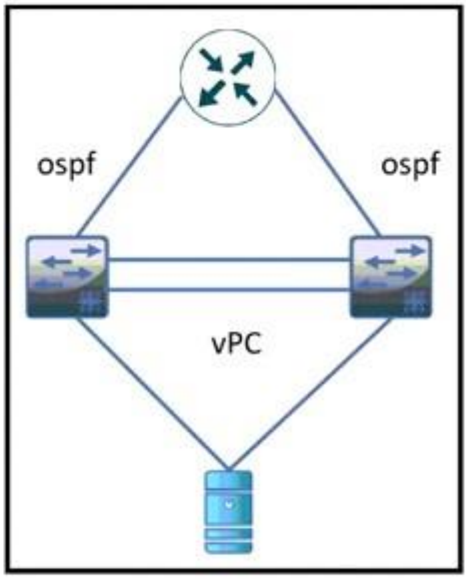
**Vendor:** Cisco

**Exam Code:** 350-601

**Exam Name:** Implementing and Operating Cisco Data Center Core Technologies (DCCOR)

**Version:** DEMO

**QUESTION 1**
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?

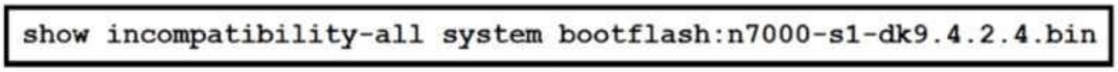


A. Set the routed uplink ports of the Cisco Nexus peers as orphans.
B. Increase the vPC delay restore timer.
C. Decrease the OSPF hello and dead interval timers.
D. Disable vPC ARP synchronize on the vPC peers.

**Answer:** B
**Explanation:**
PC Delay Restore
After a vPC peer device reloads and comes back up, the routing protocol needs time to reconverge.
The recovering vPCs leg may black-hole routed traffic from access to core until Layer 3 connectivity is reestablished.
vPC Delay Restore feature delays vPCs leg bringup on the recovering vPC peer device. vPC Delay Restore allows for Layer 3 routing protocols to converge before allowing any traffic on vPC leg.
Result is a more graceful restoration and zero packet loss during the recovery phase (traffic still get diverted on the alive vPC peer device).
This feature is enabled by default with a vPC restoration default timer of 30 seconds. The timer can be tuned according to a specific Layer 3 convergence baseline from 1 to 3600 seconds.

Reference:
https://www.cisco.com/c/dam/en/us/td/docs/switches/datacenter/sw/design/vpc_design/vpc_best_practices_design_guide.pdf

**QUESTION 2**
Refer to the exhibit. Software downgrade is required on a Cisco Nexus 7000 Series Switch. What is displayed when this command is executed?

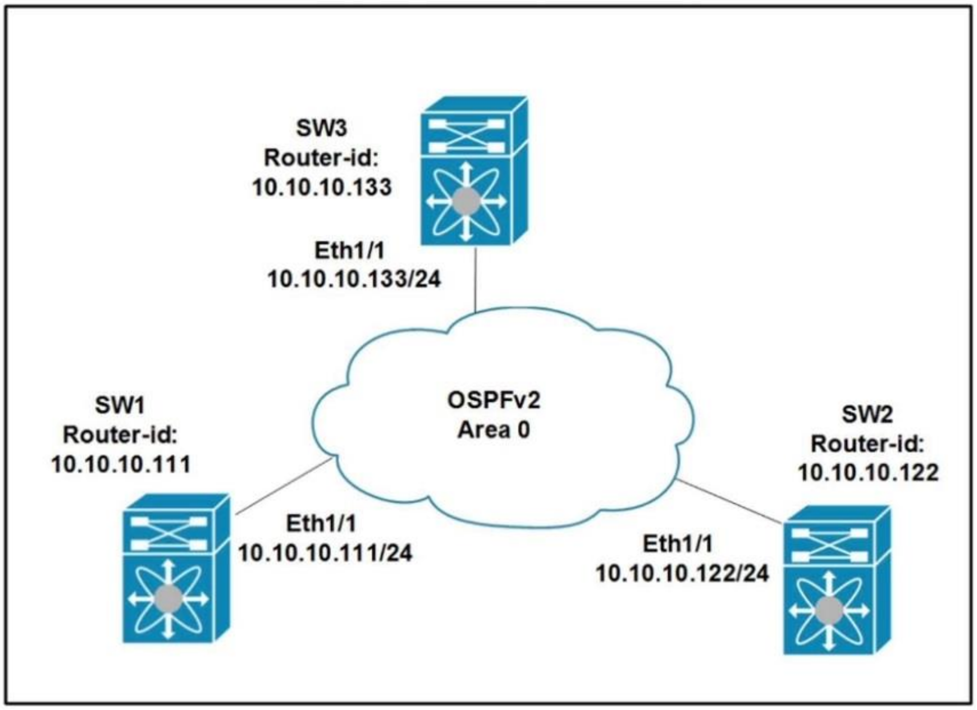


```
show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin
```

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:** A
**Explanation:**
This will inform the administrator if there are any features that will be automatically removed from the configuration.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/best_practices/cli_mgmt_guide/cli_mgmt_bp/nxos_upgrade.pdf

**QUESTION 3**
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

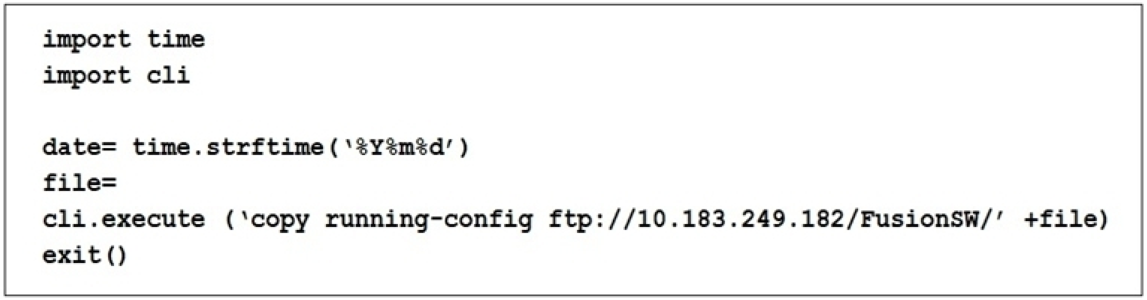
**Answer:** A
**Explanation:**
Priority in OSPF is mainly used to influence/determine a designated router/backup designated router for a network. By default, the priority is 1 on all routers. A router with a high priority will always win the DR/BDR election process.
If there is a tie, a router with the highest router ID wins the election. The router with the second highest OSPF priority or router ID will become a BDR.
Reference:
https://www.cisco.com/c/m/en_us/techdoc/dc/reference/cli/nxos/commands/ospf/ip-ospf-priority.html

**QUESTION 4**
Which two configuration settings are available in the Cisco UCS Firmware Auto Sync Server policy? (Choose two.)

A. Immediate Action
B. User Notification
C. User Acknowledge
D. Delayed Action
E. No Action

**Answer:** CE
**Explanation:**
Following are the values for the Firmware Auto Sync Server policy:
User Acknowledge - Firmware on the server is not synchronized until the administrator acknowledges
the upgrade in the Pending Activities dialog box.
No Action - No firmware upgrade is initiated on the server.
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/firmware-mgmt/gui/2-2/b_GUI_Firmware_Management_22/b_GUI_Firmware_Management_22_chapter_01111.pdf

**QUESTION 5**
Refer to the exhibit. 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?



```
import time
import cli

date= time.strftime(‘%Y%m%d’)
file=
cli.execute (‘copy running-config ftp://10.183.249.182/FusionSW/’ +file)
exit()
```

A. str.('fusion-config_') + date
B. ('fusion-config_') + date
C. ('fusion-config_ + date')
D. string(('fusion-config_') + date

**Answer:** B
**Explanation:**
See below for an example:

```
nxos9kv# python
Python 2.7.11 (default, Feb 26 2018, 03:34:16)
[GCC 4.6.3] on linux2
Type "help", "copyright", "credits" or "license" for more information.
>>> import time
>>> import cli
>>> date = time.strftime('%Y%m%d')
>>> file = ("fusion-config_') + date
>>> print(file)
fusion-config_20210329
>>> print('copy running-config ftp://10.183.249.182/FusionSW/' + file) copy running-config
ftp://10.183.249.182/FusionSW/fusion-config_20210329
```

**QUESTION 6**
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:** C
**Explanation:**
Only logical configuration includes Service Profiles!
System configuration - An XML file that includes all system configuration settings such as usernames, roles, and locales. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.
Logical configuration - An XML file that includes all logical configuration settings such as service profiles, VLANs, VSANs, pools, and policies. You can use the file generated from this backup to import these configuration settings to the original fabric interconnect or to a different fabric interconnect. You cannot use this file for a system restore.

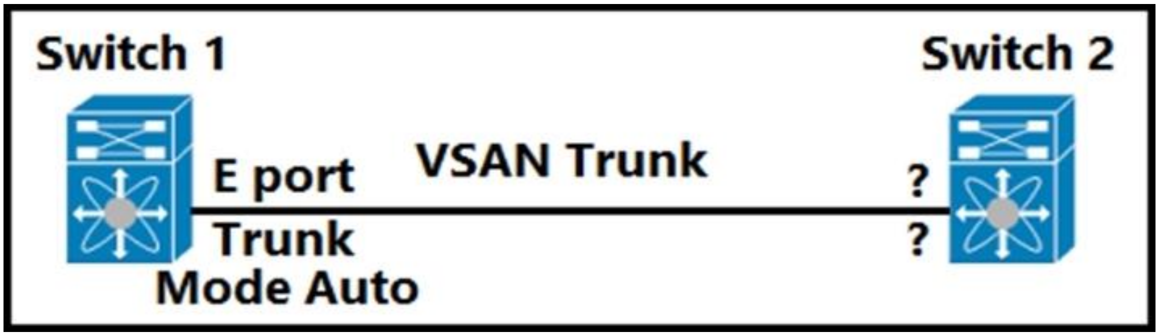
**QUESTION 7**
The Cisco UCS blade chassis must send SNMPv3 traps to a network monitoring system. The SNMP trap messages should be authenticated and have protection from closure.
Which SNMP security privileged level should be configured?

A. noPriv
B. auth
C. noAuth
D. priv

**Answer:** D
**Explanation:**
If you select V3 for the version, the privilege associated with the trap.
This can be one of the following:
• Auth—Authentication but no encryption
• Noauth—No authentication or encryption
• Priv—Authentication and encryption

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/System-Monitoring/4-0/b_UCSM_GUI_System_Monitoring_Guide_4-0/b_UCSM_GUI_System_Monitoring_Guide_4-0_chapter_0111.pdf

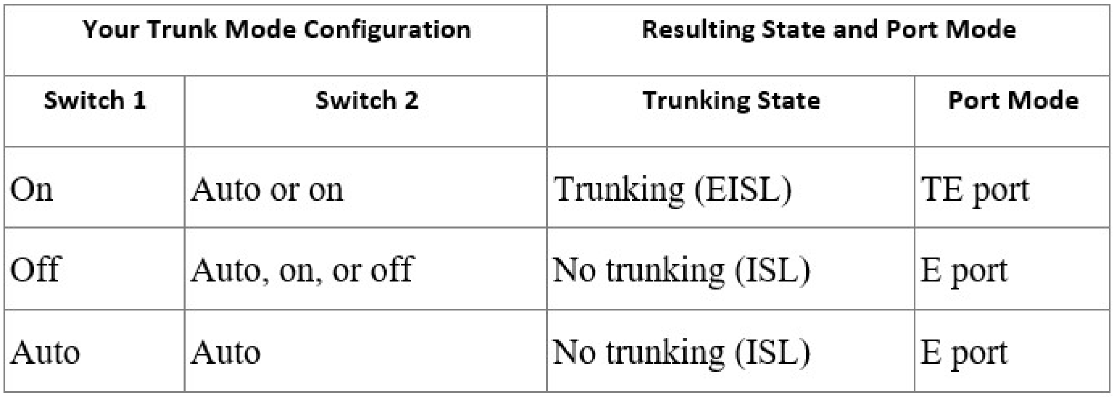
**QUESTION 8**
Refer to the exhibit. Which feature must be used to configure on switch 2 to establish a VSAN trunk between switch 1 and switch 2?



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:**
By default, trunk mode is enabled in all Fibre Channel interfaces. However, trunk mode configuration takes effect only in E-port mode. You can configure trunk mode as on (enabled), off (disabled), or auto (automatic). The default trunk mode is on. The trunk mode configuration at the two ends of an ISL, between two switches, determine the trunking state of the link and the port modes at both ends (see Table 15-1).

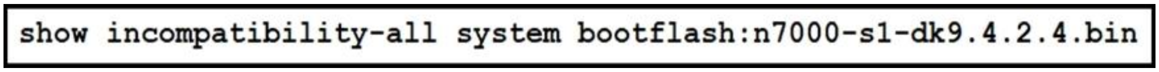
Table 15-1 Trunk Mode Status Between Switches



| Your Trunk Mode Configuration | | Resulting State and Port Mode | |
|---|---|---|---|
| Switch 1 | Switch 2 | Trunking State | Port Mode |
| On | Auto or on | Trunking (EISL) | TE port |
| Off | Auto, on, or off | No trunking (ISL) | E port |
| Auto | Auto | No trunking (ISL) | E port |

Reference:
https://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guides/cli_3_2/trnk.html

**QUESTION 9**
Refer to the exhibit. Software downgrade is required on a Cisco Nexus 7000 Series Switch.
What is displayed when this command is executed?



```
show incompatibility-all system bootflash:n7000-s1-dk9.4.2.4.bin
```

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:** A
**Explanation:**
This will inform the administrator if there are any features that will be automatically removed from the configuration.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/best_practices/cli_mgmt_guide/cli_mgmt_bp/nxos_upgrade.pdf

**QUESTION 10**
A network engineer is configuring the Cisco UCS service profile template with Ansible using this code:

**hostname: 192.168.10.23**
**username: cisco**
**password: f718c4329405726531f6247ff982**
**name: DCE-CTRL**
**template_type: updating-template**
**uuid_pool: UUID-POOL**
**storage_pronte: DCE-StgProf**
**maintenance_policy: default**
**server_pool: Container-Pool**
**host_firmware_package: 4.1(1a)**

**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. lan_connectivity_policy
C. boot_policy
D. iqn_pool

**Answer:** D
**Explanation:**
An IQN pool is a collection of iSCSI Qualified Names (IQNs) for use as initiator identifiers by iSCSI vNICs in a Cisco UCS domain. IQN pools created in Cisco UCS Central can be shared between Cisco UCS domains.
Reference:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-central/GUI-User-Guides/Server-Mgmt/1-5/b_CiscoUCSCentral_Server_Management_Guide_1-5/b_CiscoUCSCentral_Server_Management_Guide_1-5_chapter_0101.html

**QUESTION 11**
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:**
Dual switch configuration provides a slightly more complex topology with full redundancy that protects against: switch failure, link failure, and port failure. It requires two switches that may be standalone or stacked, and two 10/25GE ports, one 1GE port for CIMC management, and one Cisco VIC 1457 per server.
Trunk ports are the only supported network port configuration.
Reference:
https://www.cisco.com/c/en/us/td/docs/hyperconverged_systems/HyperFlex_HX_DataPlatformSoftware/Edge_Deployment_Guide/b-hx-edge-preinstall-checklist/m-3-and-4-node-preinstall-chklist.html

**QUESTION 12**
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(config)# **fabric forwarding anycast-gateway-mac AA:BB:AA:BB:AA:BB**
NX9K(config)# **interface VLAN-interface-name**
NX9K(config-if)# **fabric forwarding mode anycast-gateway**
B. NX9K(config)# **fabric forwarding anycast-gateway-mac AA:BB:AA:BB:AA:BB**
NX9K(config)# **interface VLAN-interface-name**

NX9K(config-if)# **vrf member vrf-name**
NX9K(config-if)# **fabric forwarding mode anycast-gateway**

C. NX9K(config)# **install feature-set fabric**
NX9K(config)# **feature-set fabric**
NX9K(config)# **fabric forwarding anycast-gateway-mac AA:BB:AA:BB:AA:BB**
NX9K(config)# **interface VLAN-interface-name**
NX9K(config-if)# **vrf member vrf-name**
NX9K(config-if)# **fabric forwarding mode anycast-gateway**

D. NX9K(config)# **install feature-set fabric**
NX9K(config)# **feature-set fabric**
NX9K(config)# **fabric forwarding anycast-gateway-mac AA:BB:AA:BB:AA:BB**
NX9K(config)# **interface VLAN-interface-name**
NX9K(config-if)# **fabric forwarding mode anycast-gateway**

**Answer:** C
**Explanation:**
We need to configure fabric forwarding anycast-gateway-mac <address> and fabric forwarding mode anycast-gateway also need to associate SVI with Anycast Gateway under VLAN configuration mode for Anycast Gateway for VXLAN Routing.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus9000/sw/7-x/vxlan/configuration/guide/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x/b_Cisco_Nexus_9000_Series_NX-OS_VXLAN_Configuration_Guide_7x_chapter_0100.html

**QUESTION 13**
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:** A
**Explanation:**
If you want to use a network-based attribute and classify IP addresses in the same subnet, you must use the MAC-based network attribute.
IP-based microsegmented EPGs do not support classification for IP addresses in the same subnet.
IP-based microsegmented EPGs are supported only when traffic requires Layer 3 routing.
If the traffic is bridged, the microsegmentation policy cannot be enforced.
Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/3-x/virtualization/b_ACI_Virtualization_Guide_3_1_1/b_ACI_Virtualization_Guide_3_1_1_chapter_0100.html

**QUESTION 14**
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.
C. Commit the changes to the active user database.
D. 1. Modify a network-operator role and add the required privileges.
   2. Assign a VDC-operator role to a user.
E. 1. Assign the network-admin role to a user.
   2. Commit the role to the switch to the active user database

**Answer:** A
**Explanation:**
User roles contain rules that define the operations allowed for the user who is assigned the role. Each user role can contain multiple rules and each user can have multiple roles.
For example, if role1 allows access only to configuration operations, and role2 allows access only to debug operations, then users who belong to both role1 and role2 can access configuration and debug operations.
You can also limit access to specific VLANs, virtual routing and forwarding instances (VRFs), and interfaces.

The Cisco NX-OS software provides four default user roles:
•network-admin—Complete read-and-write access to the entire NX-OS device (only available in the default VDC)
•network-operator—Complete read access to the entire NX-OS device (only available in the default VDC)
•vdc-admin—Read-and-write access limited to a VDC
•vdc-operator—Read access limited to a VDC
Note You cannot change the default user roles.

Reference:
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/4_1/nx-os/security/configuration/guide/sec_nx-os-cfg/sec_rbac.html#wp1431408

**QUESTION 15**
An administrator is implementing DCNM so that events are triggered when monitored traffic exceeds the configured present utilization 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:** A
**Explanation:**
You must choose either absolute value thresholds or baseline thresholds that apply to all transmit or receive traffic defined in the collection. Click the Use absolute values radio button on the last screen of the Performance Manager Configuration Wizard to configure thresholds that apply directly to the statistics gathered. These statistics, as a percent of the total link capacity, are

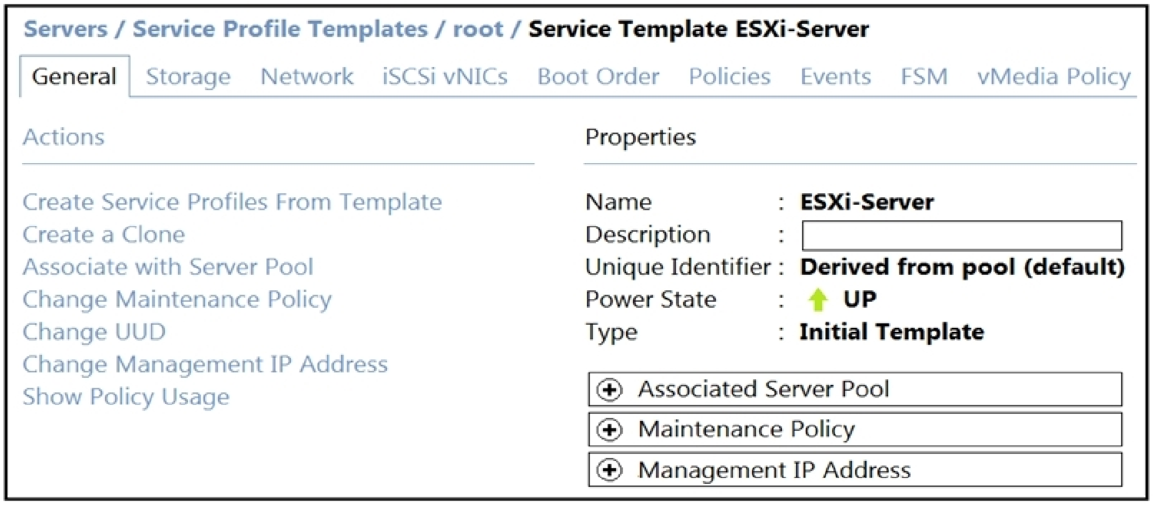
compared to the percent utilization configured for the threshold type. If the statistics exceed either configured threshold, an event is shown on the DCNM-SAN web client Events tab.
https://www.cisco.com/c/en/us/td/docs/switches/datacenter/sw/11_x/fundamentals/cisco_dcnm_fundamentals_guide_11/monitoring_performance.html

**QUESTION 16**
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

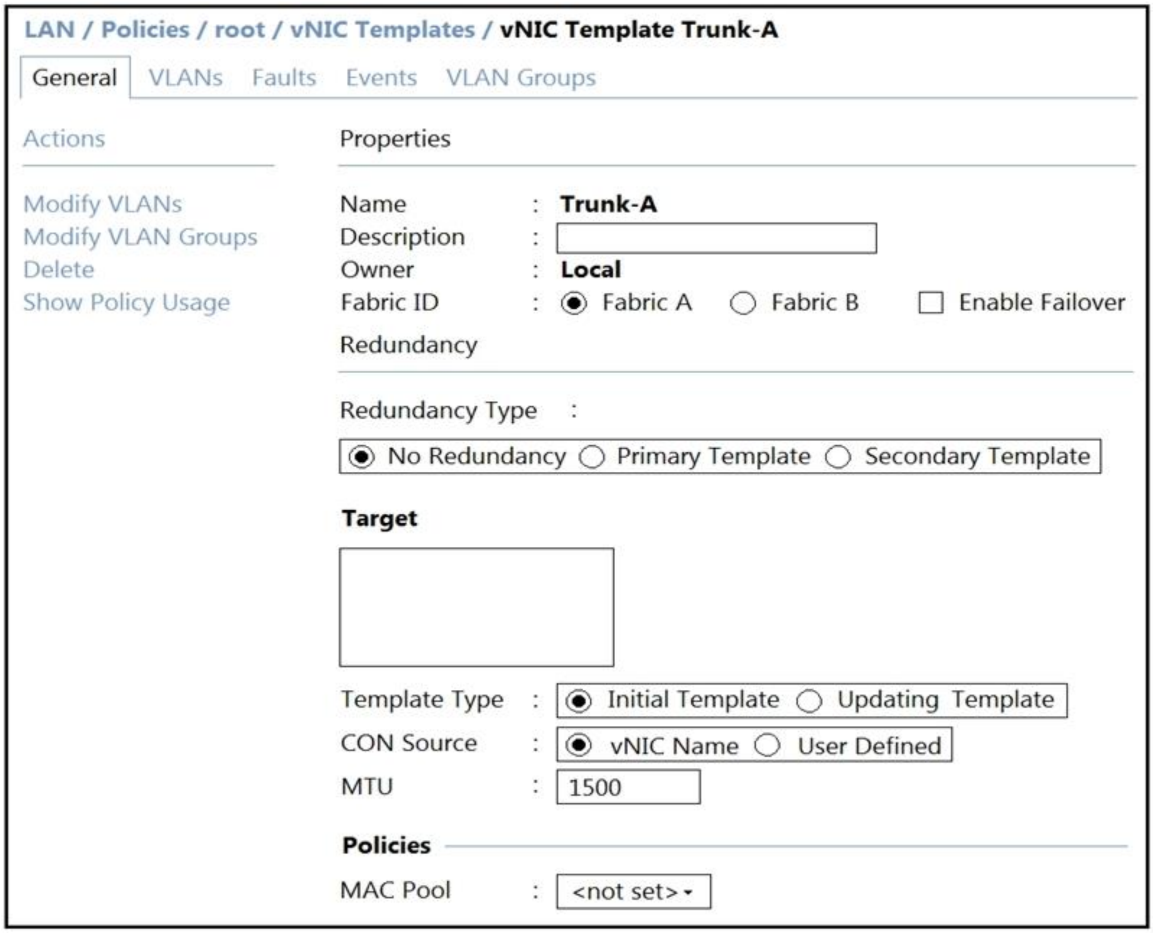
**Answer:** BE
**Explanation:**
1) The system with the lower MAC address wins as master and this election is not governed by the vPC role priority
2) Before you introduce an already isolated vPC device back into production, check the LACP roles on both boxes. If the same role, disable auto recovery with no auto-recovery under the vPC domain on both peers and reload the isolated device. After reload, the isolated device comes up with the LACP role 'none established' and can be introduced into the vPC without LACP role re-election.
Reference:
https://www.cisco.com/c/en/us/support/docs/interfaces-modules/nexus-7000-series-supervisor-1-module/119033-technote-nexus-00.html

**QUESTION 17**
Refer to the exhibits. ESXi-Server is associated to the blade server. A VLAN is 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 vNIC?


Servers / Service Profile Templates / root / **Service Template ESXi-Server**

Properties

Name : **ESXi-Server**
Description :
Unique Identifier : **Derived from pool (default)**
Power State : **UP**
Type : **Initial Template**



LAN / Policies / root / vNIC Templates / **vNIC Template Trunk-A**

General | VLANs | Faults | Events | VLAN Groups

Actions

- Modify VLANs
- Modify VLAN Groups
- Delete
- Show Policy Usage

Properties

Name : **Trunk-A**

Description :

Owner : **Local**

Fabric ID : ● Fabric A ○ Fabric B □ Enable Failover

Redundancy

Redundancy Type :

● No Redundancy ○ Primary Template ○ Secondary Template

**Target**

Template Type : ● Initial Template ○ Updating Template

CON Source : ● vNIC Name ○ User Defined

MTU : 1500

**Policies**

MAC Pool : <not set>

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:**

The VNIC template is the one where the modification of adding a VLAN is made. If we want that to apply to all server profiles which use this VNIC template, it needs to be an updated template.

**QUESTION 18**

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 same STP bridge ID from the upstream vPC switch peers. Which vPC feature must be implemented to ensure that vPC and non-vPC switches receive the same STP bridge ID from the upstream vPC switch peers?

A. System-mac 0123.4567.89ab
B. Peer-switch
C. VPC local role-priority 4000
D. Peer-gateway

**Answer:** B

**Explanation:**
The vPC peer switch is introduced to address performance concerns around these STP convergence events. This feature allows a pair of Cisco Nexus 7000 Series devices to appear as a single STP root in the Layer 2 topology. In the vPC peer switch mode, STP BPDUs are sent from both vPC peer devices. This behavior also avoids issues related to STP BPDU timeout on the downstream switches, which can cause traffic disruption. The vPC peer switch feature eliminates the need to pin the STP root to the vPC primary switch and improves vPC convergence if the vPC primary switch fails. It is important to note that the vPC peer switch is needed only when the STP root needs to be placed on the vPC pair of devices.

**QUESTION 19**
A network architect must redesign a data center network based on OSPFv2. The network must perform fast reconvergence between directly connected switches.
Which two actions must be taken to meet the requirements? (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:** CE
**Explanation:**
Detecting link and node failures quickly is number one priority for fast convergence. For maximum speed, relying on IGP keepalive times should be avoided whether possible and physical failure detection mechanisms should be used. This implies the use of physical point-to-point links whether possible.
BFD (BiDirectional Forwarding Detection) provides sub-second convergence for many protocols and is done in hardware. BFD will also only work on point-to- point links.

**QUESTION 20**
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:** BC
**Explanation:**
Following are the values for the Firmware Auto Sync Server policy:
• User Acknowledge—Firmware on the server is not synchronized until the administrator acknowledges
the upgrade in the Pending Activities dialog box.
• No Action—No firmware upgrade is initiated on the server.

Reference:
https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/firmware-mgmt/gui/2-2/b_GUI_Firmware_Management_22/b_GUI_Firmware_Management_22_chapter_01111.pdf