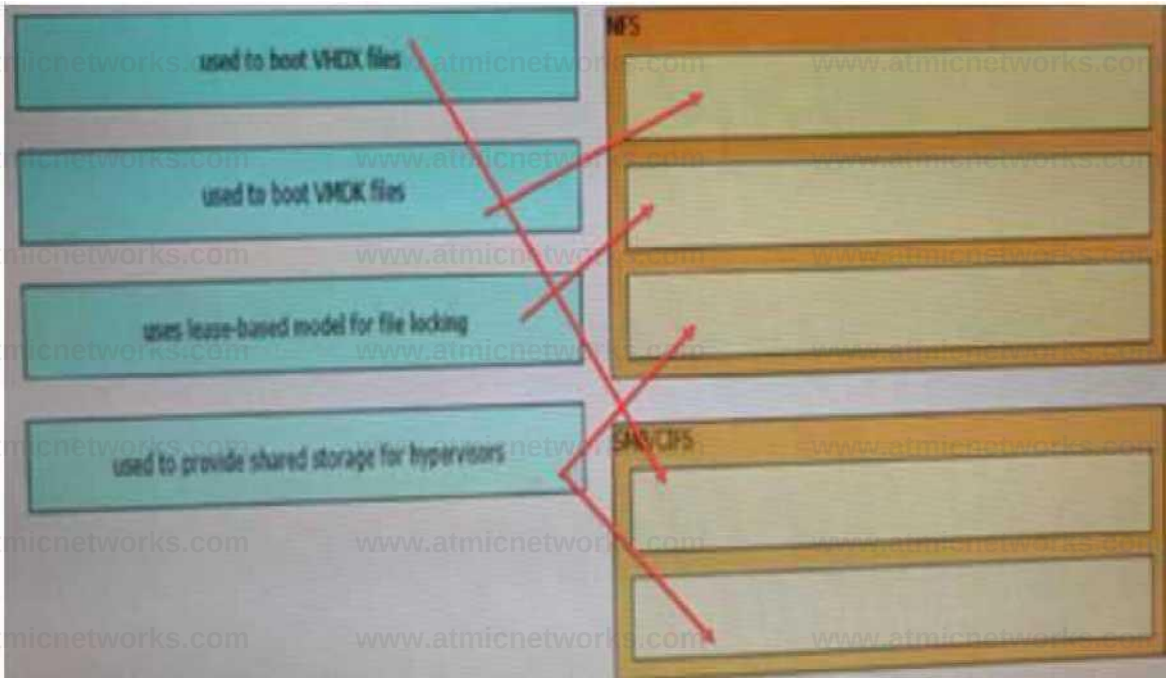
Question: 207

DRAG DROP

Drag and drop the characteristics from the left onto the NAS protocols on the right. Some characteristics are used more than once

Answer:

Explanation:



NFS:

-Used to boot VMDK files

-Uses lease-based model for file locking

-Used to provide shared storage for hypervisors

SMB/CIFS:

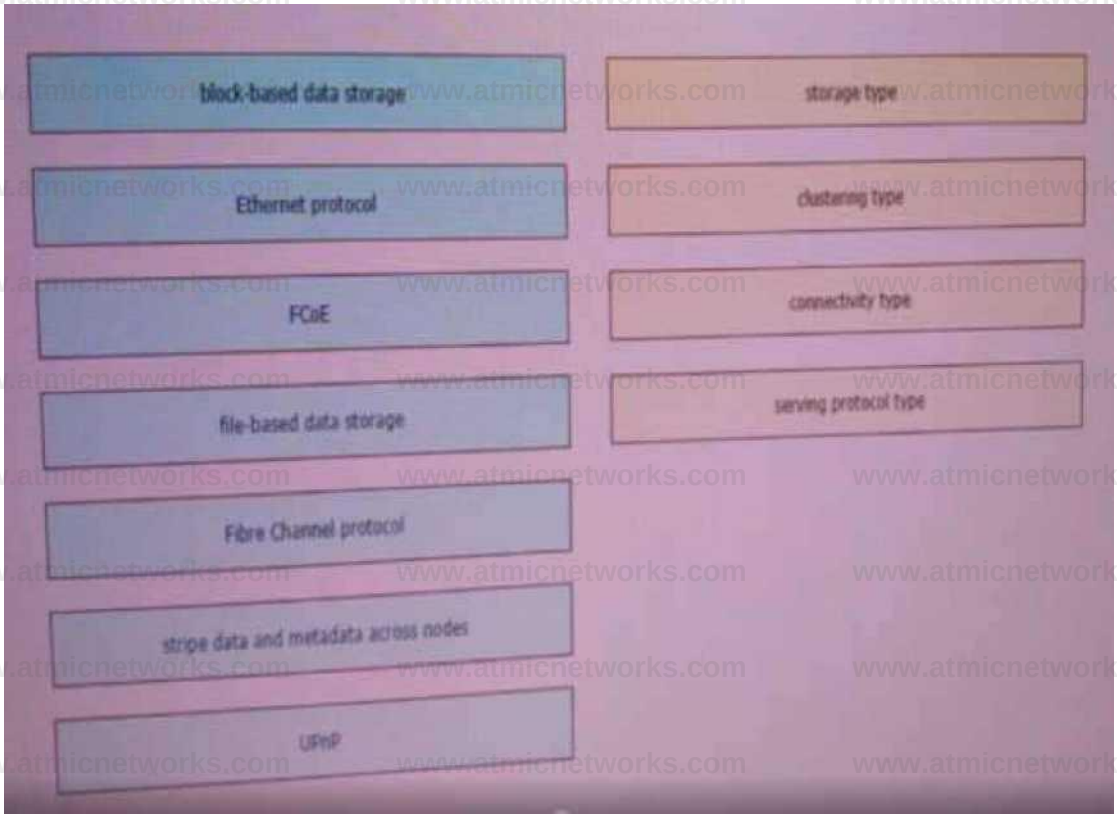
-Used to boot VHDX files

-Used to provide shared storage for hypervisors

Question: 208

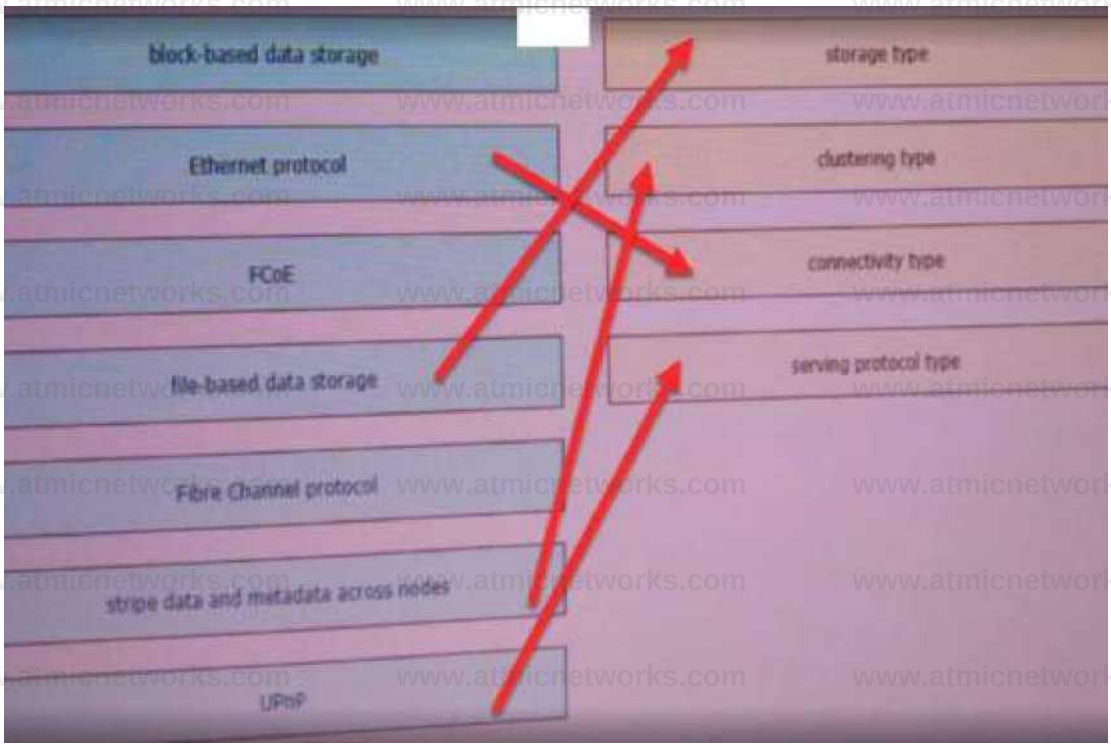
DRAG DROP

Drag and drop the NAS features from the left onto the NAS descriptions on the right. Not all features are used



Answer:

Explanation:



https://en.wikipedia.org/wiki/Network-attached_storage

Question: 209

An engineer implements SPAN configuration on an Nexus 5000 series switch. Which two commands are necessary to complete the SPAN session configuration? (Choose two)

```
N5K-Core# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
N5K-Core(config)# interface fc2/1
N5K-Core(config-if)# switchport speed 4000
N5K-Core(config-if)# no shutdown
N5K-Core(config)# interface fc2/2
N5K-Core(config-if)# no shutdown
N5K-Core(config)# monitor session 1
N5K-Core(config-monitor)# source interface fc2/1
N5K-Core(config-monitor)# destination interface fc2/2
N5K-Core(config-monitor)# no shutdown
```

A. Configure the switchport monitor under interface fc2/2

B. Configure the switchport mode SD under interface tc2/1.

C. Configure switchport speed 4000 under interface fc2/2.

D. Configure session type fc under monitor session 1.

E. Configure the switchport mode SD under interface fc2/2.

Answer: A, D

Explanation:

In the context of Cisco Data Center Core Technologies, SPAN (Switched Port Analyzer) is used to monitor network traffic. To configure a SPAN session on a Nexus 5000 series switch, an engineer would need to use specific commands. Option A, "Configure the switchport monitor under interface fc2/2," is correct as it involves setting up the monitoring port under a specific interface. Option D, "Configure session type fc under monitor session 1," is also correct as it specifies the type of session being configured for monitoring.

Reference := The explanation can be corroborated with detailed study from Cisco's official documentation and resources available on their website or the Cisco Data Center Core Technologies source book.

Question: 210

What is a recommended design choice in a topology for multipathing iSCSI traffic?

A. single initiator to dual targets

B. initiators and targets in separate subnets

C. dual initiators to a single target with bonded interfaces

D. two NICs bended together on the initiator

Answer: C

Explanation:

Multipathing iSCSI traffic is a technique to provide redundancy and load balancing for iSCSI connections between a server and a storage device. Multipathing can be achieved by using multiple initiators, multiple targets, or both. However, some design choices are more optimal than others, depending on the network topology and the capabilities of the devices involved. Option C, "dual initiators to a single target with bonded interfaces," is a recommended design choice because it provides the following benefits:

It allows the server to use two separate network interface cards (NICs) to connect to the same iSCSI target, which increases the bandwidth and availability of the connection.

It enables the use of link aggregation or bonding on the target side, which combines multiple physical interfaces into a logical interface that can handle more traffic and tolerate link failures.

It simplifies the configuration and management of the iSCSI sessions, as there is only one target to deal with, and the multipathing software can handle the path selection and failover.

Reference := The information is based on the Cisco Data Center Core Technologies (DCCOR) course, which covers the implementation of data center technologies including network, compute, storage network, automation, and security. More details can be found in the course material and official Cisco documentation on iSCSI multipathing

Question: 211

Which two actions should be taken before an upgrade is started on a Cisco MDS switch? (Choose two.)

A. check the impact of the upgrade using the show install all impact command

B. disable Cisco Fabric Services

C. back up the configuration

D. free up space on the USB3 device by deleting old Cisco NX-OS image files

E. make the primary supervisor the active supervisor

Answer: A, C

Explanation:

Before upgrading the Cisco NX-OS software on a Cisco MDS switch, it is important to perform some preparatory steps to ensure a smooth and successful upgrade process. Two of these steps are:

Check the impact of the upgrade using the show install all impact command. This command displays the compatibility and impact matrix for the upgrade, which shows the current and target versions of the software, the modules that will be upgraded, the modules that will be reloaded, and the modules that will be powered down. This information helps to plan the upgrade and minimize the disruption to the network.

Back up the configuration of the switch using the copy running-config startup-config command. This command saves the current running configuration to the startup configuration file, which is stored in the bootflash memory of the switch. This ensures that the configuration is preserved and can be restored in case of any issues during or after the upgrade.

Reference := The information is supported by the Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide, which provides detailed instructions and guidelines for upgrading the software on a Cisco MDS switch

Question: 212

Which two methods are available to Manage an ACI REST API session authentication when a user is unauthenticated?

A. POST to aaaLogin

B. POST to aaaUserLogin

C. GET aaaRefresh

D. GET to aaaListDomains

E. DELETE to aaaLogout

Answer: A, E

Explanation:

The ACI REST API is a programmatic interface that uses REST architecture to interact with the management information tree (MIT) of the Cisco Application Policy Infrastructure Controller (APIC).
The API requires authentication for users to access and manipulate the objects in the MIT. The authentication is based on username and password credentials, and the API provides several methods to manage the session authentication. Two of these methods are:

POST to aaaLogin. This method logs in a user and opens a session. The message body contains an aaa:User object with the name and password attributes, and the response contains a session token and cookie. The session token and cookie are required for subsequent requests to the API, and they have a limited validity period that can be refreshed.

DELETE to aaaLogout. This method logs out a user and closes a session. The message body contains an aaa:User object with the name attribute, and the response contains a status code indicating the success or failure of the operation. The session token and cookie are invalidated and cannot be used for further requests to the API.

Reference := The information is based on the Cisco APIC REST API Configuration Guide, which explains the usage and features of the ACI REST API, including the authentication methods89.

Question: 213

An administrator needs to configure an automated policy to shut down a link when a given threshold is exceeded on MDS switch. Which feature needs to be used?

A. Scheduler

B. RMON

C. EEM

D. Call Home

Answer: C

Explanation:

Embedded Event Manager (EEM) is a powerful tool used in Cisco devices, including MDS switches, to automate tasks and create custom scripts that react to network events. For an administrator needing to configure an automated policy to shut down a link when a threshold is exceeded, EEM is the appropriate feature to use. It allows the creation of event-driven automation scripts that can be

triggered when certain conditions are met, such as a link exceeding a specified threshold.

Reference: Cisco Data Center Core Technologies (DCCOR) training materials and Cisco's official documentation on EEM.

Question: 214

What is an advantage of using Ansible for automation as compared to puppet and chef?

A. Ansible automates the enforcement of configuration settings.

B. Ansible perform automation without installing a software agent on the target node.

C. Ansible configures a set of CLI commands on a device by using NETCONF.

D. Ansible abstracts a scenario so that set of configuration setting can be used across multiple operating systems.

Answer: B

Explanation:

Ansible is known for its agentless architecture, which means it does not require a software agent to be installed on the target nodes it manages. This contrasts with tools like Puppet and Chef, which typically require an agent to be installed on each node. Ansible uses SSH or WinRM to communicate with the nodes, making it simpler and more secure as it reduces the attack surface and the overhead of managing agents.

Reference: Comparison of DevOps tools including Ansible, Puppet, and Chef, as well as Ansible's official documentation.

Question: 215

What is required for using Ansible with HTTP/HTTPS protocol in a Cisco NX-OS environment?

A. SSH

B. Open Agent Container

C. XML management interface

D. NX-API

Answer: D

Explanation:

In a Cisco NX-OS environment, Ansible requires the NX-API to be enabled for HTTP/HTTPS protocol communication. NX-API is a REST-like API for NX-OS, providing a method for external applications to access the switch over HTTP/HTTPS, allowing for both CLI and simple object-based programming. This is necessary for Ansible to manage the device and execute automation tasks over these protocols.

Reference: Cisco's official documentation on NX-API and Ansible's documentation for Cisco NX-OS support.

Question: 216

A POAP-enabled Cisco Nexus switch will not enter POAP mode. Which two conditions should be verified? (Choose two.)

A. Bootflash must contain a special directory named POAP with poap.py file.

B. The switch is in bootup process.

C. No startup configuration is available.

D. The license file is missing on the switch.

E. No Cisco NX-OS image is present on the bootflash.

Answer: BC

Explanation:

POAP is an automatic provisioning and zero-touch deployment feature that assists device owners in the initial deployment and configuration of Nexus switches.

The feature works by checking for a local configuration script. If the script has been deleted, the switch has been reset to factory settings, or this is the first boot-up, the POAP daemon will connect to a preset list of servers to download an initial configuration file.

To perform this operation, the switch must first obtain an IP address from a local DHCP server. POAP configuration settings can also be passed through the DHCP response.

Which conditions should be verified, so they need to be TRUE. Like no startup (A) and bootup (B). C means that it needs to miss a license file and E means it needs to miss an NX-OS image.

Question: 217

AN engineer enters these commands while in EEM on a Cisco Nexus 9000 Series Switch.

event manager applet Backup-config

event timer watchdog time 1800 name timer

event cli match “copy running-config startup-config”

what is the result of applying this configuration?

A. It saves the running configuration every 1800 seconds.

B. It generates an error because no action is mentioned.

C. It executes the copy running-config startup-config command.

D. It blocks the copy running-config startup-config command.

Answer: B

Explanation:

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/93x/system- management/b-cisco-nexus-9000-series-nx-os-system-management-configuration-guide-93x/b- cisco- nexus-9000-series-nx-os-system-management-configuration-guide-93x_chapter_0100010.html

Prerequisites for EEM

EEM has the todowing prerequisites:

- Ybu must have network-adnun user privileges to configure EEM

Guidelines and Limitations for EEM

EEM has the Mowing configuration guidelines end UmltMom:

- The rnapHTium number of configurable EEM policed- <’4 500
- Action statement* wittan your user pcGcy or overriding policy should not negate each other or adversely affect the awoewted system policy.
- To allow a triggered event to process any detail! actions you must configure the EEM potcy to Mow the detain action For example. if you match a CM command in a match statement, you mufti add the event-default action statement to th EEM pobey or EEM w® not allow the CLI command to execute
- Wren you configure an EEM policy action to colled show tech commands make sure to allocate enough time tot the show tech commands to complete before the same action is called again

Question: 218

AN engineer is asked to modify an overridden policy by changing the number of FCNS database entries to 1500 and then generable a massage. What configuration will accomplish this task?

A. event manager applet fcns_policyevent fens entries max-per-switch 1500 action 1.0 syslog priority warnings msg FCNS DB entries have reached the EEM limit action 2.0 policy-default

B. event manager applet fcns_policy override _fcns_entries_max_per_switch action 1.0 syslog priority errors "CNS DB entries have reached the EEM limit" action 2.0 policy-default

C. event manager applet fcns_policy override _fcns_entries_max_per_switch event fens entries max-per-switch 1500
action 1.0 syslog priority v/arnings msg FCNS DB entries have reached the EEM limit

D. event manager applet fcns_policy action 1.0 syslog priority warnings msg FCNS DB entries have reached the EEM limit action 2.0 event-default

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The following example modifies an overridden policy by changing the number of FCNS database entries to 1500. It also generates both the configured and the default syslog messages of the default system policy

event manager applet fcns_policy override fcns_entries_max_per_switch

event fcns entries max-per-switch 1500 action 1.0 syslog priority warnings msg FCNS DB entries have reached the EEM limit.

Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/mds9000/sw/8_x/config/systemmanagement/cisco_mds9000_system_management_config_guide_8x/configuring_the_embedded_event _manager.html

Question: 219

Refer to the exhibit.

```
<?xml version="1.0" encoding="UTF-8"?><imdata totalCount="1"Xerror code="403"
text="Token was invalid (Error: Token timeout)"/></imdata>
```

An engineer configures a new application profile using REST API and receives this error massage. Which method can be used before application profile can be configured?

A. POST to aaaLogin
B. POST to aaaRefresh
C. POST to aaaLogout
D. GET to aaaListDomains

Answer: A

Explanation:

To configure an application profile using REST API, the engineer needs to first authenticate with the APIC using the POST method to the aaaLogin URI. This will return a token that can be used for subsequent requests. The error message indicates that the token is missing or expired, so the engineer needs to perform the POST to aaaLogin method again before configuring the application profile. Reference := [Cisco APIC REST API Configuration Guide]

Question: 220

An engineer is asked to manage a large-scale data center and collect information from multiple Cisco NX-OS devices using Cisco NX-OS Data Management Engine model. Which technology should be used to accomplish this goal?

A. NX-API REST

B. NETCONF

C. JSON-RPC

D. NX Yang

Answer: B

Explanation:

Cisco NX-OS Data Management Engine (DME) model is a hierarchical representation of the configuration and operational state of the Cisco NX-OS devices. It supports multiple protocols for accessing and manipulating the data, such as NETCONF, RESTCONF, gRPC, and CLI. Among these, NETCONF is the recommended technology for managing a large-scale data center and collecting information from multiple Cisco NX-OS devices using DME model, because it provides a standard, secure, and scalable way of communicating with network devices. Reference := [Cisco NX-OS Data Management Engine Model]

Question: 221

An engineer needs a utility to translate traditional Nexus CLI inputs and generate Python code using XML and JSON message formats. The solution needs to be available on a Nexus 7700 series switch. Which utility should be used?

A. NX-OS JSON-RPC

B. NX-API Sandbox

C. Guest Shell for NX-OS

D. Open NX-OS

Answer: B

Explanation:

NX-API Sandbox is a utility that allows the engineer to translate traditional Nexus CLI inputs and generate Python code using XML and JSON message formats. It is available on a Nexus 7700 series switch as a web-based tool that can be

accessed from a browser. It provides a graphical interface for entering CLI commands and viewing the corresponding Python code and output. It also allows the engineer to execute the Python code directly on the switch or copy it to a script file. Reference := [Cisco Nexus 7000 Series NX-OS Programmability Guide]

Question: 222

An engineer must configure RBAC is Cisco UCS Manager in an existing data center environment.
Which two roles can be used to configure LAN Connectivity policies? (Choose two.)

A. network-admin
B. server-profile
C. admin
D. enable
E. operations

Answer: A, C

Explanation:

In Cisco UCS Manager, RBAC (Role-Based Access Control) is used to define what users can do within the system. The roles that can be used to configure LAN Connectivity policies are typically those with administrative privileges. The network-admin role has the necessary privileges to configure network-

related settings, including LAN Connectivity policies. Similarly, the admin role has full administrative rights over all system configuration aspects, which also encompasses LAN Connectivity policies. The other roles listed do not have the appropriate level of access for this task.

Reference: The information is aligned with the Cisco Data Center Core Technologies source book, which details RBAC roles and their permissions within the Cisco UCS Manager environment

Question: 223

An engineer has a primary fabric that is named UCS-A and a secondary fabric that is named UCS-B. A certificate request that has a subject name of sjc2016 for a keyring that is named kr2016 needs to be created. The cluster IP address is 10.68.68.68.

Which command set creates this certificate request?

A. UCS-A # scope keyring kr2016

UCS-A /keyring # create certreq 10.68.68.68 sjc2016

UCS-A /keyring* # commit-buffer

B. UCS-B # scope keyring kr2016

UCS-B /keyring # create certreq ip 10.68.68.68 subject-name sjc2016

UCS-B /keyring* # commit-both

C. UCS-B# scope security

UCS-B /security # scope keyring kr2016

UCS-B /security/keyring # set certreq 10.68.68.68 sjc2016

UCS-B /security/keyring* # commit-both

D. UCS-A# scope security

UCS-A /security # scope keyring kr2016

UCS-A /security/keyring # create certreq ip 10.68.68.68 subject-name sjc2016

UCS-A /security/keyring* # commit-buffer

Answer: D

Explanation:

To create a certificate request in Cisco UCS Manager, the correct command set involves navigating to the security scope, selecting the appropriate keyring, and then creating the certificate request with the specified IP address and subject name. The commands in option D correctly follow this procedure. The commit-buffer command is used to commit the changes in UCS-A, which is the primary fabric.

Reference: This process is documented in the Cisco UCS Manager certificate management guidelines, which provide step-by-step instructions on creating certificate requests using the CLI

Question: 224

Port security is enabled on a Cisco MDS 9000 series Switch. Which statement is true?

A. Cisco Fabric Services must be disabled before enabling port security.

B. Port security can be enabled only globally and affects all VSANs.

C. Auto-learning is always enabled automatically when port security is enabled.

D. Any devices currently logged in must be added manually to the device databased.

Answer: D

Explanation:
Port security on Cisco MDS 9000 series Switches is a feature that allows administrators to restrict access to the switch ports to specific devices. When port security is enabled, it does not automatically add currently logged-in devices to the device database; they must be added manually.

This ensures that only authorized devices can access the network, enhancing the security of the SAN environment.

Reference: The Cisco MDS 9000 Series Security Configuration Guide provides detailed information on the configuration and behavior of port security, including the requirement for manual addition of devices to the database

Question: 225

When a strict CoPP policy is implemented, which statement describes an event during which packets are dropped?

A. Fifteen SSH sessions remain connected to the switch.

B. A large system image is copied to a switch by using the default VRF.

C. A ping sweep is performed on a network that is connected through a switch.

D. A web server that is connected to a switch is affected by a DDoS attack.

Answer: C

Explanation:

A strict CoPP (Control Plane Policing) policy is designed to manage the traffic flow of control plane packets to protect the control plane of routers and switches from being overwhelmed by unnecessary or malicious traffic. When a ping sweep, which involves sending ICMP echo requests to multiple hosts to identify live devices on a network, is performed on a network connected through a switch with a strict CoPP policy, excess ICMP packets can be dropped to prevent them from consuming excessive resources. Reference: Cisco Data Center Core Technologies source documents or study guide

Question: 226

Which two authentication types does Cisco UCS Manager support when configuration authentication? (Choose two.)

A. local

B. LDAP

C. 802.1X

D. Kerberos

E. PAM

Answer: A, B

Explanation:

Cisco UCS Manager supports various types of authentication mechanisms for enhanced security. Option A (local) refers to the use of locally stored user credentials within the UCS Manager for authentication. Option B (LDAP) indicates that UCS Manager can integrate with LDAP (Lightweight Directory Access Protocol) directories for user authentication, allowing centralized management of user credentials. Reference: Cisco Data Center Core Technologies source documents or study guide

Question: 227

Refer to the exhibit.

```
NEXUS    (config)#feature tacacs+
NEXUS(config)#    tacacs-server timeout 5
NEXUS(config)f    tacacs-server directed-request
NEXUS(config)#    tacacs-server deadtime 0
NEXUS    (config)#tacacs server host 10.1.50.20 port 49
NEXUS(config)♦    tacacs-server host 10.1.50.20 key 7 "Flwhgl23" timeout 1 aaa group server
NEXUS (config)#   tacacs+ ISE
NEXUS(config-tacacs+)# server 10.1.50.20
NEXUS (config-tacacs+)# deadtime 10
NEXUS(config-tacacs+)t use-vrf management
NEXUS (config-tacacs+)# source-interface mgmt 0
NEXUS (config)# aaa authentication login default group ISE
```

What is the result of implementing this configuration?

A. The TACACS+ server uses the type-6 encrypted format.

B. The switch queries the TACACS+ server by using a clear text PAP login.

C. The timeout value on the TACACS+ server is 10 seconds.

D. The switch queries the TACACS+ server by using an encrypted text PAP login.

Answer: D

Explanation:

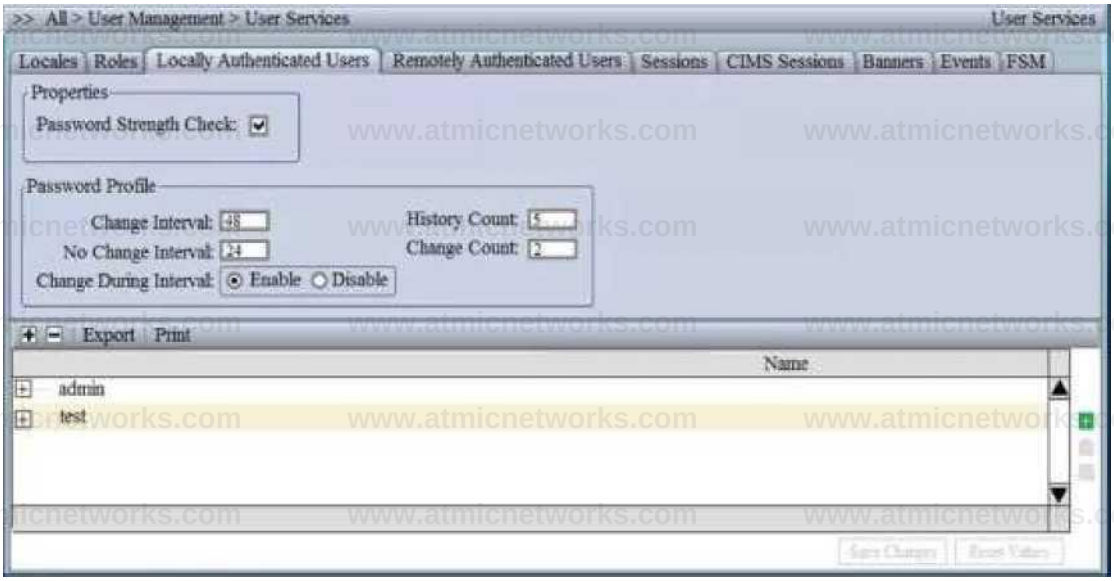
The configuration commands shown in the exhibit set up TACACS+ on a Cisco Nexus device.

The tacacs-server host command with the key argument specifies that the switch should use an encrypted key when communicating with the TACACS+ server. Therefore, the switch will query the TACACS+ server using an encrypted text PAP login. Reference: Cisco Data Center Core Technologies source documents or study guide123.

Please note that these answers are based on the information available from the Cisco Data Center Core Technologies resources and the context provided in the questions. For the most accurate and detailed explanations, it's always best to refer directly to the official Cisco documentation and study guides.

Question: 228

Refer to the exhibit.



Which setting must be configured to prevent reuse of passwords?

A. No Change Interval

B. Change Interval

C. History Count

D. Change Count

Answer: C

Explanation:

The History Count setting in a user management system is used to prevent the reuse of old passwords. It specifies the number of unique new passwords that must be used before an old password can be reused. This helps enhance security by ensuring that passwords are not easily guessable and that users are not cycling through a small set of favorite passwords.

Question: 229

An engineer is configuring AAA authentication on an MDS 9000 switch. The LDAP server is located under the IP 10.10.2.2. The data sent to the LDAP server should be encrypted. Which command should be used to meet these requirements?

A. ldap-server host 10.10.2.2 enable-ssl

B. ldap-server 10.10.2.2 port 443

C. ldap server host 10.10.2.2 key SSL_KEY

D. ldap-server 10.10.2.2 key SSL_KEY

Answer: A

Explanation:

The command "ldap-server host 10.10.2.2 enable-ssl" is used to configure AAA authentication on an MDS 9000 switch with an LDAP server located at the IP 10.10.2.2. This command ensures that the data sent to the LDAP server is encrypted using SSL, which is a protocol for securing network communication.

Reference: For more information, refer to the Cisco Data Center Core Technologies (DCCOR) study guide or source documents, specifically the sections covering AAA authentication configuration and LDAP server integration with MDS 9000 switches.

Question: 230

Refer to the exhibit.

```
switch(config)# feature dhcp
switch(config)# ip dhcp snooping
switch(config)# service dhcp
switch(config)# ip dhcp snooping vlan 100,200,250-252
switch(config)# ip dhcp relay information option
```

Which action is taken to ensure that the relay agent forwards the DHCP BOOTREQUEST packet to a DHCP server?

A. Configure the interface of the DHCP server as untrusted.

B. Configure the IP address of the DHCP server.

C. Enable the DHCP relay agent.

D. Verify the DHCP snooping bindings.

Answer: C

Explanation:

Enabling the DHCP relay agent on a switch allows it to forward DHCP BOOTREQUEST packets from clients to a DHCP server, even if they are not on the same physical subnet. This is crucial for clients to obtain an IP address and other network configuration parameters from a DHCP server that is not locally present on the subnet.

Reference: Detailed information on DHCP relay agents can be found in the Cisco Data Center Core Technologies (DCCOR) study guide or source documents, particularly in the chapters discussing DHCP configuration and management in network environments.

Question: 231

A network administrator must perform a system upgrade on a Cisco MDS 9000 Series Switch. Due to the recent changes by the security team:

- The AAA server is unreachable.
- All TCP communication between the MDS 9000 Series Switch and AAA servers is disabled.

Which actions must be used to perform the upgrade?

A. Log in locally to the MDS 9000 Series Switch using a network-admin role and download the upgrade files from

the remote TFTP server.

B. Log in locally to the MDS 9000 Series Switch using a server-admin role and download the upgrade files from the remote FTP server.

C. Log in to a server storing the upgrade files remotely using a server-admin role and download the files to the MDS 9000 Series Switch using SFTP.

D. Log in to a server storing the upgrade files remotely using a network-admin role and download the files to the MDS 9000 Series Switch using HTTP.

Answer: A

Explanation:

Since the AAA server is unreachable and TCP communication with the AAA servers is disabled, the network administrator must log in locally using a network-admin role. The upgrade files can then be downloaded from a remote TFTP server, which does not require TCP communication and can operate over UDP, thus bypassing the TCP restriction.

Reference: Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide, Release 8.x

Question: 232

An engineer must implement a VXLAN-based data center interconnect. The long-distance transport provided by a service provider is IP-based,supports a maximum MTU of 1554 bytes, and does not support outbound traffic replication. Which action must be take to build the data center interconnect?

A. Configure a route map to associate the IPs of the remote VTEPs.

B. Create an IP access list and associate it with VNI to replicate traffic to remote VTEPs.

C. Announce host reachability over BGP.

D. Implement BGP EVPN ingress replication.

Answer: C

Explanation:

In a VXLAN-based data center interconnect scenario where the transport supports a maximum MTU of 1554 bytes and does not support outbound traffic replication, the engineer must use BGP to announce host reachability. This allows for the advertisement of host routes over the BGP session, enabling remote VTEPs to learn about hosts in the interconnected data centers without relying on traffic replication.

Reference: VXLAN UNDERLAY - MTU considerations - Cisco Community2; MTU Considerations for VXLAN | Matt Oswalt

Question: 233

An engineer is performing a configuration on a Cisco Nexus 5000 Series Switch. The requirement is for the current Fibre Channel IDs in VSAN 120 to be saved across reboots. The Cisco environment also must integrate with a third-party solution that requires persistent Fibre Channel IDs for the VSAN The WWN of the Cisco switch must be 33:*8:00:05:30:00:16:df and its Fibre Channel ID 0x070128 Which command set meets these requirements?

fabric-binding database vsan 120 vsan 120 wwn 33:e8:00:05:30:00:16:df fcid 0x070128

vain 120 wwn 33:o8:00:03:30:00 16:d1 fcld 0x070128 fcdomain fold preserve vsan 120

Man 120 wwn 33:e8:00:05:30:00:16 d! fcld 0x070128 fabric-binding activate vsan 120
purge fcdomain fcld vsan 4

fcdomain fcld database
vsan 120 wwn 33:e8:00.05:30:00:16df fcld 0x070128
fcdomain fcld persistent vsan 120

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

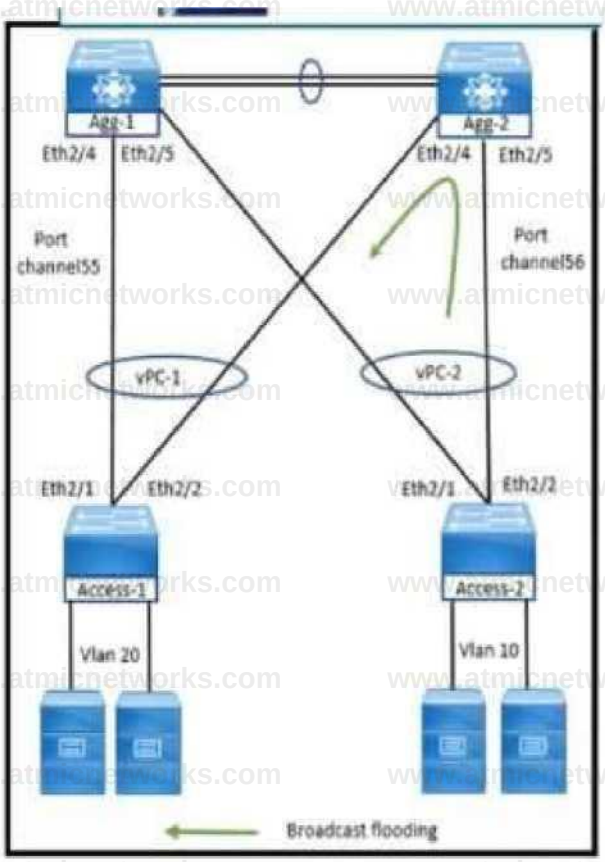
Explanation:

The correct command set is Option C, which includes the command fcdomain fcid persistent vsan 120. This command ensures that the Fibre Channel IDs (fcid) are saved across reboots for VSAN 120, meeting the requirement for persistent Fibre Channel IDs. The other commands in Option C are used to set the WWN and fcid as per the given requirements.

Reference: For a comprehensive explanation, please refer to the "Implementing and Operating Cisco Data Center Core Technologies (DCCOR)" course, which covers the skills and technologies needed to implement data center compute, LAN, and SAN infrastructure, including the management of Fibre Channel IDs

Question: 234

Refer to the exhibit.



Refer to the exhibit. What happens to the broadcast traffic when it reaches aggregation switches?

A. Only Agg-1 switch receives broadcast packets and does not forward to the peer link on Agg-2 switch.

B. Agg-1 switch prevents broadcast packets received on the vPC peer link from exiting the switch on ports Eth2M and Eth2/5

C. Agg-2 switch receives broadcast packets and stops forwarding to the peer link on Agg-1 switch.

D. Agg1 and Agg2 switches receive broadcast packets and does not forward them to me peer link or the port channel

Answer: B

Explanation:

In a vPC (Virtual Port Channel) environment, broadcast packets received on the vPC peer link are not forwarded out on the vPC member ports. This behavior is due to the vPC loop avoidance rule, which

prevents traffic received on a vPC peer link from being sent back out of the vPC member ports.

Therefore, the Agg-1 switch will prevent broadcast packets that arrive on the vPC peer link from exiting the switch on ports Eth2/4 and Eth2/5.

Reference: For more detailed information, you can refer to the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course, which covers the essentials of vPC operations and the loop avoidance mechanism

Question: 235

The VMM domain is integrated between Cisco APICs and vCenter using a distributed vSwitch. The traffic must be blocked between a subset of endpoints in an EPG based on specific VM attributes and the rest of the VMs in that EPG. Which set of actions blocks this traffic?

1 Set Wk* Uicioseginentailon under rhe EPG VMM Domain Association to 'True"
2 Set Inna.EPG Isolation to "Entweed" for the EPG
3 Set Inira-EPG Iteration to "Enforced' for the uSeg EPG

1 Sei Allow Micnwegmentatian under the EPG VMM Domain Association to "True"
2 Set tntra-EPG Isolation to "Unenforced* for the EPG
3 Set Intra-EPG isolation to "Unenforced* for the uSeg EPG

i Set Allow Mtcroscgmentation under rhe EPG VMM Domain Association to Tasc*
2 . Set Inha-EPG Isolation to "Unenforced* for the EPG
3 Set Intra-EPG Isolation to "Enforced" far the uSeg EPG

1 . Set A. low Mtcrosegme ntation under the EPG VMM Domain Association to "True"
2 Set Inha-EPG Isolation to "Enforced" far the EPG
3 Set Inua-EPG Isolation to "Unenforced* lor the uSeg EPG

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To block traffic between a subset of endpoints in an EPG based on specific VM attributes and the rest of the VMs in that EPG, the correct set of actions would involve setting “Allow Microsegmentation” under the EPG VMM Domain Association to “True” and setting “Intra-EPG Isolation” to “Enforced” for both the EPG and the uSeg EPG. This configuration ensures that microsegmentation is allowed and that intra-EPG isolation is enforced, effectively blocking the specified traffic.

Reference:

The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course provides insights into the implementation of data center technologies, including network, compute, storage network, automation, and security1.

The Cisco Community articles on VMM Integration & Troubleshooting and ACI VMM integration provide practical guidance and troubleshooting tips for integrating VMM domains with Cisco ACI23.

For detailed procedures and additional information, the configuration guides and training materials available on Cisco’s official website are valuable resources

Question: 236

An engineer must configure OSPFv2 connectivity between a pair of Cisco Nexus switches. The connection between the switches must meet these requirements:

Use unicast for updates.
Use decentralized communication of updates.

Full adjacency between switches.

Which configuration is needed to meet these requirements?

A. interface with a type of p2p network

B. stub area between the neighbors

C. filter list between the neighbors

D. virtual link between the neighbors

Answer: A

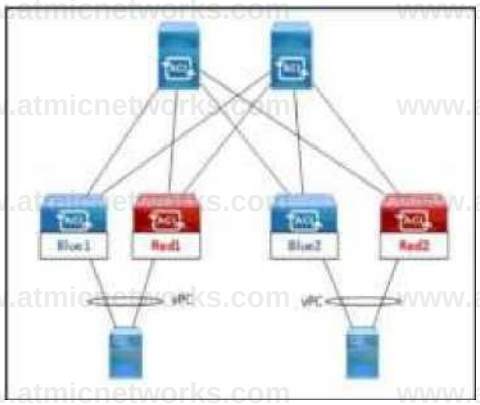
Explanation:

OSPFv2 can be configured for unicast updates and decentralized communication through a point-to- point (p2p) network type on the interface connecting the Cisco Nexus switches. This configuration ensures that OSPFv2 updates are sent directly between the two switches without the need for a designated router, meeting all listed requirements including full adjacency1.

Reference := For more information, refer to the "Implementing and Operating Cisco Data Center Core Technologies (DCCOR)" course details on Cisco's official website

Question: 237

Refer to the exhibit.



Refer to the exhibit. An engineer must schedule the firmware upgrade of the Red1 and Red2 leaf switches. The requirement is to keep the upgrade time to the minimum, avoid any service impact, and perform the parallel upgrade Which set of scheduler attributes must be used to meet these requirements?

- Configure Schedulerpolicy 1 for all four leaf switches Bluel, Blue2 Red1 and Red2
- Configure SchedulerPolicyl and SchedulerPolicy2 with a one-time window tngger that has maximum concurrent nodes 1

- Configure SchedulerPolicyl for leaf switches Bluel and Red1 and SchedulerPohcy2 for leaf switches Blue2 and Red2
- Configure SchedulerPolicyl and SchedulerPolicy2 with a one-time window tngger that has maximum concurrent nodes 2

- Configure SchedulerPolicyl for all four leaf switches Bluel, Blue2 Red1 and Red2
- Configure SchedulerPolicyl and SchedulerPolicy2 with a one-time window trigger that has maximum concurrent nodes 2

- Configure SchedulerPolicyl for leaf switches Bluel and RedI, and SchedulerPolicy2 for leaf switches Blue2 and Red2 •

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

To schedule the firmware upgrade of the Red1 and Red2 leaf switches with the requirements of minimal upgrade time, no service impact, and parallel upgrade, SchedulerPolicy1 and SchedulerPolicy2 with a one-time window trigger that has maximum concurrent nodes 2 should be used. This allows both Red1 and Red2 to upgrade simultaneously within the same maintenance window, thus minimizing the time and avoiding any service disruption.

Reference := Further details can be found in the Cisco Data Center Core Technologies documentation

Question: 238

An engineer must perform a backup operation of the Cisco UCS system. The backup must be transferred to a secure location using UDP and must contain information about VLANs, VSANs, and other policies. Also, the operations team requires the backup file to be in a human-readable format. Which configuration set meets these requirements?

A. Type: System configuration

Protocol: SCP

B. Type: Logical configuration

Protocol: TFTP

C. Type: All configuration

Protocol: FTP

D. Type: Full state

Protocol: SFTP

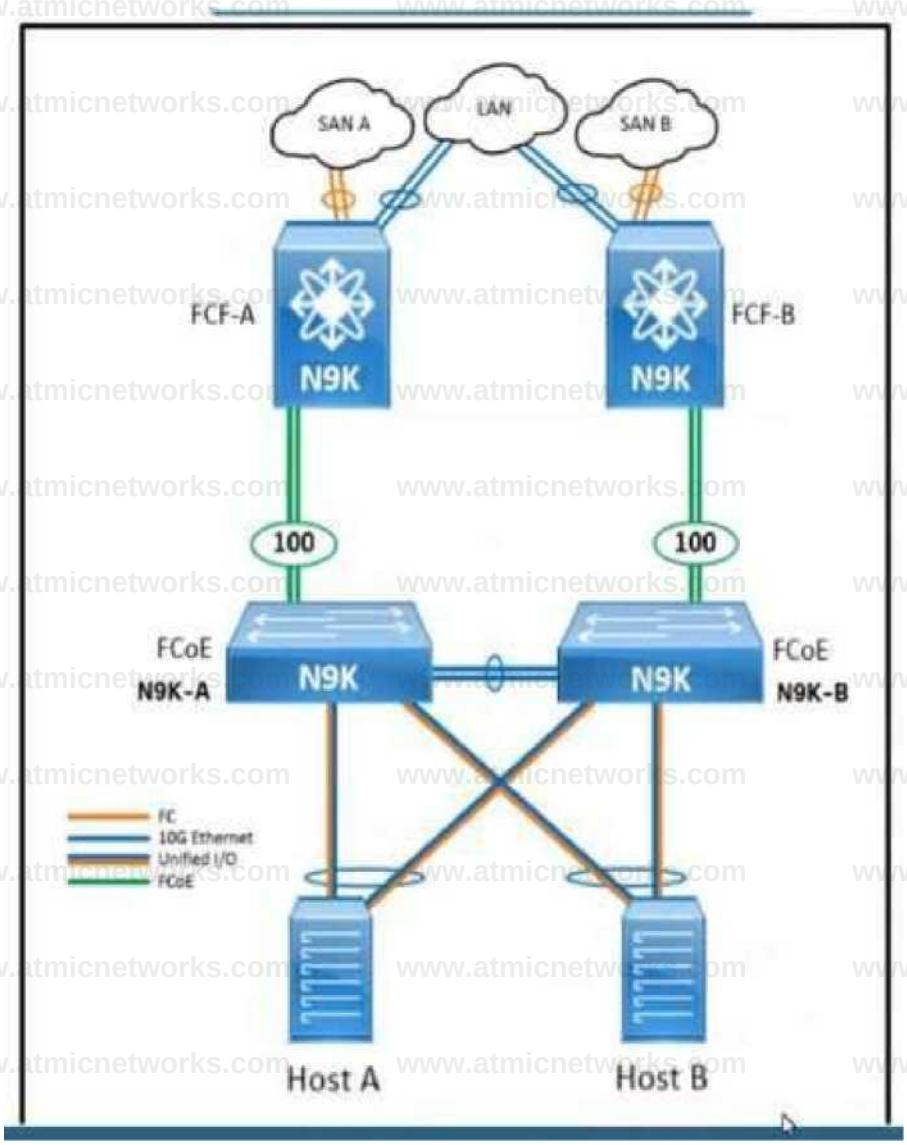
Answer: B

Explanation:

This type of backup includes information about VLANs, VSANs, and other policies and is in XML format, which is human-readable. Although the question specifies the use of UDP, none of the options provided use UDP as they are all TCP-based protocols; however, TFTP is often confused with being UDP-based because it is a lightweight protoco

Question: 239

Refer to the exhibit.



Refer to the exhibit. An engineer must configure FCoE between the N9K-A switch and the FCF-A Nexus 9000 core switch. The deployment has these characteristics:

The N9K-Aand N9K-B top-of-rack switches share the domain ID of the core switches.

The hosts are equipped with converged network adapters.

The only VSAN that is permitted to traverse port-channel 100 is VSAN 20.

Which configuration completes the FCoE configuration on the N9K-A device?

```
N9K-A( configs feature fcoe
N9K-A(config^ feature npv
N9K-A( configs interface vfc 100
N9K-A(config-if)4 bind Interface port-channel 100
N9K-A(config4f^# switchport mode F
N9K-A(C0ntg-tf> switchport trunk allowed vsan 20

N9K-A( configs feature fcoe
N9K-A( configs feature npv
N9K-A(config»s Interface vfc 100
N9K-A(config-if>#  bind interface port-channel 100
N9K-A(conflg-if p switchport mode N
N9K-A(conflg-if>« switchport trunk allowed vsan 1. 20

N9K-AI config w feature-set fcoe-npv
N9K-A(config w Interface vfc-port-channel 100
N9K-A(con0g-if)# switchport mode HP
N9K-A(config-ify» switchport trunk allowed vsan 20

N9K-A( configp feature-set fcoe-npv
N9K-A(config i» interlace vfc-port-channel 100
N9K-A(configMf)w switchport mode E
N9K-A(conflg-d)# switchport trunk allowed vsan 1. 20
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

to configure FCoE between the N9K-A switch and the FCF-A Nexus 9000 core switch with the given characteristics, the correct configuration would be the one that enables FCoE NPV mode, binds the interface to a port-channel, and allows only VSAN 20 on the trunk. Based on the provided CLI configurations, the correct answer would be Option D as it configures the switch in NPV mode and allows only VSAN 20

Question: 240

A customer undergoes an IT security review assessment. The auditor must have read-only access to the Cisco Nexus 9000 Series Switch to perform the configuration review. The customer implements this security role for the auditor:

role name audit

rule 1 permit command *

rule 2 - Output omitted -

username auditor password C4SAFF0B96EB0045$c0 role audit

Which configuration snippet must complete the configuration?

A. deny command write*

B. permit command enable

C. permit command show *

D. deny command configure terminal

Answer: C

Explanation:

The auditor requires read-only access to perform the configuration review. The permit command show * grants the auditor access to all show commands, which are typically used to view configurations and statuses without making changes, thus maintaining the read-only requirement. Reference: This is aligned with the best practices for role-based access control (RBAC) in Cisco Nexus switches, as detailed in the DCCOR course materials.

Question: 241

A Cisco ACI engineer must configure an access port on a Cisco ACI leaf switch. The access policy should be configured so that it supports L30ut connectivity concurrently with several EPGs that are mapped to this interface with the static port method. How should the access policy be configured?

A. by linking the interface policy group to multiple Attachable Access Entity Profiles

B. with a single Attachable Access Entity Profile that is linked to the corresponding routed domain and physical domain

C. with two interface policy groups that are linked to the same interface profile port selector

D. by mapping a single physical domain, mapped to the L3out and EPG interfaces

Answer: A

Explanation:

In Cisco ACI, an interface policy group can be linked to multiple Attachable Access Entity Profiles (AAEPs) to support connectivity for various EPGs with L3Outs. This setup allows for the concurrent support of L3Out connectivity and multiple EPGs on a single access port. Reference: This concept is covered in the section on ACI access policies in the DCCOR course.

Question: 242

An engineer must configure the order in which the server attempts to boot from available boot device types using Cisco Integrated Management Controller (Cisco IMC). The engineer must change the boot order configuration during the setup and apply the new requirements multiple times. The requirement is to change the Cisco IMC actual boot order so it is different from the configured boot order. Which setting accomplishes this goal?

A. Enable the system to boot with the configured boot order.

B. Set the boot configuration directly through BIOS.

C. Configure the legacy and precision boot order to be mutually exclusive.

D. Apply UEFI Secure Boot for a nonsupported operating system.

Answer: B

Explanation:

Changing the boot order during setup and applying new requirements multiple times can be achieved by setting the boot configuration directly through the BIOS. This allows the engineer to modify the boot order as needed, separate from the configured boot order in Cisco IMC. Reference: The DCCOR course discusses server boot order configuration and the use of BIOS settings for such purposes.

Question: 243

Refer to the exhibit.

```
•vent manager applet ConfigMgmt event cli match "copy run start" action 1
  syslog priority warnings msg Configuration Modified
```

Refer to the exhibit. An engineer logs all occurrences of a configuration being saved. The engineer must generate an additional log message when someone attempts to change the configuration for interface Ethernet 1/1. Which set of commands must be used to meet these requirements?

```
event manager applet CorrftgMgmt
  event ell lag Mt match -interface E#*em«1/1“
  event ell teg copy match "copy run steer
  event cil teg conf match "configure terminal" tag conf or eth or copy happens 2 In 3
  action 1 *ytlog priority warning* msg Configuration Modified action 2 event-default
```

```
event manager applet ContigMgmt
  want CM 1*0 *th match "configure terminal; Interlace Ethernet! 1" event CM tag copy match "copy tun start*
  tag eth or copy happens 1 In 2
  action 1 syslog priority warnings msg Configuration Modified action 2 event-default

event manager applet ConfigMgrnt
  event ell tag eth match "Interface Ethernet!fl"
  event ell tag copy match "copy run stair
  event ell tag conf match "configure terminal" tag conf and eth or copy happens 1 In 4H4967295 action 1 syslog priority warnings msg
  Configuration Modified

event manager applet ConfigMgrnt
  event ell tag eth match "configure terminal , Interface Ethernet! '!" event ell lag copy match "copy run start* tag eth and copy happens 11n 2
  action 1 syslog priority warnings msg Configuration Modified
```

A. Option A

B. Option B

C. Option C

D. Option D

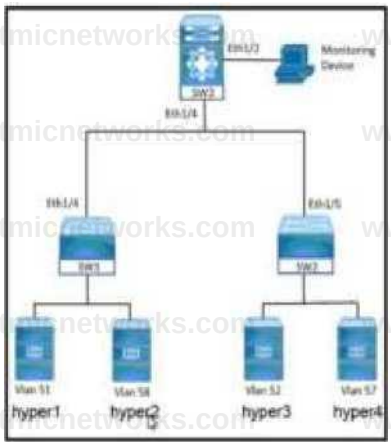
Answer: B

Explanation:

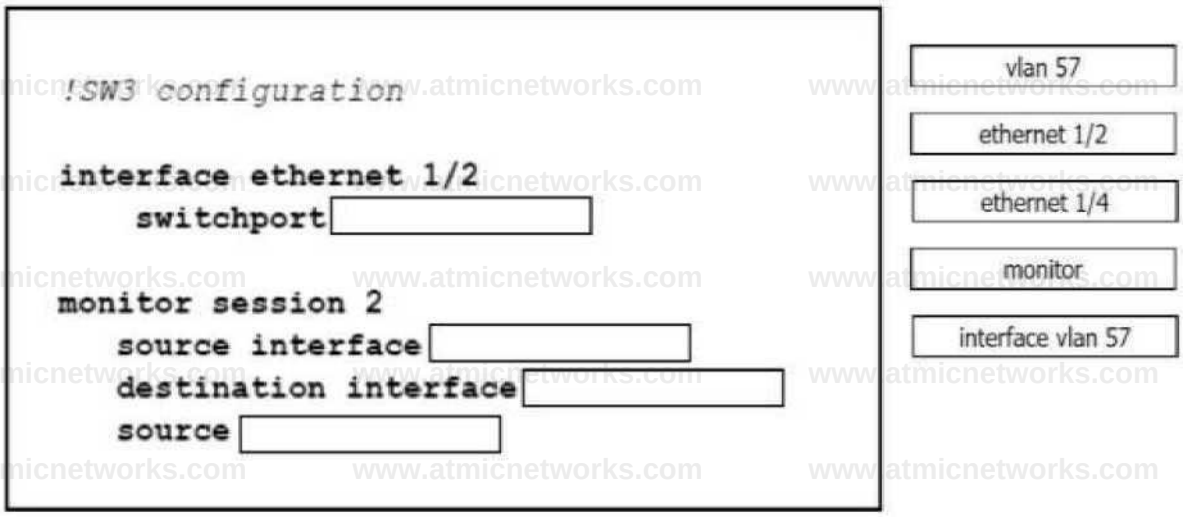
Question: 244

DRAG DROP

Refer to the exhibit.

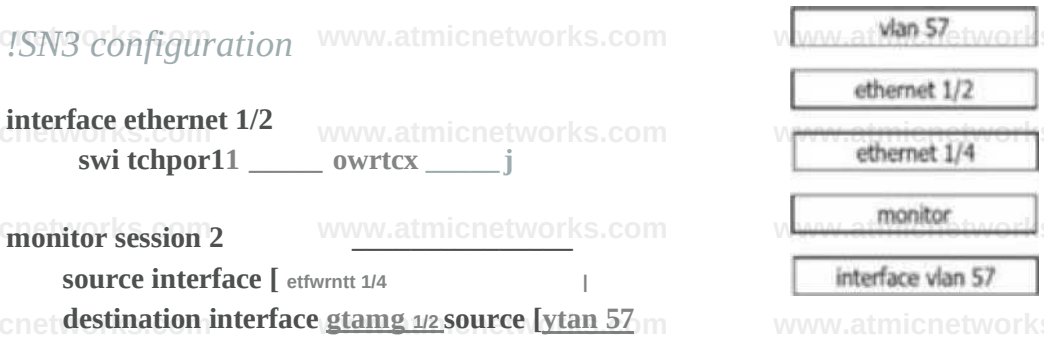


Refer to the exhibit. An engineer must monitor the Ethernet port and the corresponding VLAN traffic for the hyper4 device The SW3 device is a Cisco Nexus 7000 Series Switch Drag and drop the code snippets from the right into the boxes in the configuration to meet these requirements.



Answer:

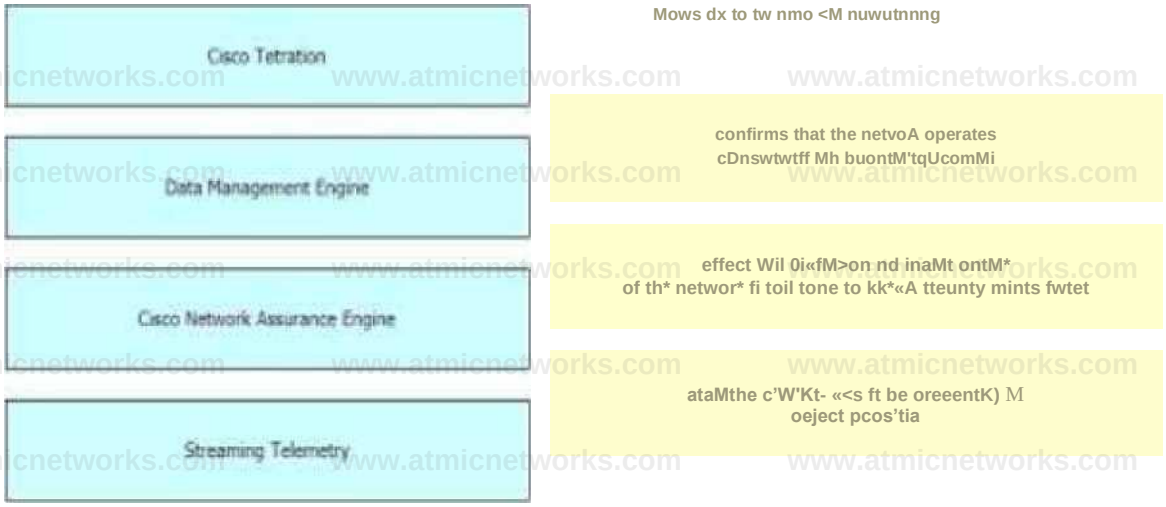
Explanation:



Question: 245

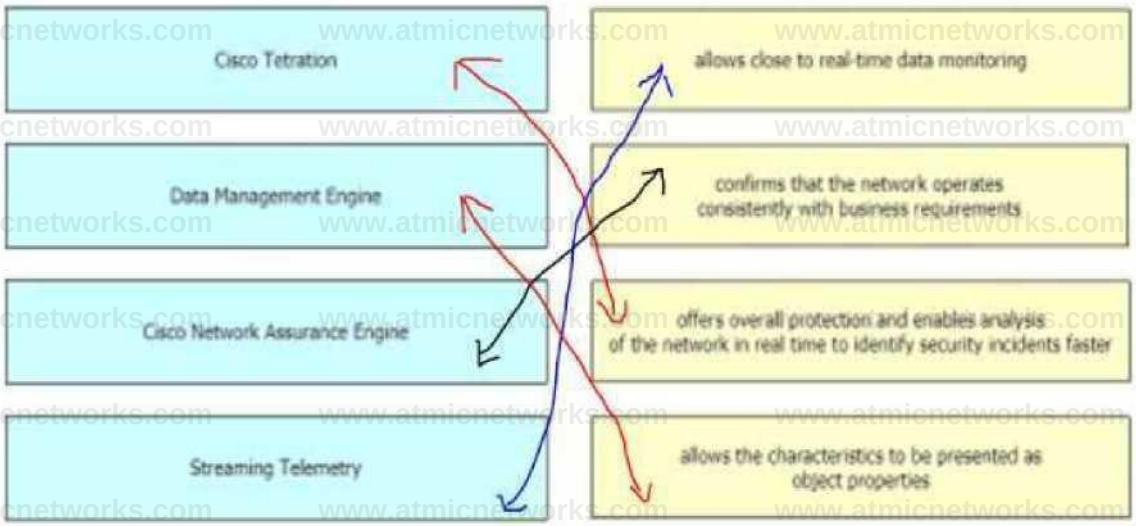
DRAG DROP

Drag and drop the network assurance concepts from the left onto the corresponding benefits on the right.



Answer:

Explanation:



Question: 246

An engineer must apply AAA configuration on a Cisco MDS 9000 Series Switch. The solution must meet these conditions:

It must use a challenge-response authentication protocol that uses MD5 hashing with an incrementally changing identifier

The RADIUS configuration must t>e automatically shared with other MDS switches in the environment.

The RADIUS server is already defined. Which command set completes the configuration?

aaa authentication login pap enable distribute radius
radius-server host 10.8.8.0 auth-port 1821

aaa authentication login mschapv2 enable radius propagate
radius authentication port 1821

aaa authentication login chap enable radius distribute
radius commit

aaa authentication login mschap enable radius commit
radius-server host 10.8.8.0

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The correct command set for configuring AAA to use CHAP with MD5 hashing and to share the RADIUS configuration across MDS switches involves using the aaa authentication login command with the radius keyword and enabling CHAP. The radius distribute command is used to share the RADIUS configuration automatically with other MDS switches in the environment.

Reference:

Cisco MDS 9000 Series Security Configuration Guide1

Configuring FC-SP and DHCHAP2

Please note that the actual commands may vary based on the specific requirements and the version of the Cisco NX-OS software running on your switch. It's always best to consult the latest Cisco documentation or a certified Cisco technical expert for the most accurate information.

Question: 247

An engineer must implement a solution that prevents untrusted DHCP servers from compromising the network. The feature must be configured on a Cisco Nexus 7000 Series Switch and applied to VLAN 10. The legitimate DHCP servers are connected to interface Ethernet 2/4. Which configuration set must be used to meet these requirements?

n7k-1 iconfig)# Ip dhcp snooping vlan 10 nZk-Kconfigfi# interface Ethernet2/4 n7k-1(config-if^ ip dhcp snooping trust

n7k-1(config)#ip dhcp snooping vlan 10
n7k-1 iconfig)# interface Ethernets
n7k-1(configs ip dhcp snooping verify vlan 10

n7k-1 <configj* ip dhcp snooping verify
n7k-1 (config)* interface Ethernets n7k-1(config-if)« ip dhcp snooping verify vlan 10

n7k-1(config)# Ip dhcp snooping verify n7k-1(config)» vlan configuration 10 n7k.1(config.vlani» Ip dhcp snooping trust

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

The DHCP snooping feature acts as a firewall between untrusted hosts and trusted DHCP servers. It validates DHCP messages received from untrusted sources and filters out invalid messages. To implement this on a Cisco Nexus 7000 Series Switch for

VLAN 10, you would enable DHCP snooping for that VLAN and then configure the specific interface connected to the legitimate DHCP servers to be trusted. This ensures that DHCP responses from the legitimate servers are allowed, while responses from any other servers are blocked.

Reference:

Cisco Nexus 7000 Series NX-OS Security Configuration Guide1

Configuring DHCP Snooping2

Question: 248

An engineer must configure a monitoring solution for a Cisco Nexus 9000 Series Switch based data center. The solution must provide real-time insight into the network health with subscription-based monitoring. The monitoring must be initiated from the client side, and the data must be sent via encryption. Which configuration steps complete the configuration?

Sei the telemetry feature on the Nexus switch Specify a certificate for telemetry transport Configure a sensor group and destination.

Enable GRPC on the Nexus switch
Generate a certificate.
Configure gNMI Inputs in Telegraf and output to InfluxDB

Configure Grafana on the Nexus switch
Specify the logging certificate
Enable syslog level 7 export to Grafana

Activate SNMPv3 on the Nexus switch Set the giobalEnforcePrlv parameter Configure an SNMP agent to pol Information

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Enable telemetry features on the Cisco Nexus 9000 Series Switch to collect and send real-time data.

Configure a secure transport mechanism, such as gRPC with TLS encryption, to ensure that the monitoring data is transmitted securely.

Set up a subscription-based monitoring service that can process the telemetry data and provide insights into the network health.

Question: 249

An engineer is performing an ISSU upgrade on the Cisco MDS 9000 Series Switch. What is the impact on the control plane of the switch?

A. It remains down until the next reboot.

B. It remains up throughout the update.

C. It remains down for more than 80 seconds but less than 140 seconds.

D. It is down for less than 80 seconds.

Answer: B

Explanation:

An ISSU upgrade on the Cisco MDS 9000 Series Switch allows for software updates with minimal impact on the switch's operation. The control plane remains up during the upgrade, ensuring continuous network operations and service availability. The process is carefully designed to prevent any significant downtime, and any brief disruption is kept well under the 120-second mark1.

Reference := For further details, you can refer to the Cisco MDS 9000 NX-OS Software Upgrade and Downgrade Guide, Release 8.x, and the Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide21.

Question: 250

A company provides applications and database hosting services to multiple customers using isolated infrastructure-as-a-service services within the same data center environment. The environment is based on Cisco MDS 9000 Series Switches. The requirement is to manage the environment by using Fibre Channel Security Protocol and to enable user authentication when the centralized AAA server is unreachable All communication between the MDS switches and the remote servers must be encrypted. Which command set must be used to meet these requirements?

aaa group server radius Radius Served aaa authentication login default RadiusServed

aaa group server radius RadiusServed
aaa authentication dhchap default group RadiusServed

aaa group server tacacs* TacacsServerl
aaa authentication dhchap default group TacacsServerl

aaa group server tacacs* TacacsServerl aaa authentication login console TacacsServant

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The command set in Option C is likely to configure the Cisco MDS switches to use FC-SP for authentication and to ensure communication remains encrypted even when the AAA server is not reachable. This would typically involve configuring the switches to fall back on local authentication databases and enabling features such as DHCHAP (Diffie-Hellman Challenge Handshake Authentication Protocol) to maintain encrypted communication12.

Reference := For a detailed configuration guide, you can refer to the Cisco MDS 9000 Series Security Configuration Guide, Release 8.x and 9.x, which provides instructions on configuring security features on external AAA servers and FC-SP and DHCHAP

Question: 251

An engineer must create an EPG called "Test". The configuration request should succeed if the Tenant called "Tenant" and the application profile called "Test" exist. The firewall policy allows only the HTTP connectivity to APIC from the user's computer. Which action accomplishes this goal?

Send <fvAEPg dn="unl/tn-Test//ap-Test//epg-Tenant" status="created"/> to APIC payload using HTTP PUT to the Cisco APIC.

Send <fvAEPg dn="unl/tn-TesVap-TesUepg-Tenant" status="created"> to APIC payload using HTTP POST to the Cisct APIC

Send <fvAEPg dn="uni/tn-Tenant/ap-TesUepg-Test" status="created"/> to APIC payload using HTTP POST to the Cisci APIC.

Send <fvAEPg dn="uni//tn-Tenant//epg-Test//ap-Test" status="created"/> to APIC payload using HTTP PUT to the CISCI APIC.

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

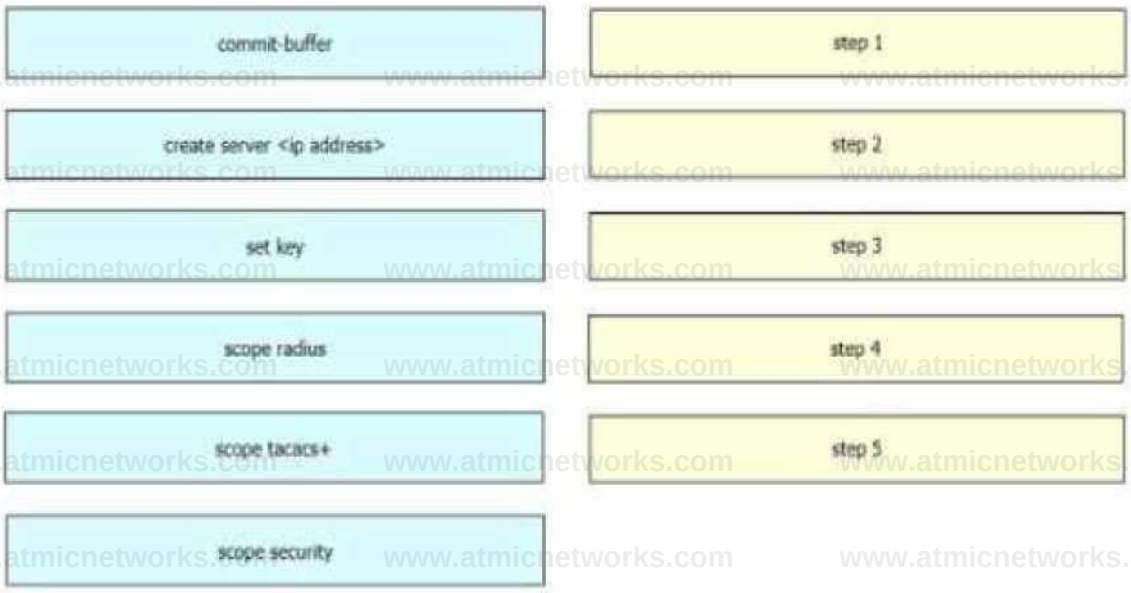
Option C correctly uses an HTTP POST request to send the necessary payload to Cisco APIC. This method is suitable for creating new resources like an EPG when the specified Tenant and application profile exist. The POST request will ensure that the configuration is applied only if the conditions are met, aligning with the requirement that the firewall policy allows only HTTP connectivity.

Reference := For further details, the Cisco APIC REST API Configuration Guide provides comprehensive instructions on using HTTP methods for APIC configurations.

Question: 252

DRAG DROP

An engineer must configure remote authentication on a Cisco UCS system. The user password must be encrypted before it is sent to the authentication server. The company security policy requires the server to be based on an open standard. Drag and drop the UCS CLI AAA configuration commands from the left into the order in which they must be implemented on the right. Not all commands are used.



Answer:

Explanation:

UCS-A# scope security

UCS-A /security # scope radius

UCS-A /security/radius # create server radiusserv7

UCS-A /security/radius/server* # set key

UCS-A /security/radius/server* # commit-buffer

Question: 253

An engineer must implement a disaster recovery policy for the Cisco UCS infrastructure. The solution must meet these criteria:

The Recovery Point Objective must be 48 hours.

The backup must use encrypted transmission.

The Recovery Time Objective must be 4 hours.

Which configuration set must be used in the scheduled backup to meet these requirements?

Protocol SFTP Schedule: Weekly

Protocol FTP Schedule Bi-Weekly

Protocol: TFTP
Schedule Bi-Weekly

Protocol SCP Schedule: Dally

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

Option A, which utilizes the SFTP protocol with a weekly schedule, aligns with the requirements. SFTP ensures encrypted transmission of data, addressing the need for secure backup. A weekly backup schedule is within the 48-hour Recovery Point Objective (RPO), as it guarantees that the most data that could be lost in a disaster is one week's worth, which is acceptable within the given RPO.

The Recovery Time Objective (RTO) of 4 hours is related to the restoration process rather than the backup schedule or protocol, so it is not directly influenced by the choice of Option A.

Reference := For more detailed information, refer to the Cisco UCS Manager Backup and Restore Guide, which provides guidelines on setting up disaster recovery policies, including backup schedules and transmission security.

Question: 254

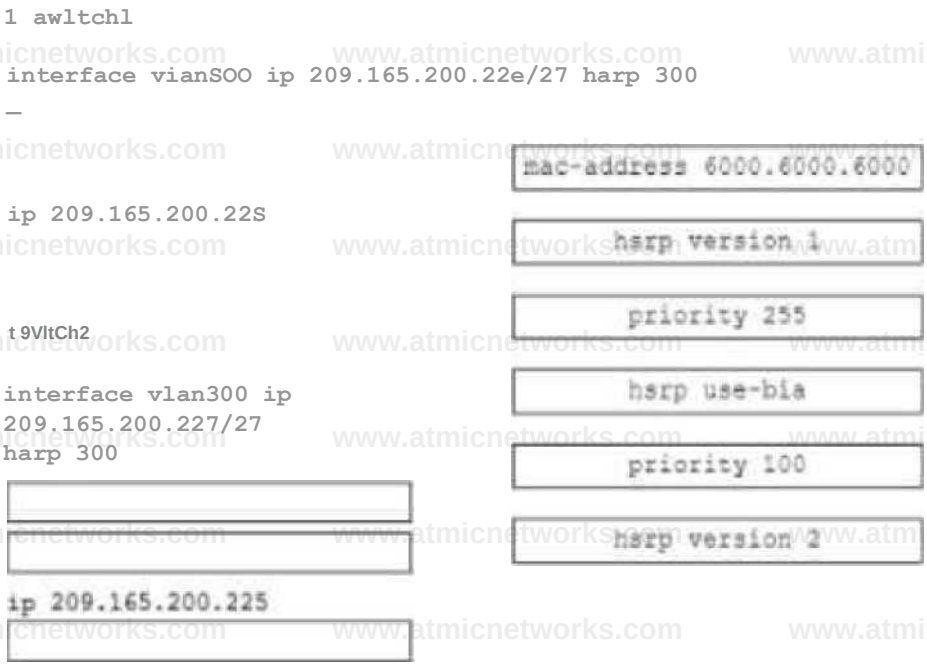
DRAG DROP

An engineer mus! configure HSRP protocol on two Cisco Nexus 9000 Series Switches running a virtual port channel. In addition, the HSRP implementation must meet these requirements:

It must allow more than 500 groups.
switch 1 must act as the primary switch.

Both switches must use a user-defined hardware address.

Drag and drop the commands from the right to complete a configuration of the HSRP on the left. The commands are used more than once. Not all commands are used.



Answer:

Explanation:

Switch 1:

Box 1 = hsrp version 2

Box 2 = priority 100

Box 3 = mac-address 6000.6000.6000

Switch 2:

Box 1 = hsrp version 2

Box 2 = priority 255

Box 3 = mac-address 6000.6000.6000

Question: 255

Refer to the exhibit.

Refer to the exhibit. Which feature set must be used to configure on switch 2 to establish a VSAN trunk between switch 1 and switch 2?

- E Port
- Trunk Mode On

- F Port
- Trunk Mode Passive

- NPot
- Trunk Mode Active

- MP Port
- Trunk Mode Auto

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The configuration in Option C likely involves setting the port to N Port and enabling Trunk Mode Active. This setup is necessary for establishing a VSAN trunk, as it allows the port to actively negotiate with the other switch to transmit and receive frames in multiple VSANs over the same physical link1.

Reference := For detailed steps and guidelines on configuring VSAN trunking on Cisco switches, you can refer to the official Cisco documentation, such as the Cisco MDS 9000 Series Fabric Switches Configuration Guides

Question: 256

An engineer must perform a software upgrade on a production Cisco Nexus 7000 Series Switch. Before the upgrade activity, the requirement is for all ports to be shut down and routing protocols to terminate gracefully. Which feature must be used to meet these requirements?

A. Configuration Profile

B. Maintenance Mode Profile

C. Switch Profile

D. Service Profile Template

Answer: B

Explanation:

The Maintenance Mode Profile feature in Cisco Nexus 7000 Series Switches is used to ensure a controlled shutdown of ports and graceful termination of routing protocols before performing a software upgrade12.

Reference := Cisco Nexus 7000 Series NX-OS Software Upgrade and Downgrade Guide12.

Question: 257

When deploying a Cisco HyperFlex edge with a pair of switches, what is the minimum number of interfaces in trunk mode required on each HX node?

A. 1

B. 2

C. 4

D. 6

Answer: B

Explanation:

When deploying a Cisco HyperFlex edge with a pair of switches, the minimum number of interfaces in trunk mode required on each HX node is two 10/25GE ports3. Reference := Cisco HyperFlex Edge Deployment Guide, Release 5.0(x)3.

Question: 258

What is a characteristic of the NFS protocol?

A. It is used for booting Cisco UCS B-Series servers.

B. It is used to access a storage array at a block level.

C. It uses UDP and HTTP as its transport.

D. It uses remote procedure calls with TCP/IP for transport.

Answer: D

Explanation:

NFS, or Network File System, is a protocol that allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed. NFS uses remote procedure calls (RPC) over TCP/IP for transport4. Reference := Wikipedia article on Network File System (NFS)4.

Question: 259

A customer asks an engineer to develop a framework that will be used to replace the process of the manual device configuration of Cisco NX-OS devices. The engineer plans to use the programmatic interface that meets these requirements:

The development team is familiar with Windows-based scripting environment using PowerShell.

The customer's security requirements mandate the use of HTTPS transport.

Which solution must be used to meet these requirements?

A. NX-API

B. VISORE

C. Open Agent Container

D. NETCONF-YANG

Answer: A

Explanation:

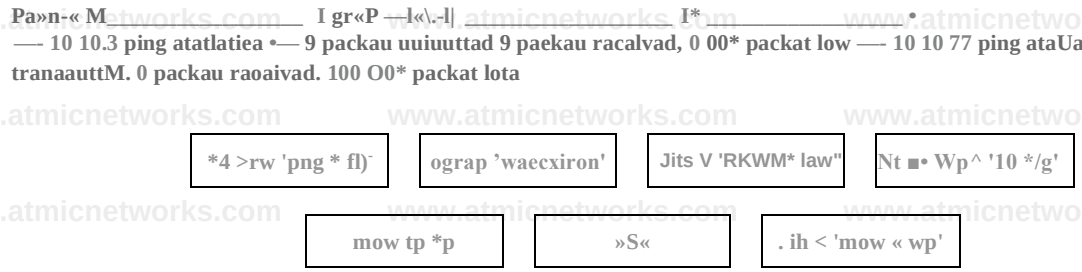
NX-API is the appropriate solution to meet the requirements specified. It allows for programmatic device configuration using a Windows-based scripting environment like PowerShell and supports HTTPS transport for secure communication1.

Reference := Cisco Nexus 9000 Series NX-OS Programmability Guide, Release 9.3(x)1.

Question: 260

DRAG DROP

A network administrator must automate the process of pinging all the IP addresses from the 10.0.0.0/8 subnet. The subnet is already present in the ARP table of the Cisco Nexus switch. Drag and drop the bash commands to generate the desired output. Not all commands are used.



Answer:

Explanation:

vsh -c "show ip arp", awk'{print "ping" $1}', vsh, egrep "statistics|loss"

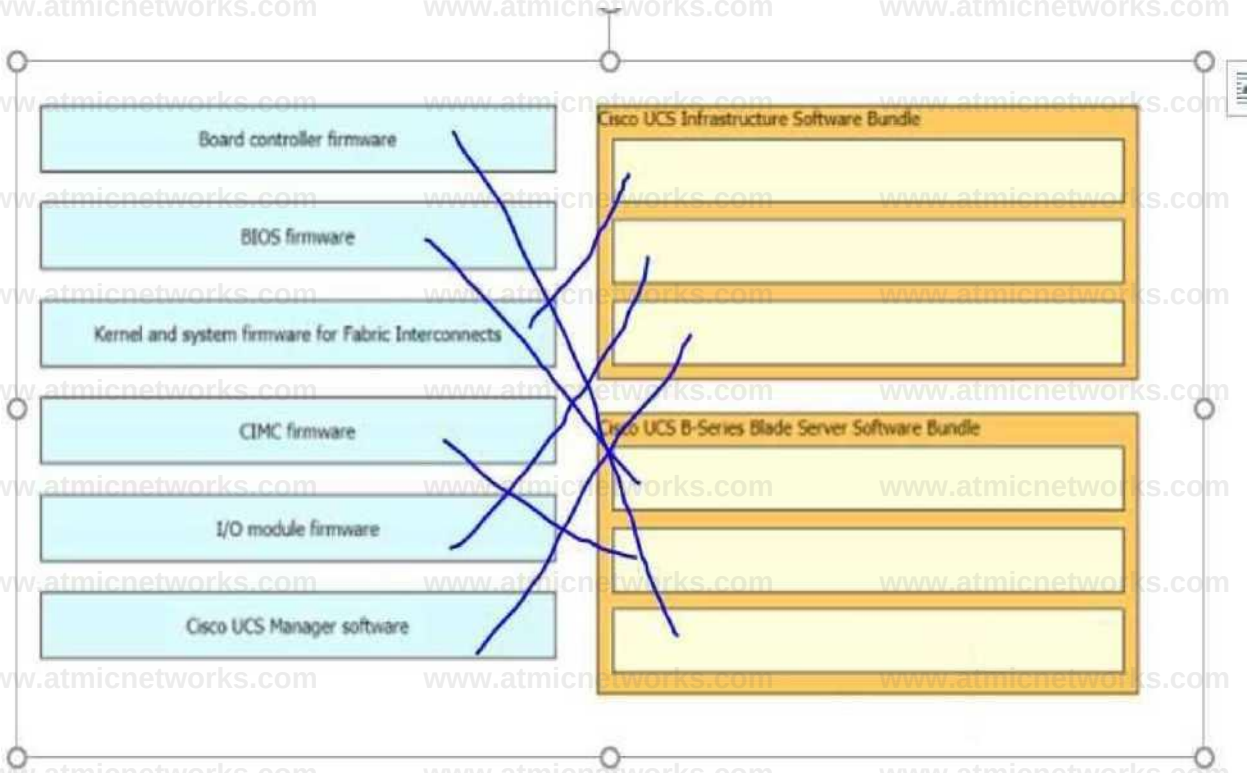
Question: 261

DRAG DROP

Drag and drop the firmware packages from the left onto the software bundles they belong to on the right.

Answer:

Explanation:



Question: 262

Refer to the exhibit.

```
show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin
```

Refer to the exhibit. Software downgrade is required on a Cisco Nexus 7000 Series Switch. What is displayed when this command is executed?

A. features and commands that are removed automatically from the configuration

B. features that are enabled automatically after the downgrade

C. compatibility of software in the system bootflash file

D. impact of a software upgrade in ISSU and chassis reload

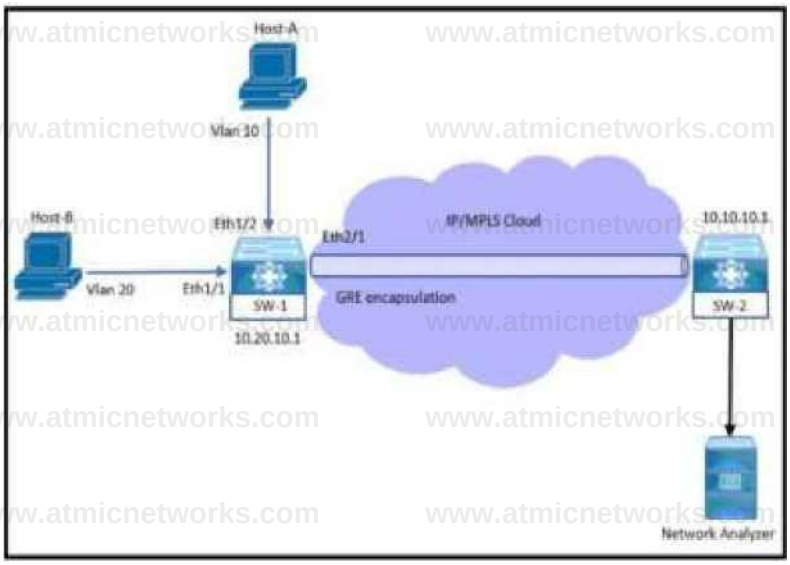
Answer: C

Explanation:

The command show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin is used to display the compatibility of the software in the system bootflash file on a Cisco Nexus 7000 Series Switch. This command is crucial for administrators to verify if the current configuration is compatible with the new software version before performing a downgrade or upgrade, ensuring that there are no conflicts or issues that could potentially disrupt network operations1.

Question: 263

Refer to the exhibit.



Refer to the exhibit. An engineer monitors ingress traffic from Host-A and all traffic for VLAN 20 from Host-B Which configuration must be implemented to monitor and export traffic to Network Analyzer?

SW-1 (config ,P **monitor session S**
SW-liconfig-moneorp **source interface ethernet 1/2 nt**
SW 1(config-mon*xp **source interface ethernet 1/1 Ct**
SW-liconfig-moniKrp **source** stat **20 both** $'W-1 (config-monfcf p **destination ip 10.10.10.1**
SW-1 (config-monCcx P **no shut**

SW 1(config P **monitor session 5 type erspar-source**
SW-1(config-erspan-srcF **source interface ethernet 1/2 nt**
SW-1 (con#g-erspan-srciP **source elan 20 both**
SWi-1 (config espan S-CP **destination ip 10 10 10.1**
SW-1(config-erspan-s»tF **erspan-id 111**
SW-1 (config-erspan-srep **no shut**

SW-1 (config P **monitor session 5 type erspan**
SW-1 (config-erspan tree **source interface ethernet 1'2 nt**
SW 11 configerspar' s ; - **source interface ethernet 11 both**
SW-1(config-espan-S't= **destination ip 10.10.10.1**
SW-1lcottfig-erspan-srcc **rrttu 1000**
SW11config-erspan. sen **no shut**

SW-1 (config P **monitor session 5**
SW-1 (config-tnoneer P **source interface ethernet 1/2 nt**
SW-1 irertfig-morv" • P **source interface ethernet 1/1 both**
SW-11 config-moneor P **source vfan 20 both**
SW 1 (config-mor#otp **destination interface ethernet 2/1**
SW-1 (config-monacrp **no shut**

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

To monitor and export traffic to a Network Analyzer, particularly ingress traffic from Host-A and all traffic for VLAN 20 from Host-B, the engineer must implement a configuration that captures the specified traffic and directs it to the Network Analyzer tool. The correct configuration will depend on the capabilities of the network devices in use and the specifics of the Network Analyzer's requirements.

The configuration must include setting up a SPAN (Switched Port Analyzer) or RSPAN (Remote SPAN) session that mirrors the desired traffic to a port connected to the Network Analyzer. This would involve specifying the source interfaces or VLANs and the destination port for the mirrored traffic.

Additionally, the configuration should ensure that the Network Analyzer is capable of receiving and processing the mirrored traffic, which may require additional settings on the Network Analyzer itself.

Question: 264

Refer to the exhibit.

```
rollback running-config checkpoint system-fm-vpc output-omitted
```

Refer to the exhibit. A network engineer is implementing a configuration checkpoint on a Cisco Nexus 9000 Series Switch. The configuration must skip any existing vPC configuration errors and must complete if there are any configuration errors.

The engineer finished the vPC domain configuration part. Which command completes the checkpoint implementation?

A. stop-at-first-failure

B. atomic

C. best-effort

D. verbose

Answer: C

Explanation:

The 'best-effort' command is used when implementing a configuration checkpoint on a Cisco Nexus 9000 Series Switch to ensure that the process skips any existing vPC configuration errors and completes even if there are other configuration errors. This command is suitable for scenarios where it's critical to proceed with the checkpoint despite errors, allowing the engineer to create a rollback point and address issues without disrupting the entire process.

Question: 265

A storage array must be connected to port ethernet1/10 on a Cisco MDS 9000 Series Switch In addition, the array must connect using the FCoE protocol and be single-homed Which configuration meets these requirements?

```
vlan database
  vlan 101 fcoe vsan 101 enable interface vfc 10 vsan 101

interface vfc 10
  switch port mode fcoe switchport access vlan 101 bind interface ethernet1/10
vlan database
  vlan 101 vsan
  vsan 101 fcoe
  vsan 101 interface vfc 10

interface ethernet1/10 switchport mode trunk bind interface vfc 10 fcoe vsan 101

vsan database
  vlan 101
  vsan 101
  fcoe vsan 101 Interface vfc 10

interface 1/10 switch port mode e fcoe vfc 10

interface vfc 10
  switchport mode f
  bind interface ethernet 1/10

vsan database
  vsan101
  vlan 101
  fcoe vsan 101
  vsan 101 interface vfc 10
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C meets the security requirements for the Cisco UCS C-Series Server. It disables unencrypted communication by enabling HTTPS, sets the session timeout to 900 seconds (15 minutes), redirects HTTP to HTTPS to divert unencrypted traffic, and changes the SSH port to a nondefault value (2022), which is essential for CLI-based management.

Reference := For further details on securing Cisco UCS C-Series Servers, refer to the Cisco UCS C- Series Servers Integrated Management Controller CLI Configuration Guide, which provides instructions on configuring service profiles, security settings, and management access.

Question: 266

An engineer implements a Cisco UCS C-Series Server that must adhere to these security requirements:

Unencrypted communication must be disabled.

The session timeout must not exceed 15 minutes.

Unencrypted traffic must be automatically diverted.

CLI-based management must use nondefault ports.

Which configuration set meets these requirements?

XML API Enabled
HTTP Port 8080 / HTTPS Port 844 3
IPMI over LAN Enabled
Randomized Encryption Key

HTTP Port: 80 / HTTPS Port 443
Session Timeout: 900
Redirect HTTP to HTTPS Enabled
SSH Port: 2022

Redfish Enabled checked
Redfish Port: 443
SSH Enabled checked
HTTPS Port 8443

SSH Enabled
SSH Port 8022
SSH Timeout: 1200
IPMI over LAN Enabled

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C meets the security requirements for the Cisco UCS C-Series Server. It disables unencrypted communication by enabling HTTPS, sets the session timeout to 900 seconds (15 minutes), redirects HTTP to HTTPS to divert unencrypted traffic, and changes the SSH port to a nondefault value (2022), which is essential for CLI-based management.

Reference := For further details on securing Cisco UCS C-Series Servers, refer to the Cisco UCS C- Series Servers Integrated Management Controller CLI Configuration Guide, which provides

instructions on configuring service profiles, security settings, and management access.

Question: 267

An infrastructure architect is analyzing the deployment type for an application. Several companies must be able to operate the application environment and integrate it with a third-party protocol. The development team also must have maximum control over their development environment, Including the operating system used, Python interpreter, and corresponding libraries. Which cloud deployment solution meets these requirements?

A. public cloud Storage as a Service

B. private cloud

Platform as a Service

C. hybrid cloud

Software as a Service

D. community cloud

Infrastructure as a Service

Answer: D

Explanation:

A community cloud Infrastructure as a Service (IaaS) deployment model is suitable for several companies that need to operate the same application environment and integrate it with third-party protocols. It allows the development team to have control over the infrastructure, including the operating system, Python interpreter, and libraries

Question: 268

Which NFS version uses the TCP protocol and needs only one IP port to run the service?

A. NFSv1

B. NFSv2

C. NFSv3

D. NFSv4

Answer: D

Explanation:

NFSv4 uses the TCP protocol and requires only one IP port (2049) to run the service. This simplifies firewall configuration and improves security by reducing the number of open ports

Question: 269

What is a benefit of independent resource scaling in Cisco HyperFlex hybrid architecture?

A. flexible expansion of compute, caching, and capacity

B. remote booting of converged servers

C. multivendor converged node hardware support

D. support for compute nodes with third-party storage

Answer: A

Explanation:

One of the benefits of independent resource scaling in Cisco HyperFlex hybrid architecture is the flexible expansion of compute, caching, and capacity. This allows for the addition of resources in the required ratios without being constrained by the limitations of traditional converged infrastructure3.

Question: 270

An engineer must perform an initial configuration of VXLAN Tunnel End-Point functionality on the Cisco Nexus 9000 Series platform All the necessary features are already enabled on the switch Which configuration set must be used to accomplish this goal?

```
SAX tonty * mertaoe looptMc^O
NXXJ canty-/# Ip eddreu 10 10 10 II-12

NA scanty* -mertaoe overiayO tyTXi canty *<>**•¥ ~ *eu'ce-*mefi>ee loopbaehO

\A •». canty* unteftaoe VLAM10
NXX tty < HMP^ eou»rce-lree<face loopbackO

NXX ranty# rnertaoe PopbKkO
M •• canty fd ipaddren 1010 10.1112

S V*, nn*^# wmrtbMMNMI
NXX-. canty /W tunnel source locpOacAO

MX'onty - UMM enemni'1 SAX canty /# ip unnumbered 'oopOockfl

SAHLconty# MftrfMt Ipopbackfi
HXXJ canty/# ip Mm* W 1010 1112

HAXi canty# M*»ftM» nvtl
SXXrortyrfrNer wuTO^ne»rf*c# w

NAx rooty - irnortK* ediemMl[1]1
NXX rooty /• ip uonuMpered tpepteeM

NXX 'nnr^j# wnprtM# i«*pb«kg
SXX twrty 4# ip Mf*M to 10 10 n W

NXWi[1] o*ty - MMK* MUNI#
NA.X canty M ip unnumbered -oopbeceO

NXX:unity- meHece n<e1
NX9K] entity I *weH* eouroeMneorface loepbecteO
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Option D is the correct configuration set for initializing VXLAN Tunnel End-Point functionality on a Cisco Nexus 9000 Series

platform. This option includes the necessary commands to configure the loopback interface, which is used as the source for the VXLAN Network Virtual Endpoint (NVE) interface, and the NVE interface itself, which is essential for VXLAN operation.

Reference := For a detailed guide on VXLAN configuration on the Cisco Nexus 9000 Series, you can refer to the Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide, which provides step-by-step instructions and best practices.

Question: 271

An engineer mus! send JSON encoded telemetry data to an external collector. The transport mechanism must prevent tampenng or forgery of the dat

a. Which protocol accomplishes this goal?

A. GPB

B. HTTP

C. gRPC

D. DTLS

Answer: B

Explanation:

DTLS (Datagram Transport Layer Security) is designed to provide security for datagram-based applications by allowing them to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery. It is suitable for securing JSON encoded telemetry data sent to an external collector1.

Question: 272

Refer to the exhibit.

Refer to the exhibit. Which action completes the vPC domain implementation?

A. Allow VLANs on the vPC peer link member interfaces.

B. Include the VRF management on the vPC domain.

C. Configure the system MAC on the vPC domain.

D. Add the vPC member ports to the vPC channel group.

Answer: D

Explanation:

Completing the vPC domain implementation requires adding the vPC member ports to the vPC channel group. This action ensures that all member ports are correctly bundled into the vPC, allowing for consistent forwarding behavior and redundancy across the vPC peer switches2.

Question: 273

An engineer must implement the FCoE on the Cisco Nexus 9000 Series Switch-based infrastructure. The deployment will contain dual-homed fabric extenders and must support jumbo frames with port channels. Which two sets of actions complete the configuration? (Choose two.)

Configure the interface with mtu 9516
Disable the feature NPIV

Create a virtual Fibre Channel interface
Sard vFC tn physical interface

Create a FCoE switch profile.
Enable config sync.

Create a dedicated V$AN for FEX
B nd VSAN to FEX uplinks

Execute fate enable-tex.
Configure FEX uplinks with mtu 9216

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: A, D

Explanation:

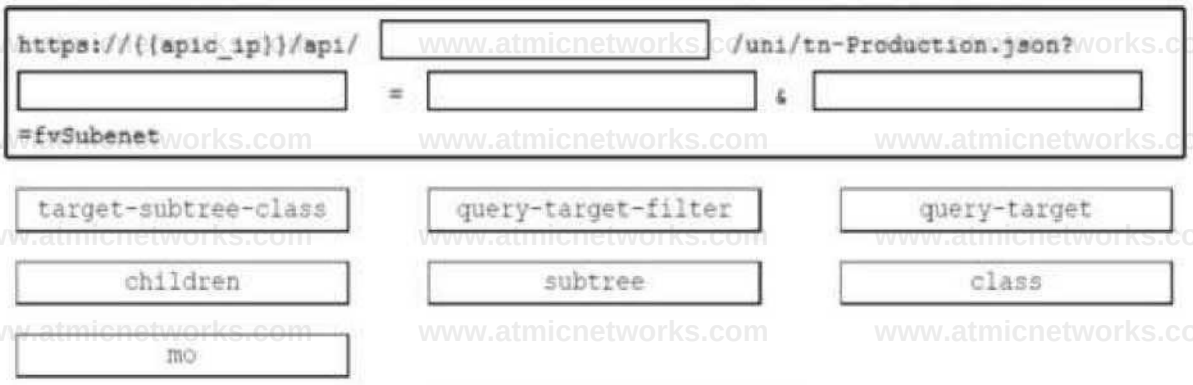
To implement FCoE on a Cisco Nexus 9000 Series Switch-based infrastructure that includes dualhomed fabric extenders and supports jumbo frames with port channels, the engineer must configure the system to handle large frame sizes and ensure FCoE functionality is enabled on the fabric extenders. The actions in Option A include configuring the interface with an MTU of 9516 to support jumbo frames and disabling NPIV, which is not required for FCoE operation on fabric extenders. Option D involves executing the command 'fcoe enable-fex' to enable FCoE on the fabric extenders and setting the MTU to 9216 on FEX uplinks to support jumbo frames1

Question: 274

DRAG DROP

Drag and drop the keywords onto the URL request to collect all the subnets configured under tenant Production using

a REST API. Not all options are used.



Answer:

Explanation:

Question: 275

Refer to the exhibit.

```
l!/bin/«nv python from cli import *

x- cli('show running-config | include address')
y= x.find('192.168.101.191/25')
z= x.find('192.168.101.192/25')
if y •” -1:
    cli ('copy tftp://192.168.101.253/initdevl.cfg bootflash: vrf management') cli ('copy
    bootflash:initdevl.cfg schedulod-config')
if z •■ -1:
    cli ('copy tftp://192.168.101.253/initdev2.cfg bootflash: vrf management')
    cli ('copy bootflash:initdev2.cfg scheduled-config’)
cli ('copy running-config startup-config')
```

Refer to the exhibit. Which information must be added to the script to complete the POAP operation on the Cisco Nexus 9000 Series Switch?

AP< token d4id8cd98f00b40960045298ecf8427e of the Cisco APIC

MD5SUM 4ld8cd98f00b204e980099&ecf8427e of the Python code

API token <Mid8cd98f00b7798033l998ecf8427e of the Cisco Nexus 9000 Series Switch

MD5SUM d4ld8cd98f00b20449800998ecf8427e of the script file

A. Option A

B. Option B

C. Option C

D. Option D

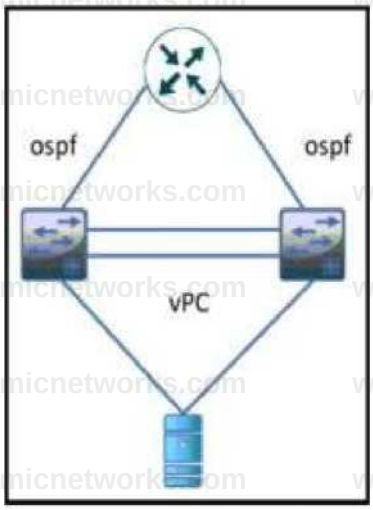
Answer: C

Explanation:

To complete the PowerOn Auto Provisioning (POAP) operation on a Cisco Nexus 9000 Series Switch, the script must include the necessary network information such as the interface IP address, gateway, and DNS server IP addresses. Option C likely contains this information, which is essential for the switch to locate a DHCP server, bootstrap itself, and download the configuration script for software image installation and configuration

Question: 276

Refer to the exhibit.



Refer to the exhibit During a vPC peer switch reload, there is packet loss between the server and the router Which action must be taken to prevent this behavior during future reloads?

A. Set the routed uplink ports of the Cisco Nexus peers as orphans.

B. Increase the vPC delay restore timer.

C. Decrease the OSPF hello and dead interval timers.

D. Disable vPC ARP synchronize on the vPC peers.

Answer: B

Explanation:

Increasing the vPC delay restore timer can help prevent packet loss during a vPC peer switch reload. This timer delays the restoration of vPCs after a peer link recovery, allowing enough time for all the systems to stabilize and for routing protocols to converge, thus avoiding potential packet loss1.

Question: 277

Refer to the exhibit.

```
N7Switch# sh run | section callhome
callhome
  email-contact admin@acme.com
  phone-contact +1-800-123-4567
  streetaddress 111 Somestreet st. Sometown, Somewhere
  destination-profile full_txt email-addr netadmin@acme.com
  transport email smtp-server 192.168.1.25 port 25
  transport email from N7Switch@acme.com
  enable
  alert-group Inventory user-def-cmd show logging last 100
N7Switch#
```

Refer to the exhibit. A network engineer is configuring the Smart Call Home feature on a Cisco Nexus Series Switch. An email must be generated that contains the last 100 lines of the log every time a new piece of hardware is inserted into the chassis. Which command must be added to the configuration to receive the email?

A. alert-group Linecard-Hardware user-def-cmd show logging last 100

B. destination-profile Operations alert-group Inventory

C. destination-profile Operations message-level 2

D. alert-group Operations user-def-cmd show logging last 100

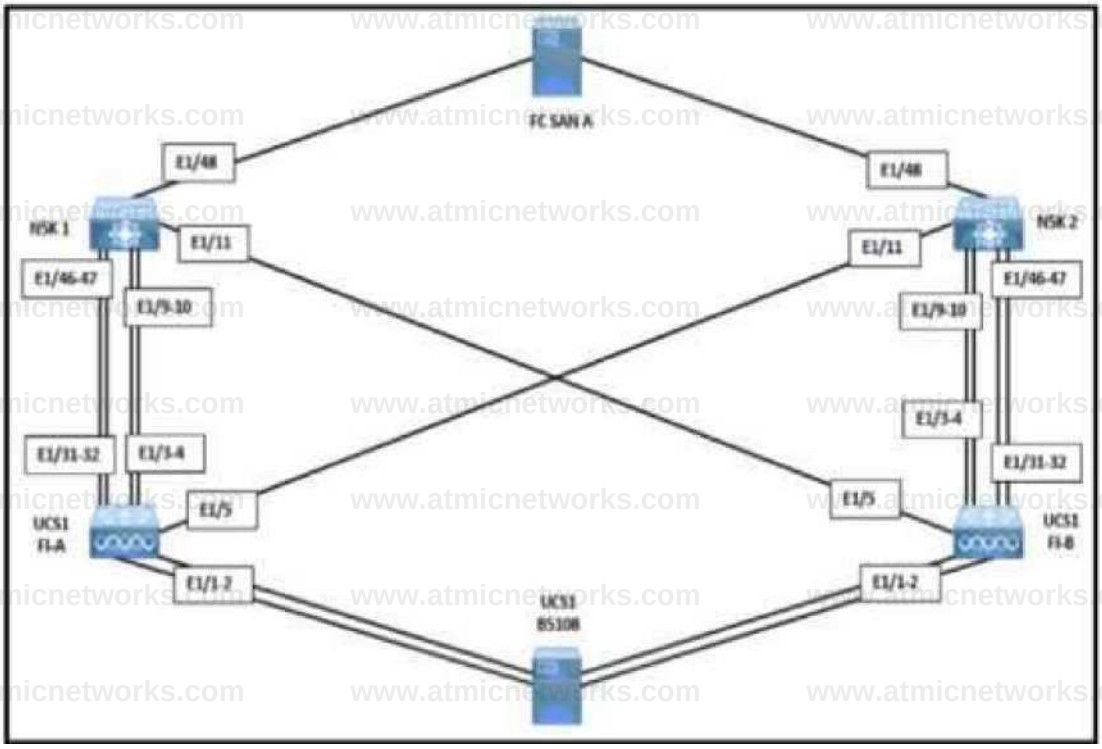
Answer: A

Explanation:

The command “alert-group Inventory user-def-cmd show logging last 100” is used to configure the Smart Call Home feature to generate an email with the last 100 lines of the log when new hardware is inserted. This command specifies the alert group ‘Inventory’ and the user-defined command to show the last 100 lines of the logging buffer

Question: 278

Refer to the exhibit.



A network engineer must configure port E1/31- 32 to forward only storage server traffic of VLAN 200 on Cisco fabric interconnects A and B. Port E1/31- 32 is not reserved for any other traffic. Which port type must be configured to accomplish this goal?

A. unified uplink

B. uplink

C. FCoE uplink

D. FCoE storage

Answer: C

Explanation:

The FCoE uplink port type is designed to carry Fibre Channel over Ethernet traffic, which is typically used for storage server communication. Configuring port E1/31-32 as FCoE uplinks will ensure that only storage server traffic for VLAN 200 is forwarded, aligning with the requirement to dedicate these ports solely for storage traffic

Question: 279

Which feature is supported with an In-Service Software Upgrade on a Cisco Nexus 9000 Series Switch?

A. configuration changes during an upgrade

B. nondisruptive upgrades via nonstop forwarding

C. zero downtime downgrades via dual supervisor modules

D. upgrades to Individual modules and line cards

Answer: B

Explanation:

The In-Service Software Upgrade (ISSU) feature on Cisco Nexus 9000 Series Switches supports nondisruptive upgrades via nonstop forwarding. This allows the switch to continue forwarding traffic while the system software is being upgraded, thereby minimizing downtime and maintaining continuous network service

Question: 280

DRAG DROP

An engineer must configure the HSRP protocol to implement redundancy using two Cisco Nexus Series Switches In addition, the HSRP must meet these requirements

Switch1 must retain the primary role if switch2 goes offline

Switch1 must retain the primary role until normal conditions are restored.

Switch1 and switch2 must ensure that the routing tables are converged before taking the active role

switch2 must retain the primary role if the default gateway is not reachable

Drag and drop the configuration commands from the right to the left to meet the requirements. The commands are used more than once Not all commands are used

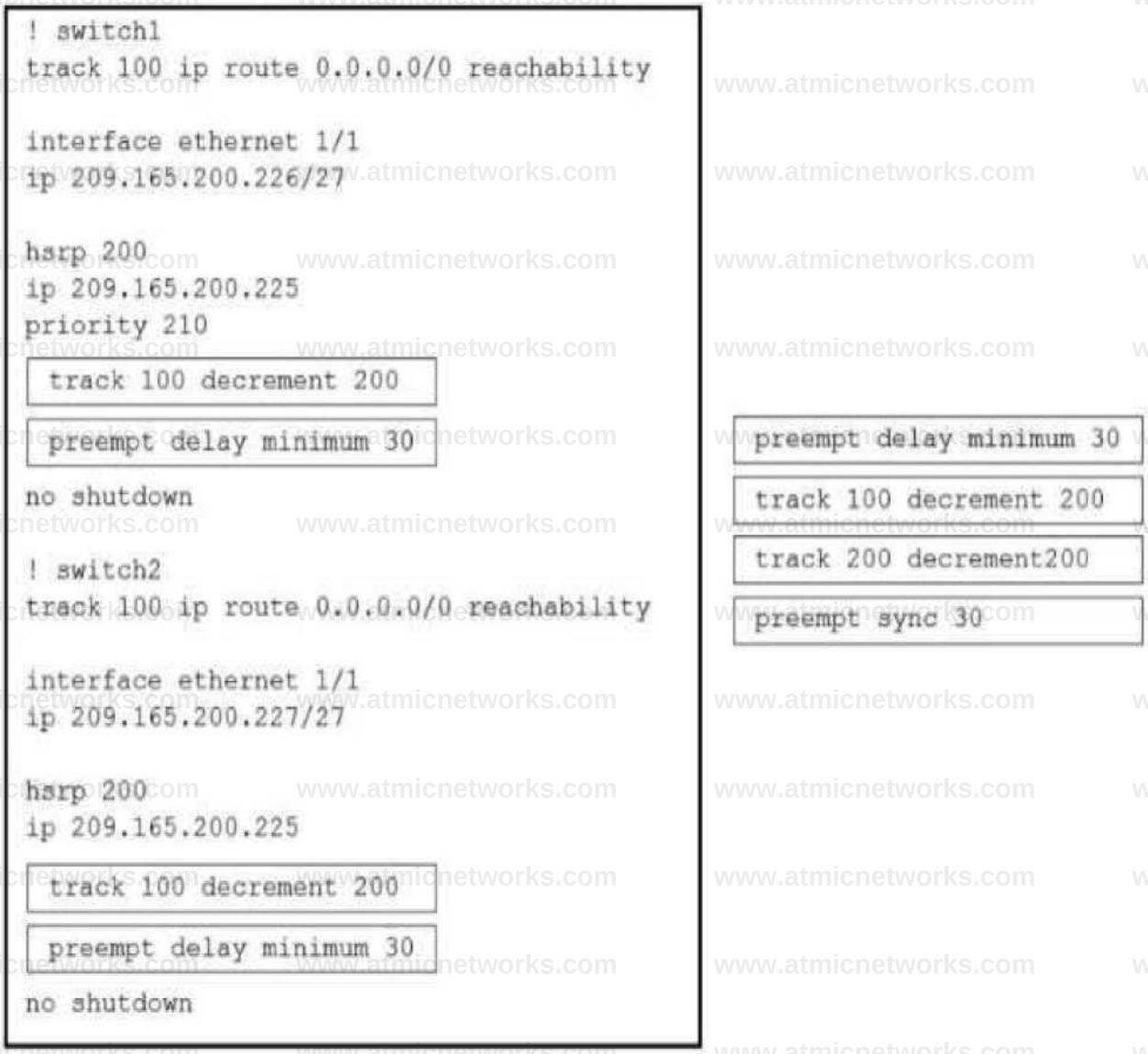
```
! switch1
track 100 ip route 0.0.0.0/0 reachability
interface ethernet 1/1 ip 209.165.200.226/27
hsrp 200
ip 209.165.200.225
priority 210
no shutdown
```

```
! switch2
track 100 ip route 0.0.0.0/0 reachability
interface ethernet 1/1 ip
209.165.200.227/27
hsrp 200
ip 209.165.200.225
no shutdown
```

```
preempt delay minimum 30
track 100 decrement 200
track 200 decrement200
preempt sync 30
```

Answer:

Explanation:



Question: 281

What is the impact of an EPLD upgrade on a Cisco MDS 9000 Series Switch?

A. The active supervisor traffic is disrupted.

B. The upgrade disrupts the management connectivity to the switch.

C. The standby supervisor module reloads multiple times.

D. The upgrade process disrupts only the module that is being upgraded.

Answer: D

Explanation:

An EPLD upgrade on a Cisco MDS 9000 Series Switch affects only the module that is being upgraded. It does not disrupt the active supervisor traffic, management connectivity to the switch, or cause the standby supervisor module to reload multiple times. The upgrade is designed to be as non-disruptive as possible1.

Question: 282

Refer to the exhibit.

Refer to the exhibit A network engineer created a new role to be assigned to the SAN users The requirement is for users to have these characteristics

permitted to show access to the system, SNMP, module, and hardware information

permitted to run debug zone and exec fcping commands

restricted from accessing show feature environment command Which configuration set meets these requirements?

MDS-B(config)# role name default-role
. Option A fig-role)# rule 5 permit show feature module

B. Option B i fig**l)# role name san-users**
i-rote)# rule 3 permit show feature system
MDS-B(config-role)# rule 4 permit show feature hardware C. Option C fig-rote)# rule 5 permit show feature module

MDS-B(config)# role name default-role
D. Option Dfig-rote)# rule 5 deny show feature environment

MDS-B(config)# role name san-users
MDS-B(config-roie)# rule 3 deny show feature environment

Answer: B

Explanation:

Option B is the correct configuration set that meets the requirements for the SAN users' role. This configuration allows users to have show access to the system, SNMP, module, and hardware information, run debug zone and exec fcping commands, and restricts access to the show feature environment command2.

Question: 283

An engineer must design an automation solution for the Cisco ACI Fabric to speed up the deployment of logical network elements for tenant provisioning. When creating a solution, the engineer must keep in mind that the tool must support these requirements:

Allow the rapid creation and removal of logical containers.

Support the creation of custom modules and data structures.

Be extensible with external libraries and modules.

Allow rapid testing of code using an on-demand execution environment.

Which automation tool meets these requirements?

A. YAML

B. Chef

C. SaltStack

D. Python

Answer: D

Explanation:

Python is a versatile scripting language that supports the rapid creation and removal of logical containers, the development of custom modules and data structures, and is extensible with a wide range of external libraries and modules. It also allows for on-demand execution, making it ideal for automating tasks in Cisco ACI Fabric

Question: 284

A network engineer is configuring the Cisco UCS service profile template with Ansible using this code.

```
hostname: 192.168 10.23
username cisco
password: f718c4329405088301f6247ff982
name: DCE-CTRL
template_type: updating-template
uuidjjool UUID-POOL
storage_profile: DCE-StgProf
mamtenance_policy default
server_pool: Container-Pool host_firmware_package: 41(1 a) bios_policy: Docker
```

Which attribute must be used to apply the iSCSI initiator identifiers to all iSCSI vNICs for the service profiles derived from the service template?

A. san_connectivity_policy

B. iqn_pool

C. boot_policy

D. lan_connectivrty_policy

Answer: B

Explanation:

The 'iqn_pool' attribute in Ansible is used to apply iSCSI initiator identifiers to all iSCSI vNICs for service profiles derived from a service template. This ensures that each iSCSI vNIC has a unique identifier for storage communication2

Question: 285

An engineer must configure the HSRP protocol between two Cisco Nexus 9000 Series Switches This

configuration is present on Nexus A.

NaausA
My Ch*n NKRP KE VS
Mv WO
uy-iwng 7 0?b4i?tk!<«c4a«lMOtt1ttbWliiaJMMl<Jl«l1 wcm-liMw 00 00 00 Jan 01 »J1 23 W 01 Aug Ji JM1
MndJiMmia 00 00 00 Jan 01 20 21 2 3 39 59 Jul 31 2 0 21
lay 1020
.•v «wn₈ ? 00«i3cd4clWcl702Ml»031S3b3«222la»2©20ta0l1a12
•CMOHIMMM 00 00.00 Jul 01 2021 23 91 99 DM 31 2021
MndJitama 00 00 00 JU 0 5 20 21 2J 5 9 39 DM 31 2021
■MWfMC fOwn# 1 '1
* 209 144 200 224'27
hart* 200
pnonty 201
* 200 140 200 229
- nsung ouqMt -
noihutaown

The final HSRP configuration must meet these requirements
The HSRP communication must be secured on both switches

Both switches must support more than 300 groups

Which two commands must be added to the HSRP configuration on Nexus A to complete these requirements? (Choose two)

A. hsrp version 1

B. hsrp version 2

C. authentication text 1020

D. authenticate md5 key-chain NHRP-KEYS

E. authentication text 1010

Answer: B, D

Explanation:

To meet the requirements of securing HSRP communication and supporting more than 300 groups, the commands needed are hsrp version 2 which allows for a greater number of HSRP groups (0-4095) and authenticate md5 key-chain NHRP-KEYS which provides MD5 authentication to secure HSRP updates.

Question: 286

An engineer configures a role for a new user in Cisco UCS Manager The role should allow the user to configure vHBAs, vNICs, and server port types.

Which role should be assigned to allow the engineer to complete this task?

A. network administrator

B. operations

C. server-compute

D. AAA administrator

Answer: A

Explanation:

The network administrator role in Cisco UCS Manager is designed to allow configuration of network- related settings, which includes vHBAs, vNICs, and server port types. This role provides the necessary privileges to manage these components

Question: 287

The Cisco UCS blade chassis must send SNMPv3 traps to a network monitoring system. The SNMP trap messages should be authenticated and have protection from closure. Which SNMP security privileged level should be configured?

A. noPriv

B. auth

C. noAuth

D. priv

Answer: D

Explanation:

The 'priv' security level in SNMPv3 provides both authentication and encryption, ensuring that SNMP trap messages are both authenticated and protected from disclosure. This level uses a combination of a username and a strong authentication and encryption mechanism to secure the messages

Question: 288

An engineer must add a new VRF (DC DC) to the network that runs with Multiprotocol Border Gateway Protocol (MP-BGP) and EVPN.The requirement for the new VRF is to allow communication of network prefixes between PE1 and PE2. Which two sets of steps should be taken to complete the VRF configuration? (Choose two)

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: B, E

Explanation:

To add a new VRF (DC DC) that allows communication of network prefixes between PE1 and PE2 using MP-BGP and EVPN, the engineer should choose Option B and Option E. These options likely include the necessary configurations for route distinguishers and route targets that facilitate the import and export of routes between the VRF instances on different PE routers1

Question: 289

A company must security harden its Cisco UCS C-Series servers. The security policy requires all out- of-band management to meet these requirements

It must encrypt all traffic

It must use nondefault ports

It must provide private administrative sessions

Which Cisco IMC corrflguraton meets the requirements?

dMit KOM SOI data! tot $ w, enabled yet data! tol 11M encrypted till .2 5*11 sol *- Mt port MM data! 'Mi *- tM Mitton mac 2 dual s M *» мı deny local yet

dttal* scope time data! >'clmc a eat enabled yet data! 'nnc ** Mt encrypted Ct dotal tent ** Mt kvm-port 1*72 data! r>rw ■" Mt mae-Mts/ons 1 data! 'CMK '* Mt 'ocal-test'on deny

dual* scope oob
data! 'cob * Mt enabled no data! 'oob H Mt encrypted yet dotal Mb *w set kvm-port 2068 data! roti "* Mt mai-Mstlons 1 data! /Mb *• Mt local-access no

•idataW scope kv<n
dMat *vm a Mt enabled yet
djQ! k/m "• Mt encrypted yes data! lvm •• tot kvm port JIM data! kvtn '» Mt mai sessions 1 data! kan *• set local-video no

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

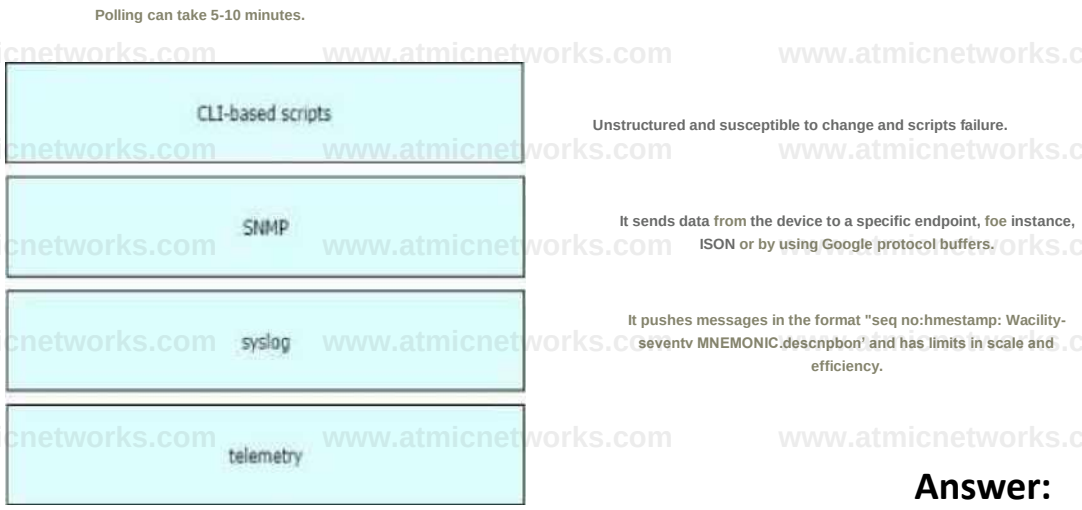
Explanation:

Option C meets the security hardening requirements for Cisco UCS C-Series servers' out-of-band management. It ensures that all traffic is encrypted, uses nondefault ports, and provides private administrative sessions, which align with the company's security policy

Question: 290

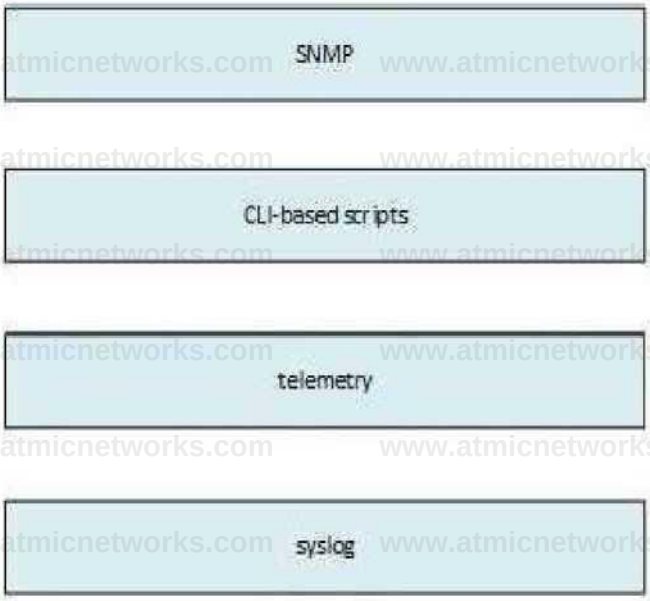
DRAG DROP

Drag and drop the mechanisms to collect data from a network from the left onto their characteristics on the right



Answer:

Explanation:



Question: 291

An engineer is implementing the Cisco ACI fabric and must create two different vPCs from leaf switches A and B. The vPCs are deployed as follows:

- vPC 1 encompasses ports Eth 1 /1 on leaf A and B and connects to server 1.
- vPC 2 encompasses port Eth1/2 on leaf A and B and connects to server 2.

A leaf switch profile listing leaves A and B is already configured Which ACI object must be created to meet these requirements?

A. two vPC interface policy groups

B. one access port interface policy group

C. two PortChannel interface policy groups

D. one vPC interface policy group

Answer: D

Explanation:

In Cisco ACI, a virtual Port Channel (vPC) allows links that are physically connected to two different ACI leaf nodes to appear as a single port channel to a third device. When configuring vPCs in ACI, you

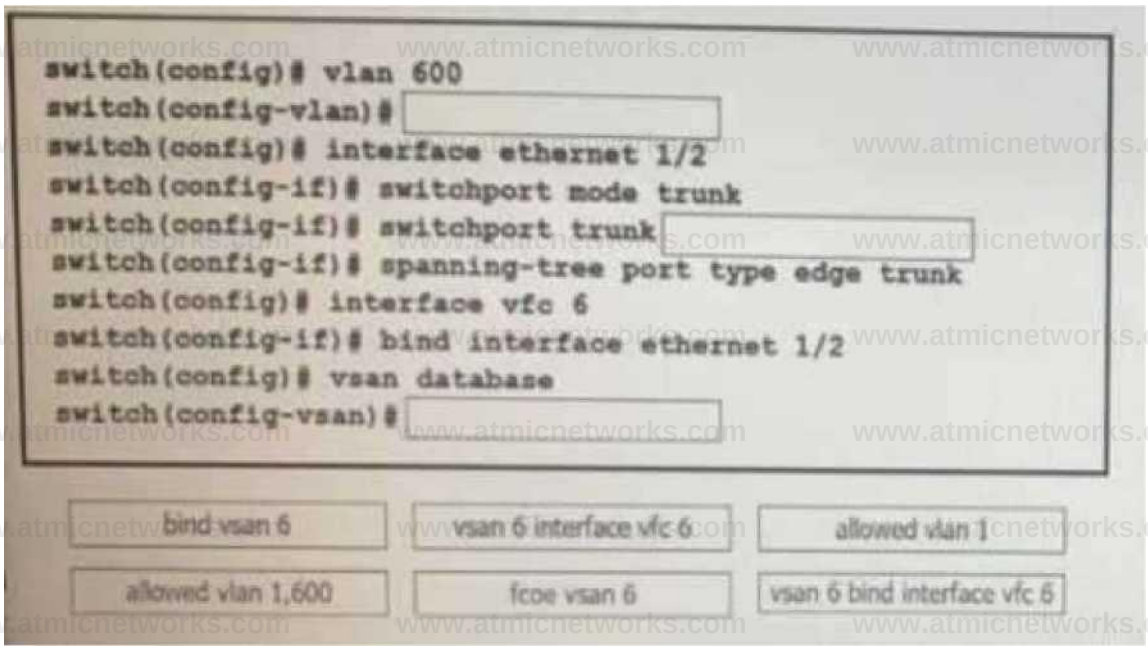
do not need to create multiple interface policy groups for each vPC. Instead, you create a single vPC interface policy group that can be applied to multiple vPCs. This is because the fabric itself serves as the multi-chassis trunk (MCT), and peer reachability is managed through the fabric, not through physical peer-links. Therefore, for the scenario described, where two vPCs are created from leaf switches A and B, only one vPC interface policy group is required.

Reference := The information is based on the best practices from the Cisco guide on Virtual Port Channel (vPC) in ACI1 and the Cisco ACI fabric access policies configuration guide

Question: 292

DRAG DROP

A network engineer must configure FCoE on an interface of a Cisco MDS 9000 Series Switch. It should be used for mapping between VLAN 600 and VSAN 6. Drag and drop the commands from the bottom into their implementation order in the FCoE configuration. Not all commands are used.



Answer:

Explanation:

•witch(config)I vlan WO _____ _____
•witch (eonfig-vlan) 11 fro war 6_____]
•witch(config)4 interface athamat 1/2
•witch(config-if)* awltchpozt soda trunk
•witch (config-lf) I •witchport trunk sloMVfvtan 1,600
•witch(config-if)• spanning-trow port typo edge trunk
•witch(config)4 intarfaco vfc 6
■witch(config-lf)(bind Intorfaca athamat 1/2
•witch(conf1g)I vaan database
•witch (confi g-vsan) | wan 6 Interface vft 6

WnO vsan6] allowed 411 [

wan 6 and Warfare vfc 61

Question: 293

An engineer must affirm the identity of the Cisco UCS Manager after a valid CA-signed keyring for HTTPS access is created. Which action completes the configuration?

A. Set Cipher Suite Mode

B. Create a trusted point

C. Implement SSLv3

D. Enable TLSv1.2

Answer: B

Explanation:

After creating a CA-signed keyring for HTTPS access in Cisco UCS Manager, the next step is to create a trusted point. This action associates the keyring with a certificate and designates the certification authority (CA) that will be recognized as valid for the system

Question: 294

An engineer must configure two Cisco Nexus 7000 series switches in the same data center to support OTV. Which command set completes the join interface configuration?

An eerier tsi tcrftjjre two Cisco Nexus 7000 Senes swtcnes in me same data tetter to support 07V Whcfi command set completes me an ratface ooragwafion'

feature oh
av site-identifier 240
interface overtax 1
ON control-gnoupZJSl.l.t
ON OaU-grouo 239,1 1.0®
ON join-interface ethernet 81
ON extend-vlan 5-10
na shutdown

Option A

Edge Device 1

interface ethernet 2/1 ip address 192.0.2.1/24 ip igmp version 3

Edge Device 2

interface ethemet 2/1 ip address 192.0.2.16/24 ip igmp version 3

Option B

Edge Device 1

```
interface ethernet 2/1
  ip address 192.0.2.1/24
  ip igmp version 3 ip pirn sparse-mode
```

Edge Device 2

```
interface ethernet 2/1
  ip address 192.0.2.16/24 ip igmp version 3
  ip pirn sparse-mode
```

C. Option C

Edge Device 1

```
interface ethemet 2/1
  ipaddress 192.0.2.1/24
```

Edge Device 2

interface ethemet 2/1 ip address 192.0.2.16/24

D. Option D

Edge Device 1 interface ethernet 2/1 ip address 192.0.2.1/24 ip igmp version 3

Edge Device 2 interface ethernet 2/1 ip address 192.0.2.1/24 ip iamp version 3

Answer: A

Explanation:

In the context of configuring two Cisco Nexus 7000 series switches to support OTV, Option A is the correct answer. The configuration involves setting up an Edge Device with specific interface ethernet and IP address settings. The commands provided in Option A are consistent with the requirements for configuring an OTV join interface on Cisco Nexus 7000 series switches. These commands ensure that the Edge Devices are properly configured to communicate over the OTV.

Question: 295

An engineer performs a Firmware Auto Install upgrade through the Cisco UCS Manager. Which two Cisco UCS

components are upgraded in the Install Server Firmware stage? (Choose two)

A. Cisco UCS C-Series Rack-Mount Server

B. I/O Modules

C. Cisco UCS Manager

D. Cisco UCS B-Series Blade Server

E. Fabric Interconnects

Answer: A, D

Explanation:

During the Install Server Firmware stage of a Firmware Auto Install upgrade through Cisco UCS Manager, the components that are upgraded include the Cisco UCS C-Series Rack-Mount Servers and the Cisco UCS B-Series Blade Servers. This stage uses host firmware packages to upgrade all servers

and their components in the Cisco UCS domain. All servers whose service profiles include the selected host firmware packages are upgraded to the firmware versions in the selected software bundles1.

Reference := Cisco Documentation on Firmware Upgrades through Auto Install

Question: 296

An engineer is implementing traffic monitoring for a server vNIC that is configured with fabric failover enabled. The requirement is for the traffic to be sent to an analyzer, even during a failure of one of the fabric interconnects. The analyzer is connected to unconfigured Ethernet ports on both fabric interconnects. Which configuration accomplishes this task?

A. Create two traffic monitoring session with different names, one per fabric Connect the analyzer connected to FI-BI the destination for both monitoring sessions.

B. Create two traffic monitoring session with different names, one per fabric.

C. Connect an analyser on each FI as the destination for the monitoring session local to the FI.

D. Create two traffic monitoring sessions with the same name, one per fabric Connect the analyze connected to FI-A as

the destination for both monitoring sessions

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To implement traffic monitoring for a server vNIC with fabric failover enabled, ensuring that traffic is sent to an analyzer even during a fabric interconnect failure, the correct configuration is to create two traffic monitoring sessions with different names, one per fabric, and connect an analyzer on each

FI as the destination for the monitoring session local to the FI. This setup allows continuous monitoring because if one fabric interconnect fails, the other can still send traffic to its connected analyzer2.

Reference := Cisco Community Discussion on Understanding Fabric Failure and Failover in UCS

Question: 297

An engineer configures a storage environment for a customer with high- security standards. The secure environment is configured in vsan 50. The customer wants to maintain a configuration and active databases and prevent unauthorized switches from joining the fabric. Additionally, the switches must prevent rogue devices from connecting to their ports by automatically learning the WWPNs of the ports connected to them for the first time. Which two configuration sets must be used to meet these requirements? (Chose two.)

port-security enable
port-security activate vsan 50

clear fabric-binding activate vsan 50
fabric-binding activate vsan 50

fabric-binding activate vsan 50 force

fcsp enable
fcsp auto-active

fcsp dhchap hash md5 sha1

A. Option A

B. Option B

C. Option C

D. Option D

E. Option E

Answer: A, C

Explanation:

To meet the high-security standards, the engineer should configure port security and fabric binding on VSAN 50. Port security prevents unauthorized devices from logging into the fabric by automatically learning and securing the World Wide Port Names (WWPNs) of devices connected to the switch ports. Fabric binding allows only authorized switches to join the fabric by creating a list of switch WWNs that are permitted to join a specific VSAN.

Question: 298

What is an advantage of NAS compared to SAN?

A. It offers enhanced NFS features.

B. It offers enhanced security features

C. It functions in an existing IP environment.

D. It provides lossless throughput.

Answer: C

Explanation:

NAS functions in an existing IP environment which is one of its advantages over SAN. SAN typically requires a separate network infrastructure, while NAS can be deployed on the existing IP network, leading to cost savings and simplified management.

Reference:

Cisco Data Center Core Technologies source documents or study guide

Cisco Learning Network Store

Cisco Data Center Solutions

Question: 299

Refer to the exhibit.

Refer to the exhibit. Which feature must be used to configure on switch 2 to establish a VSAN trunk between switch 1 and switch 2?

A. F port

Trunk Mode Passive

B. E Port

Trunk Mode On

C. N Port

Trunk Mode Active

D. NP Port

Trunk Mode Auto

Answer: B

Explanation:

To establish a VSAN trunk between Switch 1 and Switch 2, you would typically configure E Port with Trunk Mode On. This is because Switch 1 is already configured with an E port in Trunk Mode Auto, and for trunking to be established, the other switch should also be set to trunk mode but with a static configuration (On) to ensure compatibility and trunk formation.

Question: 300

A content delivery network sends video traffic to a multicast distribution device where the receiver requests the traffic from the multicast distribution device through an IGMP join message When the traffic reaches the multicast routing device from a CDN the switching network populates the multicast routing table in the group (S G) and the multicast distribution device sends the required traffic back to the receiver. Which feature is used to send back the trafic from the streamer to the receiver in the group (S G)?

A. RP

B. IGMP

C. Reverse Path Forwarding

D. Source Specific Multicast

Answer: C

Explanation:

Reverse Path Forwarding (RPF) is a feature used in IP multicast routing that ensures multicast traffic is sent back to the receiver efficiently and without looping. In the context of a content delivery network (CDN) sending video traffic, when a receiver requests traffic through an IGMP join message, the multicast routing device uses RPF to populate the multicast routing table with the correct source (S) and group (G) information. RPF checks the source of the incoming packet against the multicast routing table and forwards the packet only if it arrives on the interface that leads back to the source. This mechanism prevents traffic loops and ensures that the multicast distribution device sends the required traffic back to the receiver along the most efficient path.

Reference: The explanation is based on the principles of IP multicast routing as detailed in Cisco's Data Center Core Technologies documentation, specifically the sections on "Implementing Multicast in Data Center" and "IP Multicast Technology Overview" which discuss the role of RPF in multicast distribution

Question: 301

Which two actions are needed to configure a single Cisco APIC controller for Cisco ACI fabric for the first time? (Choose two.)

A. Register the APIC that is connected to the switch.

B. Configure the first Cisco APIC controller

C. Configure the leaf switch where the Cisco APIC is connected, using CLI to allow APIC connectivity

D. Register the switches that are discovered through LLDP.

E. Register all leaf and spine switches

Answer: B, D

Explanation:

To configure a single Cisco APIC controller for Cisco ACI fabric for the first time, you need to configure

the first Cisco APIC controller (B) and register the switches that are discovered through LLDP (D). The initial configuration

of the APIC is crucial as it sets up the controller with the necessary settings to manage the ACI fabric. Registering the switches through LLDP allows the APIC to recognize and manage the fabric switches, which is essential for the ACI fabric to function correctly. Reference: Cisco's official documentation on setting up an ACI fabric1, and the Cisco APIC Basic Configuration Guide2.

Question: 302

Which two actions should be performed before upgrading the infrastructure and firmware of multiple UCS blades? (Choose two)

A. Verify if the bootflash on the fabric interconnects m the Cisco UCS has at least 15°* available space

B. Enable Smart Call Home feature during the firmware upgrade process

C. Verify if the bootflash on the fabric interconnects in the Cisco UCS has at least 10% available space

D. Run the Check Conformance feature to verify that all your components are running the compatible firmware version after the upgrade

E. Get Full State and All Configuration backup files before beginning the upgrade

Answer: C, E

Explanation:

Before upgrading the infrastructure and firmware of multiple UCS blades, it is important to verify if the bootflash on the fabric interconnects in the Cisco UCS has at least 10% available space © and to get Full State and All Configuration backup files before beginning the upgrade (E). Ensuring sufficient bootflash space is necessary for the upgrade process to proceed without storage issues. Backing up the current state and configuration provides a recovery point in case the upgrade encounters problems. Reference: Cisco's guidelines on firmware upgrades3 and community discussions on UCS firmware updates4.

Question: 303

A customer requires a solution to orchestrate the configuration of storage arrays, firewalls, and Cisco ACI networking. Additionally, the orchestration product must support open automation and a service catalog. Which solution meets these requirements?

A. Cisco UCS Director

B. Cisco Intersight

C. Cisco Data Center Network Manager

D. Cisco Workload Optimization Manager

Answer: A

Explanation:

Cisco UCS Director is the appropriate solution for orchestrating the configuration of storage arrays, firewalls, and Cisco ACI networking. It supports open automation through various APIs and offers a service catalog that allows users to manage and deploy services across multiple domains, including compute, storage, networking, and virtualization.

Reference: The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course provides insights into the capabilities of Cisco UCS Director, including its orchestration and automation features

Question: 304

An engineer needs to connect Cisco UCS Manager to an external storage array. Due to budget limitations, the engineer must connect a Cisco UCS manager directly to an FC storage port. Which two actions must be taken to complete this connection? (Choose two)

A. Configure the fabric interconnect in FC switch mode

B. Create a storage connection policy

C. Set FC zoning to disabled when creating the VSAN

D. Configure the fabric interconnect in end host mode

E. Create the required VSAN in the SAN cloud

Answer: A, E

Explanation:

To connect Cisco UCS Manager directly to an FC storage port, the fabric interconnect must be configured in FC switch mode, which allows it to manage Fibre Channel traffic and zoning.
Additionally, creating the required VSAN in the SAN cloud is necessary to define a virtual storage area network that can be associated with the storage ports on the fabric interconnect.

Reference: Detailed steps for these actions can be found in the Cisco documentation, which outlines the process of configuring direct attached storage and FC zoning with Cisco UCS Manager

Question: 305

Which virtualization feature is provided by network-attached storage?

A. ALUA path redirection

B. hypervisor host boot LUN

C. VM cluster shared disk

D. raw device passthrough

Answer: C

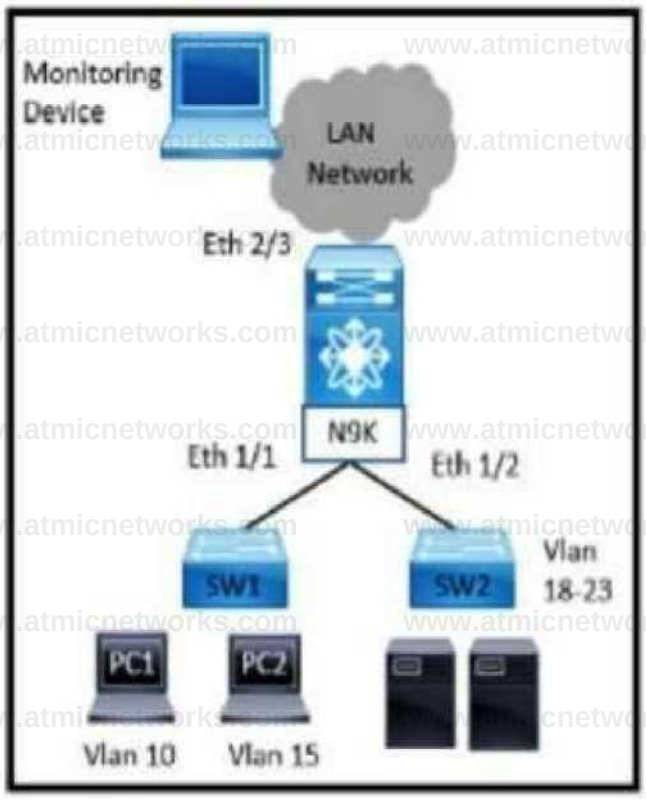
Explanation:

Network-attached storage (NAS) provides the virtualization feature of a VM cluster shared disk. This allows multiple virtual machines to access shared storage, enabling functionalities like migration, fault tolerance, and distributed resource scheduling.

Reference: VMware documentation on networked storage technologies explains how NAS supports shared datastores that can be accessed by multiple hosts concurrently, which is essential for VM cluster shared disks

Question: 306

Refer to the exhibit.



Refer to the exhibit A network administrator experiences these issues with the network:

PC1 is experiencing a buffering problem for video applications

The servers that are connected to SW2 are experiencing packet drops when they connect to the Internet

The engineer wants to configure the required traffic capture to investigate the issue further Which configuration must be implemented to monitor the traffic?

A. Option A

```
N^Kf config)# monitor session 5 nt
N9K(config)# monitor session 5 tx
```

```
N9Kfconfig monitor)# description Span_session_5 N9Klconfig monitor)# source interface
ethernet 1/1 N 'Kfconfig monitor)# source interface ethernet 1/2
N9Kf config-monitor}# destination interface ethernet 2/3
```

B. Option B

```
N9K(config)# monitor session 5 tx
N9K(config monitor)# description Span_session_5
N9K(configmonitor)# source interface ethernet 1/1
N9Kiconhg-monitor)# source interface ethernet 1/2
N9Kconfig-monitor)# destination interface ethernet 2/3
```

C. Option C

```
NMKfconhg)# monitor session 5 tx
NMKfconfig monitor)# description Span_session_5
N9K(config monitor - source vlan 10-16 rx
N9K| config-mon itor# source interface ethernet 1/2
N9K( config-monitor)^ destination interface ethernet 2/3
```

D. Option D

```
!• MMfconfig)# monitor session 6 rx
NOKfconfig monitor)# description Span_session_5
MKf config-monitor)# source vlan 10 rx
N9K( config-monitor# source interface ethernet 1/2
N\/Kf config-monitor# detonation interface ethernet 2/3
```

Answer: D

Explanation:

When configuring traffic capture to investigate issues such as buffering problems and packet drops, it's important to consider where to place the capture points. Typically, you would configure a SPAN (Switched Port Analyzer) or RSPAN (Remote SPAN) session to mirror the traffic from the affected areas to a monitoring device. The configuration would involve:

Identifying the source ports or VLANs where the issues are observed.

Specifying a destination port connected to a network analyzer like Wireshark.

Ensuring the destination port is not used for regular network traffic.

For example, a basic SPAN session configuration might look like this:

monitor session [session_number] source interface [interface_id]
monitor session [session_number] destination interface [destination_interface_id]

Reference: The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course provides insights into the capabilities of Cisco devices for traffic capture and monitoring. For detailed steps and best practices, refer to Cisco's official documentation on configuring packet capture

Question: 307

An engineer must perform a nondisruptive software upgrade on a dual supervisor Cisco Nexus 7000 series switch. What is the cause of the upgrade being disruptive?

A. The show install all impact command is not issued before the upgrade
B. The kickstart image is installed by using the Install all kickstart image system image command
C. Attempt to simultaneously upgrade more than three cards
D. Change to the configuration settings or the network connections during the upgrade process

Answer: D

Explanation:

A nondisruptive upgrade is possible only when there are no changes to the configuration settings or network connections during the upgrade process. Any such changes can lead to a disruption, which is particularly critical in a dual supervisor Cisco Nexus 7000 series switch where stability is paramount.

Reference := For an in-depth understanding, refer to the Cisco Data Center Core Technologies study materials, specifically the sections discussing software upgrades and maintenance for Cisco Nexus switches

Question: 308

An engineer must configure a named VSAN when the fabric interconnect is in Fibre Channel switch mode The VSAN

must meet these requirements:

Named VSAN must be called "VSAN 10".

VSAN ID must be 10.

FCoE ID must be 20.

VSAN 10 must be attached to port 2 in slot 1.

Which command set configures a VSAN when the fabric interconnect is in Fibre Channel switch mode?

A. Option A

```
UCS-A# scope fc-storage
UCS A/fc-storage# create vsan VSAN10 10 20
UCS-A /fc-storage/vsan * create member-port fcoe a 1 2
UCS-A /fc-storage/vsan/member-port* # commit-buffer
```

B. Option B

```
UCS-A# scope fc-traffic mon
UCS A/fc-storage# create vsan VSAN10 20 10
UCS-A /fc-storage/vsan # create member-port fcoe a 2 1
UCS-A /fc-storage/vsan/member-port* # commit-buffer
```

C. Option C

```
UCS-A# scope eth-storage
UCS-A/fc-storage# create vsan VSAN 10 10 20
UCS-A /fc-storage/vsan # create member-port fcoe a 2 1
UCS-A /fc-storage/vsan/member-port* # commit-buffer
```

D. Option D

```
UCS-A# scope fc-uplink
UCS-A/fc-storage# create vsan VSAN 10 20 10
UCS-A /fc-storage/vsan # create member-port fcoe a 1 2
UCS-A /fc-storage/vsan/member-port* # commit-buffer
```

Answer: C

Explanation:

The command set in Option C correctly outlines the steps to configure a named VSAN called "VSAN10" with the specified requirements. It includes creating the VSAN with ID 10, assigning an FCoE ID of 20, and attaching it to port 2 in slot 1.

Reference := Detailed commands and configurations for VSANs can be found in the Cisco Data Center Core Technologies documentation, particularly in the sections that cover Fibre Channel switch mode and VSAN configuration

Question: 309

A network engineer needs a tool to automate the provisioning of Cisco UCS Service Profiles. The administrator has limited programming knowledge but is skilled with scripting tools. The tool must include existing support for Cisco UCS configuration. Additionally, the administrator will eventually use the solution to manage Cisco UCS C-Series Rack Servers. Which tool meets these requirements?

A. Cisco DCNM

B. Python scripts

C. PowerShell

D. Bash scripts

Answer: C

Explanation:

PowerShell is a task automation and configuration management framework from Microsoft, consisting of a command-line shell and the associated scripting language. It is integrated with Cisco UCS Manager and provides cmdlets for automating the management of Cisco UCS domains, including Service Profiles. The UCS PowerTool is a set of PowerShell modules designed specifically for Cisco UCS, making it a suitable choice for a network engineer with scripting skills but limited programming knowledge. It supports configuration tasks for both B-Series Blade Servers and C-Series Rack Servers, aligning with the administrator's future needs.

Reference: Cisco Community discussions on UCS PowerTool + Service Profiles1 and the Cisco UCS PowerTool Scripts Index

Question: 310

Which two statements describe the process of upgrading an EPLD on a Cisco MUS 9000 Series Switch? (Choose two)

A. EPLDs are capable to be upgraded without replacing the hardware

B. The CPLDs for all the modules on a switch must be upgraded at the same time

C. An upgrade verification identifies the impact of each EPLD upgrade

D. EPLDs are only capable to be upgraded to the latest FH. D image

E. EPLD upgrades are capable to be completed without powering down the module during the upgrade

Answer: A, E

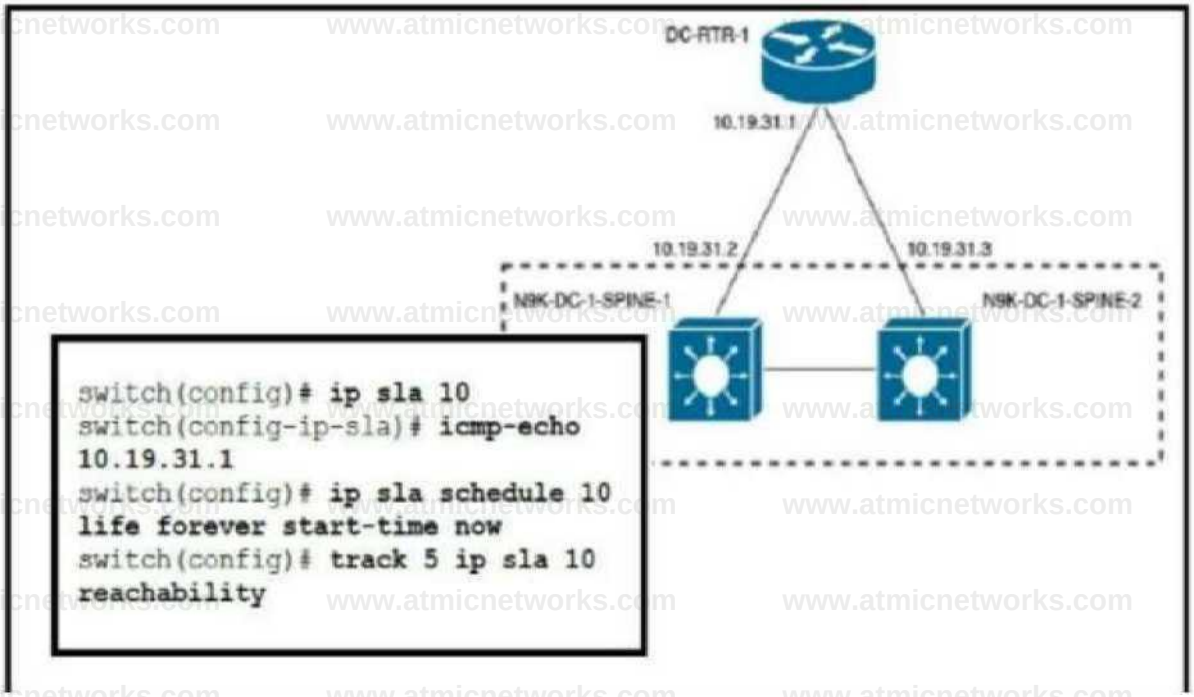
Explanation:

EPLDs (Electronic Programmable Logic Devices) can be upgraded to enhance hardware functionality or resolve known issues without the need for hardware replacement. The upgrade process is disruptive as it requires the module to power down briefly during the upgrade. However, the system performs EPLD upgrades on one module at a time, minimizing the disruption to traffic through only one module at any given time.

Reference: Cisco Community discussion on Upgrading EPLD on N9k3 and Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes

Question: 311

Refer to the exhibit.



Refer to the exhibit. An engineer must invoke a Python script that alerts the operations team when the router DC-RTR-1 becomes unreachable. Which configuration set accomplishes this task?

track 3 ip sla 10 reachability
•vent name GATEWAY-DOWN
event state down
action ell command routerdown.py

:• scheduler job name ROUTER-DOWN
job track 9 state down
actioo 1.0 cli source routerdown.py
scheme 10

event scheduler name DOWN-ROUTER
event track 2 state 1 not up
event action 1.0 command source routerdown py
event start 0:00 repeat 0 06

event manager applet ROUTER-DOWN-SIA
event track 6 state down
action 10 event-default
action 2 0 cli command source routerdown py

A. Option A

B. Option B

C. Option C

D. Option D

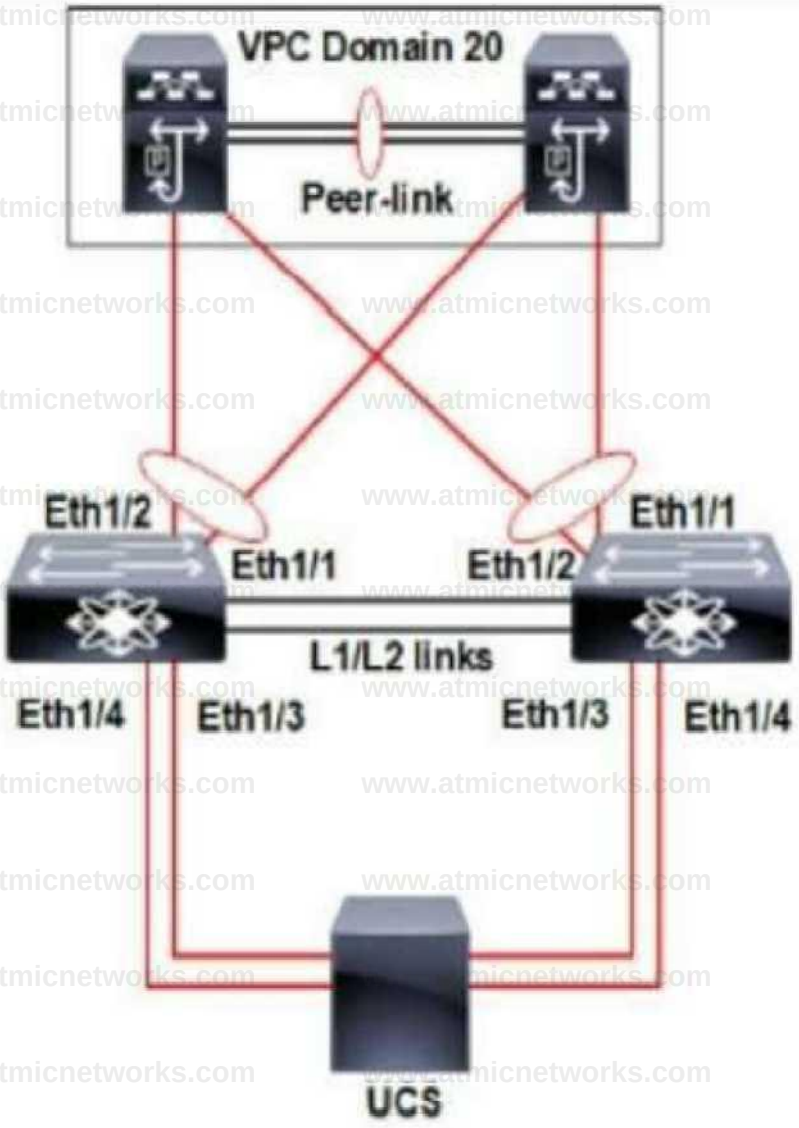
Answer: C

Explanation:

The configuration set in Option C is designed to invoke a Python script when the router becomes unreachable. It uses an event scheduler to track the state of the router and, if it is not up, it triggers the Python script "routerdown.py" at specified intervals. This setup ensures that the operations team is alerted promptly when the router DC-RTR-1 becomes unreachable, allowing for quick response and troubleshooting.

Question: 312

Refer to the exhibit.



Refer to the exhibit. A pair of Cisco Nexus switches form a vPC. A new chassis s added to the preexisting Cisco UCS domain. A new chassis must be discovered, and all links from the chassis to the LAN network must be established. Which set of actions accomplishes these requirements?

Set the chassis discovery po cy action to four imks Configure Eth1/3 and BM/4 as server pons Acknowledge the chassis

:• Set the chassis discovery policy action to four links Configure Eth V1 and Etn 12 as uplink Fibre Channel ports Set the link group preference to None

Set the chassis discovery potty action to one link Configure BhVI and Eth12 as uplink Ethernet ports Set the link group preference to Port Channel

t>

Set the chassis discovery policy action to one link
Configure Ethl/3 and Eth 14 as server ports Acknowledge Die chassis

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

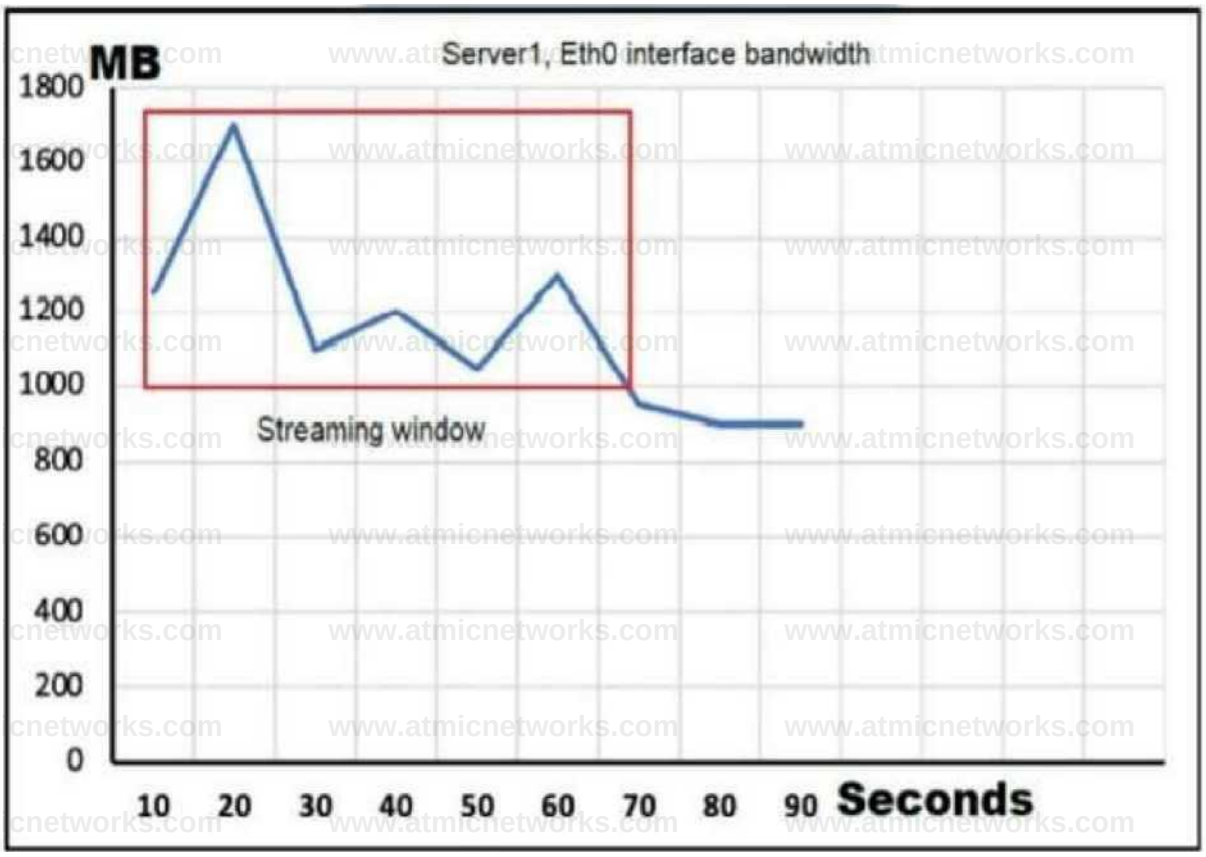
Explanation:

To discover a new chassis and establish all links from the chassis to the LAN network in a Cisco UCS domain with a vPC setup, the chassis discovery policy action should be set to one link. The Ethernet ports Eth1/1 and Eth1/2 should be configured as uplink Ethernet ports, and the link group preference should be set to Port Channel. This configuration ensures that the new chassis is properly discovered and that the links are correctly established to handle the LAN traffic.

Reference: The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course

provides detailed instructions on chassis discovery and vPC configuration. For further guidance, Cisco's official documentation on vPC best practices and configuration examples would be the appropriate references

Question: 313



Refer to the exhibit. Server1 is connected to a Cisco Nexus 9000 Series Switch via a 1-Gb port channel. The storm control is applied to the Eth0 device with a zero percent value. What does the switch do to traffic that traverses the switch interfaces during the streaming window that exceeds the bandwidth of the interfaces?

A. forwards all traffic

B. forwards half of the traffic

C. suppresses all traffic

D. drops all of the excess traffic

Answer: D

Explanation:

When storm control is applied to an interface with a zero percent value, it means that the switch will not tolerate any traffic that exceeds the bandwidth of the interfaces during a streaming window. The switch monitors the levels of incoming broadcast, multicast, and unicast traffic over a 1-second interval. When the configured threshold level is reached, further traffic in this category is dropped until the level falls below the threshold.

Question: 314

Which component is excluded by default from the host firmware package?

A. network interface controller

B. board controller

C. storage controller

D. local disk

Answer: D

Explanation:

By default, Cisco UCS Manager excludes local disks from a host firmware package to avoid data loss or corruption during firmware upgrades. The host firmware package contains firmware for other components like network interface controllers, storage controllers, etc., but excludes local disks as they might contain sensitive data.

Question: 315

An engineer must configure SAN connectivity in Cisco UCS manager. The requirement is to specify the WWPN of the storage array and set the zoning type to single initiator multiple targets. The engineer must also configure interrupt handling and queues of the vHBA interface. Which two Cisco UCS policies should be used to configure the settings? (Choose two.)

A. storage connection policy

B. SAN connectivity policy

C. vHBA policy

D. Fibre Channel adaptor policy

E. boot policy

Answer: C, D

Explanation:

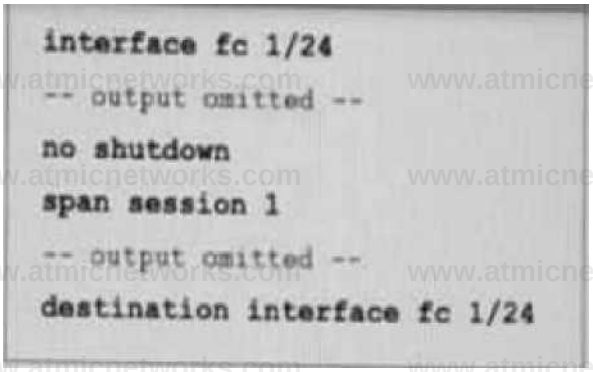
The vHBA policy in Cisco UCS Manager is used to specify the WWPN of the storage array and can be configured for zoning type as single initiator multiple targets. The Fibre Channel adapter policy is used to configure interrupt handling and queues of the vHBA interface, which are essential for SAN connectivity.

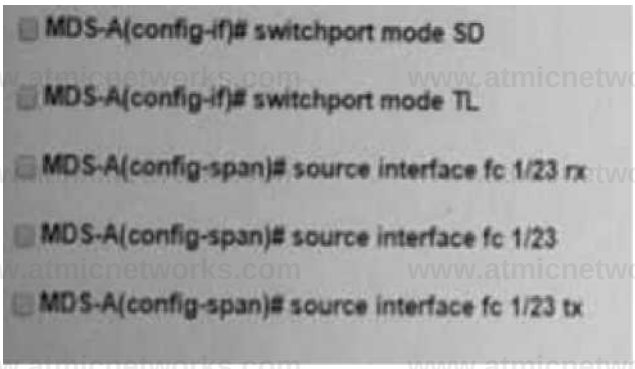
Reference: = For more detailed information, refer to the Cisco UCS Manager GUI Configuration Guide and the Cisco Data Center Core Technologies study materials

Question: 316

A network engineer must SPAN only the ingress traffic of a Cisco MDS 9000 series switch from interface fc 1/23 to interface fc 1/24. Which two configuration must be applied to complete this task?

(Choose two)





A. Option A

B. Option B

C. Option C

D. Option D

Answer: A, C

Explanation:

To SPAN only the ingress traffic on a Cisco MDS 9000 series switch, the configuration must include specifying the source interface for monitoring (fc 1/23) and setting it to capture only ingress traffic (rx). Option A and Option C contain the necessary commands to achieve this.

Reference: = Detailed steps and examples for configuring SPAN to monitor ingress traffic on Cisco MDS 9000 series switches can be found in the Cisco MDS 9000 Series System Management Configuration Guide

Question: 317

A customer data center experiences bandwidth contention that affects the servers connected to the NPV enabled switch The NPV switch is connected to the NPIV switch using two 10 Gb uplinks but the traffic originating front the connected hosts to the core switch exceeds the available bandwidth The engineers decided to add a third uplink to the NPV server to increase the available bandwidth Which set of commands must be used to provision the new uplink?

switch2(config p npv aulo-lwd-bahnce disruptive

I uplink lo NPV Core switch2(configHf)# switchport mode np

- **sw,tch2(config** MI **port-channel load-balance ethernet source-dest-poct**

I uplink to NPV Core
s^tch2(config-<f)M s witch port mode np

switch2(config MI **npv traffic-map server-interface**

I uplink to NPV Core switch2(configwf)M switchport mode npiv

sw1tch2(config MI **npv auto-load-balance**

I uplink to NPV Core switch2(config-if)* swtchport mode npiv

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

To provision a new uplink and increase the available bandwidth for the NPV enabled switch, the commands in Option A should be used. These commands will configure the additional uplink to the NPIV switch, thus addressing the bandwidth contention issues experienced by the servers.

Question: 318

An engineer must generate a checkpoint of the running configuration on a Cisco Nexus Switch. The checkpoint file name must be called "before_maintenance' and should be used for recovering the switch to its pre- maintenance state. The rollback of the checkpoint to running configuration should only occur if no errors occur. Which two configuration commands must be used to meet these requirements? (Choose two.)

A. rollback checkpoint rile before_maintenance stop-at-first-failure

B. rollback running-conflg checkpoint before.maintenance

C. checkpoint file before_maintenance

D. checkpoint before.maintenance

E. rollback running-conflg file before_maintenance atomic

Answer: C, E

Explanation:
The command checkpoint file before_maintenance is used to create a checkpoint of the current running configuration with the specified file name. The command rollback running-config file before_maintenance atomic ensures that the rollback of the checkpoint to the running configuration only occurs if there are no errors during the process. This is essential for maintaining the stability of the switch during maintenance operations.

Question: 319

An engineer mus! configure the remote SSH management connectivity for Cisco Nexus 9000 Series Switches to meet these requirements

The connectivity must be permitted from a jump host with an IP address of 10 10.10 10/24

All switches must be permitted to connect via SSH to other devices from the subnet of 10 .20.20.0/24.

Which configuration set accomplishes these requirements?

- **Hn» vty**
  ip access-class acl-1 out
  ip access-class acl-2 in

  ip access-list acl-1
  permit Ip 10.10.10.1002 any
  ip access-list acl-2
  permit tcp 10.20 20.0'32 any

  line vty
  ip access-class acl-1 In
  ip access-class acl-2 out

  ip access-list acl-1
  permit tcp 10.10.10.10 32 art^eq 22
  ip access-list acl-2
  permit tcp 10 2 0 20 0'24 any

  line vty
  ip access-class acl-1 in
  ip access-class acl-2 in

  ip access-list acl-1
  permit ip 10.10.10.10/32 any
  ip access-list acl-2
  permit tcp 10.20 20.0/32 any

  line vty
  ip access-class acl-1 in
  ip access-class acl-2 in

  ip access-list acl-1
  permit tcp 10 10 10 10'32 any eq 22
  ip access-list acl-2
  permit tcp 10.20 20 0/24 any

A. Option A

B. Option B

C. Option C
D. Option D

Answer: B

Explanation:

Option B is the correct answer because it meets both requirements stated in the question. The configuration permits SSH connectivity from a jump host with an IP address of 10.10.10.10/24 and allows all switches to connect via SSH to other devices from the subnet of 10.20.20.0/24.

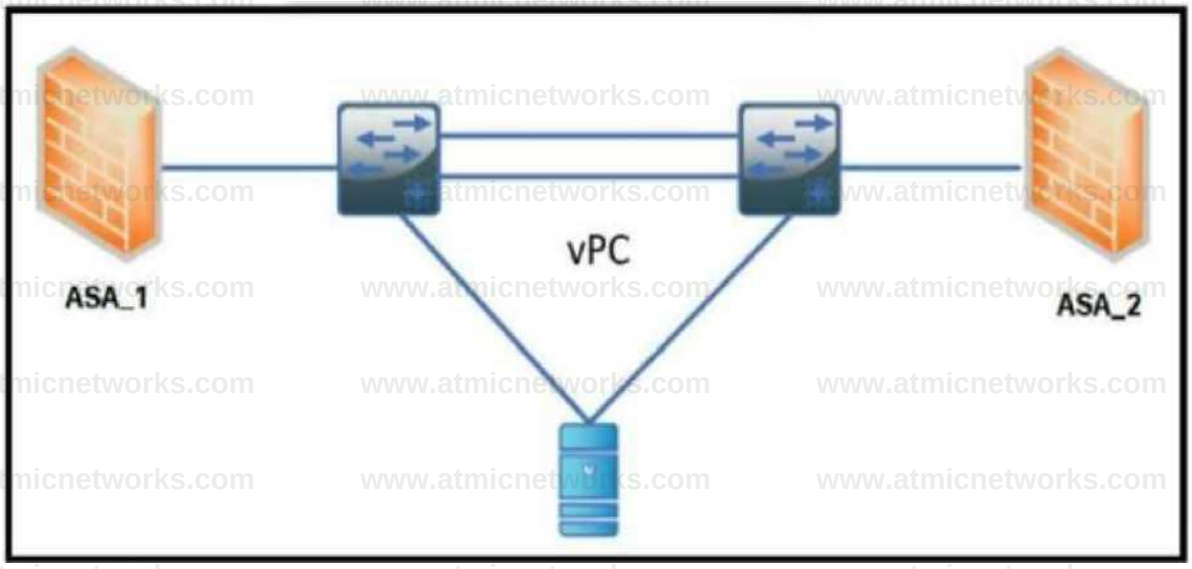
In this option, the access list acl-1 is configured to permit TCP traffic from host 10.10.10.10/32 (the jump host) on any port, and access list acl-2 is configured to permit TCP traffic from subnet 10.20.20.0/24 on any port.

The 'line vty' configuration applies these access lists for inbound (in) and outbound (out) SSH sessions respectively, ensuring that only the specified source IP addresses are allowed for remote SSH management connectivity1.

Reference: = For more detailed information, you can refer to the Cisco Nexus 9000 Series NX-OS Security Configuration Guide

Question: 320

Refer to the exhibit.



Refer to the exhibit The ASA 1 acts as a Layer 3 gateway for all servers. The servers lose the gateway connectivity when the vPC peer links go down and the vPC keepalive remains up. Which action improves the high availability in the network?

A. Create a static port channel with two links from each firewall to the switch

B. Activate the vPC orphan-port suspend feature on the switch ports connected to the firewall

C. Implement the IP reoVect feature on the vPC devices

D. Enable the vPC peer gateway feature on the vPC devices

Answer: D

Explanation:

Enabling the vPC peer gateway feature on the vPC devices allows them to act as the active gateway for packets that are addressed to the router MAC address of the vPC peer. This capability allows both vPC peers to forward traffic and eliminates traffic disruption when one of them goes down, ensuring high availability in network operations.

Reference: = For more detailed information, you can refer to the Cisco Nexus 9000 Series NX-OS High Availability and Redundancy Guide, which provides guidelines on configuring vPC peer gateway features for enhanced network stability and availability.

Question: 321

A DevOps engineer must implement a bash script to query a REST API and return the available methods.

Which code snippet completes the script?

curl 4 -X -muling code- http .'/api. ciico com BCBOapt -u admin «T41M5P3X425VO€71NB5D

A. DELETE

B. TRACE

C. POST

D. OPTIONS

Answer: D

Explanation:

The OPTIONS method is used in REST APIs to return the HTTP methods that the server supports for a specific URL. This can be useful for discovering what functionality a REST API endpoint supports.

Question: 322

An engineer must export the Cisco UCS Manager configuration for backup purposes. The requirement is to export the configuration that contains the AAA and RBAC configuration Also the file must be stored a human-readable format 'Much backup type must be selected to meet these requirements?

A. logical configuration

B. system configuration

C. fun state

D. all configuration

Answer: A

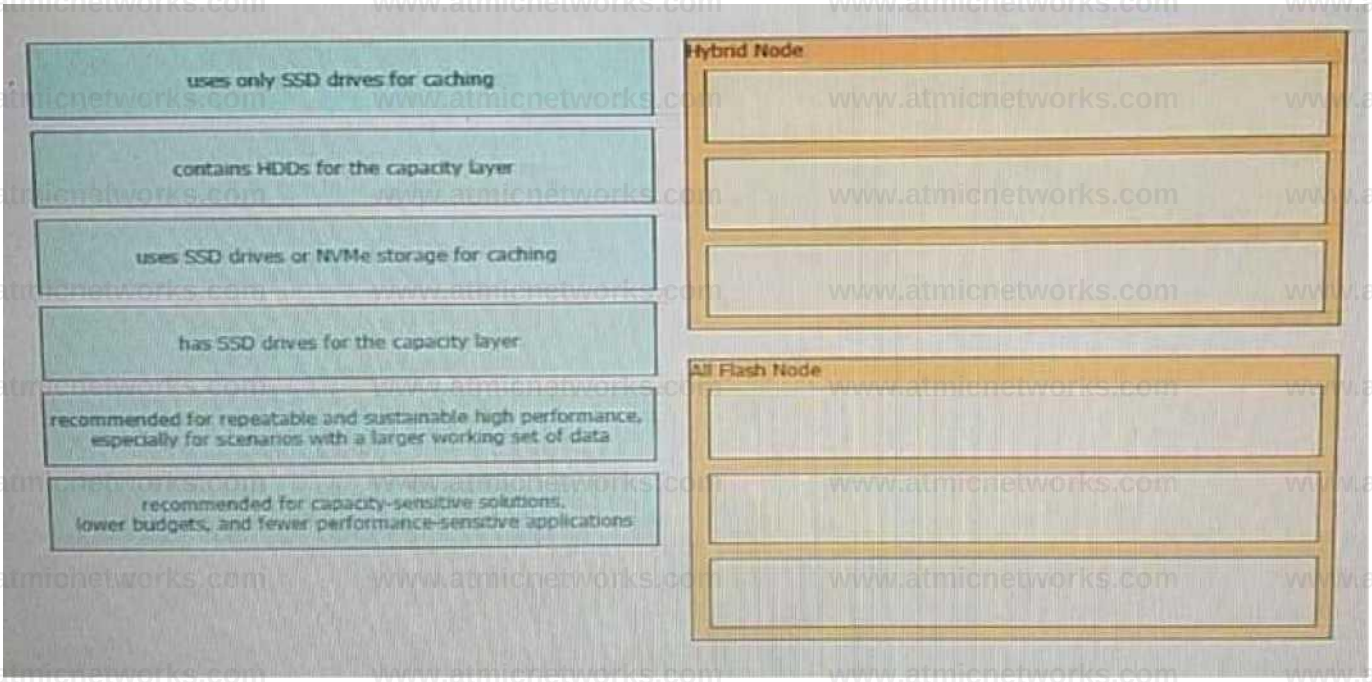
Explanation:

A logical configuration backup in Cisco UCS Manager includes the AAA and RBAC settings and is stored in a human-readable format. This backup type is suitable for backing up configurations that need to be easily reviewed and audited.

Question: 323

DRAG DROP

Drag and drop the hyperflex characteristics from the left onto the appropriate. HyperFlex Node types on the right. Not all options are used.



Answer:

Explanation:

Question: 324

A network engineer must determine the cooling requirements for a Cisco UCS C-Series Rack Server. The server with PCIe cards is configured with a fan configuration policy. Which configuration should be used for the fan policy of the server?

0 server * scope chassis
server /chassis • scope fan-policy

server chassislan-pol cy * set fan-policy high-power server /chassis/fan-poiicy‘ • commit

• server * scope chassis

server /chassis * scope fan-policy
server Ichassis/fan-polcy * set fan-policy balanced
server/chassis/fan-poitcy' * commit

server a scope server*

```
server /server t scope fan-policy
 server /server /fan-policy • set fan-policy acoustic
 server /server /fan-policy* * commit


 server t scope server
 server ^server s scope fan-policy


server server 'fan-poitcy * set fan-po icy low-pov*r server /server 'fan-poucy' • commit
```

A. Option A

B. Option B

C. Option C

D. Option D

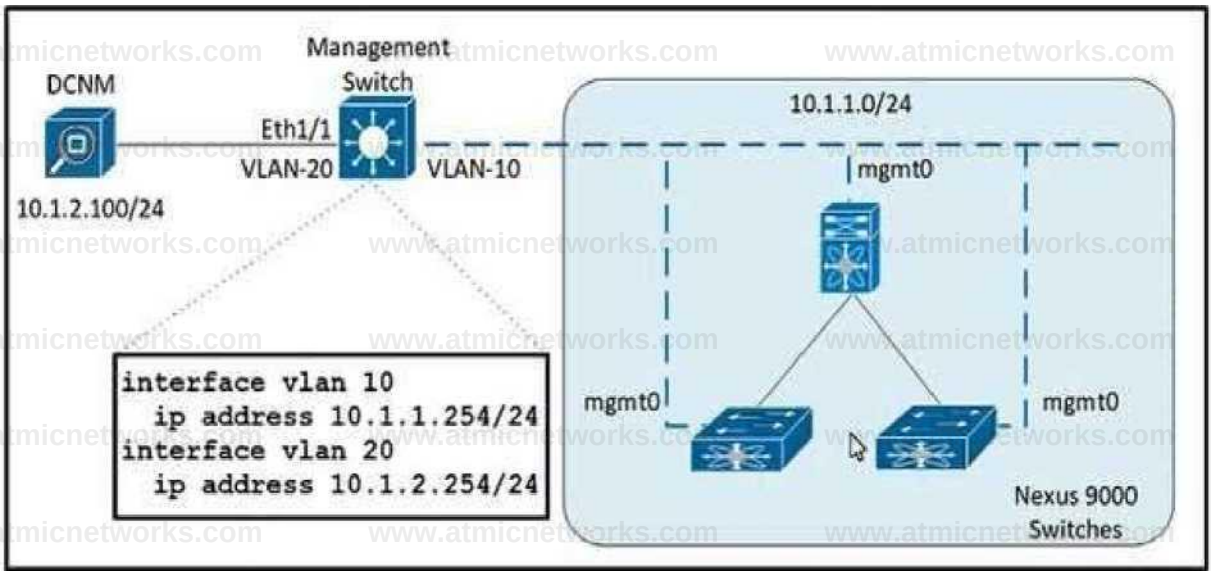
Answer: C

Explanation:

For a Cisco UCS C-Series Rack Server with PCIe cards, the fan configuration policy should be set to accommodate the additional cooling requirements of these cards. Option C, which sets the fan policy to 'balanced', would provide a middle ground between performance and energy efficiency, suitable for a server with additional components such as PCIe cards. This ensures adequate cooling while maintaining energy efficiency.

Question: 325

Refer to the exhibit.



Refer to the exhibit. An engineer must deploy 70 Cisco Nexus 9000 Series Switches in a new environment The requirement is to use Cisco DCNM as a management tool to deploy, manage and monitor the new switches. In addition. DCNM is configured with a zero-touch POAP feature to facilitate fabric creation Which action meets these requirements?

A. Configure SNMP on the new Nexus switches to send SNMP messages to the DCNM server

B. Create a SPAN session on the management switch to send the traffic from VLAN 10 to Ethernet 1/1.

C. Configure an IP helper address on interface VLAN 10 of the management switch

D. Create common credentials on all of the new Nexus switches

Answer: C

Explanation:

Configuring an IP helper address on interface VLAN 10 of the management switch is the correct action to meet the requirements. This configuration allows the management switch to forward DHCP requests from the new switches in different VLANs to the DCNM server, which can then use the zerotouch POAP feature to facilitate fabric creation.

Question: 326

A network engineer must create a script to quickly verify IP reachability for multiple hosts using ping from the Cisco NX-OS switches. The script should use the management VRF and exit the shell after execution Which script should be used to achieve this objective?

```
tclsh
foreach address {
192.168.254.1
192.168.254.2
192.168.254.3
192.168.254.4
} (ping {address source 192.168.254.254
tclquit

tclsh
foreach address {
192.168.254.1
192.168.254.2
192.168.254.3
192.168.254.4
) (ping {address source 192.168.254.254
}

wish
foreach address {
192.168.254,1
192.168.254.2
192.168.254.3
192.168.254.4
| {ping {address vrf management source 192.168 254.254

tclsh
foreach address {
192.168.254.1
192.168.254.2
192.168.254.3
192.168.254.4
} (cli ping {address vrf management source 192.168,254.254
tclquit
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

A script that uses the management VRF to ping multiple hosts and exits after execution would typically involve a loop or iteration over the host IPs, a ping command specifying the management VRF, and an exit command.

Question: 327

A storage administrator notices an increasing number of storage targets that unexpectedly reach capacity, causing periodic service interruptions The administrator must now create and submit a daily report of the environment that shows the status of the storage targets with the highest capacities Which solution provides this information?

A. Nagios Core with OpManager
B. Cisco DCNM with SAN Insight
C. SolarWinds with Slow Drain Analysis
D. Cisco Intersight with Slow Drain Analysis

Answer: B

Explanation:

Cisco DCNM with SAN Insight is the solution that provides detailed information on the status of storage targets, including capacity metrics. SAN Insight is a feature within Cisco DCNM that allows storage administrators to monitor and analyze storage network traffic, helping to identify and resolve issues such as unexpected capacity limits. It would be the appropriate tool for creating and submitting a daily report of the environment showing the status of storage targets with the highest capacities.

Question: 328

An engineer must recover the Cisco UCS system The full backup is available on a backup SCP server Which set of actions recovers the configuration of the Cisco UCS Manager?

Copy ite backup to its a USE dove Copy (he running -nnfig

Create a scheduled restore job
Retool the UCS Manager

Create an impcrvconfig task
Set the action tn Replay

Factory reset Ite fabric rnltfccnned
Setecl Uie Restore feature

A. Option A
B. Option B

C. Option C

D. Option D

Answer: A

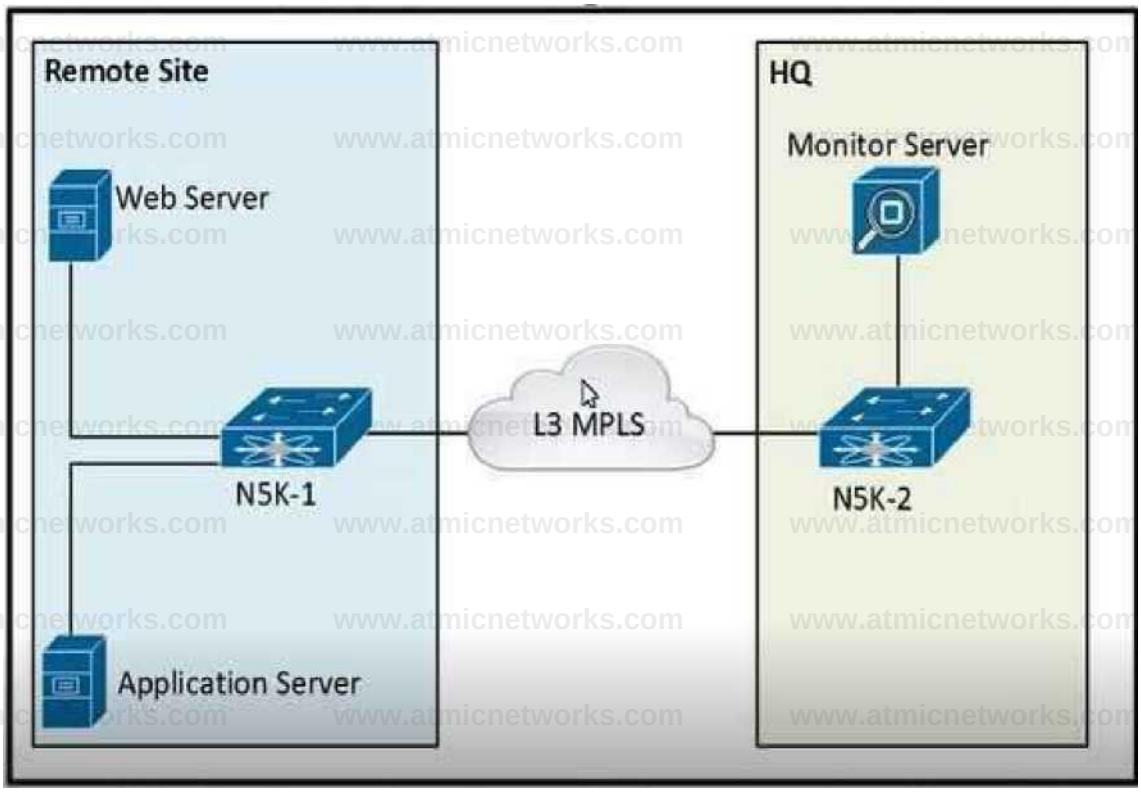
Explanation:

To recover the configuration of the Cisco UCS Manager from a full backup available on a backup SCP server, the actions in Option A should be followed. These actions typically involve accessing the Cisco UCS Manager interface, navigating to the backup and restore settings, and initiating a restore operation using the SCP protocol to retrieve the backup file from the SCP server.

Reference: = For detailed steps and best practices, you can refer to the official Cisco documentation on "Backing Up and Restoring the Configuration" in the Cisco UCS Manager guide1.

Question: 329

Refer to the exhibit.



Refer to the exhibit The communication between the web server and the application server experiences poor performance The network engineer must collect the traffic between the two servers, including the payload for more investigation The collected data must be sent from the remote site to the headquarters. Which action accomplishes this goal?

A. Configure an ERSPAN session between N5K-1 and N5K-2.

B. Configure a SPAN session between N5K-1 and N5K-2

C. Configure SNMP on N5K-1 to send the data to the monitor server

D. Configure NetFlow on N5K-1 to send the data to the monitor server

Answer: A

Explanation:

Configuring an ERSPAN session between N5K-1 and N5K-2 is the appropriate action to accomplish the goal of collecting traffic, including payload, for further investigation. ERSPAN will mirror the traffic from the source to the destination over an IP network, allowing the network engineer to capture and analyze the traffic at the headquarters.

Reference: = For more information on how to configure ERSPAN sessions on Cisco devices, you can refer to the Cisco Nexus 5000 Series NX-OS Software Configuration Guide

Question: 330

Which two actions must be taken to directly connect a Fibre Channel storage array to a Cisco UCS domain? (Choose two.)

A. Configure a new VSAN

B. Create a new vHBA dedicated to the storage array

C. Configure a Fibre Channel port channel

D. Create a Storage Connection Policy

E. Configure the Fibre Channel poet as a Fibre Channel storage port

Answer: A, D

Explanation:

To directly connect a Fibre Channel storage array to a Cisco UCS domain, configuring a new VSAN is essential as it creates a separate fabric to isolate the storage traffic. Additionally, creating a Storage Connection Policy is necessary to define how the UCS domain will communicate with the storage array, including zoning and VSAN membership.

Question: 331

An engineer upgrades the bash on the Cisco Nexus 9000 Series Switch.

```
guestsheik'S sudo [MISSING_COMMAND] /bootflash/bash-4.2_8642092948678a-r8x86_64.rpm.rpm
Preparing...
########################^^                                  [100%]
1:bash #####W##W####^^                                      [100%]
update-alternatives: Linking //bin/sh to /bin/bash
```

Which command must be sed to complete the task?

A. rpm -qa

B. rpm -Uhv

C. upgrade -U

D. update -vh

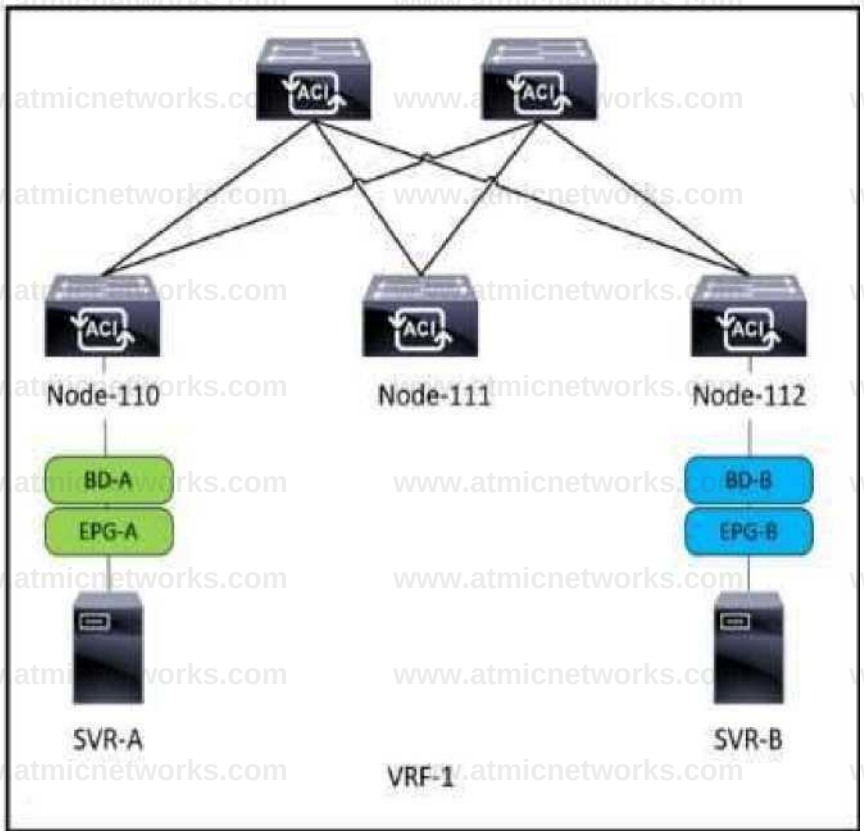
Answer: B

Explanation:

The command rpm -Uhv is used to upgrade or install an RPM package on Linux-based systems. In the context of upgrading bash on a Cisco Nexus 9000 Series Switch, this command would be used to install the new bash package from the provided file path.

Question: 332

Refer to the exhibit.



Refer to the exhibit. SVR-A in EPG-A/BD-A fails to reach SVR-B in EPG-B/BD-B. Which two conditions should be verified to analyze the traffic between the two EPGs? (Choose two.)

A. A contract exists between EPG-A and EPG-B and allows the traffic.

B. Limit Endpoint Learning is disabled on the bridge domain for EPG-B.

C. SVR-B is learned as an endpoint in EPG-B from Node-112.

D. EPG-A and EPG-B are excluded from the preferred group.

E. The bridge domain for EPG-B floods ARP packets.

Answer: A, C

Explanation:

When SVR-A in EPG-A/BD-A cannot reach SVR-B in EPG-B/BD-B, it's crucial to ensure that a contract exists between EPG-A and EPG-B that permits the traffic (Option A). Contracts in Cisco ACI act as a policy framework that dictates the types of traffic allowed between EPGs. Without an appropriate

contract, traffic will not be allowed to pass between these entities.

Additionally, verifying that SVR-B is learned as an endpoint in EPG-B from Node-112 (Option C) is essential. Endpoint learning within ACI is a process where the leaf switch learns about the endpoints connected to it. If Node-112 has not learned SVR-B as an endpoint, it will not be able to forward traffic to it, resulting in connectivity issues.

Reference: = For more information on contracts and endpoint learning, refer to the Cisco ACI documentation on the Cisco official website. Specifically, look into sections detailing ACI contracts and endpoint learning processes.

Question: 333

A bridge domain is being extended out of a Cisco ACI fabric. Between which of these components are policies used to identify the connectivity between Endpoint Groups and the external connection?

A. an external bridge domain and an external routed domain

B. internal contracts and external contracts

C. internal EPGs and external EPGs

D. L2Out and L3Out

Answer: D

Explanation:

Policies that identify the connectivity between Endpoint Groups (EPGs) and the external connection when extending a bridge domain out of a Cisco ACI fabric are associated with L2Out and L3Out components. L2Outs are used to extend Layer 2 connectivity outside the ACI fabric, while L3Outs are used for Layer 3 external connections. These policies define how the ACI fabric will communicate with external networks

Question: 334

An engineer must generate a Cisco UCS Manager backup. The backup should include all logical configuration and contain all system and logical configuration settings. Which backup type should be selected to meet these requirements?

A. system configuration

B. logical configuration

C. all configuration

D. full state

Answer: C

Explanation:

The 'all configuration' backup type in Cisco UCS Manager includes both system and logical configuration settings. This backup type is an XML file that encompasses all system and logical configurations, making it suitable for scenarios where a complete backup of all settings is required

Question: 335

Which two protocols are used by the NFSv4 protocol? (Choose two.)

A. FCP

B. TCP

C. UDP

D. Ethernet

E. IP

Answer: B E

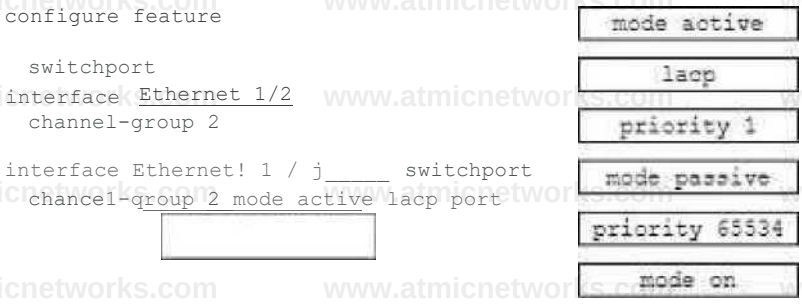
Explanation:

NFSv4 uses TCP for reliable transport and IP for network layer protocol. TCP ensures reliable delivery of packets, which is crucial for file systems, while IP is used for routing the data packets to their destination

Question: 336

DRAG DROP

An engineer must configure an LACP port channel on two Cisco Nexus 7000 Series Switches. The interface e1/2 must be a hot-standby link that initiates negotiation with other ports Drag and drop the commands from the right onto the blanks in the configuration on the left Not all commands are used



Answer:

Explanation:

```
configure terminal ________ feature[ lacy |

interface Ethernet 1/2
  switchport _____________
  channel-group 2| mode active

interface Ethernet 1/3 switchport
  cha nne1-group 2 made aetive
  lacp port| priority 1
```

mode passive

priority 65534

mode on

Question: 337

Refer to the exhibit.

```
• t/h»n/bMh Hi BEGIN HITT INFO ♦  Provides: capture
*  Required-Starti  Pascal_fa  Snetaork  (named  (tire  tayalof
atop<| ( killall -* tepdunp METV*>S?

ease •Si" in
  •tart)
    •tart
    It
  •wp>
    •  tap
    II

start() {
  tcpdump -W 3 -C 100 -i Eth1-42 -w /tmp/capture.pcap &
  RETVAL=$?
}
  •)
    •  sho "Utaqa: 90 latattlalop MTVXL-2
ease

•ait SMSVAL
```

Refer to the exhibit A network engineer must run a continuous capture on a port A script called ''capture'1 is created to start and stop the capture task Which command sequence makes the capture persistent after a reboot?

```
*  Required-Step:  Slocal_fa  {network Snamed  Sure  Sayalag
I  Descriptions  Continuous capture  script
Hi END TWIT TOTO
```

initctl add capture
initctl init capture

chkconfig -add capture
chkconfig -level 3 capture

systemctl enable capture
systemctl start capture

run bash /etc/initd/capture
run bash start-stop-daemon

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To make a capture task persistent after a reboot, the command sequence in Option C should be used. This typically involves enabling the service to start at boot time using systemctl enable and then starting the service with systemctl start. This ensures that the capture task will automatically resume after the system is rebooted4

Question: 338

A company plans to deploy a Cisco HyperFlex solution for data-intensive applications and databases The proposed solution should offer the highest performance with high consistency and low latency Which Cisco HyperFlex storage configuration should be used?

A. All-HDD

B. AII-NVMe

C. All-Flash

D. Hybrid

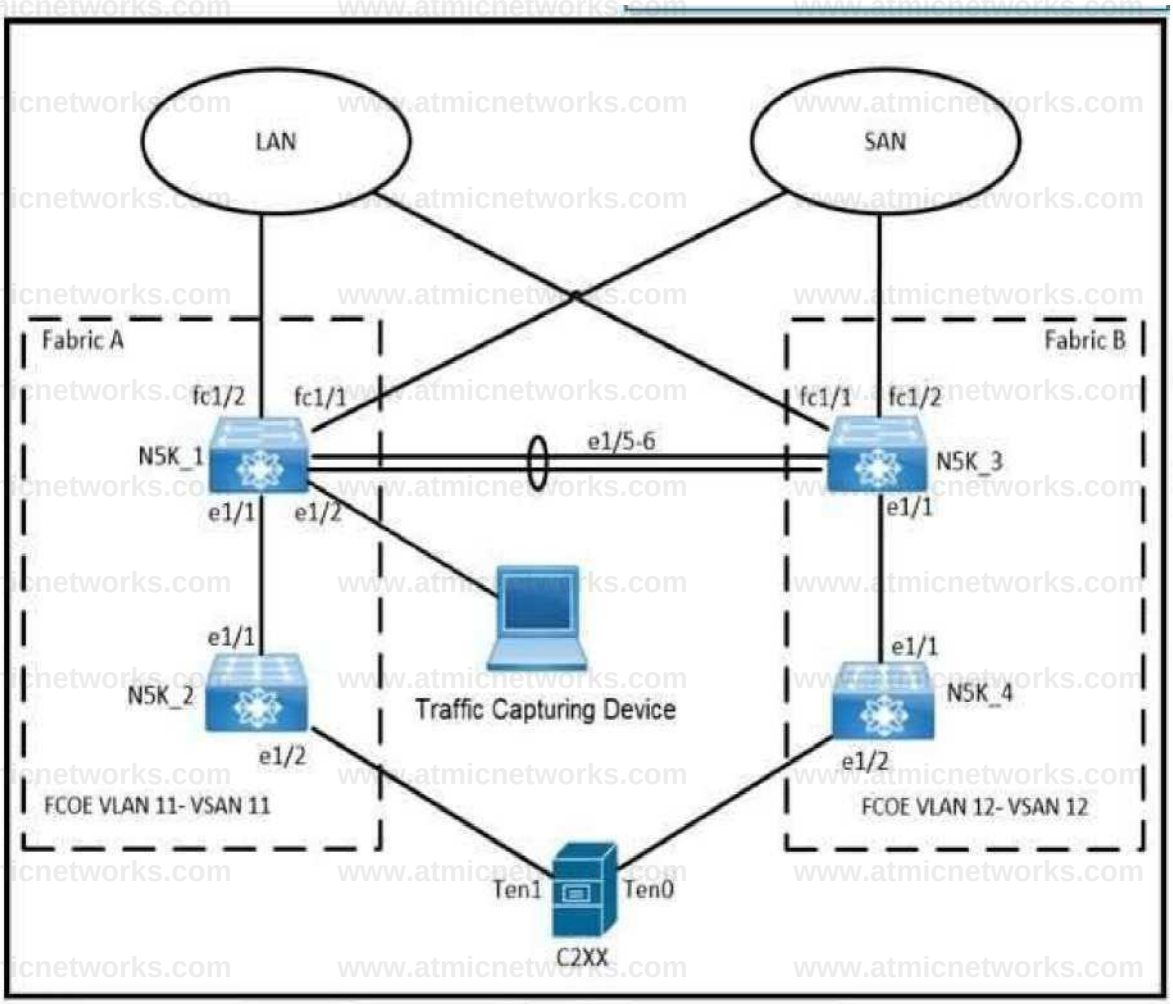
Answer: B

Explanation:

For a deployment that requires high performance with consistency and low latency, an All-NVMe Cisco HyperFlex storage configuration is the optimal choice. NVMe drives offer superior speed and efficiency compared to other storage mediums, making them ideal for data-intensive applications and databases.

Question: 339

Refer to the exhibit.



Refer to the exhibits An engineer must implement a SPAN session that sends a copy of all VLAN 11 traffic on N5K_1 to the Traffic Capturing Device The configuration that is presented is already applied

to the Cisco UCS Manager. Which additional action meets the objective'

A. Assign the VLAN to the monitored port.

B. Choose VLAN 11 under the VSANs section.

C. Select the Clear Destination feature.

D. Create a LAN traffic monitoring session.

Answer: D

Explanation:

To meet the objective of sending a copy of all VLAN 11 traffic on N5K_1 to the Traffic Capturing Device, creating a LAN traffic monitoring session is the necessary action. This session will capture the specified VLAN traffic and forward it to the designated capturing device for analysis or monitoring purposes. The existing configuration in Cisco UCS Manager needs to be complemented with this session to achieve the desired traffic capture.

Question: 340

An engineer must migrate a Cisco UCS C-Series server from Cisco SingleConnect to direct integration mode. The Cisco UCS Manager Rack Server Discovery Policy and Rack Management Connection Policy are set to immediate and Auto-Acknowledge. Which set of steps accomplishes this task?

Otooorrwc! me utwi fan me FIX
Comtn th# caiM to ipphru ports OR the tabor aOoruwvwt
Revet th# C4QD taC cl m# □«•*»'

□oconHtci ma L<MS4 man ma H *
Connect mo catM to terver pmti on mo tat* < rterxonnect
<no< me QKD IMC ct me serve*

[Wmwt ma ran a* tow mt ff X
Corned me LOUM ID apptanct ports on the lab'< tea* connect

Docomocl me iitwi tai* mo FEX
Connect mo nOMei to server perm on ma tatirr ntorronrwt 3wo.tow»tr>3f tw se**w

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To migrate a Cisco UCS C-Series server from Cisco SingleConnect to direct integration mode with immediate discovery and auto-acknowledge policies, the steps in Option C are appropriate. These steps typically involve disconnecting the cables from the FEX, connecting them to the appliance ports on the fabric interconnect, and reacknowledging the server

Question: 341

An engineer is configuring HTTPS access to Cisco UCS Manager The engineer created a keyring and created the certificate request for the keyring Cisco UCS Manager continues to receive untrusted messages from a Firefox browser and a Chrome browser Which action must be taken as the next step in the HTTPS access configuration?

A. Create a trusted point

B. Sign the certificate using the Cisco UCS Manager.

C. Obtain a validated certificate from Cisco

D. Install a trusted certificate in the browser store

Answer: A

Explanation:

After creating a keyring and generating a certificate request, the next step is to create a trusted point. This involves downloading the certificate chain from the CA authority, converting it to the required format, and creating a Trust-Point on UCS Manager where the certificate details are pasted

Question: 342

DRAG DROP

Drag and drop the technologies from the left onto the description on the right.

Answer:

Explanation:

NFSv2

NFSv4

Kerberos

RADIUS

Question: 343

A SAN administrator must Implement Infrastructure monitoring for the Fibre Channel storage environment. The storage environment consists of a standalone Cisco Nexus 9000 Series Switch and Cisco MDS 9000 Series Switches. The goal is to be able to visualize the SAN support VXLAN overlays and identify storage slow drain issues. Which monitoring solution accomplishes this task?

A. Cisco Prime Infrastructure

B. Cisco DCNM

C. Cisco APIC

D. Cisco Intersight

Answer: B

Explanation:

Cisco Data Center Network Manager (DCNM) is the monitoring solution that can fulfill the requirements of visualizing the SAN, supporting VXLAN overlays, and identifying storage slow drain issues for a Fibre Channel storage environment consisting of Cisco Nexus 9000 and MDS 9000 Series Switches3.

Question: 344

An engineer must implement private VLANs for a group of Cisco UCS 8-Series servers. The primary VLAN is present, But the secondary VLAN must Be added to Both fabrics. Which configuration set accomplishes this task?

```
UCS-A* scope eth-uplmk
UCS*A4»tn-up*nk »true* vlan vlan198t 1981
UCS-A <KtMiphnWVUn*a set sharing none

UCS-A* scope eth-upimS
UCS-A e:M>;>i™ * creel* vlan vlanIMt 1981
UCS-A '«rn»tJ nk.MAn' a set sharing isolated

UCS-A* scope eth-uplInk
UCS-A /etfwpiaik * scop* fabric a
```

```
UCS-A -elh-upbnl^atvK ■ create vlan vl*n1981 1981
UCS-A 'eth-uplaik.labri&Vtan' * set sharing private

UCS-A* scope eth-upunk
UCS-A wFMiptnk a scop* fabric a
UCS-A/*m-upfcnMabnc » create vlan vlantSBI 1981
UCS-A eth^pi.nK.'fabncvtwT * set sharing secondary
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To implement private VLANs for Cisco UCS 8-Series servers, the primary VLAN is already present, and the secondary VLAN needs to be added to both fabrics. The correct configuration set that accomplishes this task is Option C. This option includes the necessary commands to create the VLAN and set its sharing to secondary, which is required for the configuration of private VLANs in a Cisco UCS environment12.

Reference: = For detailed steps and configurations, refer to the Cisco documentation on private VLANs and UCS configuration12. It provides comprehensive guidance on setting up private VLANs in the Cisco UCS environment.

Question: 345

An engineer configures port security on a Cisco MDS 9000 Series Switch. The MDS switch configuration must meet these requirements

The switch must inmate the VSAN 4 port security database despite any conflicts.

New devices must be statically added to the switch.

Configuration changes for VSAN 4 must be applied throughout the fabric with any lodes on the fabric released

Which configuration set meets these requirements?

port-security activate vsan 4 no port-security auto-learn vsan 4 port-security allocate port-security commit vsan 4

port-security activate vsan 4
port-security manual-team vsan 4 port-security allocate
port-security commit

port-security activate vsan 4 force port-security auto-learn vsan 4 port-security distribute port-security commit

port-security activate vsan 4 force no port-security auto-learn vsan 4 port-security distribute port-secunty commit vsan 4

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The configuration set that meets the requirements for configuring port security on a Cisco MDS 9000 Series Switch is Option C. This option includes the command port-security activate vsan 4 force, which initiates the VSAN 4 port security database despite any conflicts. It omits the autolearn command, indicating that new devices must be added manually. Additionally, the port-security distribute command ensures that configuration changes are applied throughout the fabric and any locks on the fabric are released, as required1.

Reference: = For more detailed information on port security configuration for Cisco MDS 9000 Series Switches, you can refer to the Cisco MDS 9000 Series Security Configuration Guide

Question: 346

A network engineer must restore the running configuration on a Cisco Nexus 5000 Series Switch to an existing snapshot called “stable1”. The restore procedure should proceed only if no errors occur. Which configuration

should be used to accomplish this goal?

rollbeck rurwinj-config checkpost »!ib*1 bMl4itort

ronbocx checkpoint liable 1 Beu effort running-corhg Monk

rollback checkpoint»tee* 1 BeM effect njcni^eorho txitefTort

rtxibeck rurawn^onffg check po«il tiebei etomic

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The correct command to restore the running configuration on a Cisco Nexus 5000 Series Switch to an existing snapshot called “stable1” is found in Option C. The command rollback checkpoint stable1 best-effort running-config best-effort ensures that the restore procedure will proceed only if no errors occur, which aligns with the requirement stated in the question. The “best-effort” parameter is crucial as it indicates that the rollback should only proceed if it can be completed without any errors.

Question: 347

An engineer must configure a VDS port group using APIC policy. The requirements are for the frames to be mapped to a particular Layer 2 network and for the virtual machine assigned to the port group to receive all

frames passed on the virtual switch. Which two settings must be used to meet these requirements? (Choose two.)

A. forged transmits

B. VMDirectPath

C. port binding

D. promiscuous mode

E. VLAN

Answer: D, E

Explanation:

Promiscuous mode (D) allows a virtual machine to observe all traffic on the virtual switch, which is necessary for the virtual machine to receive all frames. VLAN (E) is used to map the frames to a specific Layer 2 network. These settings ensure that the virtual machine receives all traffic for the specified VLAN, fulfilling the requirements stated in the question1.

Reference: The configuration details and the role of these settings can be found in the Cisco documentation related to VDS port group parameters managed by APIC

Question: 348

An engineer is deploying a VXLAN EVPN environment for a customer. The customers environment suffers from a large amount of flooding related to hosts attempting to resolve the MAC to IP mapping on the network segment. Which feature prevents this issue from happening in the future?

A. anycast rendezvous point

B. anycast gateway

C. IP ARP SYNC

D. IP ARP suppression

Answer: D

Explanation:

IP ARP suppression (D) is used in VXLAN EVPN environments to minimize flooding. When enabled, it allows the local switch to respond to ARP requests for known hosts, thus preventing the need to flood these requests across the entire network segment1. This feature is particularly useful in scenarios where there is a large amount of ARP traffic that could potentially lead to flooding, as it reduces unnecessary broadcast traffic by handling ARP resolution within the control plane2.

Reference: The role and configuration of IP ARP suppression in VXLAN EVPN environments are detailed in Cisco's documentation and best practice guides for VXLAN BGP EVPN

Question: 349

A network administrator must create a Linux container on a Cisco Nexus Series Switch. The container requires 10 percent of the CPU of the switch and 1024 MB of RAM to run successfully. Which task provides the necessary resources?

A. Edit the container properties with the guestshell run command.

B. Increase the compute resources with the guestshell resize command.

C. Enable the Bash shell of the switch with the feature bash command

D. Modify resource allocation with the virtual-service resize command.

Answer: D

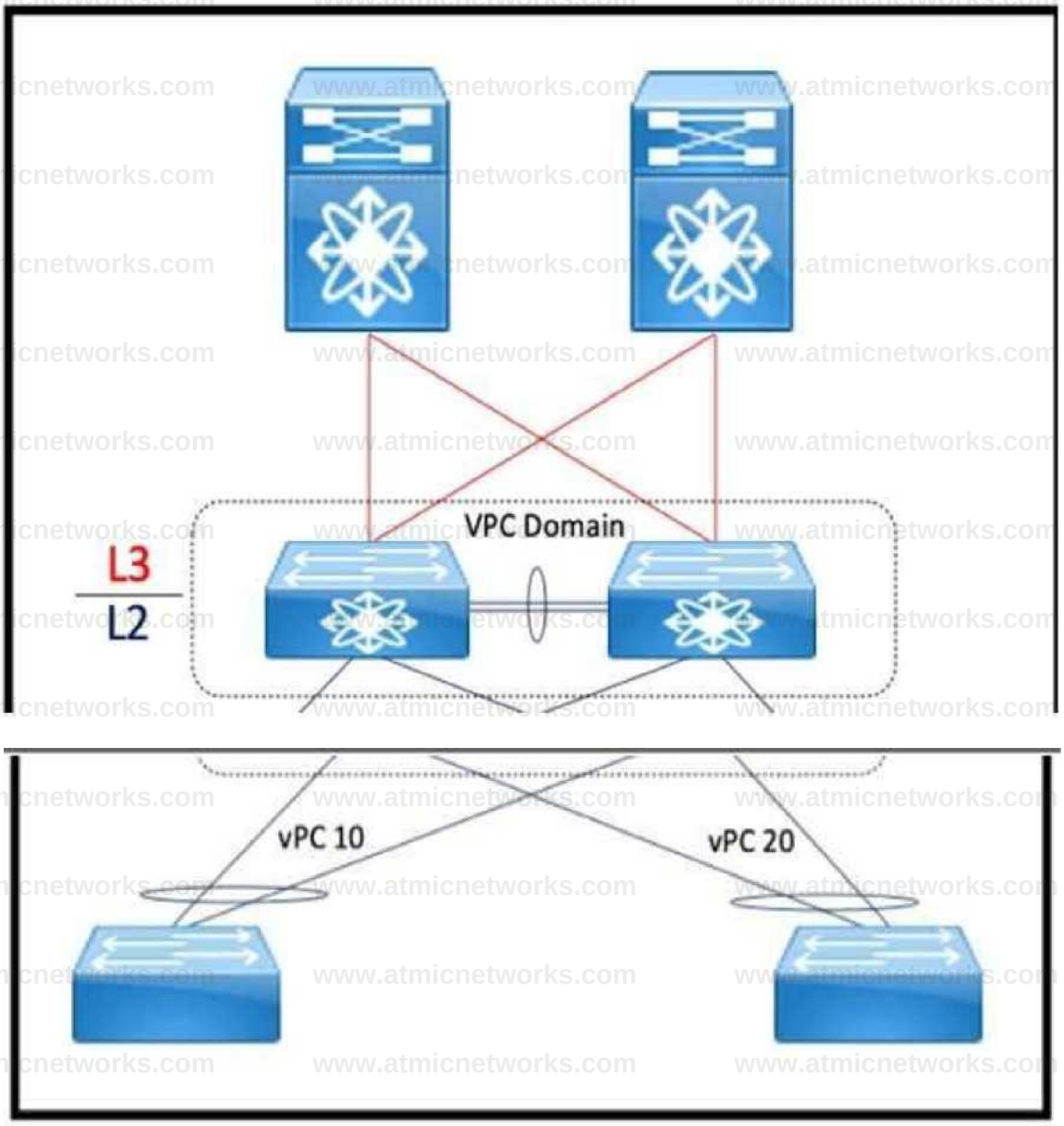
Explanation:

The virtual-service resize command (D) is used to modify the resource allocation for a Linux container on a Cisco Nexus Series Switch1. This command allows the administrator to specify the amount of CPU and memory allocated to the container, ensuring it has the necessary resources to run successfully. In this case, the command would be used to allocate 10 percent of the CPU and 1024 MB of RAM to the container1.

Reference: The usage of the virtual-service resize command for managing resources in a Linux container can be found in the Cisco Nexus 9000 Series NX-OS Programmability Guide1.

Question: 350

Refer to the exhibit.



Refer to the exhibit. A network engineer must Improve the convergence time during vPC primary peer device failure and recovery. Which set of actions is required on both vPC switches to accomplish this task?

Configure the same system priority.
Enable LACP toward the access switches.

Configure the same STP priority.
Enable the peer-swltch feature

Configure port channels with BPDU guard
Globally enable the loop guard feature.

Configure vPC role priority.
Enable the peer-gateway feature.

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

Option D is the correct choice. Configuring the vPC role priority and enabling the peer-gateway feature are recommended practices for enhancing vPC convergence times. The peer-gateway feature allows for local forwarding of packets without the need to cross the vPC peer link, which can significantly reduce convergence times during primary peer device failures and recoveries. This approach ensures that the vPC system can quickly adapt to changes and maintain traffic flow even in the event of a device failure123.

Reference: For more detailed information and best practices, you can refer to Cisco's official documentation and community discussions on vPC convergence and failure scenarios

Question: 351

A network administrator attempts to automate the provisioning of several new Cisco Nexus switches. The administrator prepares a bootstrap configuration script for the task Due to the number of switches a zero-touch provisioning solution is preferred Additionally, some switches arrive with outdated software and should be automatically upgraded as part of the provisioning workflow Which solution meets the requirements'

A. DHCP

B. Ansible

C. NX-API

D. POAP

Answer: D

Explanation:

PowerOn Auto Provisioning (POAP) is a feature that automates the process of upgrading software images and installing configuration files on Cisco devices that are deployed in a network for the first time. It is particularly useful for scenarios where multiple switches need to be provisioned without manual intervention. When a switch with POAP boots up and does not find a startup configuration, it enters the POAP mode, locates a DHCP server, and bootstraps itself with its interface IP address, gateway, and DNS server IP address. It then obtains the IP address or URL of a TFTP server and downloads the necessary scripts and software images to configure the device12.

Reference: More information about POAP and its configuration can be found in Cisco's official documentation

Question: 352

An engineer performs a Cisco UCS C480 ML M5 installation from a Cisco UCS Manager As a part of the design the server must perform an iSCSI bool from the storage array Which configuration must be performed in the SAN settings in the root organization to satisfy that condition?

A. Implement a WWPN pool

B. Create a virtual iSCSI vNIC

C. Enable a host SAN pool

D. Create an IQN suffix pool

Answer: B

Explanation:

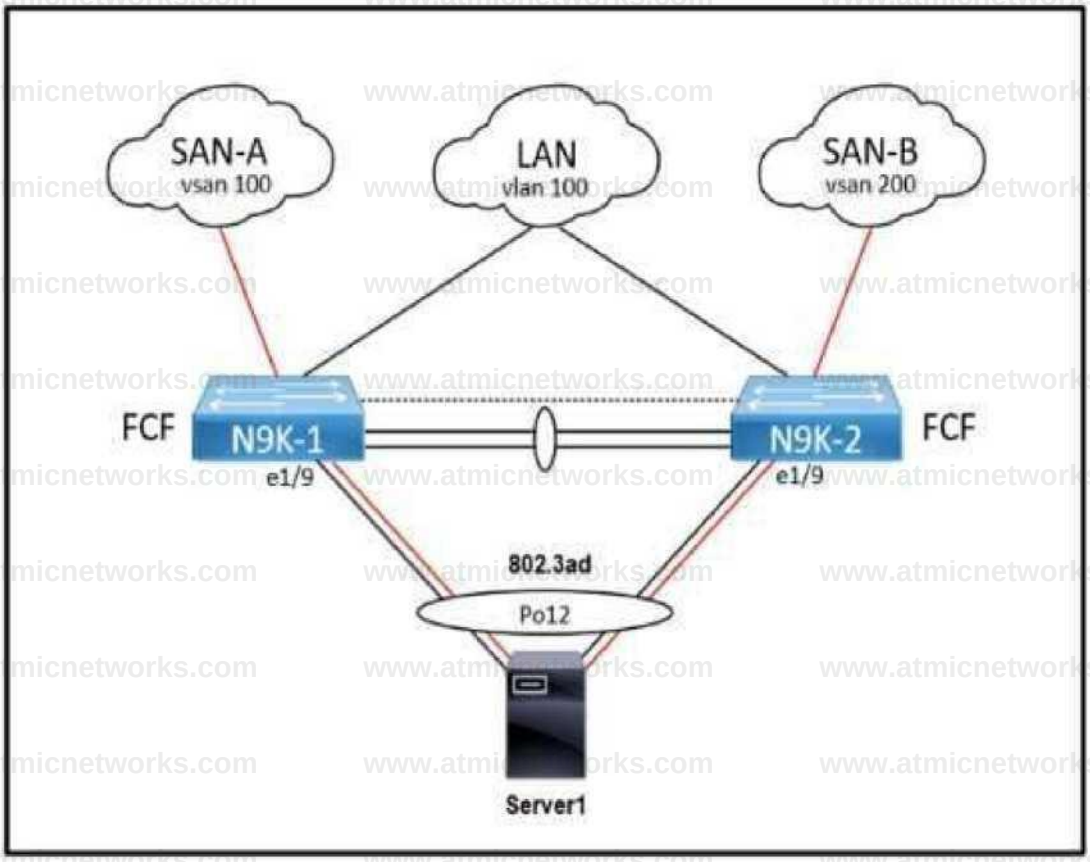
Creating a virtual iSCSI vNIC (B) is necessary for the server to perform an iSCSI boot from the storage array. This virtual iSCSI vNIC serves as an iSCSI boot firmware table (iBFT) configuration placeholder for iSCSI boot configuration. It is not an actual vNIC but is essential for the iSCSI boot process as it holds the configuration details required for the server to communicate with the storage array during the boot process1.

Reference: The process of configuring iSCSI boot in Cisco UCS Manager, including the creation of a virtual iSCSI vNIC, is detailed in Cisco's documentation

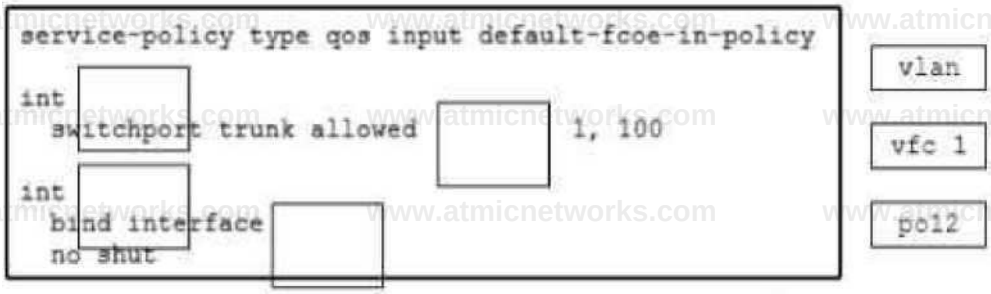
Question: 353

DRAG DROP

Refer to the exhibit.



Refer to the exhibit. An administrator must complete the unified fabric configuration between Server1 and a pair of Cisco Nexus 9000 Series Switches Drag and drop the code snippets from the right onto the blanks in the code on the left to complete the N9K-1 configuration Snippets are used more than once.



Answer:

Explanation:

Po12

Vlan

Vfc1

Po12

Question: 354

Which protocol does Cisco Hyperflex use to share data among nodes in a VMware vSphere environment?

A. CIFS

B. FCoE

C. SMB

D. NFS

Answer: D

Explanation:

Cisco HyperFlex uses the Network File System (NFS) protocol for sharing data among nodes in a VMware vSphere environment. NFS is a distributed file system protocol that allows a user on a client computer to access files over a network in a manner similar to how local storage is accessed. This protocol is commonly used in virtualized environments for ease of data sharing and management12.

Reference: The use of NFS in Cisco HyperFlex environments is documented in Cisco's official installation guides and design documents

Question: 355

An engineer must remove the running configuration of a Cisco Nexus 9000 Series Switch and replace it with a backup file without restarting the switch. The backup file is stored on an SFTP server that is reachable via the An engineer must remove the running configuration mgmt0 interface Which set of commands accomplishes this task'

```
copy sftp://admin@192.168.10.100/backup.cfg startup-config vrf mgmtO
copy startup-config running-config

configure replace $ftpJ/admin@192.168.10.100/backup.cfg vrf mgmtO
copy running-config bootflash.'.''startup-config

copy sftp /i'admin@192.168.10.100/backup cfg bootflash:///backup.cfg vrf management
configure replace bootflash7,/backup cfg

copy sftp://admin@192.168.10.100/backup.cfg startup-config vrf management
reload in 10
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

Option C is the correct choice. The commands copy sftp://admin@192.168.10.100/backup.cfg bootflash:///backup.cfg vrf management followed by configure replace bootflash:///backup.cfg will copy the backup configuration file from the SFTP server to the switch's bootflash and then replace the running configuration with the backup file without requiring a restart of the switch. This process is known as configuration replace and is a feature that allows for the replacement of the entire running configuration with a new one provided by the user1.

Reference: The procedure for performing a configuration replace on Cisco Nexus 9000 Series Switches can be found in the Cisco documentation1. It is important to ensure that the backup configuration file is a valid running configuration file and that the switch has connectivity to the SFTP server through the mgmt0 interface. The

configure replace command intelligently calculates the difference between the current running configuration and the user-provided configuration, applying only the necessary changes

Question: 356

An engineer must configure a Cisco UCS blade system that is managed by Cisco UCS Manager. All four connected interfaces between the blade system and the fabric interconnects must be used. Additionally, the connectivity must tolerate any link failure between the I/O module and the fabric interconnects. Which action accomplishes these requirements?

A. Configure port aggregation with LACP policy set to default

B. Configure Firmware Auto Sync Server policy to Auto Acknowledge

C. Configure Link Group Preference to Port Channel.

D. Configure chassis/FEX discovery pokey action to four links

Answer: C

Explanation:

Configuring Link Group Preference to Port Channel © allows the use of all four interfaces and provides link failure tolerance. This is because port channels can combine multiple physical links into a single logical link that provides high availability through redundancy. If one link in the port channel fails, traffic is automatically redistributed to the remaining links without any disruption to the network12.

Reference: The configuration of port channels and link group preferences in a Cisco UCS environment is detailed in Cisco's official documentation and community discussions related to fabric failover and high availability

Question: 357

A network administrator is creating a custom Django self-service portal that runs on a Linux server to automate the

creation of new VLANs on Cisco UCS Manager Which feature must De installed and configured on the server?

A. Cisco ucs Powertool Suite

B. Cisco DNA Center API

C. Cisco AppDynamics

D. Cisco UCS Python SDK

Answer: D

Explanation:

The Cisco UCS Python SDK (D) is a set of Python libraries that provide a method for automating the configuration and management of Cisco Unified Computing System (UCS) hardware. It allows network administrators to write custom scripts or develop applications to manage UCS environments programmatically. In the context of creating a Django self-service portal for VLAN automation, the UCS Python SDK would be used to interact with the UCS Manager's API, enabling the automation of VLAN creation and other tasks1.

Reference: The use of the Cisco UCS Python SDK for automating tasks in UCS Manager is discussed in Cisco's official blogs and community forums, where examples and best practices can be found12. The SDK provides a more direct and tailored approach for UCS automation compared to other tools, making it suitable for integration with custom Django applications.

Question: 358

An engineer implements a Python script inside a Cisco Bash shell The script contains this dictionary object

```
swltch_id_llst[1] {
   "N9K-Spine-1": "842534699747", "N9K-LeaM" "126784690".
   'N9K-Leaf-2": "56556473"
```

Which command must be used to add the 'NSK-Spine-2': '1498323434' element to the switch_id list dictionary?

```
switchJd.llst = ["N9K-Splne-2" "1498323434"]
switch Jd_l|st.update({"N9K-Splne-2": "1498323434"})
switchJdJlstappcnd«"N9K-Splnc-2": "1498323434"}) switchJd^llst *= ("N9K-Splne-2": "1498323434"}
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

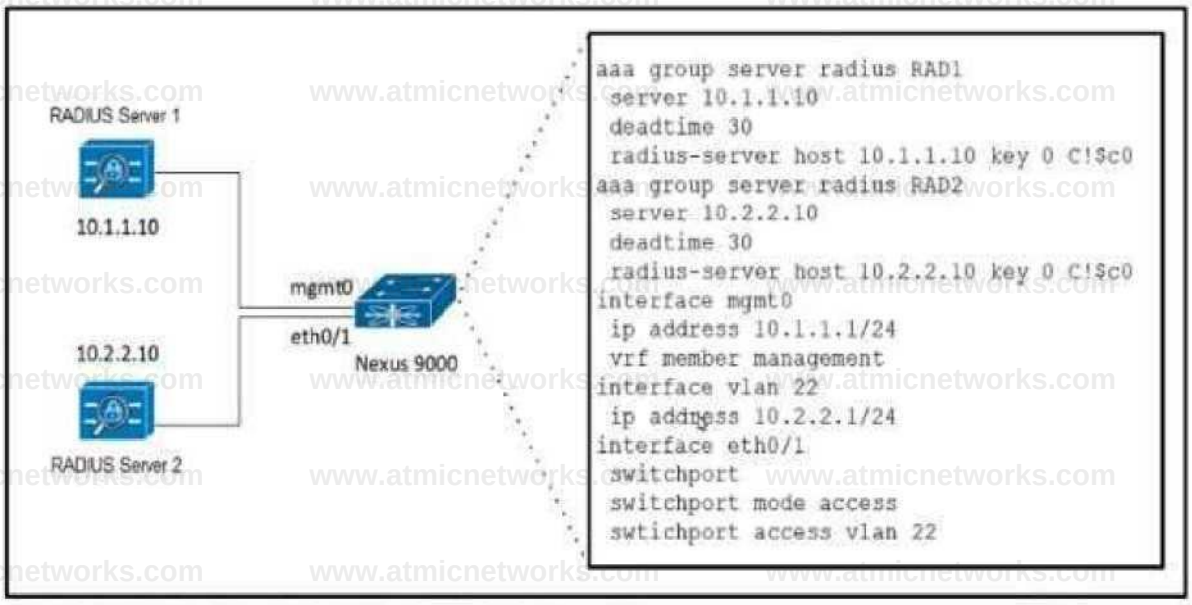
Explanation:

The update() method in Python is used to add an element to a dictionary. It takes either another dictionary object or an iterable of key-value pairs and adds them to the dictionary. If the key is already present in the dictionary, update() will update the key with the new value. Option B correctly
uses the update() method to add the new 'N9K-Spine-2': '1498323434' key-value pair to the switch_id_list dictionary.

Reference: For more information on modifying dictionaries in Python, the official Python documentation provides comprehensive guidelines and examples. It's a valuable resource for understanding the behavior of dictionary methods like update().

Question: 359

Refer to the exhibit.



Refer to the exhibit. A user must be granted management access to the Cisco Nexus 9000 Series Switch using AAA servers The RADIUS servers are configured to accept login requests from the same Layer 2 subnet of the switch The user must be permitted to log in with these requirements:

RADIUS server 1 must be used to log in via a console.

RADIUS server 2 must be used to log in via SSH.

W0hich two actions meet these requirements?

A. Enable command authorization to RAD1 and RAD2 for all successful logins.

B. Change the dead timer for RAD1 and RAD2 to 1 minute.

C. Set the RADIUS source interface to be mgmt0 for group RAD1 and VLAN 22 for group RAD2

D. Configure the authentication login to use group RAD1 for console and group RAD2 for remote access.

Answer: C, D

Explanation:

Setting the RADIUS source interface to be mgmt0 for group RAD1 and VLAN 22 for group RAD2 © ensures that login requests from the console and SSH are sourced from the correct interfaces and reach the appropriate RADIUS server.

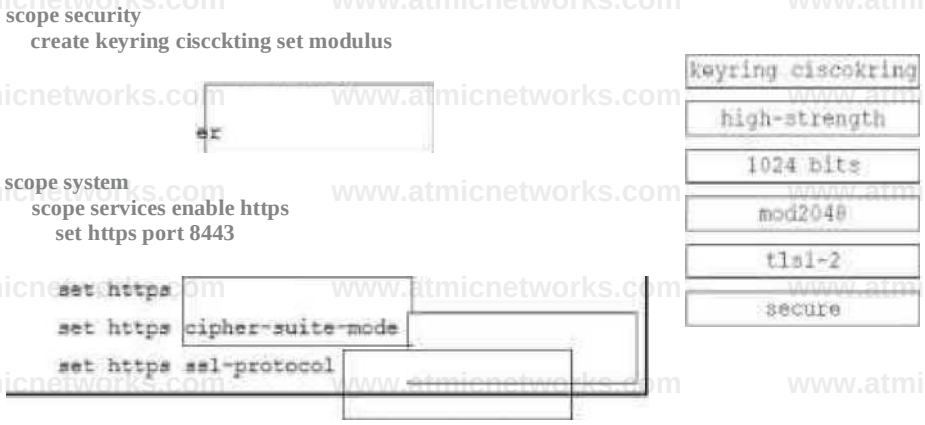
Configuring the authentication login to use group RAD1 for console and group RAD2 for remote access (D) directs the switch to use the specified RADIUS server groups for the respective login methods, aligning with the user's requirements.

These configurations ensure that management access via console and SSH is authenticated through the designated RADIUS servers as intended. It's important to apply these settings correctly in the switch's configuration to achieve the desired access control.

Question: 360

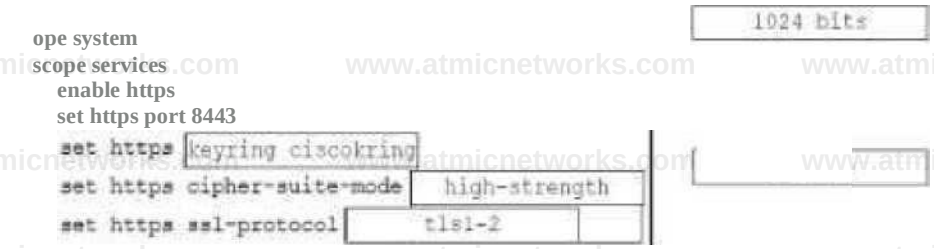
DRAG DROP

An engineer must configure Cisco UCS Manager to accept only HTTPS connections that use TLS 1 2 The cipher security level must be high and the length of the keyring key value must be 2048 bits Drag and drop the code snippets from the right onto the blanks in the code on the left to accomplish these goals Not all commands are used



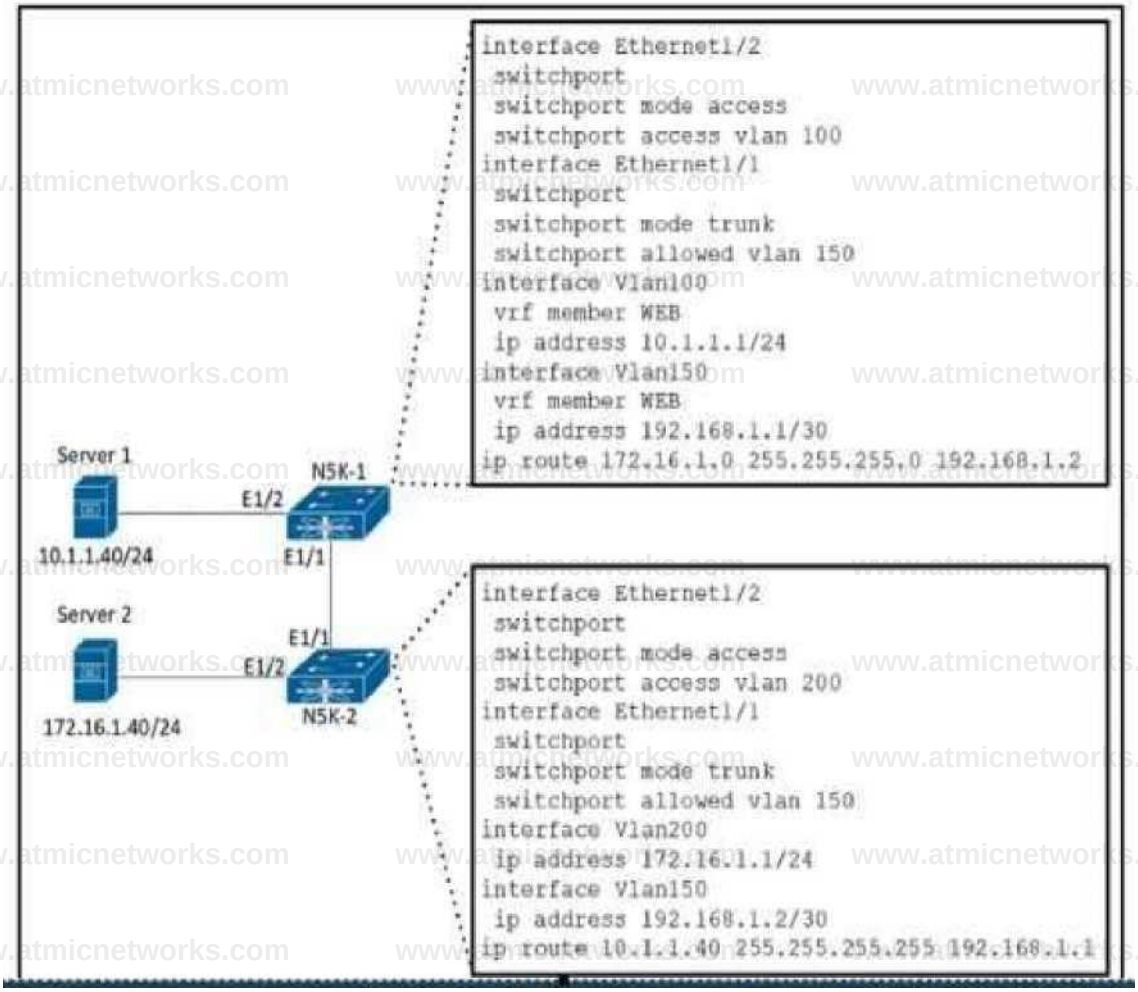
Answer:

Explanation:



Question: 361

Refer to the exhibit.



Refer to the exhibit. The gateway of Server 1 is in the VLAN 100 SVI on N5K-1 and the gateway of Server 2 is in the VLAN 200 SVI on N5K-2 Server 1 must connect to Server 2 using unidirectional traffic. Which action accomplishes this requirement?

A. Add VLAN 100 and 200 to the allowed VLANs list on the Ethernet 1/1 interface on NK5-1.

B. Assign VRF WEB membership to interfaces VLAN 150 and 200 on N5K-2.

C. Configure access VLAN 100 on interface Ethernet 1/2 on N5K-2.

D. Create a static route in VRF WEB for the subnet of Server 2 on N5K-1

Answer: D

Explanation:

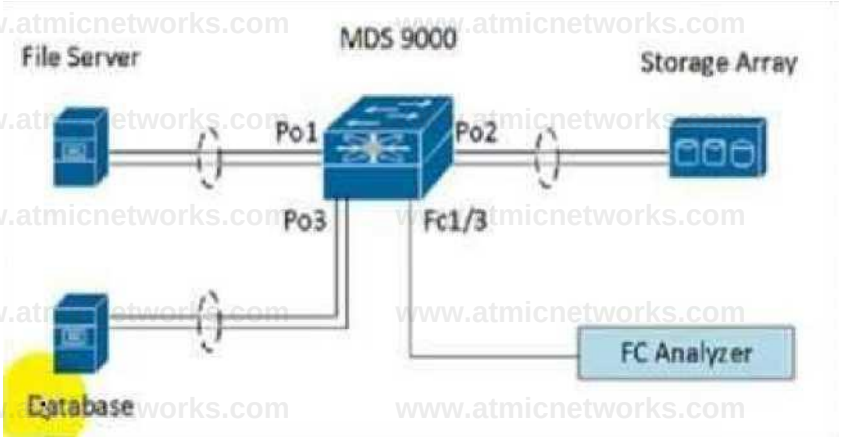
: Creating a static route in VRF WEB for the subnet of Server 2 on N5K-1 (D) will direct traffic from

Server 1 to the specific subnet where Server 2 resides. This ensures that traffic can flow from Server 1 to Server 2, even if it is unidirectional. The static route provides a specified path for the traffic to follow, which is necessary when the traffic must be unidirectional and the gateways are on different VLANs.

Reference: For further details on configuring static routes in a VRF on Cisco Nexus switches, please refer to the Cisco Data Center Core Technologies documentation, which provides guidelines on implementing routing protocols and static routes within VRF instances.\

Question: 362

Refer to the exhibit.




```
interface port-channel 1
  channel mode active
interface port-channel 2
  channel mode active
interface fc1/1-2
  channel-group 1
  no shutdown
interface fc1/4-5
  channel-group 2
  no shutdown
interface fc1/7-8
  channel-group 3
  no shutdown
vsan database
  vsan 100 name fabric1
  vsan 100 interface port-channel 1
  vsan 100 interface port-channel 2
  vsan 100 interface port-channel 3
```

Refer to the exhibit. A storage engineer must monitor the traffic from the file server to the FC analyzer. The file server and the database use the same storage array. Which configuration must be applied to the Cisco MDS 9000 Series Switch to accomplish this goal?

```
MDS-9000(contigp span session 1
MDS-9000(config.span * destination interface fclO
MDS-9000(ainflfl-span)# source interface port-channel 1
```

A. Option A
H

```
MDS-9000(configP span session 1
M0S-9000(con1ig-5panm destination interface port-channel 2
MDS-9000<t»ntlg-span|# source interface vsan 100
```

B. Option B

```
MDS-yOOOtconiigP span session 1
MDS-90Q0(config-spani# destination interface port-channel 2
MDS-9000(contig-span^ source interface fc V1
```

```
MDS-9000(configP span session 1
MDS-0000(config-spanp> destination interface vsan 100
MDS-9000fcon1ig-span)# source interface port-channel 1
```

.

C. Option C

D. Option D

Answer: C

Explanation:

The configuration must ensure that the SPAN session captures traffic from the file server's VSAN to the destination interface connected to the FC analyzer. The commands provided in the exhibit show the setup of a SPAN session with the destination interface as port-channel 2 and the source interface as VSAN 100, which is likely the VSAN associated with the file server.

Reference := For more detailed information and step-by-step guidance on configuring SPAN sessions on Cisco MDS 9000 Series Switches, you can refer to the official Cisco documentation on Implementing and Operating Cisco Data Center Core Technologies (DCCOR) available at Cisco's training and certifications page and the Cisco Community knowledge base. These resources provide comprehensive insights into deploying, securing, operating, and maintaining Cisco data center infrastructure, including the Cisco MDS Switches.

Question: 363

Where does the witness VM reside in a Cisco Hyperflex Edge deployment?

A. Windows application

B. Hyper Rex Data Platform

C. Cisco Intersight

D. local HyperFlex datastore

Answer: C

Explanation:

In a Cisco HyperFlex Edge deployment, the witness VM, known as the “Invisible Cloud Witness,” resides within Cisco Intersight. This cloud-based platform eliminates the need for a dedicated witness VM by providing a virtual witness as a service, which simplifies the deployment and ongoing operations of HyperFlex Edge clusters1234.

Reference:

Cisco HyperFlex Edge Deployment Guide, Release 5.0(x)1.

Cisco HyperFlex Systems Installation Guide for VMware ESXi, Release 5.02.

Cisco Blogs on HyperFlex and Intersight3.

Cisco’s official page on HyperFlex for Edge Environments

Question: 364

Refer to the exhibit.

```
event manager applet local-backup
    event cli ratch "copy tunning-config startup-conf15"
    "Ji-on 1 tli copy                    Motflash:
    tut rent_cor.fi 7. txt
    action * syslog msg Configuration saved and copied to iscotMa.cn action 3 event-default
```

Refer to the exhibit. A network engineer must create an EEM script that saves a copy of the running configuration to bootftash and writes a message to syslog when a user saves the configuration to a Cisco Nexus 9000 Series Switch. Which command completes the configuration set?

A. running-config

B. policy-default

c. syslog-config

D. event-default

Answer: A

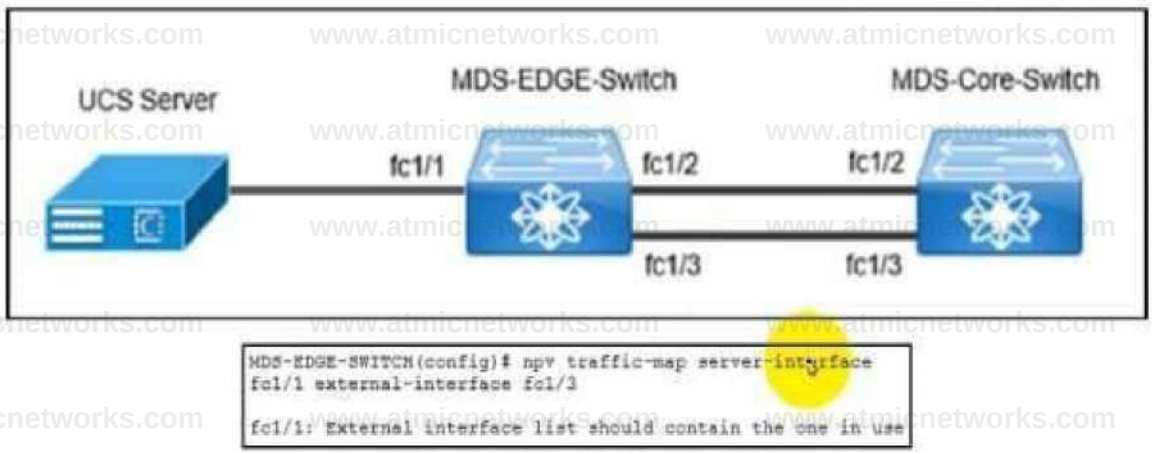
Explanation:

The command that completes the EEM script configuration for saving a copy of the running configuration to bootflash on a Cisco Nexus 9000 Series Switch is running-config. This command is used in the EEM applet to specify the source of the configuration file that needs to be copied. The complete command in the EEM applet would be action 1.0 cli command "copy running-config bootflash:/current-config.txt". This command will save the running configuration to a file named current-config.txt in the bootflash when the specified event occurs, which is when a user saves the configuration.

Reference: For more information on EEM scripts and the copy command on Cisco Nexus 9000 Series Switches, you can refer to the Cisco Data Center Core Technologies documentation and the Cisco NX- OS System Management Configuration Guide

Question: 365

Refer to the exhibit.



Refer to the exhibit. The MDS-EDGE-Switch and MDS-Core-Switch are configured with NPV and NPIV features The FLOGI from Cisco UCS is received by the MDS-Core-Switch on interface fc1/2. An engineer tried to move all traffic between the MDS-EDGE-Switch and MOS-Core-Switch from interface fc 1/2 to fc1/3, but the attempt failed. Which set of actions completes the configuration?

Disable the NPV feature in the MDSEDGE-Switch Re-enawe the NPV feature
Disable interface fcin

Disable cne NPIV feature in the MDS-EDGE-Switch.
Re-enabie the NPIV featuie.
I Disable Interface fcl/1

Shut dawn fcV1 In the MDSEDGE-Switch
Re-apply the command
Enable interface fell!

Shutdown fc1G in the I.IDS-EDGE-Swrtch
Re-apply the command
Enable interface fd/1

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

When moving traffic between switches configured with NPV and NPIV features, it's crucial to ensure that the NPV traffic management settings are correctly configured to handle the new interface allocation. This typically involves updating the NPV traffic-map and ensuring that the upstream NPIV core switch recognizes the new paths for the traffic. Additionally, the engineer may need to verify the zoning and VSAN configurations to ensure that the new interface is part of the correct VSAN and that the zoning allows for the FLOGI to be processed correctly on the new interface123.

Reference:

Cisco MDS 9000 Series Interfaces Configuration Guide, Release 8.x1.
Cisco documentation on Configuring N Port Virtualization2.

Cisco guide on N-Port Identifier Virtualization (NPIV) and N-Port Virtualization (NPV)

Question: 366

Refer to the exhibit.

```
. -ect-'ir.lt. d.fur.ctccr.s
exe:=*/us: tin/thef-client"
prog»"chef-client"
i -e •ecc'sysconfig/Sprcg 1 it . etc/ syscor.fig/Sprog config^ (CONFIG-. etc. chef/client.rb) pidfiie-ilPI'F'IE
vat.run/chef/client.pis reload!) I
sch: -r. 3"Reloading aprcg: *
      XSTVil-?7
ecf>c
re rum Jretval

            rh status g |t exi
exit 2
ease
exit 57
```

Refer to the exhibit. A developer must create a Bash script that performs a Chef Client reload in the event of a system reset. Which command completes the script?

```
killproc -n Spidfile $exec -SIGHU

          i Spidfile fexec -HUE

killpxoc -a Spidfile Jexe

killprcc -j Spilfiit lexec -HUE
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

In the context of Bash scripting for system automation, the killproc command is often used to stop a process. The correct option to complete the script for a Chef Client reload would involve sending a HUP (hang-up) signal to the Chef Client process, which is typically done to cause the process to reload its configuration without stopping the service. The command killproc -p $pidfile $exec -HUP would send the HUP signal to the process identified by the pidfile, which is the expected behavior for a Chef Client reload on a system reset.

Reference := For a detailed explanation and official documentation, the Cisco Data Center Core Technologies source book or study guide should be consulted, as well as the official Chef documentation which provides information on system and service management commands.

Question: 367

An engineer must configure Cisco Nexus 9000 Series Switches for Cisco UCS Director integration. The configuration must enable automated onboarding of the switches as they come online. For security purposes, the switches must have the bare minimum of connection methods enabled. The connection protocol must allow authentication through credentials. Which protocol must be configured on the switches to allow automated onboarding?

A. SNMP

B. Telnet

C. SSH

D. HTTPS

Answer: C

Explanation:

SSH (Secure Shell) is the protocol that allows secure remote login from one computer to another. It provides strong authentication and secure communications over unsecured channels. This protocol is preferred for automated onboarding of devices like Cisco Nexus 9000 Series Switches because it supports strong encryption and credential-based authentication, which aligns with the requirement for minimal connection methods and security. SSH is commonly used in network automation for secure command execution and file transfers.

Reference := For more information on configuring Cisco Nexus 9000 Series Switches for automation and integration with systems like Cisco UCS Director, you can refer to the Cisco Nexus 9000 Series NX-OS Programmability Guide, which details the supported manageability features and advanced automation capabilities, including Power On Auto Provisioning (POAP) and integration with automation frameworks

Question: 368

An engineer must configure a Cisco UCS domain for monitoring and management by the Cisco Intersight SaaS platform. After the setup is complete, administrators must have full control to

configure the device through Cisco UCS Manager and Intersight. Which set of actions accomplishes this task?

A. Configure Devce Connector Access Mode as Allow Control in Device Console Claim the device on Intersight as UCSM Managed Mode.

B. Configure Device Connector Access Mode as Allow Control in Cisco UCS Manager Claim the device on intersightc as Intersight Managed Mode

C. Configure Device Connector Access Moao as Allow Control in Device Console. Claim the device on intersight as Intersight Managed Mode

D. Configure Device Connector Access Mode as Allow Control in Cisco UCS Manager Claim the device on intersight as UCSM Managed Mode

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The Device Connector Access Mode should be configured as 'Allow Control' within the Cisco UCS Manager to enable full configuration capabilities. Claiming the device on Intersight as 'UCSM Managed Mode' ensures that the device can be managed through both the Cisco UCS Manager and the Intersight platform. This configuration aligns with the best practices for setting up Cisco UCS domains for integration with Intersight, allowing for seamless monitoring and management while maintaining security and control12.

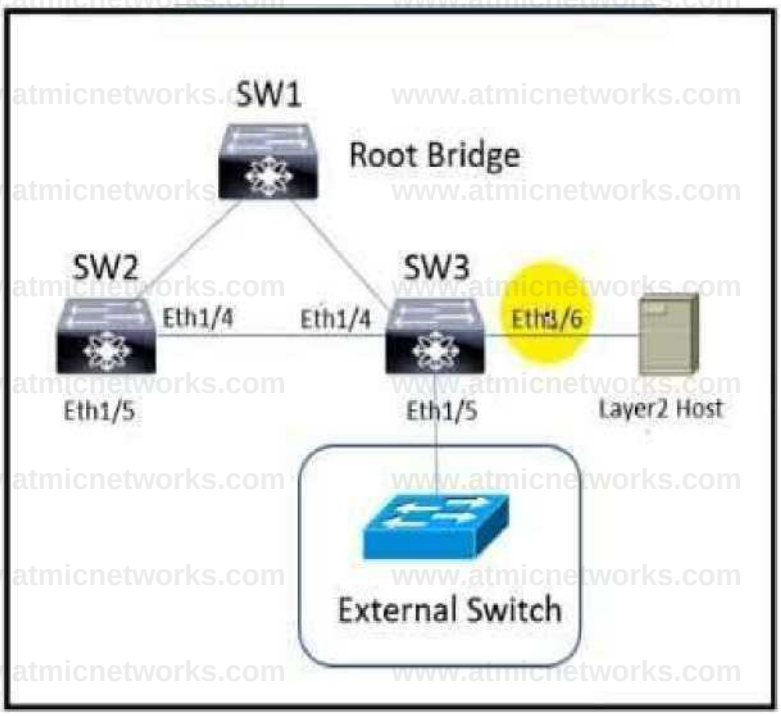
Reference := For further details on the configuration process and best practices, you can refer to the Cisco Intersight

Managed Mode Configuration Guide and other official Cisco documentation related to UCS domain profiles and Intersight integration

Question: 369

DRAG DROP

Refer to the exhibit.



Refer to the exhibit. The Cisco Nexus Series Switches SW1, SW2, and SW3 are connected via Layer 2 copper interfaces. An engineer implements loop prevention standard IEEE 802.1w on each VLAN lo provide lasier recovery from network changes or failures. The Implementation has these requirements

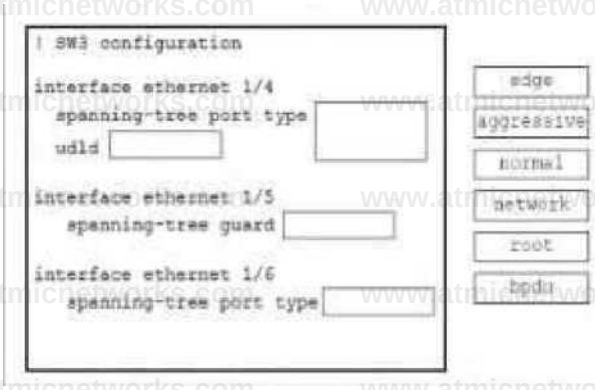
Interfaces that are connected to Layer 2 hosts must not receive STP BPDUs.

The implementation must detect unidirectional links due to one-way traffic twisted-pair links

Bridge assurance must be enabled between SW2 and SW3

The Layer 2 domain must be protected from superior BPDUs that arrive from external switches.

Drag and drop the code snippets from the right onto the blanks in the code on the left to complete the configuration for SW3. Not all code snippets are used.



Answer:

Explanation:

Network

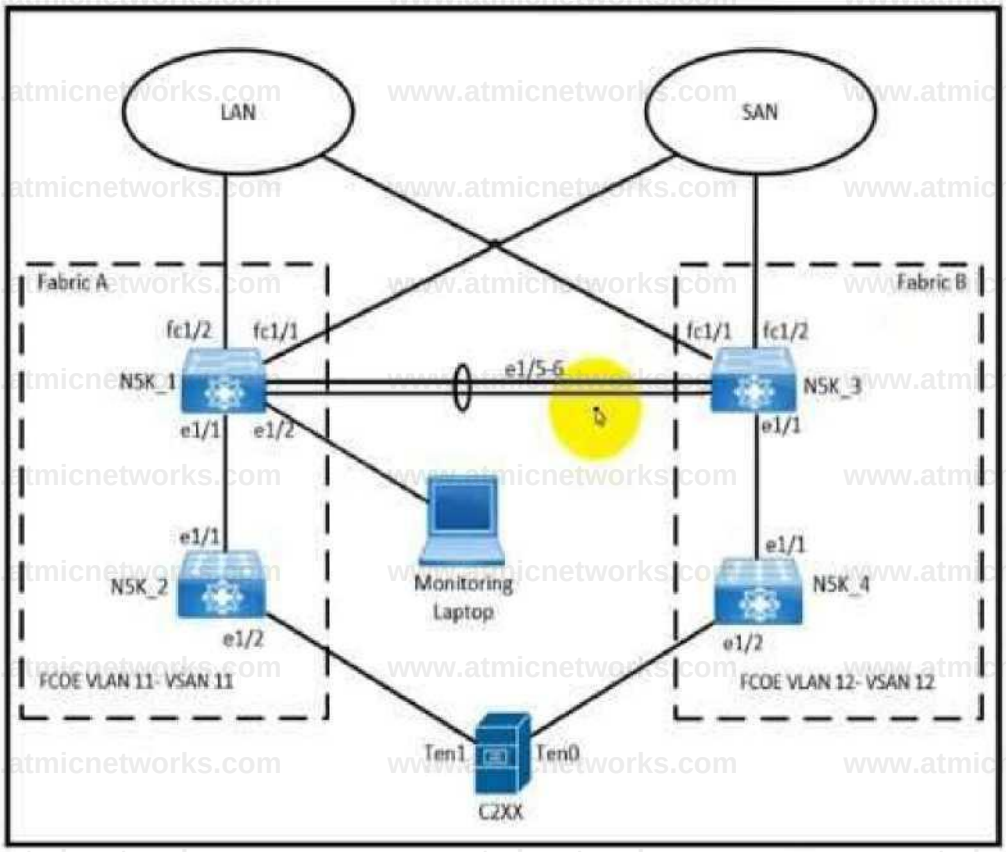
Aggressive

Bpdu

edge

Question: 370

Refer to the exhibit.



Refer to the exhibit. An engineer is creating a SPAN session to send a copy of all the Fabric-A VSAN 11 traffic on NSK_1 to the monitoring laptop. The configurator that is presented has already been applied to Cisco UCS Manager. Which action complétés the configuration?

A. Activate a NetFlow monitoring session

B. Create a SAN traffic rnonitoring session

C. Set VLAN 11 as the traffic destination

D. Select VSAN 11 as the source of traffic.

Answer: D

Explanation:

The configuration in Cisco UCS Manager needs to specify the source of the traffic for the SPAN session. Since the requirement is to monitor the traffic from VSAN 11, selecting VSAN 11 as the source will direct the traffic to the monitoring session. This is consistent with the SPAN session's purpose, which is to create a copy of the traffic for analysis or monitoring.

Reference := For more information on configuring SPAN sessions in Cisco UCS Manager, you can refer to the Cisco Data Center Core Technologies study materials and official documentation, which provide guidelines on setting up traffic monitoring solutions within a Cisco data center environment. These resources will offer detailed instructions and best practices for implementing SPAN sessions to monitor VSAN traffic.

Question: 371

An engineer must implement protection against ICMP DoS attacks on a Cisco Nexus 9000 Series Switch. The requirement is to rate-limit ICMP without denying all other ICMP traffic. The ICMP trafic currently passing through the Cisco Nexus 9000 device must not be affected. Which configuration accomplishes these goals?

A. Configure SNMP traps to send the ICMP notification if the CPU utilization is more than 90%.

B. Reconfigure the Layer 3 interfaces to be in the non-default VRF and ICMP broadcast storm control

C. Create an access list to deny ICMP traffic and apply it to all interlaces in the inside direction.

D. Apply a control plane service policy that matches all ICMP traffic to drop the traffic fiat exceeds the threshold.

Answer: D

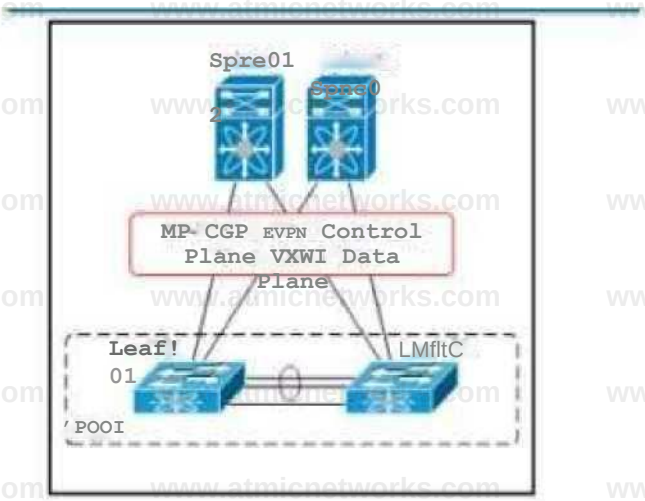
Explanation:

Applying a control plane service policy with a rate-limiting feature allows the engineer to match all ICMP traffic and set a threshold for it. Traffic that exceeds this threshold can be dropped, thus mitigating the risk of ICMP-based DoS attacks while allowing legitimate ICMP traffic to pass through. This method ensures that the current ICMP traffic is not affected as long as it does not exceed the configured rate limit12.

Reference := For detailed steps on configuring rate limits and control plane policing on Cisco Nexus 9000 Series Switches, you can refer to the Cisco Nexus 9000 Series NX-OS Security Configuration Guide12. This guide provides comprehensive information on securing your network infrastructure and protecting against various types of attacks, including DoS attacks. It also covers the configuration of security features like rate limits and control plane policies to ensure network stability and security

Question: 372

Refer to the exhibit.




```
5?ntE-01tshc* ms put
ip pin sp-eidreas 10.255.0.100 ^roup-list 225.0.0.0/9
ip pls bar rp-candidate loopbackl jrcup-lut 225.0.0.0/8
ip pis aSB sanae 232.0.0.0/8
xp pis anycast-rp 10.255.0.100 10.10.0.1
ip pis anycaat-rp 10.255.0.100 10.10.0.2

!
5?! HE*-(lit a how ran interlace JocpcacH
interface loopbackl
  ip router csrf 1 area 0.0.0.0
  ip pis aparse-scde
```

Refer to the exhibit. An engineer must implement VXIAN with anycast gateway. To accomplish this, an engineer must set up PIM Source-Specific Multicast for host reachability. Which IP address must be applied to interface loopback1 to accomplish this goal?

A. 255.0.0.1/8

B. 255.0.100

C. 10.10.0.1/32

D. 10.10.0.2/32

Answer: C

Explanation:

In a VXLAN implementation with anycast gateway, PIM Source-Specific Multicast (SSM) is used for efficient host reachability. The IP address 10.10.0.1/32 should be applied to interface loopback1 to

facilitate this setup. This address is used in conjunction with the ip pim anycast-rp command to configure the rendezvous

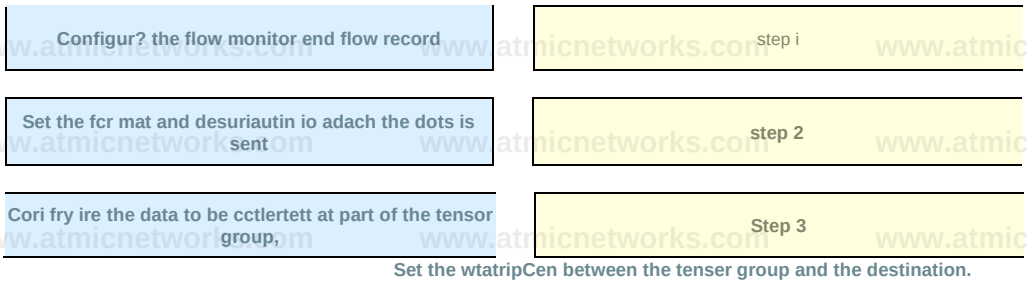
point (RP) for multicast traffic in a PIM SSM environment. The loopback interface is typically used for this purpose because it is always up and reachable as long as the device is operational.

Reference := For more detailed guidance on configuring VXLAN with anycast gateway and PIM SSM, the Cisco Data Center Core Technologies (DCCOR) study materials and official Cisco documentation should be consulted. These resources provide in-depth explanations of the technologies and step-by- step configuration instructions.

Question: 373

DRAG DROP

A network engineer must implement a telemetry solution to collect real-time structured data in a large-scale network. Drag and drop the actions from the left into the order on the right to implement the solution. Not all actions are used.



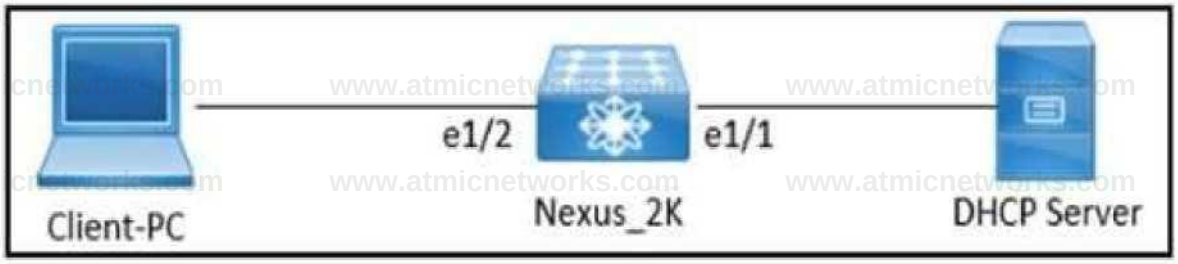
Answer:

Explanation:

1. set the format and destination to which the data is sent.
2. configure the data to be collected as part of the sensor group.
3. set the subscription between the sensor-group and the destination.

Question: 374

Refer to the exhibit.



	tart*		
27 91.566 244	».».».»	255.255.255.255	DHCP
9 61.567141	»».u	255.255.255.255	DHC
H 61.M72U	9.9.9.9	255.255.255.255	Mr
$5 61.96)116	9.9.9.9	255.755.255.255	DHCP
M«>.BM4I7	192.1M.2.1	m.iM.j.u	MP
M 6kM)B7	».«.«.•	255.255.255.255	MP
61 61.96)151	tie.a	255.255.255.255	DHC
MM 94 099 5 5 9	192.IM.2.41	172.IM.2.1	DHC

Frar MM M2 byte* an wire (2 7 36 bits). M2 bytes captured (2 7M bits) on interface \DrviceVB*.(1751F996-B4MM2WM6 5f44K2 7f6AA3)# id 1 Ethernet H, fee! Tnte)(or>7;42 9c (cO M 8) 67 42 9c). Ost Mge^oa jc J4 M (99:<b 51 ft MM)
.net Protocol Version 4, fegt 192 168.2 48. Ost: M2.IM 2 1
User tat agree Protocol, 5rc Port M, Ost Port 67 * Dynamic Host Configuration Protocol (trirase)
Renege typo Boot Request (1) Hardware type: Ethernet (fall) Hardware address length: 6 Mops: 8 Transaction ID. 9«14ge5a2c Seconds elapsed: 9 loot* flags. 9x9909 (Unicast) Client IP address: 192 161 2.49 Your (client) IP address 0.9 99 Hext server IP address: 0.0.0.0 Relay agent IP address: 9 9.9.9 Client RM address IntelCor.67:42 9c (<9 b« 83:67:42:«c) Client hardware address padding. OOOOOOQOOOOOOQOMMM Server host naae not given loot file naae net given Ragle cookie: DHCP Option- (5J) DHCP Hostage Type (Release) Option: (54) DHCP Server Identifier (192.IM.2.1) Option (91) Client identifier Option: (255) (nd padding
owwoodoooeowMooQooMowwoiKwoooMowwMMOBooooodwx^^

Refer to the exhibit. An engineer is troubleshooting intermittent connectivity issues between the client PC and the DHCP server. What does the last package captured from the Cisco Nexus 2000 Series Switch indicate?

A. The DCHP server releases the IP address from the client.

B. The client receives an IP address from the DHCP server.

C. The DHCP server sends an IP address via a broadcast message.

D. The client sends a unicast message to receive an IP address from the DCHP server.

Answer: A

Explanation:

The last packet indicates a DHCP Release message, which is sent by the client to the DHCP server to release the assigned IP address. This is typically done when the client no longer requires the IP address, or before the client shuts down to ensure the IP address can be reassigned. The packet capture showing a DHCP Release message confirms that the client is informing the DHCP server that it is releasing its current IP address.

Reference := For further understanding of DHCP operations and troubleshooting connectivity issues, the Cisco Data Center

Core Technologies source book provides detailed explanations. Additionally, Cisco's official documentation and resources on their website offer extensive guidance on managing and troubleshooting DHCP in Cisco environments. These materials are essential for network engineers working with Cisco Nexus series switches and dealing with DHCP-related issues.

Question: 375

Due to a newly announced security advisory, a company has been Informed that they must update the configuration of 500 network devices that ate deployed n their network. The engineering team must assist the operations team to prepare for this update. The operations team does not have direct access to the network devices and must log in via a Linux server. This Is the first time that the team is making a network-wide configuration and must change all devices without first installing additional software on the network devices. The operations team is unfamiliar with automation and scripting technologies. Which automation tool must be used to accomplish this goal?

A. Chef

B. Ansible

C. Puppet

D. Saltstack

Answer: B

Explanation:

Ansible is known for its agentless architecture, which means it does not require any software to be installed on the target devices. It can manage the devices using SSH, which is typically available on most Linux servers. This makes it suitable for scenarios where the operations team needs to update configurations across a large number of devices without direct access1.

Reference := For more information on how Ansible works and its capabilities for network automation, you can refer to the official Ansible documentation and resources available on the Ansible website1. These resources provide detailed guidance on using Ansible for network automation tasks, including configuration updates and management.

Question: 376

An engineer must configuration a backup and restore of Cisco UCS Manager during the weekend maintenance windows. The configuration must be restored to its original state on Monday morning. The end users can make changes only to the Service Profile configuration. Which set of actions meets these requirements?

A. Schedule a system backup to run at the start of every weekend and manually import the backup on Monday morning.

B. Schedule a system backup to run at the start of every weekend and schedule the import of the backup to run on Monday morning

C. Schedule a logical backup to run at the start of every weekend and manually import the backup on Monday morning.

D. Schedule a logical backup to run at the start of every weekend and schedule the import of the backup to run on Monday morning.

Answer: D

Explanation:

A logical backup includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies1. Since the end users are only allowed to make changes to the Service Profile configuration, a logical backup is appropriate as it will capture the state of these configurations without including system settings. Scheduling the logical backup at the start of the weekend ensures that the latest configurations are saved before any changes occur. Scheduling the import of this backup on Monday morning will restore the configurations to their state at the time of the backup, thus reverting any changes made by the end users during the weekend1.

Reference := The Cisco UCS Manager documentation provides detailed instructions on how to schedule backups and imports, which can be found in the official Cisco resources1. These documents outline the steps for setting up scheduled backups and imports, ensuring that the UCS Manager configuration can be restored to a specific state as required.

Question: 377

An engineer must implement a new VRF that permits communication between all endpoint groups (EPGs) by default. The new EPGs and bridge domains (BDs) that are created in the new VRF must not require additional configuration to permit traffic between the newly created EPGs or BDs. Which action accomplishes this goal'

A. Provide and consume a permit any contract on the VRF level

B. Create a VRF in the common tenant.

C. Place all EPGs in the preferred group.

D. Implement a global contract.

Answer: C

Explanation:

Placing all EPGs in the preferred group within a VRF allows for communication between them without the need for additional contracts. This is because the preferred group feature in Cisco ACI allows EPGs within the same VRF to communicate with each other by default, bypassing the need to provide and consume contracts1. This simplifies the configuration process when new EPGs and bridge domains are added, as they inherit this communication capability by being part of the preferred group1.

Reference := For more information on the implementation of VRFs and the use of the preferred group feature in Cisco ACI, you can refer to the Cisco documentation on "Use vzAny to Automatically Apply Communication Rules to all EPGs in a VRF".

and other related resources1. These documents provide detailed guidance on how to configure VRFs and EPGs to achieve seamless communication within the network infrastructure.

Question: 378

DRAG DROP

An engineer must configure a control plane policy on a Cisco Nexus 9000 Series Switch that is located at IP 192.168 20.1 that moots those requirements

Only HTTP. RDP. and ICMP traffic is permitted from subnet 192.168.10.0/24.

The committed information rate must be 54000 pps.

The burst size must be 128 packets.

Any other traffic must be dropped.

Drag and drop the code snippets from the bottom onto the blanks in the code on the top to complete the configuration.

Not all code snippets are used

ip icaicliit pennithoat*
pannit top U2.1M.W.0/M |
pennit top 193.166.10.0/31 heat 192.163.20.1 eq 3389
pennit leap 192.166.10.0/24 boat 192.168.20.1

claas-map^ypecontrcl^leneratch-iny hosts crap

policy-cap type control-plane hoetapnap

police cir 94000 pcs be 128 packets |

IW.168,20.1 eq 443
inform transmit violet ■oup it

class permithosrs anertt violate drop]

Answer:

Explanation:

```
ip access-list permithosts
  permit tep 192.168.10.0/24 host 192.168.20.1 eq 443
  permit tep 192.168.10.0/24 host 192.168.20.1 eq 3389
  permit ieme 192.168.10.0/24 host 192.168.20.1

class-map type control-plane match-any hostsemap
  match[access-group name permithostsj

policy-map type control-plane hostspmap
  class hostsemap
  police cir 54000 pps be 128 packets conform transmit violate drop
```

```
host 192.168.20.1 eq 443

access-group name permithosts

class hostsemap

conform transmit violate drop

class permithosts
```

Question: 379

An engineer must configure Cisco Nexus 9000 Series Switches for Cisco UCS Director integration The configuration must enable automated onboarding of the switches as they come online. For security purposes, the switches must have the bare minimum of connection methods enabled. The connection protocol must allow authentication through credentials. Which

protocol must be configured on the switches to allow automated onboarding?

A. SNMP

B. Telnet

C. SSH

D. HTTPS

Answer: C

Explanation:

SSH (Secure Shell) is the protocol that allows secure remote login from one computer to another. It provides strong authentication and secure communications over unsecured channels. This protocol is preferred for automated onboarding of devices like Cisco Nexus 9000 Series Switches because it supports strong encryption and credential-based authentication, which aligns with the requirement for minimal connection methods and security. SSH is commonly used in network automation for secure command execution and file transfers1.

Reference := For more information on configuring Cisco Nexus 9000 Series Switches for automation and integration with systems like Cisco UCS Director, you can refer to the Cisco Nexus 9000 Series NX-OS Programmability Guide, which details the supported manageability features and advanced automation capabilities, including Power On Auto Provisioning (POAP) and integration with automation frameworks

Question: 380

An engineer must implement access control tor Cisco UCS Manager. The configuration must meet these requirements.

All users and user groups must be configured using Active Directory.

User1 must have full access to the Fabric Interconnect infrastructure and network security operations

User1 must have full access to the storage operations configuration.

Which action must be performed on Cisco UCS to meet the requirements?

A. Create a custom rote tot the user and RADIUS for the role-mapping for Active Directory.

B. Execute a built-in role for the user and LDAP lor the role-mapping for Active Directory.

C. Create a custom role tor the user and LDAP for the rote-mappings for Active Directory.

D. Execute a built-in role for the user and RADIUS for the role-mapping for Active Directory.

Answer: C

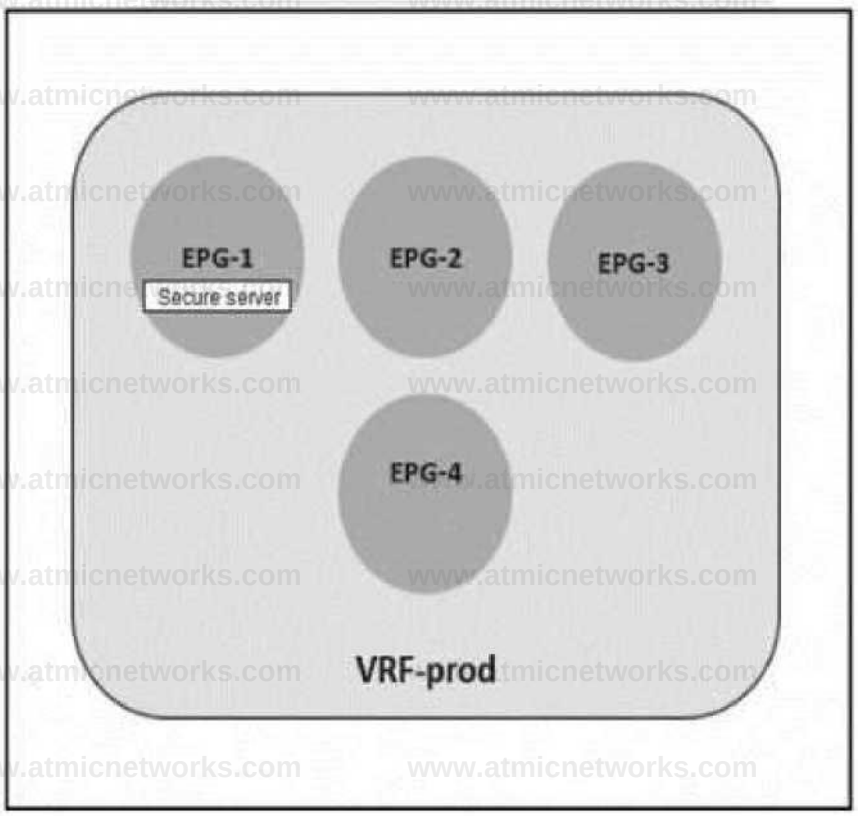
Explanation:

To meet the specified requirements, a custom role needs to be created for User1 that grants full access to both the Fabric Interconnect infrastructure and network security operations, as well as storage operations configuration. This custom role ensures that User1 has the necessary permissions across different areas of the UCS Manager. Using LDAP for role-mapping with Active Directory allows for the integration of UCS Manager with the existing AD infrastructure, enabling centralized management of user credentials and access rights12.

Reference := The process for integrating Cisco UCS Manager with Active Directory and configuring custom roles can be found in the official Cisco documentation, such as the Cisco Secure Access Control System Configuration Guides and the Cisco Community discussions on UCS Manager and Active Directory integration12. These resources provide step-by-step instructions and best practices for setting up access control in UCS Manager using Active Directory.

Question: 381

Refer to the exhibit.



Refer to the exhibit. A secure server that provides services to EPG-2 must be placed in EPG-1. The remaining EPGs—EPG-2, EPG-3. and EPG-4—must communicate without any contracts. Which set of actions accomplishes this goal?

Exclude EPG-2 EPG-3. and EPG-4 from the preferred group
Configure a contract between EPG-2 and EPG-3

Include EPG-2, EPG-3. and EPG-4 in the preferred group.
Configure a contract between EPG-1 and EPG-2.

Include EPG-1 and EPG-2 in the preferred group.
Configure a contract between EPG-2 and EPG-3

Exclude EPG-2. EPG-3, and EPG-4 from the preferred group
Configure a contract between EPG-1 and EPG-3.

A. Option A

B. Option B

C. Option C

D. Option D

Answer: B

Explanation:

Including EPG-2, EPG-3, and EPG-4 in the preferred group allows these EPGs to communicate with each other without requiring any contracts. This is because the preferred group feature in Cisco ACI allows EPGs within the same VRF to communicate by default. However, since the secure server in EPG-1 must provide services to EPG-2, a contract is required between EPG-1 and EPG-2 to facilitate this communication while maintaining the security and policies necessary for the server.

Reference := For more detailed information on configuring EPGs and contracts in Cisco ACI, you can refer to the Cisco Data Center Core Technologies (DCCOR) study materials and official Cisco documentation. These resources provide comprehensive guidance on the implementation and management of EPGs, contracts, and preferred groups within a Cisco ACI environment.

Question: 382

A network administrator is using the Cisco ESA with Cisco AMP to upload files to the cloud for analysis. The network is congested and is affecting communication. How will the Cisco ESA handle any files which need analysis?

A. Cisco AMP calculates the SHA-256 fingerprint, caches it, and periodically attempts the upload.

B. The Cisco ESA immediately makes another attempt to upload the file.

C. The file is queued for upload when connectivity is restored.

D. The file upload is abandoned.

Answer: C

Explanation:

The file is queued for upload when connectivity is restored

Question: 383

What is a benefit of using Cisco Tetration?

A. It collects telemetry data from servers and then uses software sensors to analyze flow information.

B. It collects near-real time data from servers and inventories the software packages that exist on servers.

C. It collects policy compliance data and process details.

D. It collects enforcement data from servers and collects interpacket variation.

Answer: A

Explanation:

. It collects telemetry data from servers and then uses software sensors to analyze flow information

Question: 384

A network engineer must migrate a Cisco WSA virtual appliance from one physical host to another physical host by using VMware vMotion. What is a requirement for both physical hosts?

A. The hosts must run Cisco AsyncOS 10.0 or greater.

B. The hosts must have access to the same defined network.

C. The hosts must run different versions of Cisco AsyncOS.

D. The hosts must use a different datastore than the virtual appliance

Answer: B

Explanation:

When using VMware vMotion to migrate a Cisco WSA virtual appliance from one physical host to another, it is essential that both physical hosts have access to the same network configurations. This includes the same defined networks to which the interfaces on the virtual appliance are mapped. This requirement ensures that the virtual appliance retains its network connectivity and continues to function correctly after the migration1.

Reference := For more information on the requirements and process of migrating a Cisco WSA virtual appliance using VMware vMotion, you can refer to the Cisco Secure Email and Web Virtual Appliance Installation Guide1.

Question: 385

A Cisco Nexus 7000 Series switch runs VXLAN, and interface Ethernet 7/30 is configured as a trunk port. Which command set configures the switch to act as a gateway for VLAN 50?

interface Ethernet7/30

no switchport

no shutdown

service instance 1 vni

no shutdown

A.

encapsulation profile VSI_50_TO_500 default

A. encapsulation profile vni VSI_50_TO_500

dot1q 500 vni 50

bridge-domain 500

member vni 50

interface Vlan500

ip address 10.50.50.51/24

B.

encapsulation profile vni VSI_50_TO_500

dot1q 500 vni 50

bridge-domain 500

member vni 50

interface Bdi500

jp address 10.50.50.51/24

C.

encapsulation profile vni VSI_50_TO_500

dot1q 50 vni 500bridge-domain 50

member vni 500

interface Bdi50

ip address 10.50.50.51/24

D.

encapsulation profile vni VSI_50_TO_500

dot1q 50 vni 500

bridge-domain 50

member vni 500

interface Vlan50

ip address 10.50.50.51/24

Answer: D

Explanation:

To configure a Cisco Nexus 7000 Series switch to act as a gateway for VLAN 50 in a VXLAN environment, the correct command set includes defining a service instance for the VLAN, specifying the encapsulation profile, and associating the VLAN with a bridge domain and a VNI. The commands should map VLAN 50 to VNI 500 and then configure an SVI (Switched Virtual Interface) for VLAN 50 with an IP address. This allows the switch to route traffic

for VLAN 50, acting as a gateway1.

Reference := For detailed configuration steps and explanations, you can refer to the Cisco Nexus 7000 Series NX-OS VXLAN Configuration Guide, which provides comprehensive information on setting up VXLAN gateways and integrating VXLAN with traditional VLANs

Question: 386

What is a benefit of using the Cisco UCS Lightweight upgrade feature?

A. Security updates are scheduled with the next reboot of the fabric interconnects.

B. All servers are rebooted to push the latest updates.

C. The firmware version of a component is updated only when it has been modified.

D. A soft reboot is available for the fabric interconnects.

Answer: C

Explanation:

The Cisco UCS Lightweight Upgrade feature offers the benefit of updating the firmware version of a component only if there has been a modification. This means that not all components will be updated in every service pack, which can reduce downtime and the potential for disruptions caused by unnecessary updates1.

Reference := For more information on the Lightweight Upgrade feature, you can refer to the Cisco UCS Central Administration Guide, Release 2.0

Question: 387

An engineer must suggest a deployment model for a newly developed application. The engineer has a small starting budget and lacks technical knowledge and infrastructure to implement storage, operating system, and database services to

support the application deployment. The engineer also needs usage data related to the service and the ability to elastically scale the deployment as customer demands grow. Which two models must be used to meet the

requirements?

(Choose two.)

A. private cloud

B. platform as a service

C. software as a service

D. infrastructure as a service

E. public cloud

Answer: B, E

Explanation:

Platform as a Service (PaaS) provides a platform allowing customers to develop, run, and manage applications without the complexity of building and maintaining the infrastructure typically associated with developing and launching an app. Public cloud services are offered over the internet and are available to anyone who wants to purchase or use them. They are ideal for an engineer with a small budget and limited technical knowledge because they provide a cost-effective, scalable infrastructure that can grow with customer demand2.

Reference := For further details on cloud deployment models, including PaaS and public cloud, you can explore resources such as cloud deployment model comparisons and examples provided by various cloud service providers

Question: 388

An engineer needs to install a new package on a Cisco Nexus 9000 Series Switch. What is the impact of running the install commit <filename> command on the switch?

A. The switch is restarted after the upgrade is complete

B. The package is used after the switch is restarted.

C. The previous package that was in use is deleted from bootflash.

D. The package is used in the running configuration.

Answer: B

Explanation:

When you run the install commit <filename> command on a Cisco Nexus 9000 Series Switch, it schedules the new package to be used after the next reboot of the switch. This means that the current running configuration isn't immediately affected by the new package, but it will be incorporated once the switch is restarted.

Question: 389

An engineer is implementing traffic monitoring for a server vNIC that is configured with fabric failover enabled. The requirement is for the traffic to be sent to an analyzer, even during a failure of one of the fabric interconnects. The analyzer is connected to unconfigured Ethernet ports on both fabric interconnects. Which configuration accomplishes this task?

A. Create two traffic monitoring sessions with different names, one per fabric
Connect the analyzer connected to FI-B as the destination for both monitoring sessions.

B. Create two traffic monitoring sessions with the same name, one per fabric.

Connect an analyzer on each Fl as the destination for the monitoring session local to that FI.

C. Create two traffic monitoring sessions with the same name, one per fabric.
Connect the analyzer connected to FI-A as the destination for both monitoring sessions.

D. Create two traffic monitoring sessions with different names, one per fabric.

Connect an analyzer on each FI as the destination for the monitoring session local to the FI

Answer: D

Explanation:

For traffic monitoring with fabric failover enabled, it's important to ensure that traffic can still be analyzed even if one of the fabric interconnects fails. By creating two separate traffic monitoring sessions, each with a unique name and connected to an analyzer on each fabric interconnect, you can maintain continuous monitoring. This setup ensures that traffic is sent to the analyzer regardless of the state of either fabric interconnect.

Reference: For more detailed information, please refer to the official Cisco documentation on their website or the specific study materials for the Cisco Data Center Core Technologies certification.

Question: 390

A network engineer must deploy a configuration backup policy to the Cisco UCS Manager. The file generated from this backup must have a snapshot of the entire system that should be used to restore the system during disaster recovery. The backup file must be transferred insecurely by using the TCP protocol. Which configuration backup settings meet these requirements?

A. Type: All Configuration

Protocol: SCP

B. Type: Logical Configuration

Protocol: SFTP

C. Type: Full State

Protocol: FTP

D. Type: System Configuration

Protocol: TFTP

Answer: C

Explanation:

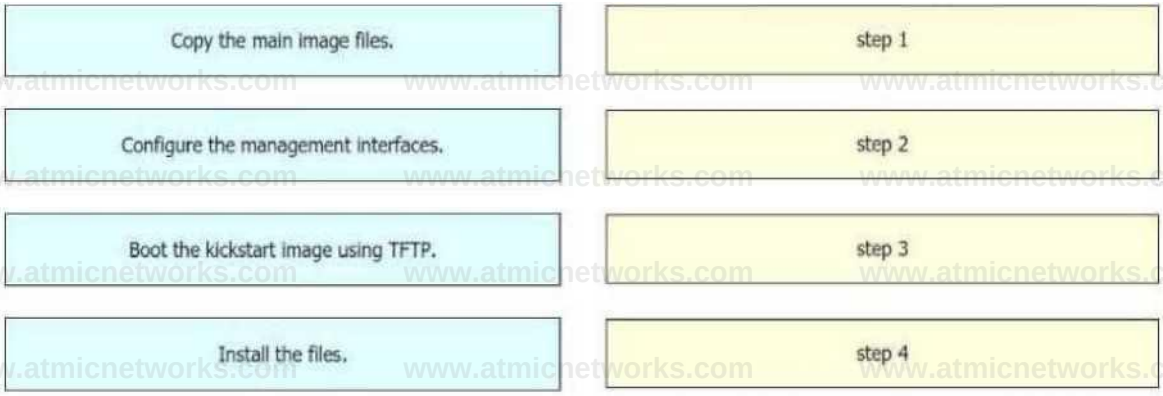
The 'Full State' backup type in Cisco UCS Manager is designed to capture a snapshot of the entire system, which includes all configuration settings, system logs, and the operating system. This comprehensive backup can be used to fully restore the system in the event of a disaster recovery scenario. The 'Full State' backup is the only option that provides a complete system snapshot, making it the ideal choice for disaster recovery purposes.

Reference: The information regarding backup types and their purposes can be found in the Cisco Data Center Core Technologies source book, specifically in the section discussing system maintenance and backups within the Cisco UCS Manager platform.

Question: 391

DRAG DROP

Drag and drop the steps on the left onto the order that they must be implemented on the right to recover a fabric interconnect when there is no working image on the bootflash.



Answer:

Explanation:

Boot the kickstart Image using TFTP.

Configure the management interfaces.

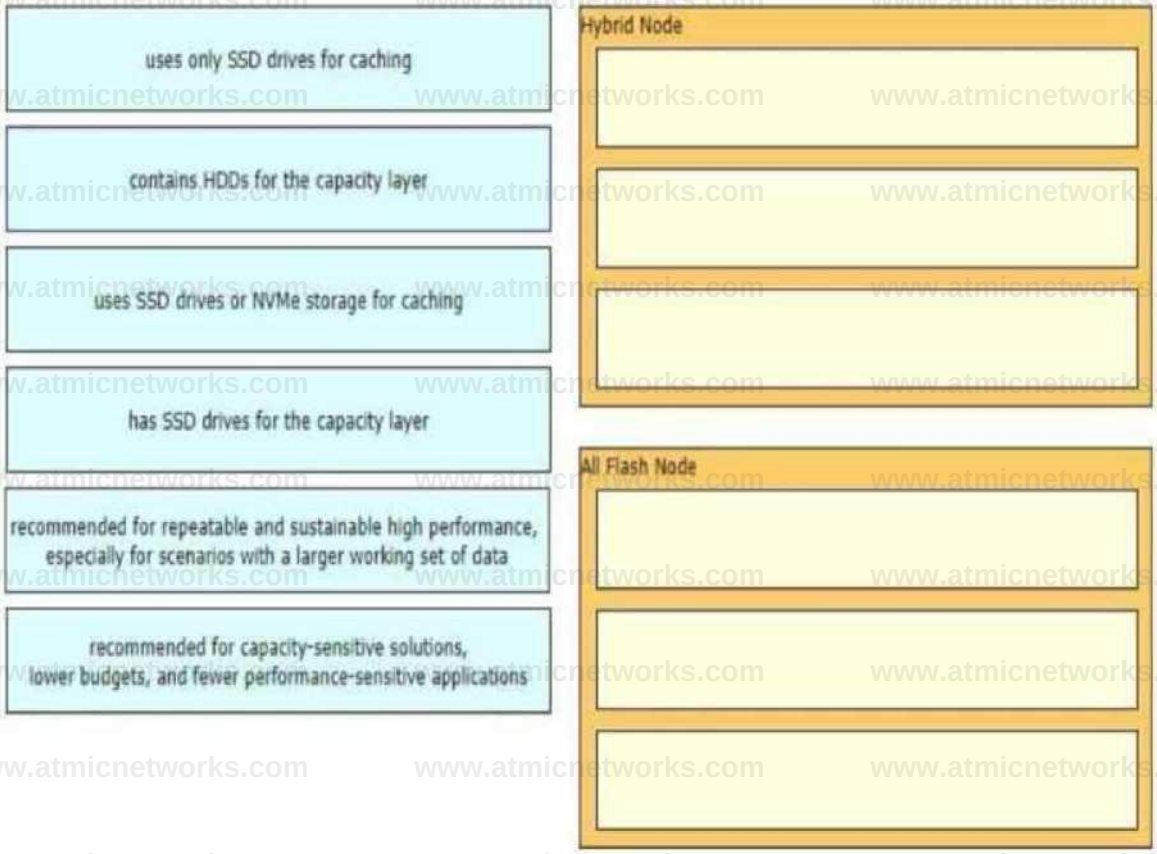
Copy the main Image files.

Install the files.

Question: 392

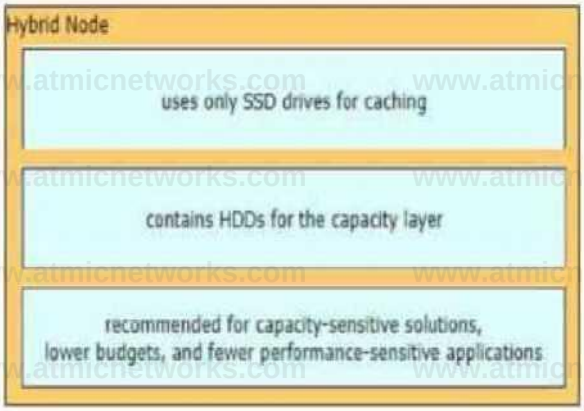
DRAG DROP

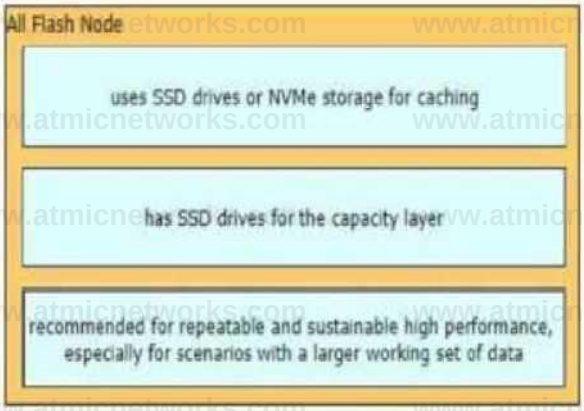
Drag and drop the Hyperflex characteristics from the left onto the appropriate Hyper Hex node types on the right.



Answer:

Explanation:





Question: 393

Refer to the exhibit.

```
N9K-1# show running-config interface Ethemetl/1
  switchport access vlan 10
  spanning-tree port type edge
  switchport port-security aging tine 33
  switchport port-security maximum 3
  switchport port-security mac-address sticky switchport port-security

N9K-1# show mac address-table interface ethemet 1/1
Legend:
        * - primary entry, G - Gateway MAC, (R) - Routed MAC, 0 - Overlay MAC
        age - seconds since last seen,* - primary entry using vPC Peer-Link, (T)
        - True, (F) - False, C - ControlPlane MAC, - - vsan
   VLAN     MAC Address       Type       age     Secure NTFY Ports
        —+-----------------+ ------- 4---------+ -----+ --- +-----------------
♦    10     0050.7966.6801   secure    -          T      F    Ethl/1
♦    10     0050.7966.6802   secure    -          T      F    Ethl/1
♦    10     0050.7966.6803 secure -               IF Ethl/1
```

An engineer configures port security on a Cisco Nexus 9000 Series Switch. The requirement is to prevent any newly learned MAC addresses from forwarding traffic on the interface. Also, the already learned MAC addresses must not be affected by the changes. Which configuration meets these requirements?

A. switchport port-security violation shutdown

B. switchport port-security violation isolate

C. switchport port-security violation protect

D. switchport port-security violation restrict

Answer: C

Explanation:

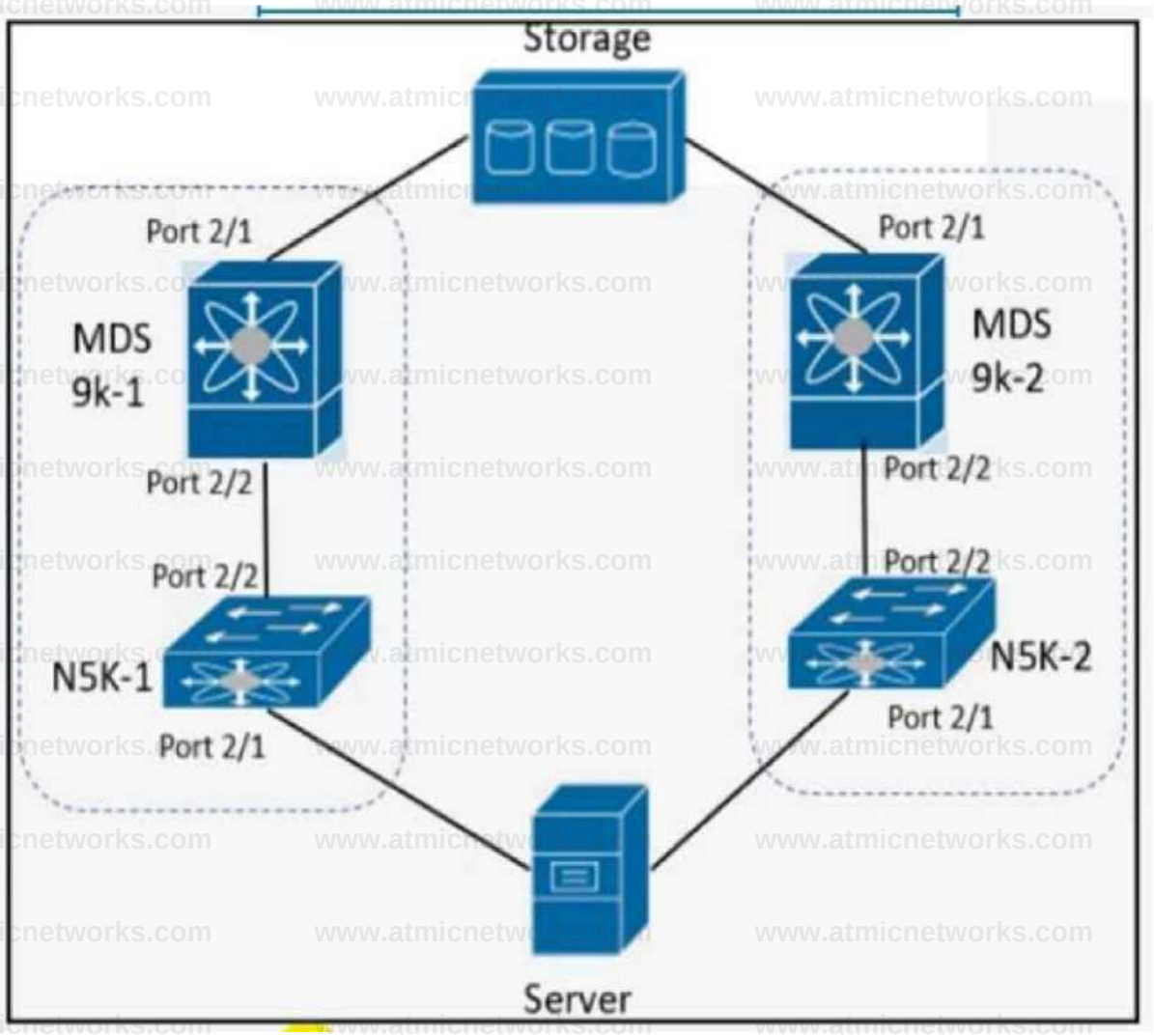
The 'protect' violation mode in port security is designed to drop packets with unknown source MAC addresses without affecting the interface's state. This mode ensures that traffic from already learned MAC addresses continues to be forwarded while preventing any new MAC addresses from forwarding traffic until a sufficient number of secure MAC addresses are removed or the maximum count is increased. This configuration aligns with the requirement to not affect already learned MAC addresses.

Reference := For further reading and detailed understanding, refer to the Cisco Data Center Core Technologies study guide and source documents available on the Cisco Learning Network Store and Cisco's official solutions page for data center virtualization.

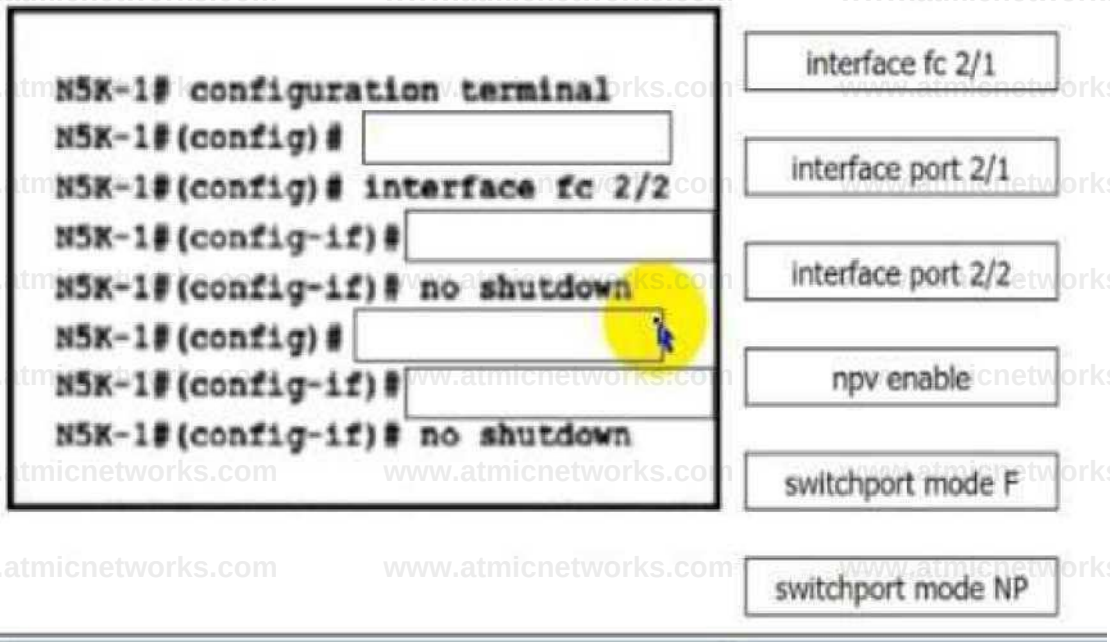
Question: 394

DRAG DROP

Refer to the exhibit.



The server is sending traffic to the storage server using Fiber Channel protocol. The requirement is for the N5K-1 to forward traffic to MDS9k-1. Drag and drop the configuration steps from the right to complete the configuration for N5K-1 on the left. Not all configuration steps are used.



Answer:

Explanation:

npv enable, switchport mode F, interface fc2/1, switchport mode NP

Question: 395

Which two features are used to allow a nondisruptive upgrade for the ISSU process? (Choose two.)

A. connectivity management processor

B. nonstop forwarding

C. graceful restart

D. stateful switchover

E. advanced services license

Answer: B, D

Explanation:
The In-Service Software Upgrade (ISSU) process is designed to upgrade the system software with minimal disruption to the network. Nonstop forwarding (NSF) and stateful switchover (SSO) are two features that work together to maintain packet forwarding and switch state information during the ISSU process. NSF allows the router to continue forwarding packets even when the route processor is failing over, while SSO synchronizes state information between redundant route processors to ensure a seamless transition during a failover1.

Reference := For a deeper understanding of the ISSU process and its associated features, you can refer to Cisco's official documentation on In-Service Software Upgrade (ISSU), which provides detailed information on how NSF and SSO contribute to a nondisruptive upgrade

Question: 396

Refer to the exhibit.

An engineer must configure a Fibre Channel device alias named TEST for a device attached to port fc1/9 of a Cisco Nexus

Series Switch. Which command set completes the configuration?

A)

SITE-A-MDS-Fabnc-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SlTE-A-MDS-F^bric-A (config-device-ahas-db)# device-alias name TEST pwwn 50:00:14:42:d0:0c:f5:20 SITE-A-MDS-Fanric-A (config-device-alias-db^ device-alias commit

B)

SITE-A-MDS-Fabric-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SITE-A-MDS-Fabnc-A (config-device-alias-db)# device-alias name TEST pwwn 50:00:14:42:d0:0c:f5:20 SITE-A-MDS-Fabric-A (confia-device-alias-db)# exit

C)

SITE-A-MDS-Fabric-A# configure terminal
SITE-A-MDS-Fabric-A (config)# device-alias database
SITE-A-MDS-Fabric-A (config-device-alias-db)# device-alias name TEST pwwn 50:00:14:40:47:b0:0c:f5 SITE-A-MDS-Fabric-A (config-device-alias-db)# exit

D)

SITE-A-MDS-Fabric-A# device-alias database
SITE-A-MDS-Fabnc-A (device-alias-db)# device-alias name TEST pwwn 50:00:14:40:47:b0:0c:f5
SITF-A-MDS-Fabric-A (confio-device-alias-dbUt device-alias commit

A. Option

B. Option

C. Option

D. Option

Answer: A

Explanation:

To configure a Fibre Channel device alias named TEST for a device attached to port fc1/9 on a Cisco Nexus Series Switch, the correct command set is found in Option A. The commands should be entered in configuration mode, starting with accessing the device-alias database, creating the devicealias named TEST with the specified pwwn, and committing the changes to the database123.

Reference := The process for configuring a Fibre Channel device alias on a Cisco Nexus Series Switch is detailed in the Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide and other Cisco documentation related to SAN

switching and device aliases

Question: 397

A network engineer must configure a Cisco MDS switch to use the local user database for console access if all AAA servers are unreachable. Which configuration should be applied to complete this task?

A. aaa authentication login default fallback error local

B. aaa authentication login console fallback error local

C. aaa authentication login default local

D. aaa authentication login console local

Answer: B

Explanation:

This configuration ensures that if AAA servers cannot be reached, the switch will fall back to using the local user database for authentication when accessing the console. The fallback error local keyword specifies that the local database should be used in case of an error in reaching the AAA servers1.

Reference := For more information on configuring AAA on Cisco MDS switches, you can refer to Cisco's official documentation and community discussions which provide insights into setting up authentication methods for different access scenarios1. These resources explain how to configure the switch to handle authentication locally when remote AAA servers are not available.

Question: 398

Refer to the exhibit.

A network engineer is using tcpdump to capture a snapshot of OSPF-related traffic on a specific Cisco NX-OS switch port. For security reasons, the capture must be taken using an embedded container that is already deployed on the Cisco Nexus device. Which command completes the script?

A. guestshell

B. guestshell-bash

C. run guestshell

D. run bash

Answer: C

Explanation:

The command run guestshell is used to access the Guest Shell on Cisco NX-OS devices. Guest Shell is a secure, Linux-based environment that runs as a virtualized application container on the device. It allows network administrators to use Linux utilities and scripts, enhancing automation and monitoring capabilities. In this scenario, using run guestshell would enable the engineer to utilize the tcpdump utility within the container to capture OSPF-related traffic on the switch port1.

Reference := For more information on using Guest Shell for traffic capture and other advanced features on Cisco NX-OS devices, you can refer to the Cisco documentation on Embedded Packet Capture (EPC) and Guest Shell configuration1

Question: 399

Which file service protocol allows the files to appear locally mapped to the client and provides view, store, and update capabilities on a remote Linux-based storage repository that also serves as a distributed file system standard for NAS?

A. NFS

B. FTP

C. iSCSI

D. IFS

Answer: A

Explanation:

NFS, or Network File System, is a file service protocol that allows files to be accessed over a network in a manner similar to how local storage is accessed. NFS provides the capability for clients to view, store, and update files on a remote Linux-based storage repository. It is widely used as a distributed file system standard for Network Attached Storage (NAS) because it allows the files to appear locally mapped to the client, facilitating easy file sharing and management1.

Reference := The use of NFS in NAS environments is well-documented in Cisco Data Center Core Technologies source documents and study guides, which explain how NFS works and its role in providing distributed file system services

Question: 400

Refer to the exhibit.

```
import time
import cli

date= time.strftime('%Y%m%d')
file=
cli.execute ('copy running-config ftp://10.183.249.182/FusionSW/' + file)
exit()
```

Which command needs to be added to the line starting with the "file" keyword to have the generated running-config file with the name 'fusion-config_' and current date?

A. string(Cfusion-config_') + date)

B. ('fusion-configj) + date

C. str.ffusion-configj) + date

D. (*fusion-config_ * date')

Answer: B

Explanation:

The correct command to add to the script is option B, which concatenates the string 'fusion-config_' with the variable date to form the filename. This will result in a filename that includes the desired prefix followed by the current date, matching the format specified in the question.

Reference := For more information on scripting and automation within Cisco environments, you can refer to the Cisco Data Center Core Technologies documentation, which includes guidelines on using Python scripts for network configuration and management tasks.

Question: 401

Which Cisco UCS Manager XML encoded backup type must be used to back up user names, roles, and service profiles?

A. Full State Configuration

B. Logical Configuration

C. All Configuration

D. System Configuration

Answer: D

Explanation:

The System Configuration backup type in Cisco UCS Manager is specifically designed to back up system settings such as user names, roles, and locales. This XML file does not include the actual data on the servers but captures all the system configuration settings, which can be imported to the original fabric interconnect or to a different one. However, it cannot be used for a system restore.

Reference: Cisco UCS Manager Administration Management Guide

Question: 402

Which two configuration settings are available in the Cisco UCS Firmware Auto Sync Server policy? (Choose two.)

A. Immediate Action

B. User Acknowledge

C. No Action

D. Delayed Action

E. User Notification

Answer: B, C

Explanation:

The Firmware Auto Sync Server policy in Cisco UCS Manager allows administrators to set when and how firmware versions on recently discovered servers should be upgraded. The policy options include 'User Acknowledge', which requires an administrator's acknowledgment to initiate the firmware upgrade, and 'No Action', which means no firmware upgrade will be initiated on the server. These settings ensure that firmware upgrades are controlled and do not occur without the necessary administrative oversight.

Reference: Using Firmware Automatic Synchronization Server Policy

Question: 403

A company plans to migrate some of its services to the cloud. The company does not want to manage or control the underlying cloud infrastructure. It also wants to maintain control over the deployment of its applications and configuration settings of the application-hosting environment. Which cloud service model meets these requirements?

A. Infrastructure as a Service

B. Function as a Service

C. Platform as a Service

D. Software as a Service

Answer: C

Explanation:

Platform as a Service (PaaS) is the cloud service model that allows companies to manage and control their application deployments and configuration settings without having to manage the underlying cloud

infrastructure. PaaS provides a platform including infrastructure, operating systems, and development tools, enabling companies to focus on the development and management of their applications

Question: 404

What is a benefit of Cisco HyperFlex All-Flash Stretched cluster deployment as compared to All-HDD Stretched cluster deployment?

A. lower cost

B. lower number of IOPS

C. higher cost

D. higher number of IOPS

Answer: D

Explanation:

Cisco HyperFlex All-Flash Stretched clusters provide a higher number of Input/Output Operations Per Second (IOPS) compared to All-HDD Stretched clusters. This is due to the faster data access speeds of flash storage, which results in better performance and lower latency for applications, especially those requiring high throughput and fast processing2

Question: 405

Refer to the exhibit. A network engineer must configure an authentication solution for Cisco UCS

with these conditions:

- Two-factor authentication must be enabled for all UCS user authentication.
- All AAA packets must be encrypted and use TCP port 49 to establish communication.

Which set of actions needs these requirements?

A. Create the LDAP provider.

Change the LDAP group rule in an LDAP provider.

B. Create the RADIUS group mapping.

Change the RADIUS group rule in a RADIUS provider.

C. Remove the LDAP provider.

Create a TACACS+ provider in user management.

D. Delete the LDAP group mapping.

Create a RADIUS provider in user management.

Answer: C

Explanation:

The requirements specify the need for two-factor authentication and encrypted AAA packets using TCP port 49, which is the default port for TACACS+. TACACS+ provides additional security features suitable for two-factor authentication, unlike LDAP. Therefore, removing the LDAP provider and creating a TACACS+ provider in user management would fulfill these requirements.

Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials and Cisco's official documentation on authentication solutions.

Question: 406

A customer asks an engineer to develop an orchestration solution to automate repetitive tasks. The

customer operations team must integrate the tool with its existing automation framework. The customer asks for the tool to support these requirements:

- The customer's security requirements mandate the use of SSH transport.
- No extra software must be installed on the managed systems.
- The support staff has limited knowledge of scripting languages, so the solution must be easy to read and use declarative language.

Which solution meets these requirements?

A. PowerShell
B. Ansible
C. Chef
D. Puppet

Answer: B

Explanation:

Ansible meets the requirements as it uses SSH for transport, does not require agent software to be installed on managed systems, and uses YAML for its playbooks, which is a human-readable data serialization standard, making it easy to read and use for people with limited knowledge of scripting languages.

Reference: Cisco's official documentation on network automation orchestration solutions and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course materials.

Question: 407

An engineer is automating a Cisco Nexus 9000 Series Switch using the NX-OS API. Which code snippet creates a local user called "tacuser" with an expiration date of 22 November?

A)

POST http;//10.91.12.14/a pi/m o/sys/use re x t. js o n

```
aaaUserEp": (
“children": [
{
  "aaaUser": {
    "attributes": {
      "allowExpired": "no",
      "expiration": "2021-11-22T00:00:00.000+00:00",
      "expires": "yes",
      "name": "tacuser",
      "pwd": "AKw47PS3:g4M410:Fs01",
      "pwdEncryptType": "clear"
    }
  }
}
```

B)

GET http://10.12.14.91/api/mo/sys/userext/user-tacuser.json


```
aaaUserEp": {
"attributes": {
  "chlldAction": "add",
  "dn": "sys/userext",
  "lcOwn": "local",
  "modTs":"2021-11-22T00:00:00.000+00:00"
  "pwdSecureMode": "yes",
  "pwdStrengthCheck": "no",
  "status":"",
  "uid": "0"
```


C)

```
HEAD http://10.14.91.12/api/policymgr/mo/uni/userext.json
(
  "aaaUser": {
    “name": "tacuser”,
    “phone”:"".
    "pwd":"H97NW894SDASgQL“,
    “expire”: "yes",
    "aaaUserDomain”: {
      "description”:"”,
      "name": “all”, "rn":“userdomain-aH"
    }


PUT http://10.91.14.12/api/policymgr/mo/uni/

{
  "aaaUser": {
    “email": "tacuser@cisco.com",
    “name": "tacuser”,
    “createdAt": "2020-09.11 T00:00:00.090210Z",
    "authorizations": {
      "authorizedZone": "VDC1",
      "expiresAt": "2021-11.22700:00:00.000+00:00“
      "authorizedByName": "OPS", "authorizedByEmail":
      "ops@tompany.com"
    }
  }
}
```

A. Option A

B. Option B

C. Option C

Answer: C

Explanation:

The code snippet in Option C correctly sets up a local user named “tacuser” with an expiration date of 22 November. In the NX-OS API, the “expiresAt” attribute is used to specify the expiration date for a user account,

which should be formatted in the ISO 8601 standard. The snippet provided in Option C, "expiresAt": "2021-11-22T00:00:00.000+00:00", correctly applies this format to set the expiration date to 22 November 2021. Reference := For further details, refer to the Cisco Data Center Core Technologies source documents or study guide available on the official Cisco Learning Network Store and Cisco's solution listings for data center virtualization.

Question: 408

An engineer must create a scheduler configuration to create two backup jobs per day. The backup file must be copied to a server in the operations VRF. Which configuration accomplishes this task?

A)

```
scheduler schedule name CNFGBACKUP
job name BACKUP JOB
    copy running-config tftp:/10.19.11.12/$(SWITCHNAME)-$(TIMESTAMP).cfg vrf operation;
    time start now repeat 12:00
```

B)

```
scheduler schedule name CNFGBACKUP
job name BACKUP-JOB
    show tech-support | redirect vrf operations tftp:/10.19.11.12/S(SWITCHNAME)-S(TIMESTAMP).cfg time
    start daily 12:30 0:30
```

C)

```
scheduler schedule name CNFGBACKUP
job name BACKUP-JOB
    copy startup-config tftp:/10.19.11.12/$(SWITCHNAME)-$(TIMESTAMP).cfg
    time dally 12:30 0:30
```

D)

```
scheduler schedule name CNFGBACKUP
job name BACKUP-JOB
    copy vrf operations config tftp:/10.19.11.12/S(SWITCHNAME)-S(TIMESTAMP).cfg
    time start 12:30 repeat 12
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The configuration in Option D is a scheduler configuration for creating backup jobs. It specifies a schedule name, job name, and the command to copy configurations to a server in the operations VRF using TFTP protocol. The time start and repeat options are used to schedule two backup jobs per day.

Reference := This explanation is based on the principles found in the Cisco Data Center Core Technologies documentation, which details the use of scheduler configurations for backup purposes. For more in-depth information, please refer to the Cisco Data Center Core Technologies source book or the official Cisco documentation at Cisco Data Center Virtualization.

Question: 409

Refer to the exhibit.

```
Step 20 Enter no (no is the default) if you ace satisfied with the configuration

The following configuration will be applied:

switchname CiscoMDS
  interface mgmtO
    ip address 192.168.10.10 subnetmask 255.255.255.0 no shutdown
  ip default-gateway 192.168.10.1
  telnet server enable no ssh server enable no system default switchport shutdown
  system default switchport trunk mode on no zone default-zone permit vsan 1-4093
  zoneset distribute full vsan 1-4093
Would you like to edit the configuration? (yes/no) [nJ: no

Step 21 Enter yes (yes is default) to use and save this configuration.

Use this configuration and save it? (yes/no) (y]: yes
```

An engineer is configuring a Cisco MDS 9000 Series Switch for the first time. After the initial setup process, the name server at IP 192.168.10.11 is missing from the configuration. Which set of actions completes the configuration?

A. Enter no at step 21 and reinitialize the installer. Press the Esc key to access ROMMON mode.

B. Enter no at step 21 and reload the switch. Configure the advanced IP options.

C. Enter yes at step 21 to edit the configuration. Add the line dns-server 192.168.10.11.

D. Enter yes at step 21 and log in. Modify the startup configuration DNS

Answer: C

Explanation:

The question involves an engineer configuring a Cisco MDS 9000 Series Switch and noticing that the name server with IP 192.168.10.11 is missing from the configuration. The correct action to complete the configuration is option C, “Enter yes at step 21 to edit the configuration. Add the line dns-server 192.168.10.11.” This step allows the engineer to modify the initial setup process’s outcome by adding the missing DNS server information directly into the configuration before saving it.

Reference: For further details, refer to the Cisco Data Center Core Technologies source documents or study guides available on the official Cisco Learning Network Store and Cisco’s solution listings for data center virtualization.

Question: 410

An engineer is implementing a Cisco ACI fabric and must use static VLAN range as part of a VMM deployment. The static VLAN must be incorporated into the dynamic VLAN pool. The existing VLAN pool is set for dynamic allocation. Which action accomplishes this goal?

A. Add the VLAN to the pool configured with Inherit Allocation Mode from parent.

B. Change the existing VLAN pool to static allocation mode.

C. Add a static VLAN allocation range to the VLAN pool.

D. Create a static reservation within the dynamic VLAN pool.

Answer: C

Explanation:

In a Cisco ACI fabric, when implementing a Virtual Machine Manager (VMM) domain, VLANs can be allocated dynamically or statically within a VLAN pool. To incorporate a static VLAN into a dynamic VLAN pool, the correct approach is to add a static VLAN allocation range to the VLAN pool. This allows for the specific VLAN to be

reserved and used consistently for certain applications or services, while still maintaining the flexibility of dynamic allocation for other VLANs within the pool.

Question: 411

A network engineer connects the CNA interface of a server to a switch. The switch must bring down all of the VLANs on the interface that are not enabled for FCoE, but the VLANs that are enabled for FCoE should continue to carry SAN traffic without interruption. Which configuration should be applied to the switch to achieve this objective?

A. switch(config)# interface Ethernet 2/1 switch(config-if)# shutdown lan

B. switch(config)# interface vfc 2 switch(config-if)# shutdown lan

C. switch(config)# Interface Ethernet vfc 2 switch(config-if)# shutdown force

D. switch(config)# interface Ethernet 2/1 switch(config-if)# shutdown force

Answer: D

Explanation:

To achieve the objective of bringing down all VLANs on an interface that are not enabled for FCoE while allowing those that are enabled for FCoE to continue carrying SAN traffic, the shutdown force command should be applied to the Ethernet interface. This command ensures that only the non-FCoE VLANs are shut down, and it does not affect the operation of the VLANs carrying FCoE traffic. The shutdown force command is used specifically to override any configurations that might prevent the interface from being shut down, such as EtherChannel or Spanning Tree Protocol (STP) settings.

Reference: The solution aligns with Cisco's best practices for managing VLANs in a Cisco ACI environment, particularly when dealing with FCoE traffic. For more detailed information, refer to the Cisco documentation on FCoE configurations and VLAN management in the context of Cisco ACI fabrics, which can be found in the Cisco Data Center Core Technologies (DCCOR) study materials and on the Cisco official website under the Data Center and Virtualization section1

Question: 412

An engineer needs to connect Cisco UCS Fabric Interconnect (FI) to an external storage array. Due to budget limitations, the engineer must connect a Cisco UCS FI directly to an FC storage port. Which two actions must be taken to complete this connection? (Choose two.)

A. Configure the fabric interconnect in FC switch mode.

B. Set FC zoning to disabled when creating the VSAN

C. Create a storage connection policy.

D. Configure the fabric interconnect in end-host mode,

E. Create the required VSAN in the SAN cloud.

Answer: A, E

Explanation:

When connecting a Cisco UCS Fabric Interconnect (FI) directly to an external storage array using a Fibre Channel (FC) storage port, it is essential to configure the FI in FC switch mode. This mode allows the FI to manage FC traffic and zoning, which is necessary when bypassing an upstream SAN switch. Additionally, creating the required Virtual Storage Area Network (VSAN) within the SAN cloud is crucial for isolating and managing the traffic between the FI and the storage array. The VSAN provides a unique identifier that enables the direct connection and communication between these devices.

Reference: The configuration steps for direct attachment of a storage array to a Cisco UCS FI are detailed in Cisco's official documentation and support forums1. Specifically, the process involves setting the FI in FC switch mode and creating the necessary VSAN for the connection1. These references provide guidance based on Cisco's recommended practices for such configurations.

Question: 413

An engineer must configure a Cisco MDS 9000 Series Switch for traffic analysis from the storage array. The storage array is connected to the interface fc2/1 in VSAN 10 and the traffic analyzer to fc4/2. The capture file

must include ingress and egress traffic between the switch and the storage array. Also, only traffic in VSAN 10 must be captured. Which configuration set meets these requirements?

A)

```
interface fc4/2 switchport mode auto no shutdown

span session 1
    source interface fc2/1 rx destination interface fc4/2 source filter
    vsan 10 no suspend
```

B)

```
interface fc4/2
    switchport mode trunk
    switchport trunk allow vsan 10 no shutdown
!
span session 1
    source interface fc2/1 tx destination interface fc4/2 rx no
    suspend
```

C)

```
interface fc4/2 switchport mode SD no shutdown

span session 1
    source interface fc2/1 destination interface fc4/2 source filter
    vsan 10
```

D)

```
interface fc4/2 switchport mode ST no shutdown

span session 1 source interface fc2/1 destination interface fc4/2
    source filter vsan 10
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: D

Explanation:

The correct configuration for capturing both ingress and egress traffic between a Cisco MDS 9000 Series Switch and a storage array, specifically for VSAN 10, is found in Option D. This configuration involves setting up a SPAN session on the switch. The SPAN session is configured to monitor the source interface connected to the storage array (fc2/1) and send the captured traffic to the destination interface connected to the traffic analyzer (fc4/2). The source filter vsan 10 command ensures that only traffic from VSAN 10 is included in the capture, which aligns with the requirements specified.

Reference: For more detailed information on configuring SPAN sessions on Cisco MDS 9000 Series Switches, please refer to the Cisco MDS SAN-OS documentation, which provides guidelines on traffic monitoring and analysis in a Cisco data center network environment. Additionally, the Cisco Data Center Core Technologies (DCCOR) study materials offer insights into best practices for implementing traffic analysis solutions in a data center context.

Question: 414

A customer deploys a media server to distribute streaming videos to network clients. The requirement is to allow the video feed to reach only requesting clients. The shared trees must not propagate the video feed if no clients from that tree request it. To reduce configuration touchpoints, the solution must support the automatic discovery and announcement of RP-set information. Each router in the network is responsible for selecting the RP. Which configuration set meets these requirements?

A)

router(config-if)# ip pim bidir-enable router(config)# ip pim ssm default router(config)# ip igmp version 3

B)

router(config-if)# ip pim dense-mode router(config)# ip pim rp-

address 1.1.1.1 router(config)# ip pim rp listener

C)

router(config-if)# ip pim sparse mode router(config)# ip pim bsr-candidate LoO routerfconfig)# ip pim rp-candidate LoO

D)

router(config-if)# ip pim sparse-sense mode router(config)# ip pirn auto-rp
router(config)# ip pim send-rp-announce

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The configuration that meets the requirements for a media server to distribute streaming videos only to requesting clients, without propagating the video feed through shared trees if there are no requests, and supporting automatic discovery and announcement of RP-set information, is Option C. This option likely includes the use of Protocol Independent Multicast (PIM) in sparse mode, which is suitable for environments where multiple routers need to dynamically discover the Rendezvous Point (RP) for multicast groups. The configuration would also involve commands to enable Auto-RP for the automatic announcement and discovery of RPs.

Reference: The explanation is based on the principles of multicast routing and PIM operation as described in Cisco Data Center Core Technologies documentation. For more detailed information, the "Implementing and Operating Cisco Data Center Core Technologies (DCCOR v1.2)" course material and the Cisco official documentation on multicast routing would be the appropriate references.

Question: 415

Refer to the exhibit.

```
int fc1/1-2 switchmode rate dedicated
channel-group 100 force no shut

int san-port-channel 100
switchport trunk allowed vsan 1
switchport trunk allowed vsan add 100
```

An engineer is connecting a Cisco MDS 9700 Series Multilayer Director to a downstream Cisco Nexus 5672UP switch. Which command set must be used to complete the configuration?

A)

```
int san-port-channel 100
switchport mode te
switchport trunk mode off
channel mode on
```

B)

```
int san-port-channel 100
switchport mode te
switchport trunk mode auto
channel mode on
```

C)

```
int san-port-channel 100
switchport mode e
switchport trunk mode on
channel mode active
```

D)

```
int port-channel 100
switchport mode e
switchport trunk mode on
channel mode active
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: A

Explanation:

When configuring the connection between a Cisco MDS 9700 Series Multilayer Director and a Cisco Nexus 5672UP switch, it's important to consider the following:

Ensure compatibility: Verify that both devices are running compatible NX-OS versions to ensure they can communicate properly.

Configure interfaces: Set up the interfaces on both devices with the appropriate type (E, F, or TE), speed, and other relevant settings.

Establish connectivity: Use the show interface command to confirm that the interfaces are up and the show flogi database command to verify that the Fibre Channel login has been successful.

Zoning configuration: Configure zoning on the MDS 9700 to control access between devices connected to the fabric.

VSAN setup: Ensure that the Virtual Storage Area Network (VSAN) is correctly configured and that both switches are part of the same VSAN if required for the topology.

Reference:

Cisco MDS 9700 Series Multilayer Directors documentation1.

Cisco Nexus 5672UP switch documentation

Question: 416

Cisco Nexus 9000 Series Switches are configured with LACP protocol and default aging timers. What is the impact on the LACP peer during an ISSU upgrade?

A. The LACP peer connection terminates.

B. The LACP peer session remains up.

C. The LACP peer renegotiates the adjacency.

D. The LACP peer connection resets.

Answer: B

Explanation:

During an In-Service Software Upgrade (ISSU) on Cisco Nexus 9000 Series Switches, the LACP peer session is designed to remain up without any renegotiation or reset. This is because ISSU is a process that allows for software upgrades without disrupting the normal operation of the network. The default LACP timers and the ISSU process are designed to work together to maintain the session state even during the upgrade process. The Nexus upgrade process will force the chassis itself to upgrade disruptively if LACP fast is used, which is not the default setting. A disruptive upgrade means the chassis itself will fully reload, impacting all ports on the switch, not just the LACP fast ones. However, with the default aging timers, the LACP peer connection should not be affected1.

Reference:

Cisco Nexus 9000 Series NX-OS Software Upgrade and Downgrade Guide2.

Cisco Community discussions on LACP and ISSU impact

Question: 417

A network architect must design an automation solution to initially support networking and also support the server infrastructure in the future. To keep configuration consistency, the network team requires a solution that enforces the desired state of the network and reverts any manual configuration. Which solution meets these goals?

A. NX-API

B. Ansible

C. Terraform

D. Puppet

Answer: C

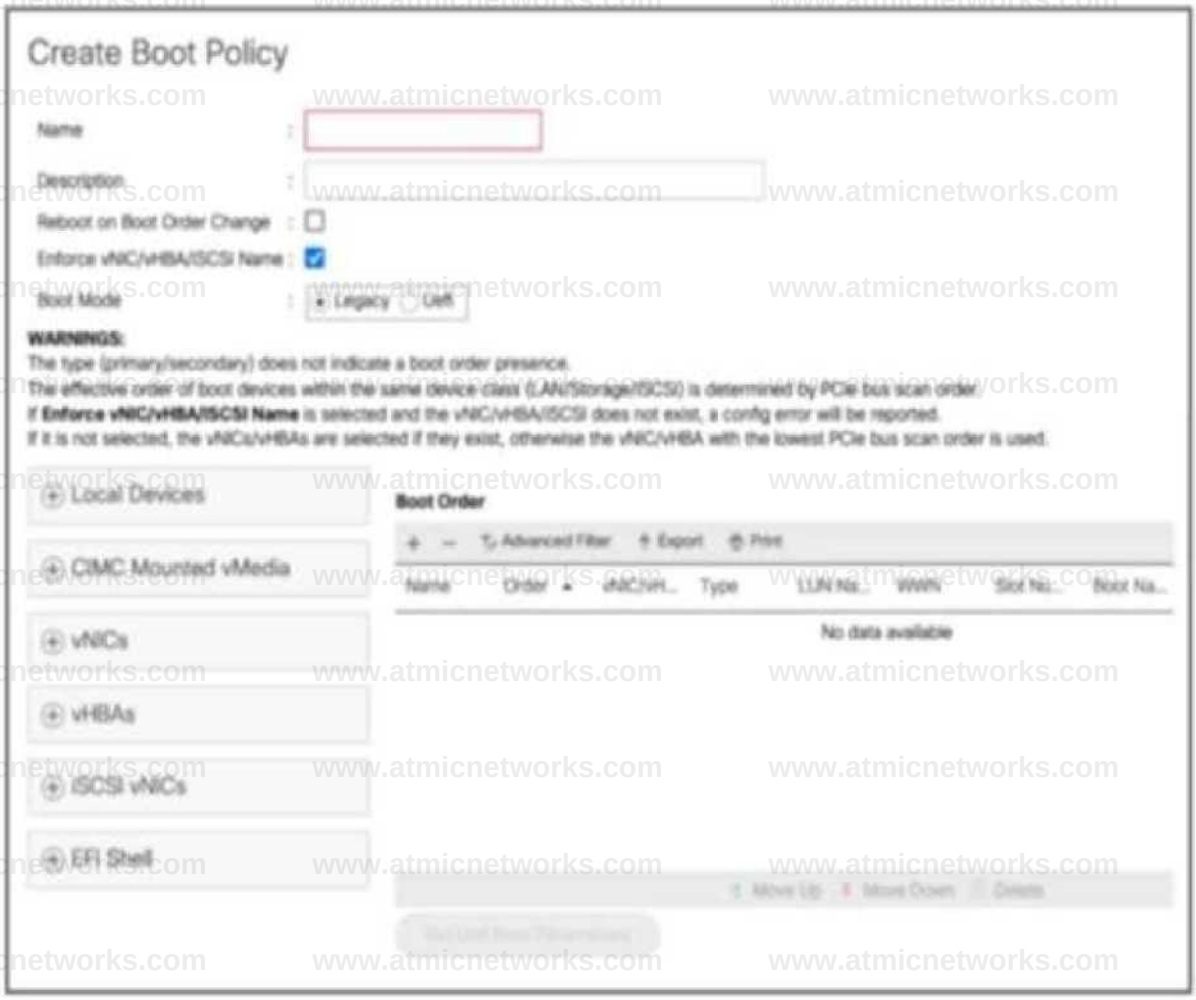
Explanation:

Terraform is an infrastructure as code (IaC) tool that allows users to define both cloud and onpremises resources in human-readable configuration files that can be versioned, reused, and shared. In the context of Cisco Data Center Core Technologies, Terraform can be used to enforce the desired state of the network by automatically managing, updating, and reverting configurations as needed to maintain consistency. It supports a wide range of Cisco products and can be extended to manage server infrastructure in the future.

Reference: The Implementing and Operating Cisco Data Center Core Technologies (DCCOR) course provides insights into the essentials of automation and security in data centers, including the use of IaC tools like Terraform for enforcing desired state configuration1. Additionally, the Implementing Automation for Cisco Data Center Solutions (DCAUI) course further explores the implementation of automation solutions, including Terraform, in Cisco data centers2

Question: 418

Refer to the exhibit.



An engineer installs a new Cisco UCS B-Series server. The requirement is to install an operating system on a LUN that is provided by the Fibre Channel storage array. Which two steps must be configured in the boot policy to accomplish this goal? (Choose two.)

A. Disable Enforce vNIC^HBA/ISCSI Name

B. Add Local CD/DVD and SAN Boot.

C. Configure a SAN Boot Target with a WWPN

D. Set Boot Order to External USB and LAN Boot

E. Create (SCSI VNICs and add Local LUN

Answer: B, C

Explanation:

To install an operating system on a LUN provided by the Fibre Channel storage array, the engineer needs to configure the

boot policy to include a SAN Boot Target with a WWPN (World Wide Port Name). This ensures that the server can communicate with the specific LUN on the storage array during the boot process. Additionally, adding Local CD/DVD and SAN Boot in the boot policy provides flexibility for installation sources, ensuring that both local and networked storage options are available during boot. Reference := Cisco Data Center Core Technologies source documents or study guide

Question: 419

An engineer must perform a POAP deployment of a Cisco Nexus 9000 Series Switch The switch must automatically receive its software image and configuration file upon power-on. Also, only UDP is permitted between the Nexus 9000 switch and the server that hosts the Cisco NX-OS system images Which set of actions completes the configuration'

A. Enable option 67. Define TFTP transfer protocol

B. Enable option 43 Define HTTP transfer protocol.

C. Enable option 46. Define TFTP transfer protocol

D. Enable option 35. Define HTTP transfer protocol.

Answer: A

Explanation:

PowerOn Auto Provisioning (POAP) on Cisco Nexus 9000 Series Switches automates the process of upgrading software images and installing configuration files on devices being deployed for the first time. When a device with POAP boots without a startup configuration, it enters POAP mode, locates a DHCP server, and bootstraps itself with its interface IP address, gateway, and DNS server IP addresses. The device also obtains the IP address of a TFTP server and downloads a configuration script that enables the switch to download and install the appropriate software image and configuration file. Since only UDP is permitted between the Nexus 9000 switch and the server hosting the Cisco NX-OS system images, the TFTP transfer protocol, which uses UDP, must be defined1.

Reference:

Cisco Nexus 9000 Series NX-OS Fundamentals Configuration Guide, which details the use of POAP and the requirements for network infrastructure including a DHCP server and a TFTP server

Question: 420

An engineer must integrate Cisco ACI with a VMware vSphere environment. The requirement is to use a VMware Distributed Virtual Switch and to assign the encapsulation VLAN of the EPG from the VLAN pool. Which configuration set accomplishes this goa?

A. Create a VMM domain association under the EPGs Create a VLAN pool with static alocated VLANs.

B. Create a physical domain association under the EPGs Create a VLAN pool with static alocated VLANs.

C. Create a physical domain association under the EPGs. Create a VLAN pool with oVnarmc alocated VLANs

D. Create a VMM domain association under the EPGs Create a VLAN pool with dynamic alocated VLANs.

Answer: D

Explanation:

In Cisco ACI, integrating with a VMware vSphere environment using a VMware Distributed Virtual Switch (DVS) requires creating a Virtual Machine Manager (VMM) domain association under the Endpoint Groups (EPGs). This allows the ACI fabric to extend its policy model to the virtual environment managed by vSphere. The encapsulation VLAN of the EPG is then assigned from a VLAN pool. To ensure that the VLANs are dynamically allocated and can be managed efficiently, a VLAN pool with dynamic allocation should be used. This setup allows for automated management of VLANs and avoids conflicts or manual errors in VLAN assignment12.

Reference:

Cisco ACI with VMware VDS Integration documentation1.

Cisco ACI Virtualization Guide

Question: 421

An engineer must allow communication between the APIC controller and an OpenStack OpFlex agent. The agent is running on a compute node directly plugged to a Cisco ACI leaf switch. The engineer must enable and extend Infra VLAN

on the port facing the compute and extend the Infra VLAN to the host. Which action must be taken to meet these requirements?

A. Enable the Infra VLAN on the Interface Profile policy

B. Enable the Infra VLAN on the Attachable Access Entity Profile.

C. Add the infra VLAN via the physical domain.

D. Add the infra VLAN via the VMM domain.

Answer: B

Explanation:

To facilitate communication between the APIC controller and an OpenStack OpFlex agent, it's necessary to enable the Infra VLAN on the Attachable Access Entity Profile (AAEP). The AAEP is used in Cisco ACI to group interfaces that share common policies and extending the Infra VLAN to these interfaces allows the OpFlex agent, which is part of the Cisco Application Centric Infrastructure (ACI), to communicate with the APIC controller. This setup is crucial for the OpFlex agent to function correctly, as it relies on the Infra VLAN for communication with the APIC controller1.

Reference:

Cisco ACI Installation Guide for Red Hat OpenStack Using the OpenStack Platform 13 Director1.

Cisco ACI Installation Guide for Red Hat OpenStack Using the OpenStack Platform 16.1 Director

Question: 422

Refer to the exhibit.

```
Switch1# show checkpoint summary
1) pim-checkpoint:
Created by admin
Created at Tue, 00:50:29 22 Jun 2021
Size is 24,855 bytes
User Checkpoint Summary
--------------------------------------------------------------------------------
Description: Created by Admin.

2) system-fm-pim:
Created by admin
Created at Tue, 00:08:57 22 Jun 2021
Size is 24,834 bytes
System Checkpoint Summary
--------------------------------------------------------------------------------
Description: Created by Feature Manager.
```

Which command must be used to restore configuration changes made by disabling the PIM feature and skipping any errors?

Refer to the exhibit. Which command must be used to restore configuration changes made by disabling the PIM feature and skipping any errors?

A. rollback running-config checkpoint new-checkpoint stop-at-first-failure

B. rollback running-config checkpoint new-checkpoint verbose

C. rollback running-config checkpoint system-fm-pim-best-effort

D. rollback running-config checkpoint system-fm-pim atomic

Answer: C

Explanation:

The command rollback running-config checkpoint system-fm-pim-best-effort is used to restore the configuration changes made by disabling the PIM feature and skipping any errors. In Cisco Data Center Core Technologies, it's essential to understand that rollback is a feature that allows administrators to take a snapshot of the configuration before making changes, so they can quickly roll back if needed. The system-fm-pim-best-effort option ensures that the rollback occurs even if there are errors encountered during the process, ensuring that as much of the previous state is restored as possible.

Reference:

Cisco Nexus: Configuration Rollback Overview and Guidelines1.

IP Multicast: PIM Configuration Guide

Question: 423

An engineer troubleshoots an Fibre Channel deployment on a Cisco MDS 9000 Series Switch. What does this output indicate about port channel 1?

```
mds9509# show int po1
port-channel 1 is trunking
  Hardware is Fibre Channel
  Port WWN Is 24:01:00:0d:ec:20:ba:00
  Admin port mode Is F, trunk mode Is on
  snmp link state traps are enabled
  Port mode is TF
  Port vsan is 1
  Speed is 8 Gbps
  Trunk vsans (admin allowed and active) (1,20)
  Trunk vsans (up) (1,20)
  Trunk vsans (isolated) ()
  Trunk vsans (initializing) ()
  5 minutes input rate 112 bits/sec, 14 bytes/sec, 0 frames/sec
  5 minutes output rate 152 bits/sec, 19 bytes/sec, 0 frames/sec 25787798 frames
    input, 14359038212 bytes
      0 discards, 0 errors
      0 CRC, 0 unknown class
      0 too long, 0 too short
    23082 frames output, 1013152 bytes
      0 discards, 0 errors
    18 input OLS, 14 LRR, 29 NOS, 0 loop inits
    17 output OLS, 0 LRR, 21 NOS, 0 loop Inits
  Member[1]: fc4/2
  Member[2]: fc4/8
  Interface last changed at Thu Mar 6 06:27:36 2020
```

A. Port channel1 is configured to be an ISL.

B. Port channel1 is configured to connect to a host bus adapter.

C. Port channel1 is configured to connect to anNPIV switch.

D. Port channel1 is configured to connect to anNPV switch.

Answer: A

Explanation:

The output indicates that port channel 1 is trunking, which means it is configured to be an InterSwitch Link (ISL). ISLs are

used in Fibre Channel networks to connect switches and maintain the fabric topology. The “port mode is F” in the output also confirms that it’s an ISL, as F-ports are used for Fabric (switch) ports connecting to N-ports on another switch or node.

Reference:

Cisco MDS 9000 Series Switches Configuration Guides

Cisco Data Center Infrastructure - Design Guide

Question: 424

Which component is upgraded by using an EPLD upgrade on a Cisco Nexus 9000 Series Switch?

A. dual-homed fabric extenders

B. BIOS

C. field-programmable gate arrays

D. ISSU of the NX-OS version

Answer: C

Explanation:

An EPLD (Electronic Programmable Logic Device) upgrade on a Cisco Nexus 9000 Series Switch is used to upgrade the field-programmable gate arrays (FPGAs). FPGAs are integrated circuits that can be configured by a customer or a designer after manufacturing – hence “field-programmable”. They are used in Cisco switches to provide hardware functionalities in all modules, and EPLD image upgrades enhance hardware functionality or resolve known issues1.

Reference:

Cisco Nexus 9000 Series FPGA/EPLD Upgrade Release Notes

Question: 425

An engineer deploys a new Cisco Nexus 5000 Series Switch in an existing environment with strict security policies. The new device should meet these requirements:

Secure end-user ports with minimum configuration effort.

Log security breaches and require manual recovery.

Retain the switch configuration if the device restarts.

Which configuration must be used?

A.

```
switchport port-security
switchport port-security max 1
switchport port-security violation shutdown
```

B.

```
switchport port-security .
switchport port-security violation shutdown
switchport port-security mac-address dynamic
```

C.

```
switchport port-security
switchport port-security max 1
switchport port-security mac-address sticky
```

D.

```
switchport port-security
switchport port-security violation restrict
switchport port-security mac-address sticky
```

Answer: C

Explanation:

The configuration in option C, which includes commands such as switchport port-security, switchport port-security violation restrict, and switchport port-security mac-address sticky, meets the security requirements specified. This configuration secures the end-user ports by limiting the number of MAC addresses allowed on the port, logs security breaches without shutting down the port (restrict mode), and retains the MAC address configuration even if the device restarts (sticky option).

Reference:

Cisco Nexus 5000 Series NX-OS Security Configuration Guide

Cisco Data Center Core Technologies (DCCOR) study materials

Question: 426

An engineer must perform backup and restore of the Cisco UCS Manager configuration. The configuration must be stored on a remote server via XML encoding. The backup must store the configurations of the chassis. FEX, rack servers. lOMs, and blade server. Which set of actions accomplishes these goals?

A. Perform a logical configuration backup and run the replace import method.

B. Perform a ful state configuration backup and run the restore procedure.

C. Perform a system configuration backup and run the merge import method

D. Perform an all configuration backup and run the system restore procedure.

Answer: B

Explanation:

A full state configuration backup in Cisco UCS Manager includes a snapshot of the entire system, which is stored as a binary file. This backup type is ideal for disaster recovery as it can restore or rebuild the configuration on the original fabric interconnect or recreate the configuration on a different fabric interconnect. It is important to note that this backup type cannot be used for an import but is specifically designed for system restoration.

Reference:

Cisco's official documentation on "Backing Up and Restoring the Configuration" provides a detailed

guide on the backup types and procedures within Cisco UCS Manager1.

The "Cisco UCS Manager Administration Management Guide 4.2" further elaborates on backup operations, considerations, and the system restore process

Question: 427

An engineer must optimize ARP responses and reduce unnecessary ARP broadcasts over the VXLAN/EVPN fabric. Which action accomplishes these tasks?

A. Configure ip proxy-arp under the VLAN SVI associated with the VXLAN VNI.

B. Configure ip proxy-arp within the VXLAN VNI configuration under the VTEP NVE interface.

C. Configure suppress-arp within the VXLAN VNI configuration under the VTEP NVE interface.

D. Configure suppress-arp under the VLAN SVI associated with the VXLAN VNI.

Answer: C

Explanation:

ARP suppression is a feature used in VXLAN/EVPN environments to optimize ARP responses and reduce unnecessary ARP broadcasts across the fabric. When ARP suppression is enabled, the local VTEP (VXLAN Tunnel Endpoint) can respond to ARP requests for known IP-to-MAC address bindings, which are learned via the BGP EVPN control plane. This prevents the need for ARP broadcasts to be sent across the entire VXLAN fabric, thus optimizing the ARP response mechanism and reducing broadcast traffic1.

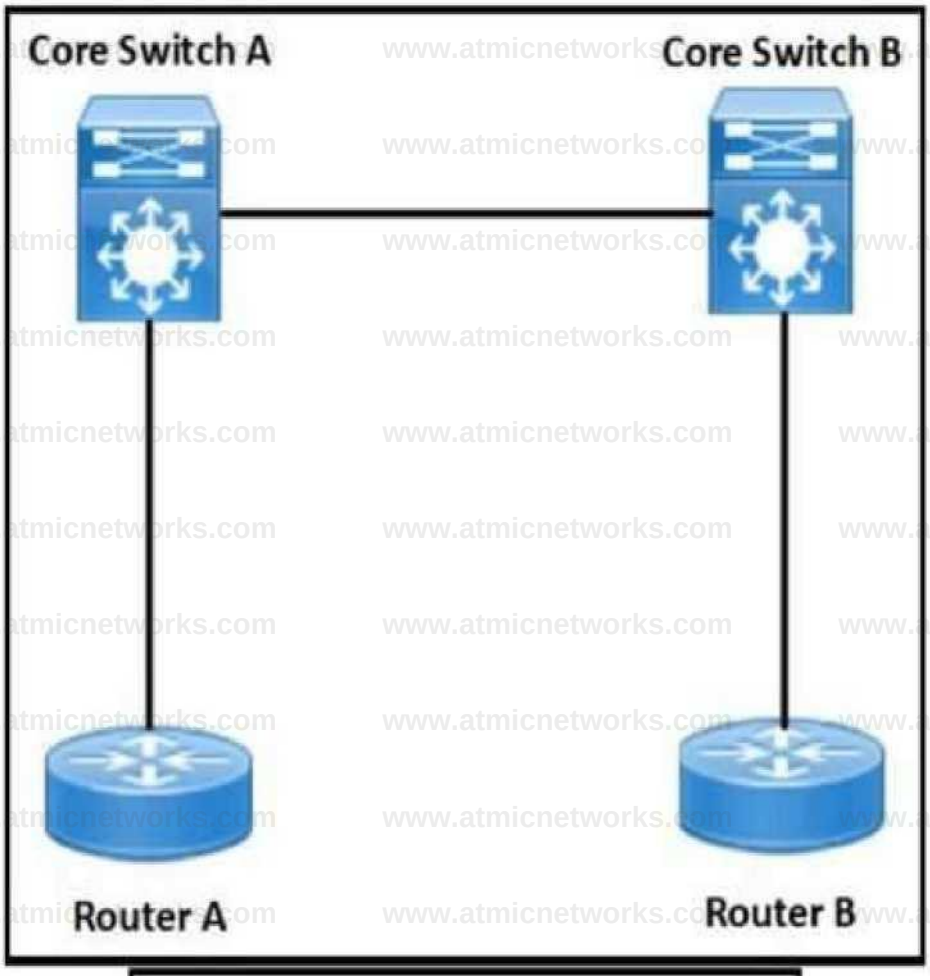
Reference:

Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide2.

Community discussions on ARP suppression in VXLAN/EVPN

Question: 428

Refer to the exhibit.




```
feature vn-segment-vlan-based
feature nv overlay

vlan 10
  vn-segment 10010

Interface Loopback0
   ip address 10.10.0.1/32
   ip pim sparse mode
```

A network engineer configures the VXLAN between the routers in a data center. The VLAN 10 must be extended between routers A and B. The initial VXLAN configuration is completed on Router

A. Which configuration finishes the VXLAN configuration on Router A?

A.

vrf context tenantl vni 10010

Interface nve1 source-Interface loO no shutdown

member vni 10010 interface 10.10.0.1

B.

system bridge-domain 10

member vni 10010 interface nve1 no shutdown source-interface loO

C.

Interface nve1

no shutdown source-interface loO vni 1010012

rd auto

D.

Interface nve1 no shutdown source-interface loO member vni 10010 mcast-group 231.1.1.1

Answer: B

Explanation:

To finish the VXLAN configuration on Router A for extending VLAN 10 between routers A and B, the correct configuration would involve setting up the NVE interface, associating it with the VNI that corresponds to VLAN 10, and specifying the peer VTEP IP address for Router B. This setup will ensure

that the VLAN is extended over the VXLAN tunnel between the two routers.

Reference :=

Cisco Data Center Core Technologies (DCCOR) study materials.

Cisco Nexus 9000 Series NX-OS VXLAN Configuration Guide1.

Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide

Question: 429

Refer to the exhibit.

Refer to the exhibit. An engineer must configure a QoS policy that controls only vHBA traffic. Which policy must be used to meet this requirement?

A. Best Effort

B. Fibre Channel

C. Gold

D. Platinum

Answer: B

Explanation:

The QoS policy that controls only vHBA traffic is the Fibre Channel policy. In Cisco UCS, the Fibre Channel policy is specifically designed to manage the quality of service for traffic related to virtual Host Bus Adapters (vHBAs), which are used for Fibre Channel over Ethernet (FCoE) storage networking. This policy ensures that the storage traffic is appropriately prioritized and managed within the system.

Reference:

Cisco UCS Manager GUI Configuration Guide, which provides details on configuring QoS policies for vHBA traffic.

Cisco Data Center Core Technologies (DCCOR) study materials, which cover the concepts of QoS and vHBA configuration in a Cisco data center environment.

Question: 430

An engineer requires the Cisco Fabric Services to distribute NTP configuration only to the members within the scope of a VSAN that belongs to a Cisco Unified Network. Which scope distribution must be selected to meet this requirement?

A. Logical scope
B. Physical scope
C. Uncoordinated scope
D. Coordinated scope

Answer: A

Explanation:

Cisco Fabric Services (CFS) offers a logical scope distribution mode that allows configurations to be distributed within the scope of a VSAN. This mode is suitable for features like NTP, where the configuration database is applicable only within a VSAN. It ensures that changes are contained within the specific VSAN, preventing any impact on other VSANs in the network.

Reference:

Cisco's official documentation on Configuring and Managing VSANs1 provides a detailed explanation of VSANs, their

advantages, and how they can be managed using CFS.

The Cisco Fabric Services guide2 further elaborates on the features of CFS, including the logical scope distribution mode and its relevance to features like NTP.

Community discussions on NTP configuration3 can also provide practical insights into the application of these settings in real-world scenarios.

Question: 431

A new user with access privileges in the Finance department moves to a new Admin department. The user must have access privileges to the Admin department data and applications inside the Cisco UCS Manager Which set of changes must be implemented in Cisco UCS Central for the user to acquire the privileges?

A. Create an Admin user account and remove the authentication service for the Finance privileges.

B. Disable the Finance user account and add the authentication service for the Admin privileges.

C. Create a new locale Admin and add the Admin department to the Admin locale. Delete the old locale

D. Finance and remove the Finance department from the Finance locale.

Answer: C

Explanation:

In Cisco UCS Central, user privileges are managed through roles and locales. When a user moves departments, their access privileges need to be updated to reflect their new role. By creating a new locale for the Admin department and adding the user to this locale, the user's access privileges are updated to include the Admin department's data and applications. The old Finance locale should be deleted, or the user should be removed from it, to revoke the previous access privileges1.

Reference:

Cisco UCS Central Administration Guide1.

Cisco UCS Central User Accounts and Role-Based Access Control Overview2.

Assigning User Privileges in Cisco UCS documentation

Question: 432

A network engineer must download a firmware image from a remote location to a Cisco UCS Fabric Interconnect. The software bundle is over 232 MB in size. The file transfer must use encryption and authentication Which protocol must be used to accomplish this goal?

A. RDP

B. HTTPS

C. SCP

D. TFTP

Answer: B

Explanation:

When downloading a firmware image to a Cisco UCS Fabric Interconnect, especially from a remote location, it is crucial to use a protocol that provides both encryption and authentication to ensure the security and integrity of the file transfer. HTTPS (Hypertext Transfer Protocol Secure) is the protocol that meets these requirements. It is widely used for secure communication over a computer network within a web browser, with encryption provided by Transport Layer Security (TLS), which ensures that the transfer of the firmware image is secure and authenticated1.

Reference:

Cisco UCS Manager Firmware Management Guide, which provides detailed instructions on managing firmware through UCS Manager, including downloading firmware images to the Fabric Interconnect

Question: 433

A network engineer must configure a Fibre Channel interface on the Cisco MDS 9000 Series Switch The configuration must meet these requirements

- The interface must be disabled when the bit errors threshold Is exceeded
- Buffer-to-buffer credits must be set to the maximum value

- The interface must have full bandwidth allocated for its port group

Which command set configures a Fibre Channel interface that meets these requirements?

A.

```
interface fc1/1
switchport bit-errors
switchport fcrxbbcredit 220 mode Fx
switchport rate-mode dedicated
```

B.

```
interface fc1/1
switchport ignore bit-errors
switchport fcrxbbcredit 255 mode Fx no switchport rate-mode
```

C.

```
interface fc1/1
no switchport ignore bit-errors switchport fcrxbbcredit 255 mode Fx switchport rate-mode dedicated
```

D.

```
interface fcl/1
no switchport bit-errors
switchport fcrxbbcredit 220 mode Fx
no switchport rate-mode
```

Answer: A

Explanation:

The command set in option A is the correct one for configuring a Fibre Channel interface on the Cisco MDS 9000 Series Switch to meet the specified requirements. The “no switchport bit-errors” command ensures that the interface is disabled when the bit errors threshold is exceeded. The “switchport fcrxbbcredit 220 mode Fx” command sets buffer-to-buffer credits to their maximum value, ensuring optimal performance and flow control. Lastly, “no switchport rate-mode” ensures that the interface has full bandwidth allocated for its port group, maximizing data throughput and efficiency.

Reference:

Cisco MDS 9000 Series Fabric Switches Configuration Guide

Cisco Data Center Core Technologies (DCCOR) study materials

Question: 434

Refer to the exhibit.

An engineer must set access to Cisco IMC. The access must be allowed by logging onto the https //datacenter local web page The configuration presented is on the Cisco UCS C240 Series Server Which set of commands completes the configuration?

A)

```
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 *# set dns-use-dhcp-enabled yes
Server /cimc/network *# commit
```

B)

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 192.168.1.10
Server /cimc/network *# set v4-netmask 255.255.255.0
Server /cimc/network *# set v4-gateway 192.168.1.12
Server /cimc/network *# commit
```

C)

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 192.168.1.10
Server /cimc/network *# set v4-netmask 255.255.255.0
Server /cimc/network *# set preferred-dns-server 192.168.3.20
Server /cimc/network *# commit
```

D)

```
♦ scope else
/ci®- ♦ scope network
, *m . n-tw < ♦ set vlan-enabled yes is n. w . •• set vlan-id 10
j in .' *w < H set vlan-priority 32 in n w '♦ set preferred-dns-server
  192.168.3.20
```

/ c 1® ' / n * w > r I • I coeeu t

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

To set access to Cisco IMC (Integrated Management Controller) and allow logging onto the https://datacenter.local web page, the correct set of commands is found in option C. These commands will configure the network settings on the Cisco UCS C240 Series Server to enable web access to the Cisco IMC interface. The configuration typically involves setting the correct IP address, gateway, and other network parameters that align with the data center's network design.

Reference :=

Cisco UCS C-Series Servers Integrated Management Controller CLI Configuration Guide

Cisco Data Center Core Technologies (DCCOR) study materials

Question: 435

```
switchllshow run interface Vian 10

interface vianlO
 description Service Datacenter-Rack-A ip address
 209.165.200.225 255.255.255.224

end
switchlI
```

Refer to the exhibit An engineer must mirror the traffic on a switch The engineer locates the server port that requires monitoring on switch1, but the packet sniffer is on switch2 The engineer must configure the source IP address on switch1 Much command accomplishes this goal?

A. monitor session 10 type erspan-source

B. monitor erspon origin ip-address 209.165.200.225

C. source ip 209.165.200.225

D. source interface vbn512

Answer: B

Explanation:

The correct command to configure the source IP address on switch1 for mirroring traffic to a packet sniffer located on switch2 is option B, “monitor erspan origin ip-address 209.165.200.225”. This command sets the origin IP address for the Encapsulated Remote SPAN (ERSPAN) session, which allows traffic from a source port on one switch to be monitored on a destination port on another
switch across an IP network.

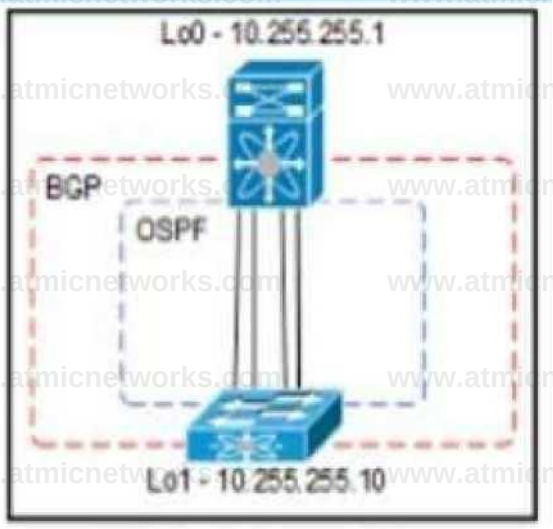
Reference:

Cisco Nexus 9000 Series NX-OS System Management Configuration Guide

Cisco Data Center Core Technologies (DCCOR) study materials

Question: 436

DRAG DROP



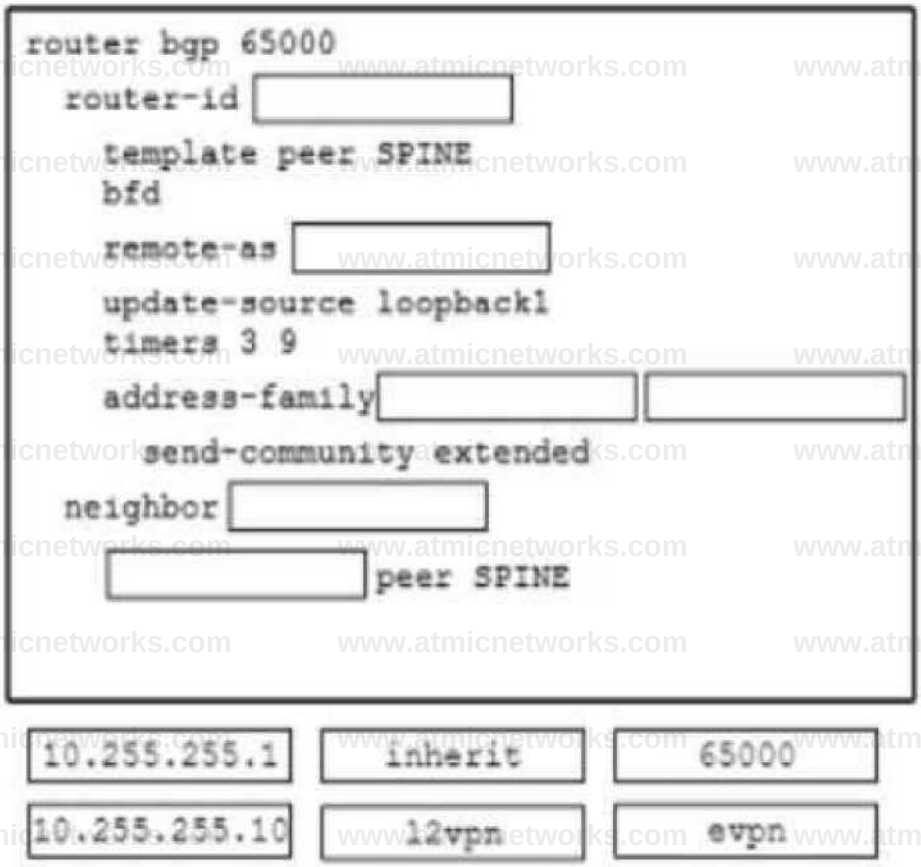
Refer to the exhibit An engineer must provision a VXLAN deployment The OSPF has already been configured as the underlay protocol All BGP configurations will be performed using the template method The deployment must meet these requirements

The local update source for leaf switches must be loopback 1

The router ID must be the local loopback IP address

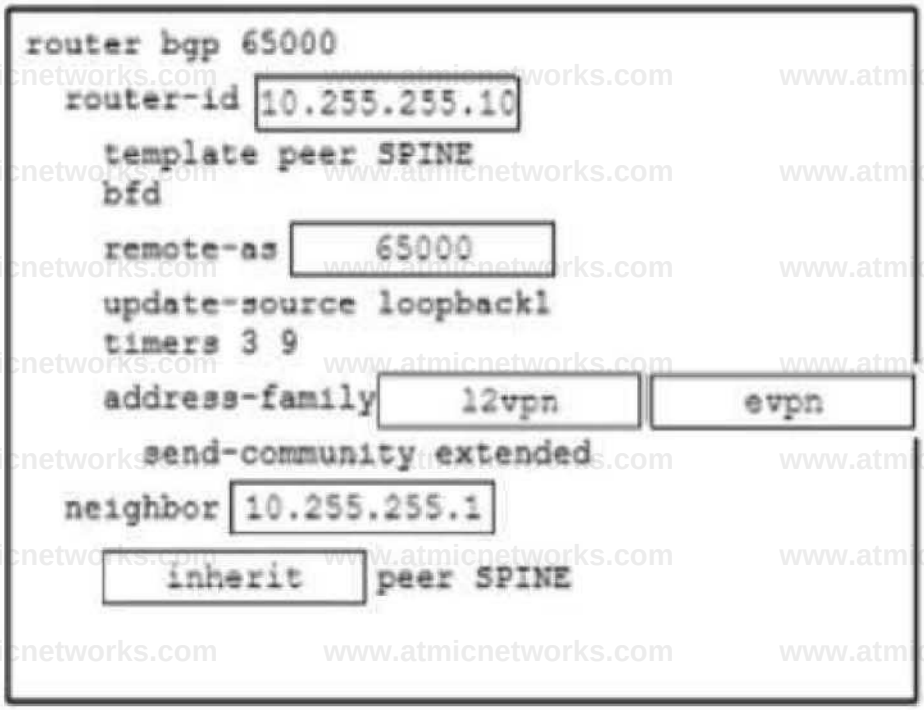
The external BGP connections must use a template name

Drag and drop the configuration snippets from the bottom to complete the configuration



Answer:

Explanation:



Question: 437

DRAG DROP

Drag and drop the NAS and NFS concepts from the left onto the definitions on the right.

Answer:

Explanation:

NFS

Data storage and file sharing requests are sent and received

The protocol is regularly used on Linux segment

NAS

Software is deployed on a lightweight OS that is embedded in the hardware

The vendor-agnostic protocol is supported on any hardware and OS

Question: 438

An engineer is implementing the Cisco ACI fabric and wants to reduce the amount of TCAM resources consumed by the fabric The engineer also needs to ensure that all EPGs m a VRF consume the same services Which action should be taken to meet these requirements?

A. Configure a single contract provided and consumed in all EPGs

B. Configure preferred groups in the VRF for al EPGs

C. Implement an unenforced VRF

D. Implement vzAny feature

Answer: A

Explanation:

In Cisco ACI, TCAM resources can be optimized by configuring a single contract that is provided and consumed by all EPGs within a VRF. This approach ensures that all EPGs consume the same services, thus reducing the number of individual contracts and associated TCAM entries. By having a common contract, the ACI fabric can efficiently manage access control policies and service insertion without the need for multiple, redundant entries in the TCAM, which can lead to resource exhaustion. Reference: The information is based on the best practices for TCAM management in Cisco ACI fabrics, as detailed in the Cisco community discussions and Cisco's official documentation on TCAM resource issues and workarounds12. Additionally, the concept of using a single contract for multiple EPGs is supported by the Cisco ACI Endpoint Security Group (ESG) Design Guide, which outlines the steps for implementing a single ESG for open communication between subnets (EPG

selectors)

Question: 439

An engineer must deploy a Cisco UCS C-Series Server with a single VIC 1455 integrated into a Cisco UCS Manager cluster. Two fiber connections

are available, and the deployment has no fabric extenders. Which set of actions accomplishes this goal?

A.

Reset the system using Cisco IMC to its factory default settings.

Attach VIC port 1 and 3 to Fabric Interconnects.

B.

Configure VIC attached ports as Uplink ports on fabric interconnects.

Insert 1000Base-T RJ45 SFP in VIC port 1 and 3.

C.

Reset the system using Cisco IMC to its factory default settings.

Insert 1000Base-T RJ45 SFP in VIC port 1 and 3.

D.

Configure VIC attached ports as Uplink ports on fabric interconnects.

Attach VIC port 1 and 3 to Fabric Interconnects.

Answer: A

Explanation:

To deploy a Cisco UCS C-Series Server with a single VIC 1455 integrated into a Cisco UCS Manager cluster without fabric extenders, the system should be reset to factory default settings using Cisco IMC. After the reset, VIC ports 1 and 3 should be attached to the Fabric Interconnects. This process ensures that the server is recognized by the UCS Manager and can be managed accordingly. The VIC 1455 supports multiple Ethernet and Fiber Channel over Ethernet speeds, making it suitable for direct connection to Fabric Interconnects1.

Reference :=

Cisco UCS VIC 1400 Series Best Practices in Ethernet Fabric White Paper1.

Cisco UCS C-Series Server Integration with Cisco UCS Manager 4.0 documentation2

Question: 440

An engineer must configure device aliases for a Cisco MDS 9000 Series Switches-based SAN fabric. The configuration must meet these requirements:

- The engineer must be prompted before the changes are committed to the database.
- Pending changes must be explicitly displayed on the console.

Which command accomplishes this task?

A. device-alias enhanced

B. device-alias commit

C. device-alias confirm-commit

D. device-alias distribute diffs-only

Answer: C

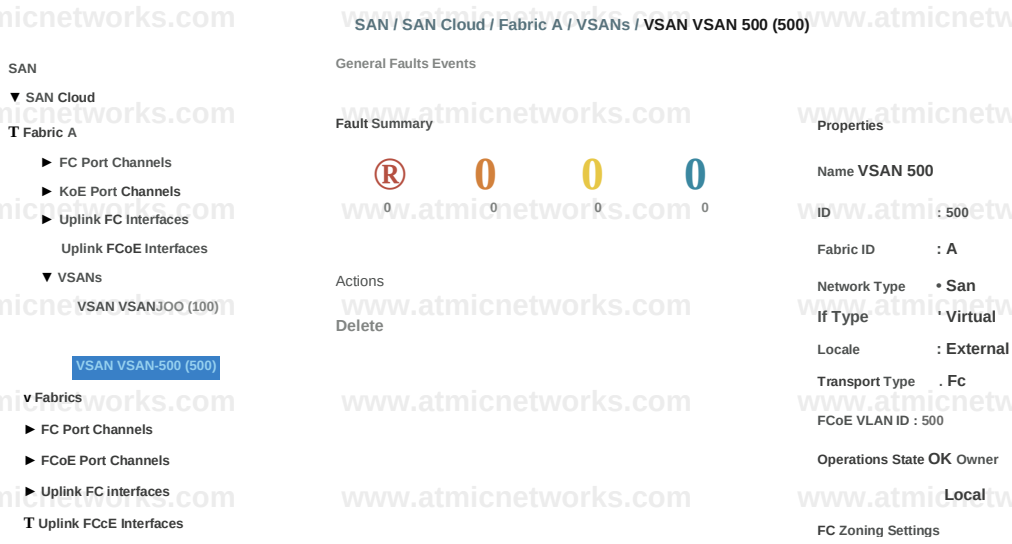
Explanation:

The device-alias confirm-commit command is used in Cisco MDS 9000 Series Switches to ensure that changes made to device aliases are confirmed before being committed to the database. This command prompts the user for confirmation and displays the pending changes explicitly on the console, which aligns with the requirements stated in the question.

Reference: For more detailed information, you would typically refer to the Cisco Data Center Core Technologies study guide or the official Cisco documentation for the MDS 9000 Series.

Question: 441

Refer to the exhibit.



An engineer configures an FCoE connection between a Cisco UCS and a Cisco Nexus 9000 Series Switch. The UCS FI-A

connects to the Nexus switch using interface e1/12. All relevant configurations have been completed on the Nexus switch to support FCoE

deployment. Which action must be taken on Cisco UCS Manager to complete the configuration?

A. Trunk VLAN 500 on interface e1/12.

B. Create a Virtual Fibre Channel Interface.

C. Change the Transport Type to FCoE.

D. Configure an FCoE uplink interface.

Answer: C

Explanation:

In the context of configuring an FCoE connection between a Cisco UCS and a Cisco Nexus 9000 Series Switch, changing the transport type to FCoE in the Cisco UCS Manager is essential. This action ensures that the data traffic is encapsulated using FCoE, enabling seamless communication over Ethernet networks while maintaining Fibre Channel protocol characteristics.

Reference := For more detailed information, you can refer to the Cisco Nexus 5000 Series NX-OS Fibre Channel over Ethernet Configuration Guide1, which provides comprehensive guidelines on configuring FCoE, including the importance of changing the transport type to support FCoE deployment.

Question: 442

An engineer must configure a Cisco MDS 9000 Series Switch to store generated log messages to a file. The file must store logs of the severity of "warning" and above, and the file size must not exceed 20,000 bytes.

Which command accomplishes this task?

A. logging logfile LogFile 5 size 2000

B. logging logfile messages 2 size 2500

C. logging logfile Local 4 size 20000

D. logging logfile Logs 3 size 160000

Answer: C

Explanation:

The command logging logfile Local 4 size 20000 configures the Cisco MDS 9000 Series Switch to store log messages with a severity of “warning” (which corresponds to severity level 4) and above. The size parameter is set to 20000 bytes, which ensures that the log file does not exceed the specified maximum size1.

Reference:

For detailed information on configuring system message logging on Cisco MDS 9000 Family switches, you can refer to the Cisco documentation on system message logging1.

Question: 443

An engineer must configure a Fibre Channel port channel on a Cisco Nexus 9000 Series Switch. The configuration must meet these requirements:

- A port-channel protocol negotiation is performed with the peer ports.
- The trunk mode must be explicitly configured for the interfaces.
- VSANs from 10 to 20 must be allowed.

Which command set configures the devices to meet the requirements?

A.
```
interface port-channel 10
channel mode auto
switchport trunk mode on
switchpoll trunk allowed vsan 10-20
```

B.
```
interface san-port-channel 10
channel mode on
switchport trunk mode on
switchport trunk allowed vsan 10, 20
```

C.
```
interface san-port-channel 10 channel mode active
switchport trunk mode on
switchport trunk allowed vsan 10-20
```

D.
```
interface port-channel 10 channel mode on
switchport trunk mode active switchpoll trunk
allowed vsan 10, 20
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

The command set in Option C is the correct configuration for a Fibre Channel port channel on a Cisco Nexus 9000 Series Switch that meets the specified requirements. The commands in this option perform port-channel protocol negotiation with peer ports using the "channel mode active" command, explicitly configure the trunk mode with "switchport trunk mode on," and allow VSANs from 10 to 20 with "switchport trunk allowed vsan 10-20."

Reference: For further details, you would refer to the Cisco Nexus 9000 Series NX-OS SAN Switching Configuration Guide, which provides instructions on configuring Fibre Channel port channels and related settings.

Question: 444

Refer to the exhibit.

```
switch# show fabric-binding database active vsan 10

Vsan   Logging-in Switch WWN      Domain-id

10     21:00:00:00:00:00:00:10     Any
10     21:00:00:00:00:00:00:20     20
10     21:00:00:00:00:00:00:30     30
[Total 3 entries]
```

An engineer must configure fabric binding on a Cisco MDS 9000 Series Switch to match the output.
Which fabric database configuration accomplishes this goal?

A)

```
CISCOMDS(config)# fabric-binding database vsan 10
CISCOMDS(config-fabric-binding)# swwn 21:00:00:00:00:00:00:10
CISCOMDS(config-fabric-binding)# nwwn 21:00:00:00:00:00:00:20 domain 20
CISCOMDS(config-fabric-binding)# nwwn 21:00:00:00:00:00:00:30 domain 30
```

B)

```
CISCOMDS(contig)♦ vsan database
CISCOMDS(config-vsan-db)♦ swwn 21:00:00:00:00:00:00:10 any
CISCOMDS(config-vsan-db)1 nwwn 21:00:00:00:00:00:00:20 domain 20
CISCOMDS(config-vsan-db)♦ nwwn 21:00:00:00:00:00:00:30 domain 30
```

C)

```
CISCOMDS(config)# vsan database
CISCOMDS(config-vsan-db)# swwn 21:00:00:00:00:00:00:10
CISCOMDS(config-vsan-db)# nwwn 21:00:00:00:00:00:00:20 domain 20
CISCOMDS(config-vsan-db)# nwwn 21:00:00:00:00:00:00:30 domain 30
```

D)

```
CISCOMDS(config)I fabric-binding database vsan 10
CISCOMDS(config-fabric-binding)i swwn 21:00:00:00:00:00:00:10 domain any
CISCOMDS(config-fabric-binding)9 nwwn 21:00:00:00:00:00:00:20 domain 20
CISCOMDS(config-fabric-binding)t nwwn 21:00:00:00:00:00:00:30 domain 30
```

A. Option A

B. Option B

C. Option C

D. Option D

Answer: C

Explanation:

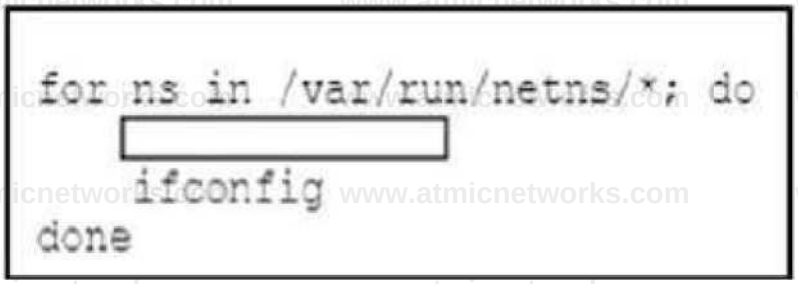
The correct answer is option C. The fabric binding configuration in option C matches the output required for the Cisco MDS 9000 Series Switch. Fabric binding enhances the security of the SAN fabric by allowing only authorized switches to join the fabric. The configuration includes specifying the switch world wide name (swwn), domain ID, and member world wide node name (nwwn) to ensure

that only the specified devices can participate in the fabric.

Reference: For more information on fabric binding and its configuration, you can refer to the Cisco MDS 9000 Series Fabric Switches Configuration Guide and the Implementing and Operating Cisco Data Center Core Technologies (DCCOR) study materials.

Question: 445

Refer to the exhibit.



An engineer must create a Bash script to run in the Cisco NX-OS Guest Shell. The script must loop through the available namespaces and output all registered interfaces. Which code snippet completes the script?

A. chvrf "Sns";

B. echo "$ns";

C. ifconfig "$ns";

D. vrfinfo'Sns";

Answer: C

Explanation:

The Bash script is designed to loop through the available namespaces and output all registered interfaces within the Cisco NX-OS Guest Shell. The correct code snippet to complete the script is option C, ifconfig "$ns". This command will display the network configuration for each namespace, allowing the engineer to view all registered interfaces.

Reference: The use of ifconfig in conjunction with namespace variables is a common practice in network scripting to retrieve interface information. For more detailed information on scripting in Cisco NX-OS, you can

refer to the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Question: 446

An engineer must automate the provisioning of Cisco ACI objects using the Terraform tool. The engineer must ensure that APIC counts the authentication login requests against the threshold to avoid a DOS attack. Which configuration must be used in Terraform to accomplish these goals?

A. resources with user ID and password

B. resources with signature-based authentication

C. provider with user ID and password

D. provider with signature-based authentication

Answer: D

Explanation:

To automate the provisioning of Cisco ACI objects using Terraform while ensuring that APIC counts the authentication login requests against the threshold to avoid a DOS attack, signature-based authentication should be used. This method involves obtaining an authentication token from Cisco APIC, which will use the token to authenticate. However, APIC counts these authentication requests and applies a threshold to prevent DOS attacks. After too many attempts, the user ID and password authentication method may fail as the threshold is exceeded. To circumvent this issue, signaturebased authentication is recommended, where a signature is calculated using a private key and passed with the request. This signature is then used to authenticate the user without being counted against the threshold, thus avoiding the risk of exceeding it and failing authentication.

Reference: The information is based on the Terraform documentation provided by CiscoDevNet

Question: 447

Refer to the exhibit.

```
1  configure terminal
2  scheduler job name SACKUF_J05
3  cli eery runr.inc-ccnfig bootflash:/S (NAhE) .$ (TDESTAMF) .c
4  exit
5  scheduler schedule name BACKUP_SCHEDULE ' job name BACKUP JOB
                r
```

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

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.

Reference: This explanation is based on the Cisco NX-OS documentation, which provides guidelines on how to schedule tasks using the NX-OS scheduler feature. The documentation is part of the Cisco Data Center Core Technologies study materials.

Question: 448

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 I Get-UcsVlan -name SVLAN I Remove-
ucsvianMemberPorr -swirchld 3 -Slotld 1 - Portld 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
```

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.

Reference: The explanation is based on the Cisco UCS Manager PowerShell module documentation, which provides details on scripting and automation capabilities for managing Cisco UCS environments.

Question: 449

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?

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 the nxapi certificate enable command is crucial as it activates the uploaded certificate, which is necessary for establishing secure HTTPS connections.

Reference: The configuration guidelines are based on the Cisco Nexus 9000 Series NX-OS Programmability Guide, which details the steps for enabling and configuring NX-API REST and DME database on Cisco Nexus switches1.

Question: 450

Refer to the exhibit.

```
switch(config)I vlan access-map span filter 5
switch(config-access-map)I natch ip address match_Server_pkts switch(contig-
access-nap)I 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 ca ptures the traffic?

A.

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. The monitor session command is then used to apply this access list to a SPAN session, ensuring that only traffic from the specified server is captured.

Question: 451

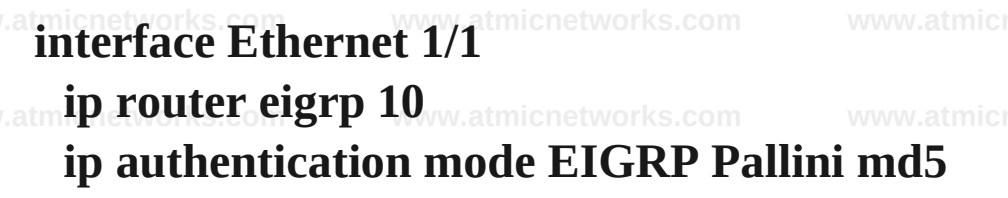
Refer to the exhibit.

```
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)

B)



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.

Reference: = For further details, you can refer to the official Cisco documentation on EIGRP authentication and configuration for Nexus switches available on the Cisco website.

Question: 452

DRAG DROP

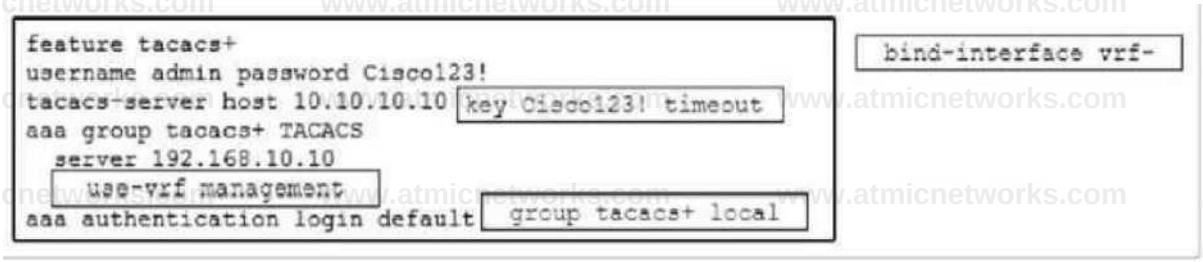
All logins to a Cisco Nexus 9000 Series Switch must pass through the TACACS+ server at IP address 192.168.10.10. The configuration must meet these requirements:

- 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.

Answer:

Explanation:



Question: 453

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?

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.

Reference: The configuration approach is based on best practices for enabling jumbo frames on Cisco UCS blades, as described in the Cisco documentation1. The MTU size of 9216 bytes is commonly used in data center environments to enable jumbo frames

Question: 454

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.)

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. The Operations role allows for the modification of operational aspects such as logs and power management, while the Administrator role provides full access to all configurations and settings within the UCS domain1.

Reference: = For more detailed information on user roles and permissions in Cisco UCS, you can refer to the Cisco UCS Manager Administration Management Guide2 and other official Cisco documentation1.

Question: 455

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?

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.

E. 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.

Reference: = For a more in-depth understanding of multicast traffic flow in a vPC environment, you can refer to Cisco's official documentation on multicast forwarding in vPC based on the location of the source1, as well as community discussions and technical articles available on the Cisco Community website

Question: 456

Refer to the exhibit.

```
WARNING; Retrying (Retry(total-0, connect-Hone, read—None, rcdircct-Nonc, status-
Nene)) after connection broken by
•NcwConnccticnExror(* <pip._vendor.urliib3.connection.ETTPSConnccticn object at
0x7f5b537c8£10>: 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?

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 command sudo chvrf management pip install Markdown to install the package within the management Virtual Routing and Forwarding (VRF) context, which has access to the internet.

Reference: = For more information on managing packages in the guest shell of Cisco Nexus switches, refer to the Cisco Nexus 9000 Series NX-OS Programmability Guide.

Question: 457

Refer to the exhibit.

The UW< Moa lint the loin loppMVdkyCiKaDCSV

Rak	llwripiM
pl-Aal-adma	tawduccd m Caen Neem 5000 scran ranches nd FCaE, a tote In nImtrmtraic LAS mi SAN features
nctu cd-adorn	General rek to admizmsaic LAN features
las-ncriarrk -adxan	General rate to adminmrate LAN features
sxmetwark-adKin	General rok to admirrttralc SAN featim
un-afoun	iHsnduccd in Cisco Nexus SOW senes switches and F CoE. a role to adnunenase SAN features
sen er-adoni	t ratsMuccd tn the 1 IcxAttach feature. a role that adnuratfriie* FC sen er host feature
\r?K'Attain	bemdueed tn the Storage Media F*rxptaMi (SME) feature, a tele that adnmntram SME feature
unc-stg-adnuo	hnraduccd in the Storage Media Eacnpram (SME)) feature, a role that aJnuruMxato SME Murage
*rx-lnK-admin	Ltccvduccd in Ac Storage Media Eacnptaun (SME) feature a rok that adntaatraio SME Lex Matugemea:
tmereruven	kosdnetd in the Storage Media Incnphen (SME) feature, a role that adnrar.i rates SME rAiu.cn
DCtUVd<pCt3ta>(	General net* cd. operator role
dnKX-q*g admin	11m role n added to pederm cpcratioas oeh in loupe Management utndcm
acecm-abnia	Um rale n ntruhfeerd to perform operatMitn a Imafoce Manager * nhm far all fabnes

»»«»ft*.-efcnn"™ »•»«>“>

Rata	Perapectna
pduhadme	Adnoa Pcnpcctne
EcOkceGadsui	
tan^adxin	
taa-acT* nA-adnu>	
bo-ncrocrk-adnan | Web Cікм)	
MW .J- n	Sena AAma Penpextrve
HI ,_:-- ri	SME Fanpectroc
unost!-a±ntn	
une-lmc-Ahnia	
unc^cwerj	
rem eel operator	Operator Fcnpocmc
Lm-aonwi-admai SAN Chen: i	
screw-adnta	
dc*icr*«fg'adnuD	

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.)

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 of network operator and access-admin should be assigned. The network-operator role permits device operations within Interface Manager, and the access-admin role is likely to have the necessary permissions to manage user access without exposing sensitive admin and configuration options.

Reference: = For more information on user roles and permissions in Cisco Data Center Network Manager (DCNM), you can refer to the official Cisco documentation and guides related to DCNM user role configuration.

Question: 458

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?

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:

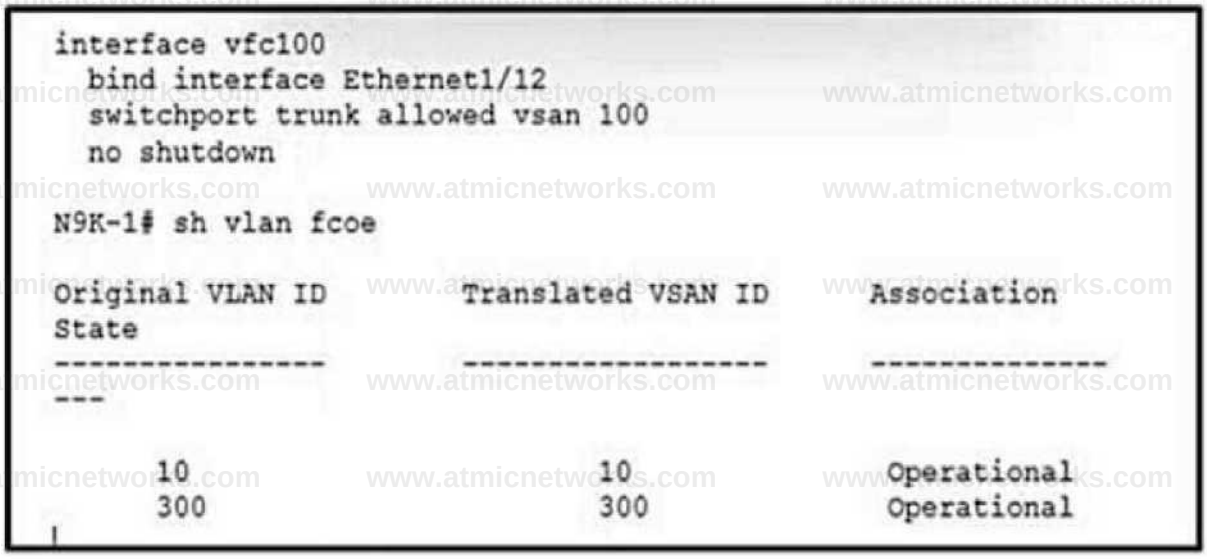
In the context of Cisco Nexus switches, VRF (Virtual Routing and Forwarding) is used to create multiple virtual routing tables within a single switch. By using the default VRF for the scheduler job, the engineer ensures that the TFTP server, which is reachable in the global routing table, can be accessed 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.

Reference: For more detailed information, please refer to the official Cisco documentation for Nexus 3000 Series Switches or the Implementing and Operating Cisco Data Center Core Technologies

(DCCOR) study materials.

Question: 459

Refer to the exhibit.



```
interface vfc100
  bind interface Ethernet1/12
  switchport trunk allowed vsan 100
  no shutdown
N9K-1# sh vlan fcoe

Original VLAN ID        Translated VSAN ID      Association
State
----------------        ------------------      -------------
---

      10                        10                Operational
      300                       300               Operational
```

An engineer configures FCoE in a newly installed data center. Which configuration must be applied to activate VSAN 100 on VFC100?

A. Map an FCoE VLAN to VSAN 100.

B. Allow VSAN 100 on interface eth1/12.

C. Issue the shutdown lan command on VFC 100.

D. Configure a VLAN on VFC 100.

Answer: B

Explanation:

The configuration snippet in the exhibit shows that VSAN 100 is allowed on interface Ethernet1/12 with the command “switchport trunk allowed vsan 100”. This means option B, “Allow VSAN 100 on interface eth1/12”, is the correct answer. In Cisco Data Center Core Technologies, it’s essential to allow specific VSANs on an interface to enable traffic flow for those VSANs.

Reference: Implementing and Operating Cisco Data Center Core Technologies (DCCOR) - Configuring FCoE

Question: 460

An engineer is designing a cloud solution for an organization. The security requirements mandate that the cloud must be hosted in a local data center but leverage the remote data center for remote backups. Additionally, the workloads in the data center must be scaled out to a known cloud provider in the future. Which cloud deployment model must be used to meet these requirements?

A. public cloud

B. hybrid cloud

C. private cloud

D. edge cloud

Answer: B

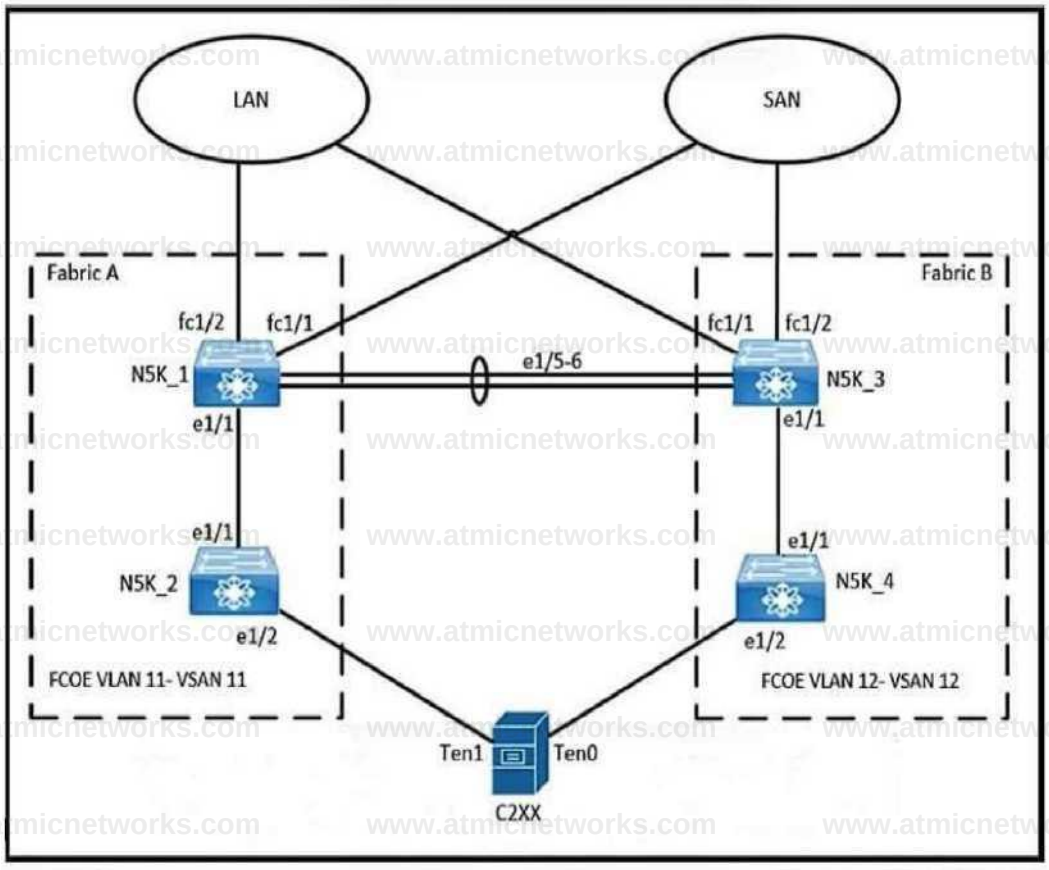
Explanation:

The hybrid cloud model is the most suitable for the described scenario. It allows for a combination of local (private) cloud infrastructure with remote (public) cloud services. This model supports hosting the primary workloads in a local data center, utilizing remote data centers for backups, and provides the flexibility to scale out to a public cloud provider when necessary. The hybrid cloud model offers the benefits of both private and public clouds, including security, scalability, and flexibility, which aligns with the organization's requirements.

Reference: For more information on cloud deployment models and their use cases, you can refer to the Cisco Data Center Core Technologies (DCCOR) study materials or the official Cisco documentation on cloud solutions.

Question: 461

Refer to the exhibit.




```
N5K_1(config)# feature fcoe
N5K1(config)I vlan 100
N5K_1(config)♦ vsan database
N5K_1(config-vsan-db)# vsan 11

N5K_1(config)♦ vlan 11
N5K_1(config-vlan)♦ fcoe vsan 11

N5K_1(config)♦ vlan 100

N5K_1(config)♦ interface ethernet 1/1
N5K_1(config-if)# switchport mode trunk
N5K_1(config-if)♦ switchport trunk allowed vlan 11, 100
N5K_1(config-if)# no shutdown
```

An engineer must configure FCoE with these requirements:

- VLAN 100 must be used to carry the Ethernet traffic.
- Fabric A must use FCoE on VLAN 11 and VSAN11.
- Fabric B must use FCoE on VLAN 12 and VSAN 12.

- vfc 10 on Fabric A must be bound to Ethernet 1/1 on N5K_1.
- vfc 11 on Fabric B must be bound to Ethernet 1/1 on N5K_2.

Which interface vfc 10 configuration accomplishes these requirements?

A)

```
N5K_1(config)# int vfc 10
N5K_1(config-if)# switchport mode sd
N5K_1(config-if)# switchport trunk allowed vsan 11,100
N5K_1(config-if)# bind interface eth 1/1
N5K_1(config-if)# no shutdown
```

B)

```
N5K_1(config)# int vfc 10
N5K_1(config-if)# switchport mode e
N5K_1(config-if)# switchport trunk allowed vsan 11
N5K_1(config-if)# bind interface eth 1/1
N5K_1(config-if)# no shutdown
```

C)

```
N5K_1(config)I int vfc 10
N5K_1(config—if)# switchport mode f
N5K1(config-if)* switchport trunk allowed vlan 11,100
N5K1(config-if)i bind interface eth 1/1
N5K_1(config-if)I no shutdown
```

A. Option A

B. Option B

C. Option C

Answer: A

Explanation:

The configuration for interface vfc 10 that meets the requirements is Option A. This option correctly binds vfc 10 to Ethernet 1/1 on N5K_1, which is part of Fabric A, and allows VLAN 11 for FCoE traffic as well as VLAN 100 for Ethernet traffic. The configuration ensures that VLAN 11 is used for FCoE on VSAN11, which is specific to Fabric A, and also includes VLAN 100 as required for Ethernet traffic.

Reference: = For further details on configuring FCoE and binding virtual fibre channel (vfc) interfaces to physical Ethernet interfaces on Cisco Nexus 5000 Series Switches, you can refer to the Cisco Data Center Core Technologies (DCCOR) study materials or the official Cisco documentation on FCoE configuration.

Question: 462

An engineer must configure port aggregation between two Cisco MDS 9000 Series Switches. The solution must meet these requirements:

- Suspend member interface if parameters mismatch.
- Load-balance traffic on multiple ports.
- Support traffic from multiple VSANs.

Which port channel configuration must be used?

A. Port type: FT Port -

Port channel mode: Active

B. Port type: F Port -

Port channel mode: On

C. Port type: E Port -

Port channel mode: Active

D. Port type: TE Port -

Port channel mode: On

Answer: C

Explanation:

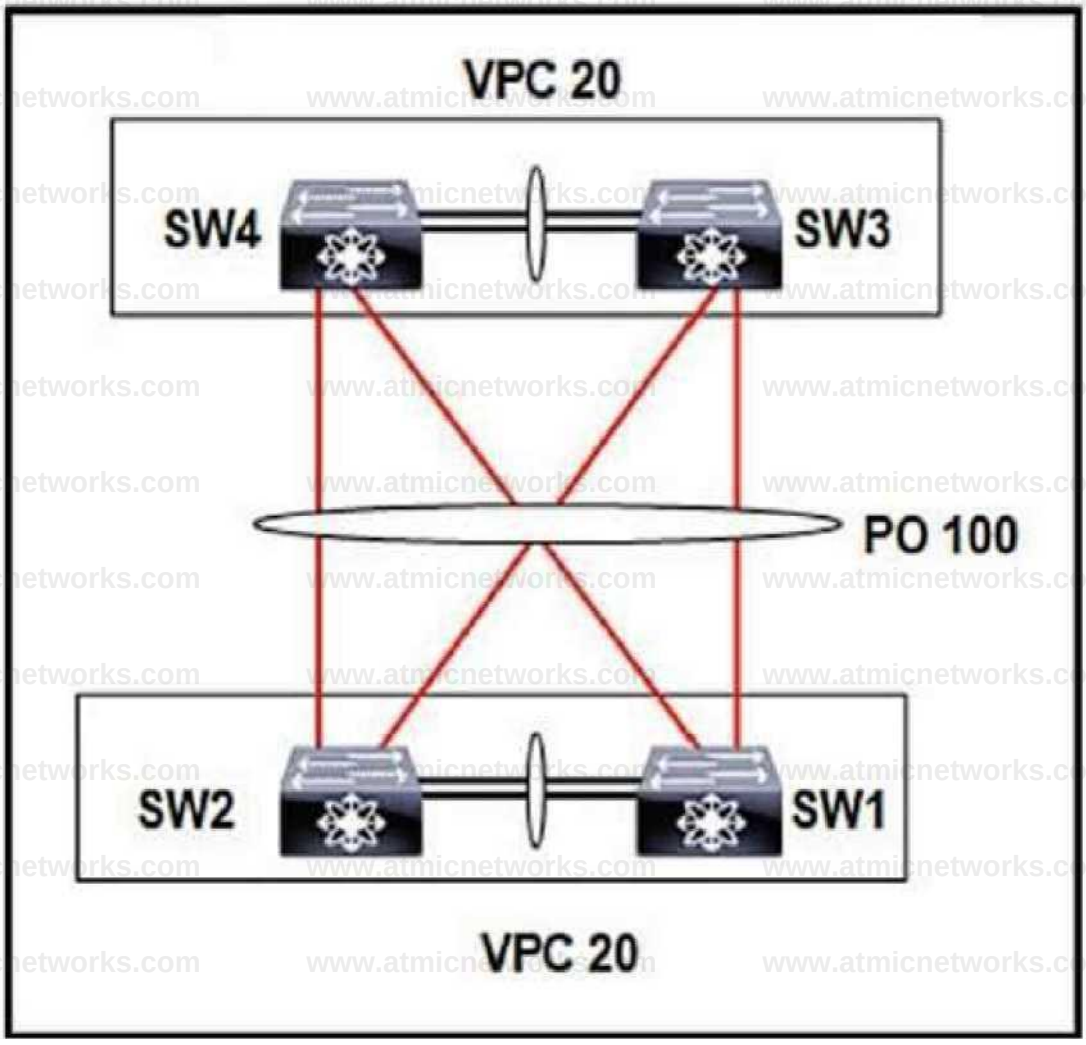
The requirements listed are indicative of a need for a port channel configuration that supports Enhanced ISL (EISL) or E Port channels. These channels are used for inter-switch links (ISLs) between Cisco MDS switches and can carry traffic for multiple VSANs. The 'Active' mode is necessary to ensure that the port channel will

suspend an individual member link if there is a configuration mismatch, which is a feature of the PortChannel protocol LACP (Link Aggregation Control Protocol). This mode also supports load balancing and can handle traffic from multiple VSANs12.

Reference: For more detailed information on configuring port channels on Cisco MDS 9000 Series Switches, you can refer to the Cisco MDS 9000 Series Interfaces Configuration Guide12.

Question: 463

Refer to the exhibit.



Two data center fabrics use VPC data center interconnect. The system MAC value on SW1 is 00:23:04:ee:be:20. Which value must be set to configure the system MAC address?

A. 00:23:04:ee:be:14 on SW3

B. 00:23:04:ee:be:20 on SW3

C. 00:23:04:ee:be:14 on SW2

D. 46:43:32:e5:92:80 on SW2

Answer: B

Explanation:

In a vPC (Virtual Port Channel) data center interconnect, both vPC peer devices must have the same system MAC address to ensure that remote switches perceive them as a single logical switch. Since the system MAC value on SW1 is 00:23:04:ee:be:20, the same value must be configured on SW3 to maintain consistency in the vPC domain and ensure seamless communication between the two data center fabrics connected through this vPC interconnect.

Reference: = The explanation can be inferred from Cisco's official documentation and resources related to configuring and managing vPCs, ensuring that both peer devices in a vPC domain are configured with identical parameters, including the system MAC address.

Question: 464

Refer to the exhibit. A Cisco data center environment is implemented with vPC. The web server replies using the SVI MAC address as the Layer 2 header instead of the HSRP MAC address on VLAN 23. This behavior causes packet drops on the Cisco Nexus 9000 Series Switches due to the vPC loop prevention mechanism. The requirement is for the vPC feature to allow N9K_1 and N9K_2 to forward traffic between the NAS server and the web server, even if the HSRP's MAC address is not used on Layer 2 headers for VLAN 23. Which feature must be used to accomplish this goal?

A. ARP Sync

B. Object Tracking

C. L3 Peer Router

D. Peer Gateway

Answer: D

Explanation:

The Peer Gateway feature on Cisco Nexus switches is designed to address the exact scenario described. When enabled, it allows the vPC peer switches to forward traffic based on the SVI MAC address, even if it is not the HSRP MAC address. This is particularly useful in cases where end devices do not use the HSRP virtual MAC address for the gateway and instead use the physical MAC address of one of the HSRP routers1. By using the Peer Gateway feature, both N9K_1 and N9K_2 will be able to forward traffic for VLAN 23, ensuring that the packets are not dropped due to the vPC loop prevention mechanism123.

Reference: = This information is supported by Cisco's documentation on Nexus 5500 Platform Layer 3 and vPC Operations, which explains the use of the peer-gateway command to allow Layer 3 forwarding in scenarios where the destination MAC of the incoming packet is the MAC of its vPC peer switch1. Additionally, discussions in the Cisco Community confirm the necessity of this feature when certain devices on the network do not properly send traffic to the MAC address specified in the ARP234

Question: 465

An engineer implements an environment with multiple traffic types on a consolidated I/O link between Cisco Nexus 9000 Series Switch and MDS

9000 Series Switch. The configuration must meet these requirements:

- The unified I/O link must support LAN and SAN traffic.
- A single, multipurpose Ethernet transport must be used.
- The configuration must discard MAC addresses that are not part of the current fabric.
- The QoS markings must be preserved.

Which configuration set meets the requirements?

A.MDS-A(config)# interface fcip4 -

MDS-A(config-if)# use-profile 8 -

MDS-A(config-if)# peer-info ipaddr 200.200.100.7

B.N9K-2(config)# interface Eth2 -

N9K-2(config-if)# switchport mode trunk

N9K-2(config-if)# auto qos trust dscp

C.MDS-B(config)# interface fc3 -

MDS-B(config-if)# switchport trunk mode on

MDS-B(config-if)# switchport trunk allowed vsan 2-5

D.N9K-1(config)# fcoe fcmap 0e.fc.1d

N9K-1(config)# int vfc 1 -

N9K-1(config-if)# bind interface e1/3

Answer: B

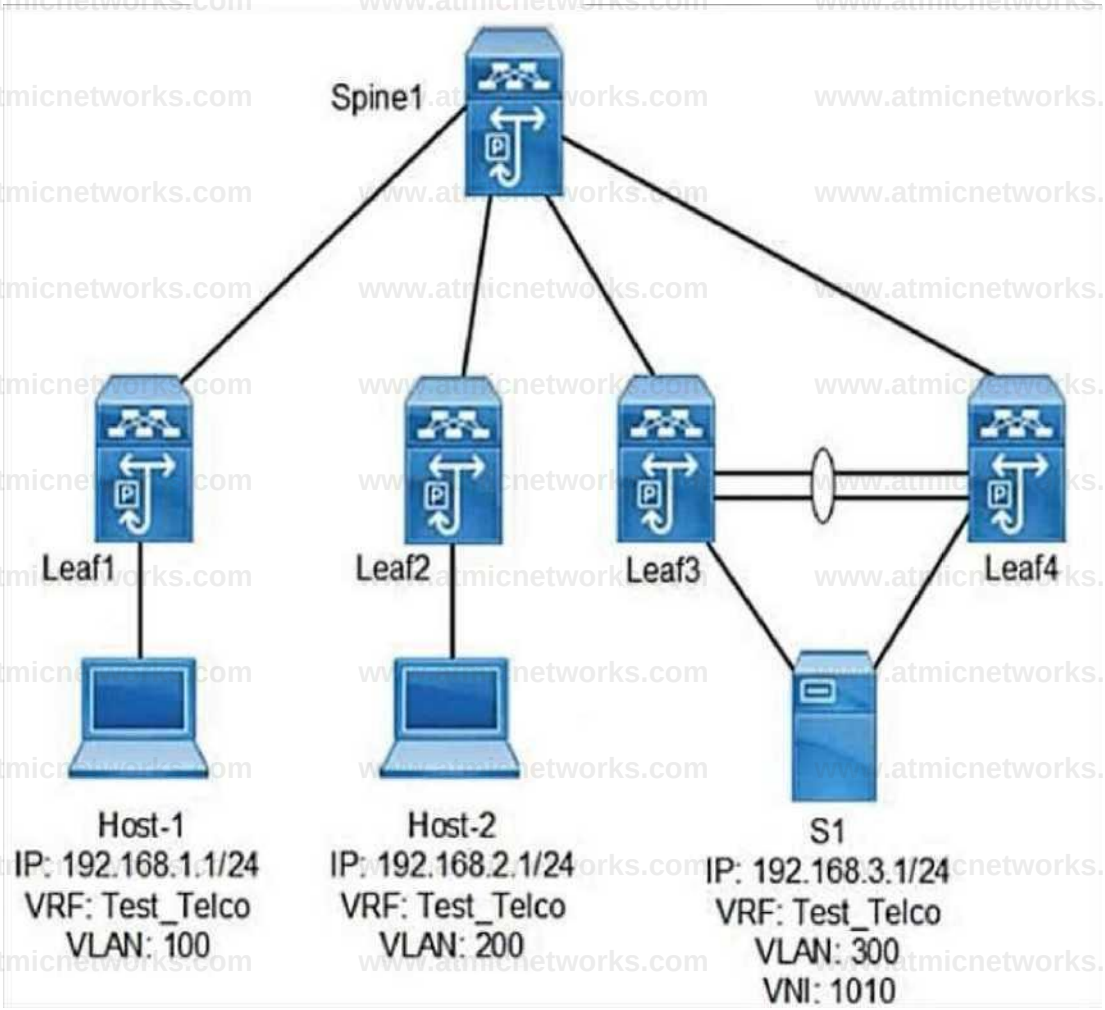
Explanation:

The correct configuration for a unified I/O link that supports both LAN and SAN traffic using a single Ethernet transport is to configure the interface as a trunk port. This allows multiple VLANs (for LAN traffic) and VSANs (for SAN traffic) to coexist on the same physical link. The auto qos trust dscp command ensures that the Quality of Service (QoS) markings are preserved, which is essential for maintaining traffic prioritization across the network.

Reference: For more detailed information, please refer to the Cisco Data Center Core Technologies study materials and official documentation available on the Cisco website. These resources provide comprehensive guidance on configuring and managing Cisco Nexus and MDS switches in a data center environment.

Question: 466

Refer to the exhibit.



A VXLAN data center fabric consists of three hosts mapped to different VLANs. Ingress VTEPs perform Layer 2 bridging and Layer 3 routing. Egress VTEPs only perform a Layer 2 bridging lookup. Which VNI values must be set to allow inter-VNI communication?

A. VLAN 100 to Layer 2 VNI 2020 -

Test_Telco_VRF to Layer 3 VNI 5050

B. VLAN 100 to Layer 2 VNI 2020 -

VLAN 200 to Layer 2 VNI 5050

C. VLAN 100 to Layer 2 VNI 2020 -

Test_Telco_VRF to Layer 3 VNI 1010

D. VLAN 100 to Layer 2 VNI 1010 -

VLAN 200 to Layer 2 VNI 1010

Answer: C

Explanation:

In a VXLAN data center fabric, inter-VNI communication requires mapping Layer 2 (L2) VLANs to their respective L2 VNIs and associating them with the correct Layer 3 (L3) VNI that corresponds to the VRF. In this case, VLAN 100 is mapped to L2 VNI 2020, and for inter-VNI routing to occur, it must be associated with an L3 VNI that corresponds to the VRF, which is Test_Telco_VRF to L3 VNI 1010. Reference: For more detailed information, you can refer to the Cisco Programmable Fabric with VXLAN BGP EVPN Configuration Guide1 and the Data Center VXLAN EVPN guide

Question: 467

Refer to the exhibit.

```
| |http://APIC-I?/api/node/mo/uni.json HTTP/1.1
Content-Type: application/json
Cache-Control: no-cache

{
    "ohysDcaP": {
        ”1        I”: {
          "name": "test_ohy_dmn",
          "dn": "uni/phys-test_phy_dmn”
        },
        "children": [{
          "infraRsVlanNs": {
            "attributes": {
              "tDn": "uni/infra/vlanns-[test_vlan]-
              dynamic"
            }
          }
        })
    }
}
```

A network engineer must configure the physical domain and attach a VLAN pool to it. Which two commands accomplish this goal? (Choose two.)

A. attributes

B. PATCH

C. GET

D. POST

E. variables

Answer: A, E

Explanation:

In the context of configuring a physical domain and attaching a VLAN pool to it, the commands “attributes” and “variables” are typically used within the configuration scripts. The “attributes” command is used to define specific attributes for elements within the configuration, such as naming conventions or paths. The “variables” command is used to declare variable elements that can be dynamically assigned or modified.

Question: 468

An engineer must perform a configuration backup of an existing Cisco UCS Manager environment. The backup file must contain all vNIC, vHBA,and service profile template settings. Also, the engineer must validate the backup before import and requires an XML output format. Which backup type must be used to meet these requirements?

A. full state

B. all configuration

C. logical configuration

D. system configuration

Answer: C

Explanation:

The logical configuration backup type in Cisco UCS Manager includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. This backup type is suitable for the engineer’s requirements as it contains all vNIC, vHBA, and service profile template settings. Additionally, the logical configuration backup is in XML format, which allows for validation before import1.

Reference:

Cisco documentation on “Backing Up and Restoring the Configuration” provides detailed information on the

different backup types and their contents1.

For further reading on UCS Manager backup operations and types, refer to the Cisco UCS Manager Administration Management Guide

Question: 469

An engineer is implementing VSANs on a Cisco MDS 9000 Series Switch with a native Fibre Channel. The deployment must meet these requirements:

- The host on port fc1/1 must be assigned to VSAN 10.
- The port channel 10 ISL must pass multiple VSANs, including VSAN 10.

Which configuration set meets these requirements?

A. Activate VSAN 10 in the vFC interface.
Associate VSAN 10 to interface vfc 1/1.

Enable vsan F-port-channel-trunk on the ISL.

Set encapsulation EISL on the switch port.

B. Create VSAN 10 in the VSAN database.
Bind VSAN 10 to interface fc1/1 in the VSAN database.

Enable VSAN trunking on the ISL.

Allow VSAN 10 on the ISL.

C. Configure VSAN 10 in the interface configuration.
Attach VSAN 10 to the VSAN database.

Enable VSAN trunking on fc1/1.

Filter all VSAN on the ISL.

D. Disable VSAN 1 in the VSAN database.
Assign VSAN 10 to the ISL.

Enable VSAN trunking on the port channel members.

Permit VSAN 10 in the FLOGI database.

Answer: B

Explanation:

To meet the deployment requirements for implementing VSANs on a Cisco MDS 9000 Series Switch, the correct steps are to create VSAN 10 in the VSAN database and bind it to the interface fc1/1. This assigns the host on port fc1/1 to VSAN 10. Additionally, enabling VSAN trunking on the Inter-Switch Link (ISL) and allowing VSAN 10 on the ISL ensures that the port channel 10 can pass multiple VSANs, including VSAN 10. This configuration allows for the segregation of traffic and maintains the isolation of different VSANs while still permitting communication across the shared physical infrastructure12.

Reference:

Cisco documentation on "Configuring VSANs and Interfaces" provides detailed steps on creating and managing VSANs1.

The "Cisco MDS 9000 Series Fabric Configuration Guide" further elaborates on managing VSANs and their associated interfaces

Question: 470

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?

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.

Reference :=

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

Question: 471

DRAG DROP

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

- ethl/1 uses clear text password.

```
1
2
3 SKI(config-if)t ip
4 SKI(config-if)I ip ospf
5 SKI(config-if)I ip ospf                    0 P05SW1
6 SKI(config)# interface ethernet 1/2
7 SKI(config-if)t ip router ospf 1 area
8 0.0.0.0
9 SKI(config-if)t ip ospf authentication
                                             3 md5 3 2b7cf4643b66b22
```

message-digest	mode	message-digest-key
authentication-key	authentication	key

Answer:

Explanation:

```
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 [authentication]
5 SW1(config-if)# ip ospf [key] 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 [mode]
9 SW1(config-if)# ip ospf [message-digest] 3 md5 3 2b7cf4643b66b22
```

message-digest-key

authentication-key

Question: 472

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?

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+.

Reference: For further details, refer to Cisco's official documentation on Role-Based Access Control (RBAC) in the Cisco MDS 9000 Series Switch configuration guides. These resources explain how to assign roles and permissions for configuring various features on the switch.

Question: 473

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?

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:

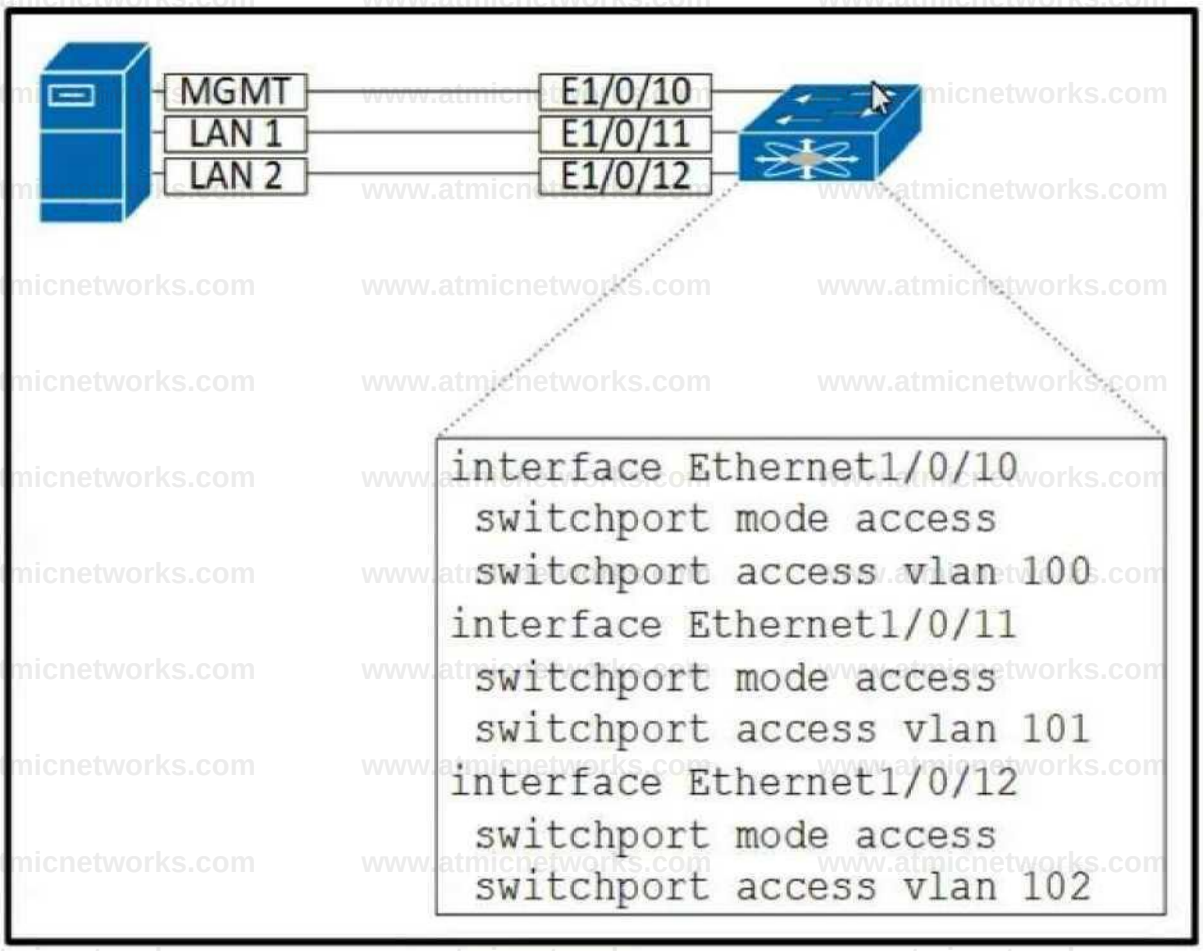
The command aaa authentication login default group ISE local configures the Cisco Nexus Series Switch to use TACACS+ for authentication by default and specifies a fallback to local authentication if the TACACS+ server becomes unavailable. This ensures that users are authenticated against the TACACS+ 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 account1.

Reference :=

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: 474

Refer to the exhibit.



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 KYM. Which configuration set meets these requirements?

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: 475

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?

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: 476

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?

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: 477

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?

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

Explanation:

Question: 478

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?

A. scheduled

B. timer-automatic

C. immediate

D. user-ack

Answer: D

Explanation:

Question: 479

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?

A. Full State

B. All Configuration

C. System Configuration

D. Logical Configuration

Answer: A

Explanation:

Question: 480

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.)

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: BC

Explanation:

Question: 482

What is a feature of an electronic programmable logic device upgrade on a Cisco MDS 9000 Series Switch?

A. Only the modules that are being upgraded are disrupted.

B. An EPLD upgrade is disruptive on all modules.

C. The standby supervisor module can perform the upgrade.

D. An EPLD upgrade is nondisruptive on all modules.

Answer: A

Explanation:

Question: 483

An engineer implements an Application Performance Monitoring (APM) solution. The solution runs in a vSphere infrastructure where the vSwitch support for promiscuous mode is disabled for security reasons. As a result, the final implementation must receive a copy of bidirectional traffic to a load balancer that is connected to a Cisco Nexus 93108 Series Switch. The APM solution supports GRE encapsulated traffic. Which configuration must be applied to the switch to meet this requirement?

A. interface vlan1

switchport monitor

destination ip 10.1.1.1

exit

monitor session 1 rx

monitor session 1 tx

source interface ethernet1/9

B. monitor session 1 both

source interface ethernet 1/9

destination interface ethernet 1/12

erspan-id 1

vrf mgmt0

filter vlan 3

no shut

C. configure terminal

monitor session 1 type erspan-source

erspan-id 1

destination ip 10.1.1.1

source interface ethernet 1/9 both

vrf default

no shut

D. interface ethernet 1/9

erspan-id 1

monitor session 1 type erspan-source

interface mgmt0

monitor session 1 type erspan-destination

destination ip 10.1.1.1

no shut

Answer: C

Explanation:

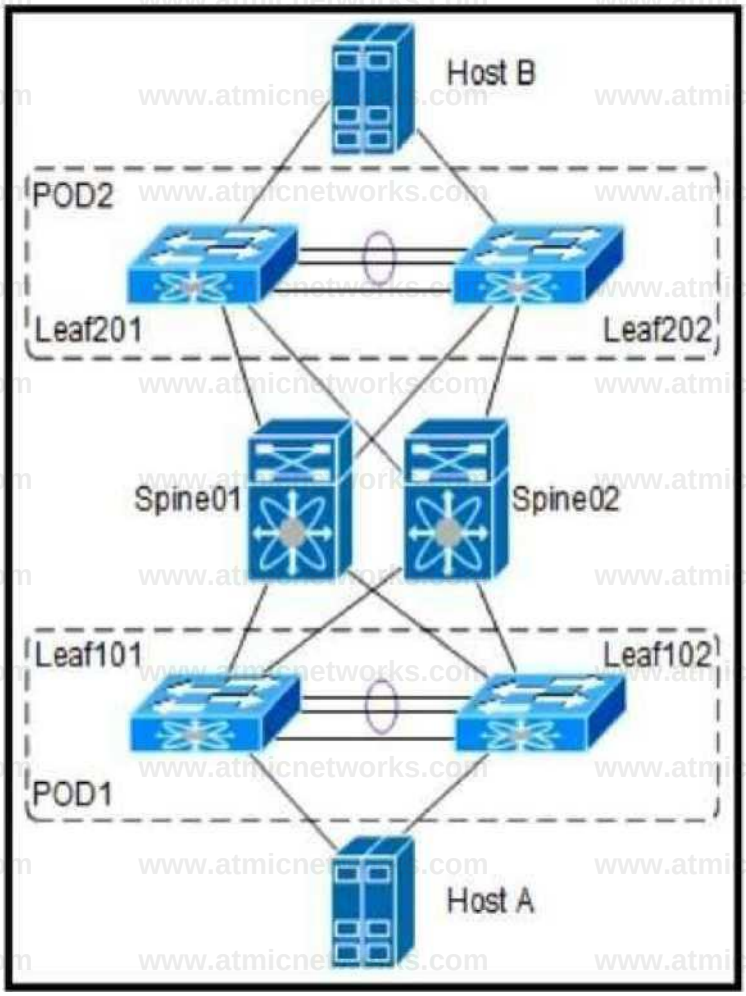
APM supports ERSPAN. This will be ERSPAN destination. We need source session from switch.

https://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst3850/software/release/16-3/configuration_guide/b_163_consolidated_3850_cg/b_163_consolidated_3850_cg_chapter_01001 010.pdf

Question: 484

DRAG DROP

Refer to the exhibit.

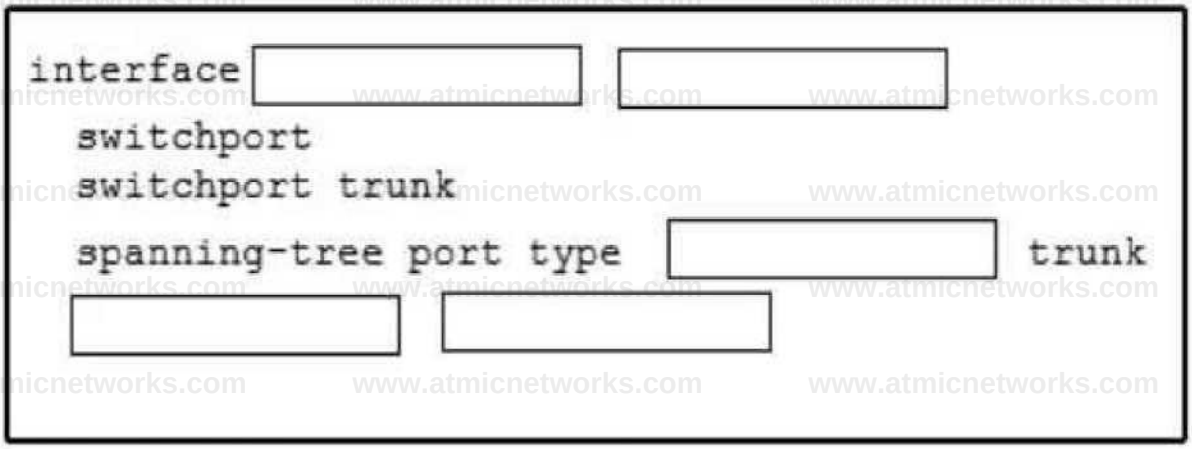


LEAF-101# show vpc orphan-ports
Note:
----------::Going through port database. Please be patient.::

VLAN	Orphan Ports
500	Po2
501	Po2
502	Po2
503	Po2

During a recent outage, a network engineer discovered that host A started to experience intermittent connectivity, when Leaf102 was down. Drag and drop the code snippets from the bottom onto the boxes in the code to resolve the problem. Not all code snippets are used.

Answer Area



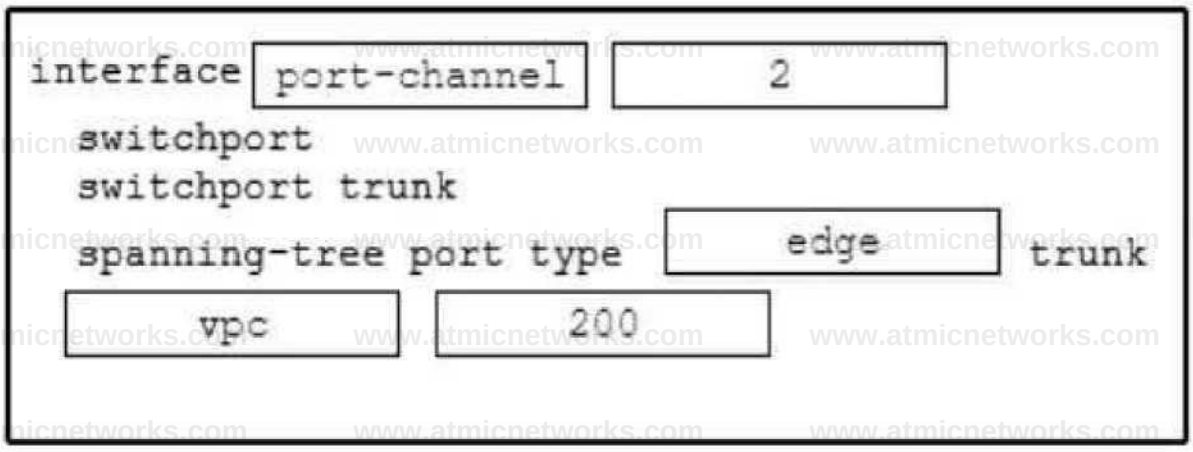
vpc | edge | 200

port-channel | 2 | network

Answer:

Explanation:

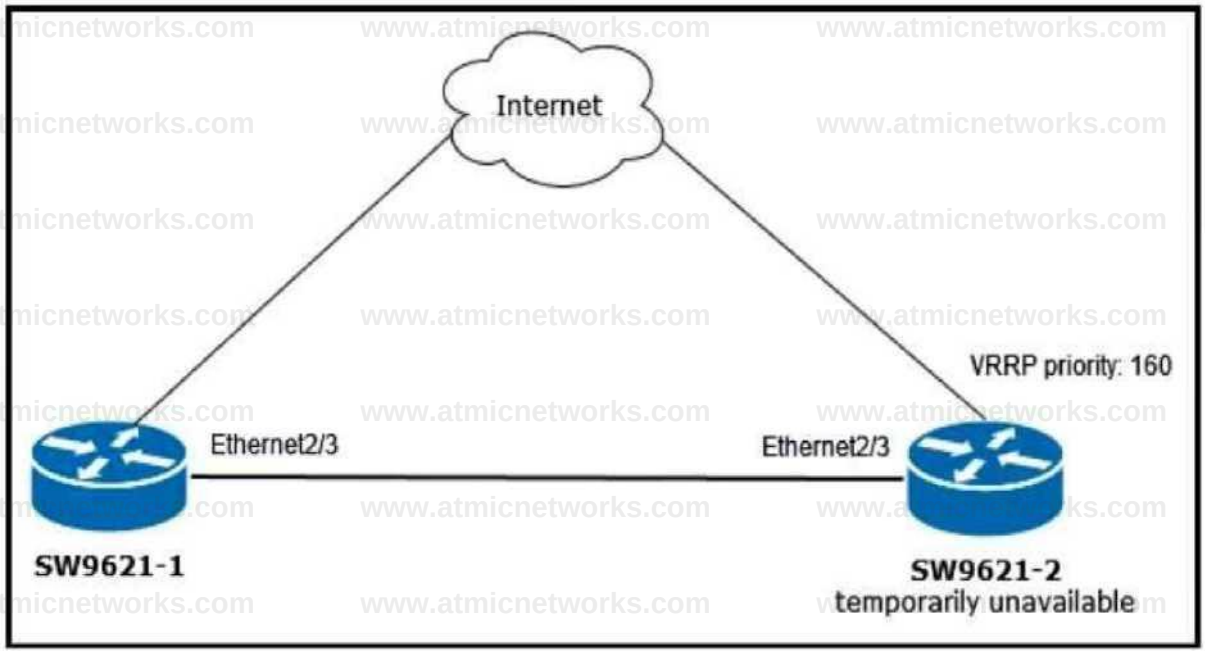
Answer Area



network

Question: 485

Refer to the exhibit.



What happens to the VRRP configuration when the router SW9621-2 becomes operational?

```
SW9621-1# show vnp detail
  Ethernet2/3 - Group 100 (IPV4)
    State is Master
    Virtual IP address is 192.168.30.100
    Priority 100, Configured 100
  Forwarding threshold(for VPC), lower: 1 upper: 100
    Advertisement interval 3
    Preemption enabled
    Authentication text "D458F7B032E4632090EF06EE5A"
    Virtual MAC address is 0000.5e00.0164
    Master router is Local
```

A. The SW9621-2 router becomes a new active master.

B. The SW9621-1 router becomes a new active master after 3 seconds.

C. The SW9621-1 router remains an active master.

D. The SW9621-2 router becomes an active master after 3 seconds.

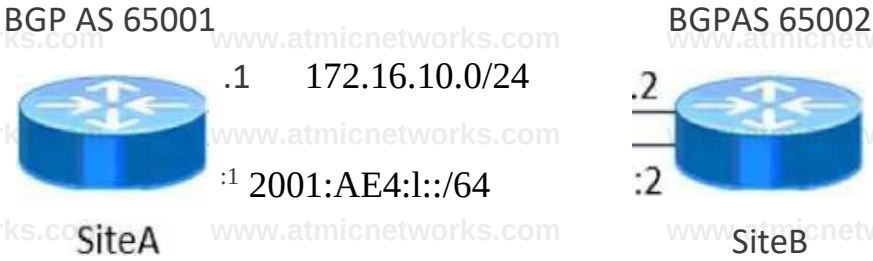
Answer: A

Explanation:

Question: 486

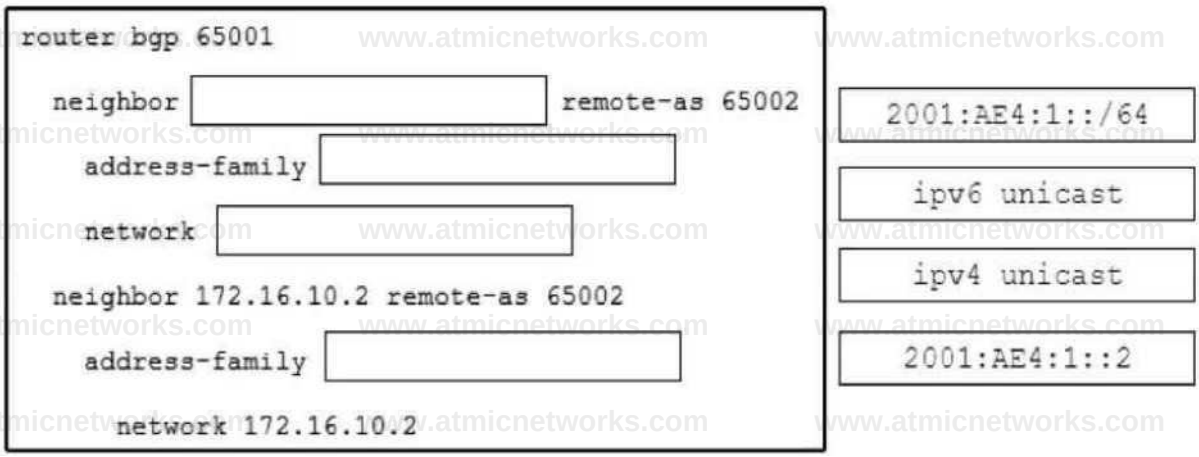
DRAG DROP

Refer to the exhibit.



An administrator is deploying BGP to geographically connect two data center sites. Both sites are configured for dual-stack routed protocols. The administrator must inject the IPv6 network 2001:AE4:1::/64 into the IPv6 unicast database. Drag and drop the SiteA commands from the right into the blanks in the configuration on the left. Commands are used more than once.

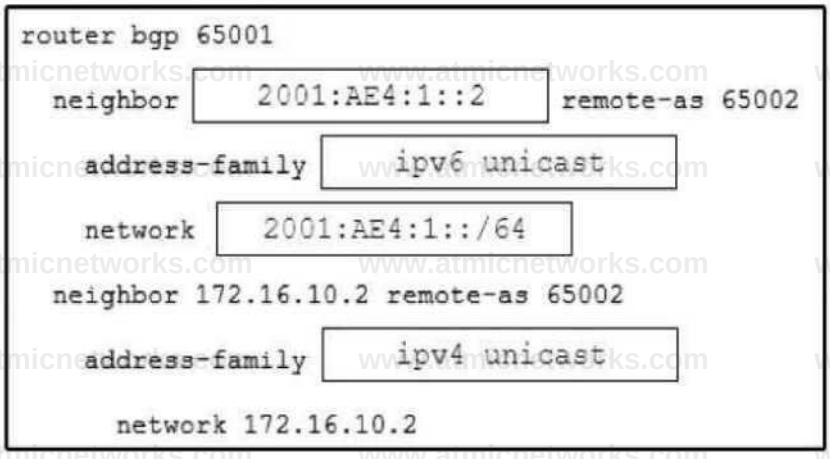
Answer Area



Answer:

Explanation:

Answer Area



Question: 487

What is the impact of a nondisruptive upgrade on fabric and modular switches?

A. The upgrade disrupts the control plane for more than 120 seconds.

B. During the upgrade, new devices cannot log in to the fabric.

C. If a zone server merge is in progress, the upgrade continues without interruption.

D. When the installation is complete, the system BIOS must be updated.

Answer: B

Explanation:

Question: 488

DRAG DROP

Drag and drop the command snippets from the bottom onto the boxes in the code to complete a Python script that displays a list of interfaces on a Cisco Nexus 9000 Series Switch using on-box Python. Not all command snippets are used.

Answer Area

```
»> cli('configure terminal ; interface loopback 5; no shut')
intflist:j son.      (did('show interface brief'))
» while i < len (                    ['TABLE_interface']['ROW_interface']):
..intf=intflist('TABLE interface']['I                    ']['i]
..if                    ['state']        'up' :
..prit intf['interface']
mgmtO loopback2 loopback5
```

dumps	loads	inflist
TABLEincerface	intf	ROW_interface

Answer:

Explanation:

Answer Area

```
»> cli('configure terminal ; interface loopback 5; no shut')
intflist:j son. »>  loads  (clid('show interface brief'))
i=0
>» while i < len (  inflist  ['TABLE interface']['ROW interface']):
    intf=intflist('TABLE_interface'][' ROW interface ' 1 [i]
  ..i=i+l
  . .if  intf  [ 'state']  'up' :
...prit intf['interface']
```

```
mgmtO
loopback2
loopback5
```

dumps loads inflist

TABLE incerface intf ROW interface

https://www.cisco.com/c/en/us/td/docs/dcn/nx-os/nexus9000/102x/programmability/cisco-nexus- 9000-series-nx-os-programmability-guide-release-102x/m-n9k-python-api-101x.html

Question: 489

Refer to the exhibit.

```
"TABLE_asn": { "ROW asn": { "asii": "10", "TABLE vrf": ( "ROW_vrf": {
"vrf": "default", "TABLE_peer": { "ROW_peer": | "peer_handle": "0",
"peer_ipaddr": "10.13.0.2" "peer ifname": "Ethl/1", "peerholdtime": "13",
"peer  srtt":  "6",  "peer^rto":  "50",  "peer_xmitq_count":  "0",
"peer_last_seqno": "4", "peer_uptime": "PT46M49S"
```

1

```
    }
}
```

Refer to the exhibit. An engineer uses Python in Cisco NX-OS guest shell to retrieve the configuration of the EIGRP ASN on interface eth1/1.

The engineer has written this script:

>>> import json

```
>>> from cli import*
```

Which command set must be used to retrieve the value of the 'asn' key?

A.
```
>>> output = json.loads(clid('show ip eigrp neighbors'))
>>> output['TABLE_asn']['ROW_asn']['asn']
```

B.
```
>>> output = json.dumps(clid('show ip eigrp neighbors'))
>>> output['TABLE_asn']['ROW_asn']['asn']
```

C.
```
>>> output = json.dumps(clid('show ip eigrp neighbors'))
>>> output['asn']
```

D. >>> output = json.loads(clid('show ip eigrp neighbors'))

>>> output['asn']

Answer: D

Explanation:

- ethl/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.

```
SKI(config)* router ospf 1
SKI(config-router)I interface ethernet 1/1
                          router ospf 1 area 0.0.0.0
```