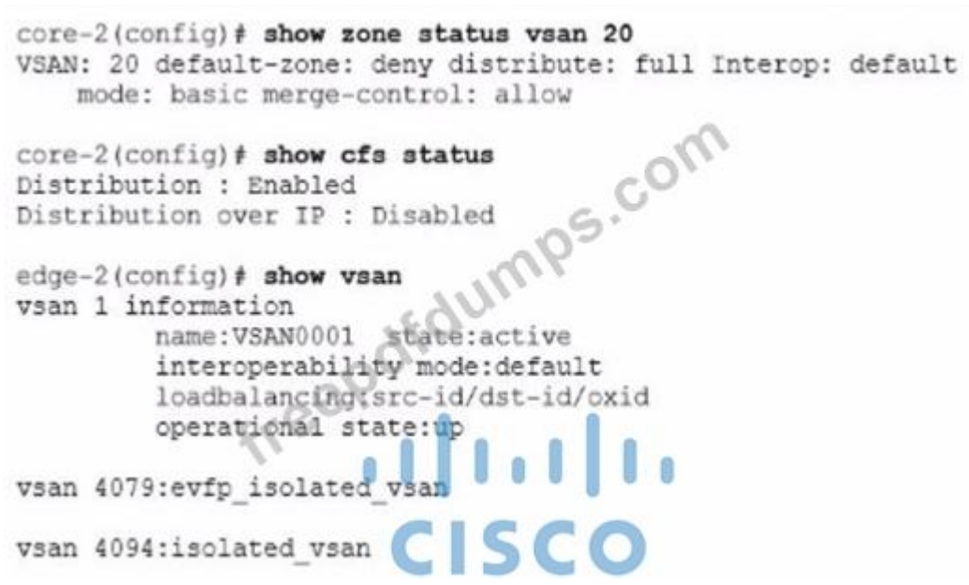
Cisco.300-615.v2026-07-24.q105

Exam Code:	300-615
Exam Name:	Troubleshooting Cisco Data Center Infrastructure
Certification Provider:	Cisco
Free Question Number:	105
Version:	v2026-07-24
# of views:	130
# of Questions views:	1050
https://www.freepdfdumps.com/Cisco.300-615.v2026-07-24.q105.html	

NEW QUESTION: 1



Refer to the exhibit. An engineer is configuring zone distribution on the Cisco Nexus 9000 Series Switch After initial configuration, the zone distribution for VSAN 20 from core-2 to edge-2 fails Which action resolves the issue?

A. Issue permit distribute on core-2

B. Change interop mode on core-2 to 1

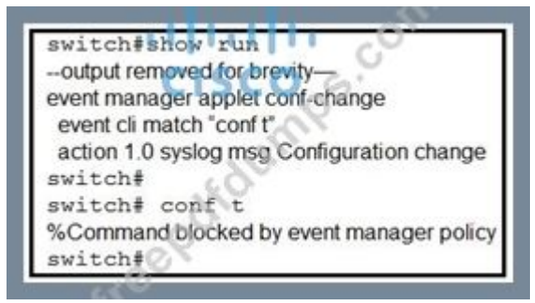
C. Set port mode to NP on edge-2

D. Create VSAN 20 on edge 2

Answer: (SHOW ANSWER)

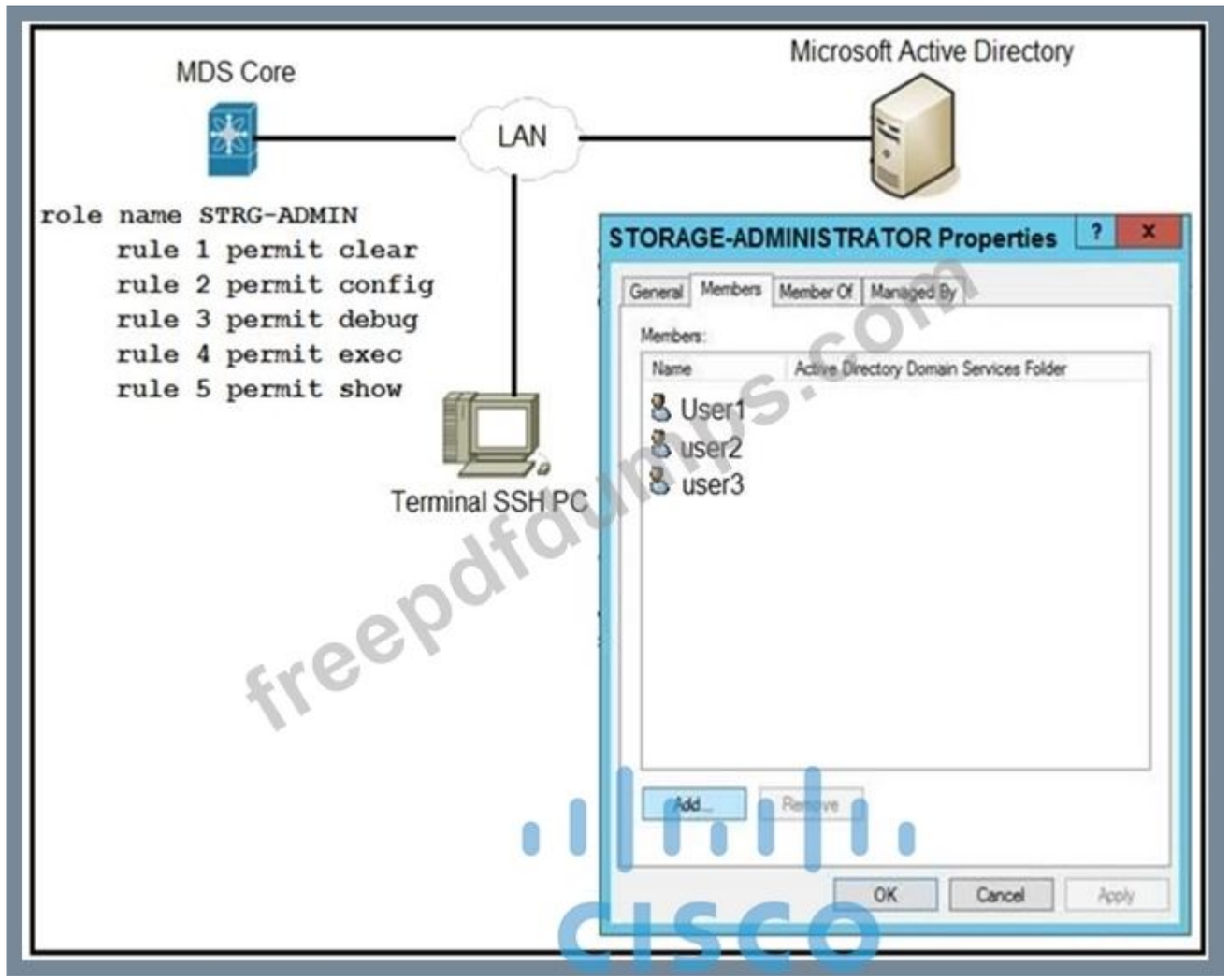
Issue permit distribute on core-2 is the correct fix under Cisco SAN troubleshooting practice. The issue described involves VSAN, Cisco Nexus, Nexus 9000, Cisco Nexus 9000, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 2
Refer to the exhibit.



A network engineer configures an EEM script to get a syslog notification after a configuration change. This message appears when the engineer must make a new configuration to this switch. Which configuration did the engineer neglect to apply in the script for it to function properly?
A. event cli match 'configure terminal'
B. event policy-default count 1 time 100
C. event syslog occurs 10
D. action 2.0 event-default
Answer: (SHOW ANSWER)
action 2.0 event-default is the required fix because the automation failure is caused by execution context, syntax, or resource state around EEM. On Cisco Nexus switches, automation is not a single feature; EEM policies, CLI actions, Guest Shell Linux commands, REST payloads, and scheduled jobs are evaluated by different subsystems. A script can fail even while the switch itself has connectivity or the command works interactively. The selected answer supplies the missing requirement, such as the correct event/action, DNS or resource setting, API URI, payload format, feature enablement, or reboot needed for a Guest Shell change to take effect. The other choices address adjacent features but do not satisfy the failing subsystem. After applying the fix, the engineer should verify the policy registration, job result, API response code, or Guest Shell runtime state and confirm that the intended command is no longer blocked or silently ignored.

NEW QUESTION: 3
Refer to the exhibit.



An engineer is troubleshooting why user1, user2, and user3 from group STORAGE- ADMINISTRATOR in Microsoft Active Directory cannot log in to the Cisco MDS SSH CLI. Which action resolves the issue?

A. Configure the role name to match the group name on Microsoft Active Directory.

B. Include specific users into MDS role configuration.

C. Configure SSH logins on Cisco MDS switch.

D. Integrate Cisco MDS with Microsoft Active Directory.

Answer: (SHOW ANSWER)

Configure the role name to match the group name on Microsoft Active Directory is the correct fix under Cisco SAN troubleshooting practice. The issue described involves MDS, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target.

The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 4

A network engineer is implementing the Cisco ACI Fabric and notices that the Leaf-1 switch is registered, has an assigned name, but is displayed as inactive in the APIC. After further investigation, it became clear that the leaf switch was recently moved from another Cisco ACI environment. Which action resolves the problem?

A. Clean reload the Leaf-1 switch
B. Define the new TEP address for Leaf-1
C. Change the clock offset from low to high between apic 1 and Leaf-1
D. Modify the ISIS interface peering IP address between apic 1 and Leaf-1
Answer: (SHOW ANSWER)
The answer is Clean reload the Leaf-1 switch because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references ACI, APIC; those technologies fail in predictable ways when required parameters do not match or when the required control- plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post- change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

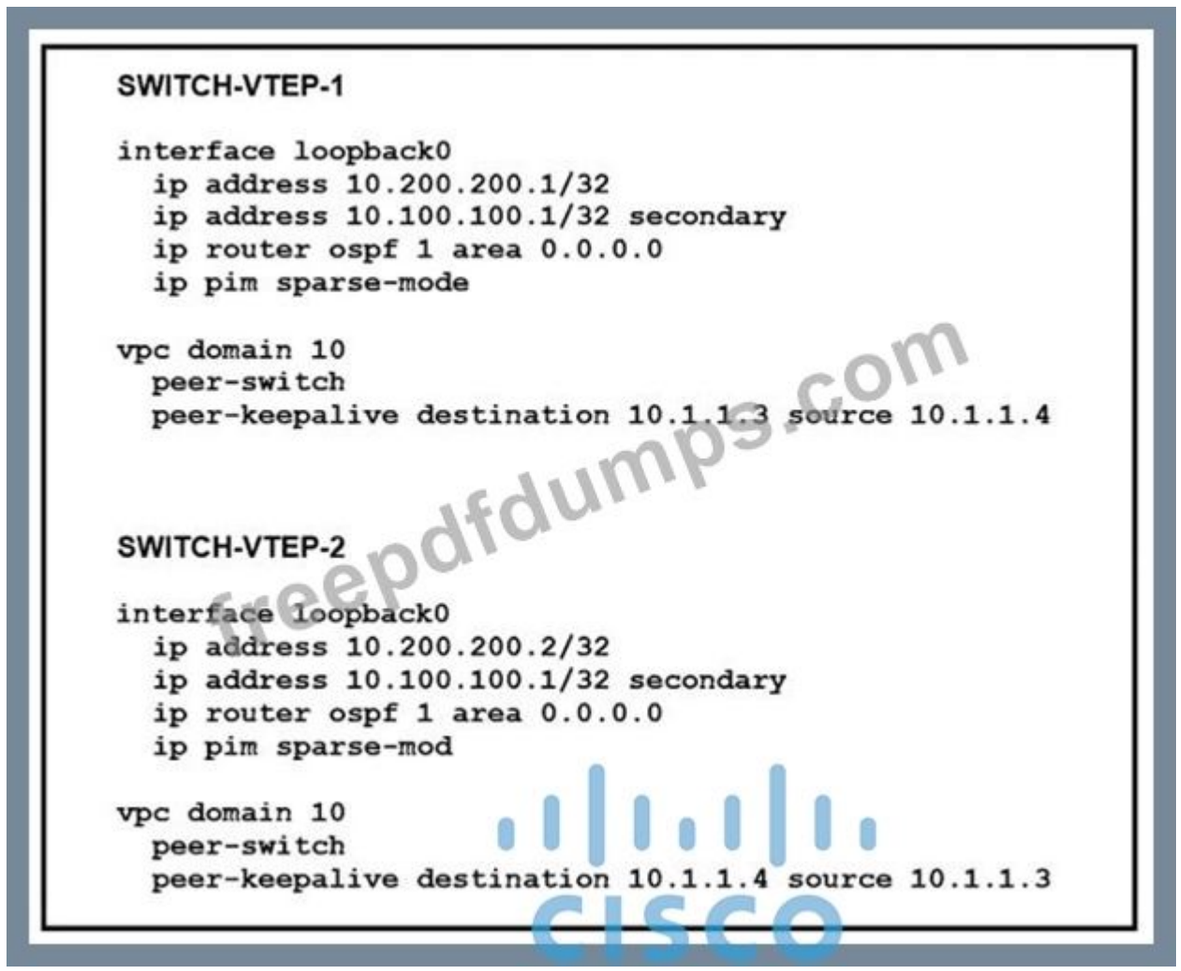
NEW QUESTION: 5

```
[root@guestshell admin]# pip install Markdown
Collecting Markdown
  Retrying (Retry(total=4, connect=None, read=None,
redirect=None)) after connection broken by
'NewConnectionError('<pip.
_vendor.requests.packages.urllib3.connection.VerifiedHTTPSConnec
tion object at 0x23f6850>: Failed to establish a new connection:
[Errno -2] Name or service not known',)': /simple/markdown/
  Could not find a version that satisfies the requirement
Markdown (from versions: )
No matching distribution found for Markdown

[root@guestshell admin]# sudo ip netns exec management ping
8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=59 time=15.8 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=59 time=15.9 ms
64 bytes from 8.8.8.8: icmp_seq=3 ttl=59 time=16.7 ms
```

Refer to the exhibit. A network engineer fails to install applications in a newly deployed Guest Shell on a Cisco Nexus 9000 Series Switch. Which action in the Guest Shell resolves the issue?
A. Add a domain and name server to the resolv.conf file.

B. Install the networking RPM before the PIP install.
C. Configure the mgmt0 IP address.
D. Define the management VRF.
Answer: A (LEAVE A REPLY)
The selected option, Add a domain and name server to the resolv.conf file, is correct for the automation path described. Cisco NX-OS requires precision in EEM applets, scheduler jobs, Guest Shell operations, and REST
/NX-API syntax. The affected element is Guest Shell, Cisco Nexus, Nexus 9000, Cisco Nexus 9000; therefore, the fix must be applied to the component that actually executes the action. For EEM, that means a valid event detector and explicit actions, with event-default when the matched CLI command should continue.
For Guest Shell and Bash, DNS, proxy, resource allocation, and reboot behavior are local to the Linux container. For REST calls, the class name, method, authentication, and XML/JSON structure must match the APIC or NX-OS object model. The distractors usually change the switch globally or alter an unrelated command. Cisco DCIT automation troubleshooting confirms the fix by checking the returned error, then rerunning the exact job, script, or API operation in the same context.

NEW QUESTION: 6



Refer to the exhibit. One of the vPC VTEPs fails to route VXLAN traffic to vPC connected hosts. When the issue was being diagnosed, it was discovered that the packets that were expected to be forwarded to the MAC address on the SWITCH-VTEP-1 are instead forwarded to the MAC address on SWITCH-VTEP-2 and then dropped. Which action resolves the issue?
A. Configure a distributed anycast gateway on both peers
B. Configure ip arp synchronize under the VPC domain on both peers
C. Configure peer-gateway under the VPC domain on both peers

D. Configure a different secondary IP address for one of the vPC peers

Answer: (SHOW ANSWER)

The selected resolution is Configure peer-gateway under the VPC domain on both peers because the failure is in the Fibre Channel/FCoE control path around vPC, VXLAN. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 7

```
Ethernet1/47 is up
admin state is up, Dedicated Interface
  Belongs to Po100
  Hardware: 100/1000/10000/25000 Ethernet, address: 002a.10a3.1cd4 (bia 002a.10a3.1cd4)
  Description: LEAF-SW-01 Eth1/47 (VPC Peer)
  MTU 9216 bytes, BW 10000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 10 Gb/s, media type is 10G
  Beacon is turned off
  Auto-Negotiation is turned on  FEC mode is Auto
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
```

```
Ethernet1/47 is up
admin state is up, Dedicated Interface
  Belongs to Po100
  Hardware: 100/1000/10000/25000 Ethernet, address: 002a.10a3.1cd5 (bia 002a.10a3.1cd5)
  Description: LEAF-SW-01 Eth1/47 (VPC Peer)
  MTU 9216 bytes, BW 1000000 Kbit, DLY 10 usec
  reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, medium is broadcast
  Port mode is trunk
  full-duplex, 1 Gb/s, media type is 10G
  Beacon is turned off
  Auto-Negotiation is turned off  FEC mode is Auto
  Input flow-control is off, output flow-control is off
  Auto-mdix is turned off
  Rate mode is dedicated
  Switchport monitor is off
  EtherType is 0x8100
```

Refer to the exhibit. A network configures a vPC between a pair of Cisco Nexus 9000 Series Switches. The LACP port channel has already been configured, but the port channel fails to be established. Which configuration resolves the issue?

A. no switchport

B. port-type fabric

C. speed auto

D. medium p2p

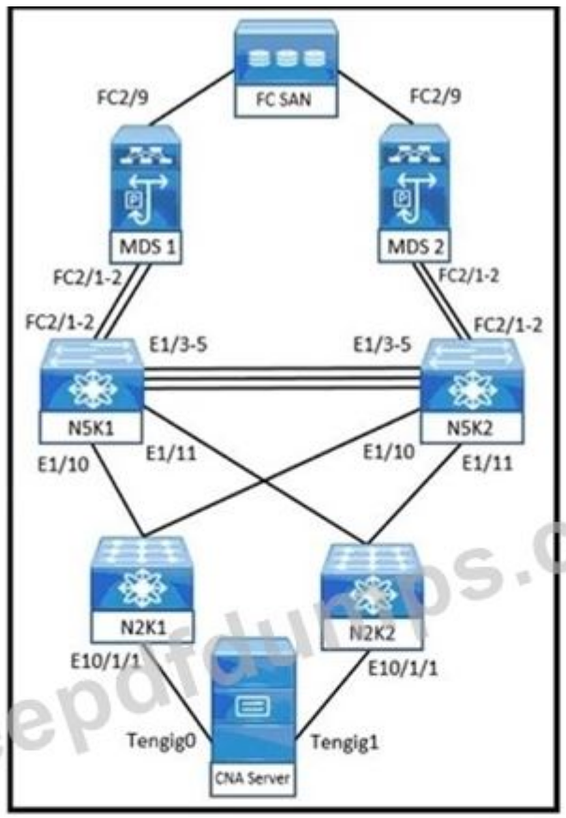
Answer: (SHOW ANSWER)

The answer is speed auto because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references vPC, LACP, Cisco Nexus, Nexus 9000, Cisco Nexus 9000; those technologies fail in predictable ways when required parameters do not match or when the required control-plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host- route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post- change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 8
An engineer troubleshoots a VXLAN EVPN data center. The applications in the data center fail to reach the DNS server that is located at IP 10.10.10.10. The engineer examines the BGP EVPN routing table and notes that the IP prefix route covers the DNS server is missing. Which action resolve the issue?
A. Set the IP prefix route to represent [5]:[0] :[0]:[32] :[10.10.10.10]/224 in the routing table.
B. Configure an IP ARP entry to represent [2]:[0] :[0]:[48] :[0050.569f.1285]:[32] :[10.10.10.10]/272 in the routing table
C. Set the IP prefix route to represent [2]:[0] :[0]:[48] :[0050.569f.1285]:[0] :[0.0.0.0]/216 in the routing table
D. Configure an IP ARP entry to represent [4]:[0300.0000.00fc.bd00.0309l[32] :[10.10.10.10]/136,n the routing table
Answer: (SHOW ANSWER)
The correct remediation is Set the IP prefix route to represent [5]:[0] :[0]:[32] :[10.10.10.10]/224 in the routing table. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on VXLAN, EVPN, BGP, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF.
This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 9
The external routes fail to propagate to leaf switches in Cisco ACI fabric Which two actions resolve the issue?
(Choose two.)
A. Enable the VTEP pool in the fabric
B. Assign an MP-BGP AS number to the fabric.
C. Specify the spine nodes as route reflectors
D. Associate the correct contract to the L30ut.
E. Configure an MP-BGP area.
Answer: B,C (LEAVE A REPLY)
Assign an MP-BGP AS number to the fabric; Specify the spine nodes as route reflectors is the valid corrective action because the failure described is a protocol or fabric state problem, not a generic connectivity issue. For BGP, ACI, Cisco troubleshooting expects the engineer to compare both endpoints of the relationship: vPC peers must agree on consistency parameters, HSRP peers must exchange hellos in the same VLAN and version context, OSPF/BGP peers must match the attributes required for stable adjacency, and VXLAN EVPN must advertise the correct host or prefix information. The selected option restores that required state.
The other options either operate on the wrong layer, change a value that is not used to form the relationship, or would make the peer relationship less deterministic. A clean validation is to inspect the control-plane table first, then verify the forwarding table, and finally test end-to-end traffic. This is the Cisco-preferred approach because it avoids random changes and confirms that the fabric is forwarding based on correct protocol state.

NEW QUESTION: 10




```
N5K1# show platform software fcoe_mgr event-history errors
1) Event:E_DEBUG, length:93, at 203962 usecs after Wed Jun 12
20:33:04 2019 [102] fcoe_mgr_vfc_ac_eval(4946):
DEBUG:shut:Sending event to delete protos of vfc1 due to 62
2) Event:E_DEBUG, length:119, at 197505 usecs after Wed Jun 12
20:33:04 2019  [102] fcoe_mgr_fc2_msg_handler(5706): proto
if_index 1e000000 p_proto (nil)and oxid 8805fc2 usrhandle 0[0]
iuhdr type:1
3) Event:E_DEBUG, length:91, at 197053 usecs after Wed Jun 12
20:33:04 2019 [102] fcoe_mgr_proto_ac_eval(1847): >Bringing down
PROTO 1e000000 due to
truly missing fka
```

Refer to the exhibit. An engineer discovered a VFC interface in a down state on a Cisco Nexus Switch. Which action resolves the problem?

A. Change the cable between the switch and the server

B. Reset the Cisco Nexus port toward the file server

C. Update the CNA firmware and driver versions

D. Modify the fip keepalive message time to 30 seconds

Answer: (SHOW ANSWER)

The correct answer is Update the CNA firmware and driver versions. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV/NPIV, or port-security policy. This question focuses on firmware, Cisco Nexus, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to

change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator-to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 11
An engineer is implementing a storage VDC, but fails. Which two prerequisites must be in place before a storage VDC is implemented? (Choose two.)
A. M-Series module
B. ESSENTIALS license
C. STORAGE-ENT license
D. FCoE license
E. F-Series module
Answer: D,E (LEAVE A REPLY)
The selected resolution is FCoE license; F-Series module because the failure is in the Fibre Channel/FCoE control path around FCoE. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 12
Refer to the exhibit.

```
[admin@guestshell ~]$ sudo yum install docker
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
Could not retrieve mirrorlist http://mirrorlist.centos.org/?release=7&arch=x86_64&repo=os&infra=stock error w
14: curl#6 - "Could not resolve host: mirrorlist.centos.org; Unknown error"


 One of the configured repositories failed (Unknown),
 and yum doesn't have enough cached data to continue. At this point the only
 safe thing yum can do is fail. There are a few ways to work "fix" this:

     1. Contact the upstream for the repository and get them to fix the problem.

     2. Reconfigure the baseurl/etc. for the repository, to point to a working
        upstream. This is most often useful if you are using a newer
        distribution release than is supported by the repository (and the
        packages for the previous distribution release still work).

     3. Disable the repository, so yum won't use it by default. Yum will then
        just ignore the repository until you permanently enable it again or use
        --enablerepo for temporary usage:

            yum-config-manager --disable <repoid>

     4. Configure the failing repository to be skipped, if it is unavailable.
        Note that yum will try to contact the repo. when it runs most commands,
        so will have to try and fail each time (and thus. yum will be be much
        slower). If it is a very temporary problem though, this is often a nice
        compromise:

            yum-config-manager --save --setopt=<repoid>.skip_if_unavailable=true

Cannot find a valid baseurl for repo: base/7/x86_64
[admin@guestshell ~]$ ping mirrorlist.centos.org
ping: unknown host mirrorlist.centos.org
```

```
[admin@guestshell ~]$ cat /etc/resolv.conf
[admin@guestshell ~]$
```

An engineer fails to install Perl in the guest shell on a Cisco Nexus 9000 Series Switch. Which two actions must be taken in the guest shell to resolve the issue? (Choose two.)

A. Add the DNS server and suffix.

B. Add a default gateway and nameserver.

C. Install the unbound resolver package using curl.

D. Configure domain-name and nameserver under the management VRF.

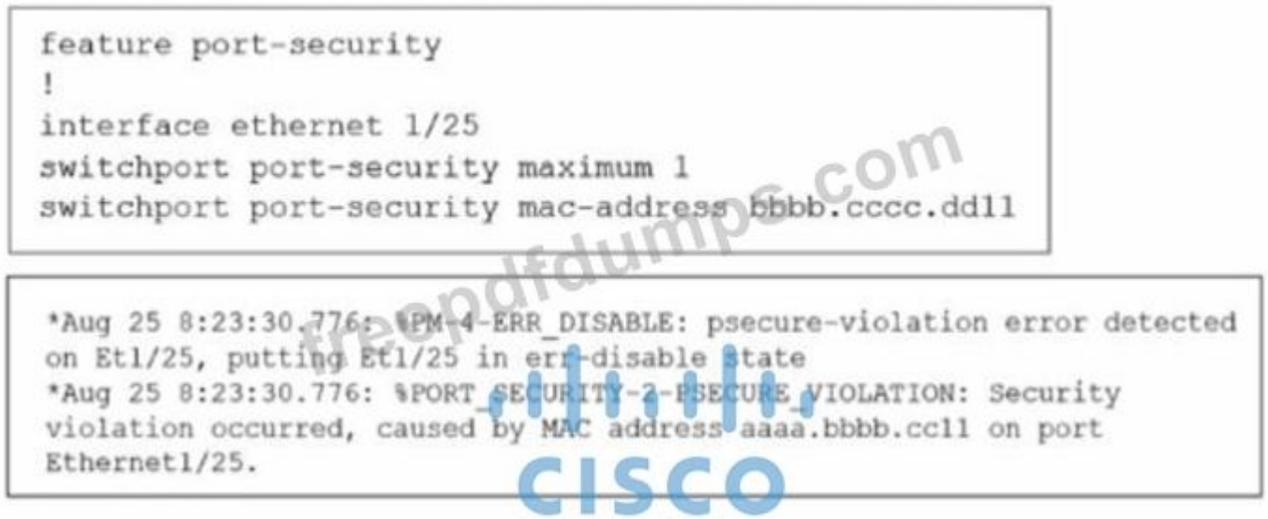
E. Export the http_proxy and https_proxy environment variables

Answer: A,D (LEAVE A REPLY)

Add the DNS server and suffix; Configure domain-name and nameserver under the management VRF resolves the problem because the symptom is specific to the automation subsystem handling Guest Shell, Cisco Nexus, Nexus 9000, Cisco Nexus 9000. Nexus automation failures are frequently caused by a missing EEM event statement, absent event-default action, invalid REST path, incorrect JSON or XML syntax, Guest Shell DNS/resource settings, or a scheduler feature that is not enabled. The selected answer corrects that execution prerequisite. The wrong options may make sense for normal switch forwarding, but they do not repair the automation control path. Cisco documentation treats Guest Shell as a separate Linux environment and EEM as a policy engine that can intercept CLI events; both must be validated from their own

operational state. A proper verification is to confirm the policy is registered, run the job or API call again, review the response or syslog output, and ensure that normal CLI behavior is preserved after the automation fires.

NEW QUESTION: 13



Refer to the exhibit. An engineer connected a Cisco UCS-C Series server to port Ethernet 1/25 on the Cisco Nexus Series Switch. After the cable is connected, the server does not have connectivity to the network and the port light indicator shows as disabled. Which command set resolves the issue?

A. interface ethernet 1/25
switchport port-security maximum 1
switchport port-security mac-address aaaa.bbbb.cc.11
switchport port-security violation protect

B. interface ethernet 1/25
switchport port-security maximum 1
switchport port-security mac-address aaaa.bbbb.cc.11

C. interface ethernet 1/25
switchport port-security maximum 2
no switchport port-security mac-address bbbb.cccc.dd11

D. interface ethernet 1/25
switchport port-security maximum 1
switchport port-security mac-address bbbb.cccc.dd11

Answer: D (LEAVE A REPLY)

The correct action is interface ethernet 1/25 switchport port-security maximum 1 switchport port-security mac- address bbbb.cccc.dd11. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves UCS, Cisco Nexus, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.

NEW QUESTION: 14

Refer to the exhibit.
The FCoE traffic fails to traverse the vfc2 interface. The VSAN 102 is configured for vfc2. Which action resolves the issue?
A. Enable LLDP on the interface vfc2
B. Activate DCBX on the N9K switch
C. Activate DCBX on the interface e101/1/2
D. Enable LLDP on the neighbor switch
Answer: D (LEAVE A REPLY)
The correct answer is Enable LLDP on the neighbor switch. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV/NPIV, or port-security policy. This question focuses on VSAN, FCoE, DCBX, LLDP, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator-to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 15
An engineer must upgrade all components in a Cisco UCS domain to the same package version, but the upgrade process fails to complete. Which set of Auto Install actions resolves the problem?
A. Install Infrastructure Firmware, then Install Server Firmware.
B. Install infrastructure Firmware, then Install Hypervisor Firmware.
C. Install Hypervisor Firmware, then Install Infrastructure Firmware
D. Install Server Firmware, then Install Infrastructure Firmware
Answer: A (LEAVE A REPLY)
Install Infrastructure Firmware, then Install Server Firmware is correct because the failure is tied to the UCS managed state of UCS, firmware, Auto Install. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table.
If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

NEW QUESTION: 16

An engineer configures FCoE between a set of ESXi hosts and a Cisco Nexus 5000 Series Switch. The Converged Network Adapter of the host fails to receive the response from the Cisco Nexus device. Also, the VFC interface is in a down state and the FIP adapter fails to receive 802.1q tagged frames. The host interface is configured for VLAN trunking. Which action resolves the issue?

A. Activate the reception of Xoff pause frames from the server

B. Configure the UF link as a spanning-tree edge port

C. Enable the active STP port state on the bound Ethernet interface

D. Set the bound Ethernet trunk interface to non-FCoE native VLAN

Answer: (SHOW ANSWER)

The correct answer is Set the bound Ethernet trunk interface to non-FCoE native VLAN. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV /NPIV, or port-security policy. This question focuses on FCoE, Cisco Nexus, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator-to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 17

What does this adapter output indicate?

adapter 1/6/1 (fls): 2# lunlist 9

vnic: 9 lifid: 6

- FLOGI State : flogi est (fc_id Oxac0e04)
- PLOGI Sessions
- WWNN 50:0a:09:83:8d:53:43:44 WWPN 50:0a:09:83:8d:53:43:44 fc_id 0x000000
- LUN ' s configured (SCSI Type, Version, Vendor, Serial No.)
- LUN ID: Ox0000000000000000 access failure

-REPORT LUNs Query Response

- Nameserver Query Response

-WWPN: 54:b1:6a:94:64:3e:73:44

A. The configured initiator LUN ID does not match the configured target LUN ID

B. The target device configuration does not allow the initiator to access the LUN

C. The port types between the target and initiator are incorrectly configured

D. The target of the configured zone does not match the target of the configured boot order

Answer: D (LEAVE A REPLY)

The target of the configured zone does not match the target of the configured boot order is the required SAN- side correction. In Cisco storage fabrics, symptoms such as isolated ports, missing targets, failed zone merges, vFC down state, or inaccessible LUNs are rarely solved by changing a random endpoint setting. The engineer must

validate the FC control-plane dependency associated with FLOGI, PLOGI, vNIC: VSAN assignment, trunk allowance, FSPF parameters, fcdomain uniqueness, NPIV support, NPV uplink behavior, DCBX/LLDP negotiation, and active zoning. The selected answer is the one that restores that dependency. Other choices may be valid operational commands in a different failure, but they do not address the precise point where fabric membership or access control is broken. Cisco guidance is to verify the active database and the operational database separately because a configured object is not necessarily active in the fabric. Post- remediation checks should include interface state, VSAN status, FLOGI/PLOGI, zoneset membership, and target visibility from the initiator.

NEW QUESTION: 18
Refer to the exhibit.

```
event manager applet config_monitor
event cli match "conf t"
action 1.0 snmp-trap strdata "User has entered into configuration mode"
```

The EEM script fails to send an SNMP trap when a user attempts to enter configuration mode. Which configuration is missing from the script?
A. event statement
B. event-default action statement
C. policy-default action statement
D. IP address of the SNMP server
Answer: (SHOW ANSWER)
event statement resolves the problem because the symptom is specific to the automation subsystem handling EEM, SNMP. Nexus automation failures are frequently caused by a missing EEM event statement, absent event-default action, invalid REST path, incorrect JSON or XML syntax, Guest Shell DNS/resource settings, or a scheduler feature that is not enabled. The selected answer corrects that execution prerequisite. The wrong options may make sense for normal switch forwarding, but they do not repair the automation control path.
Cisco documentation treats Guest Shell as a separate Linux environment and EEM as a policy engine that can intercept CLI events; both must be validated from their own operational state. A proper verification is to confirm the policy is registered, run the job or API call again, review the response or syslog output, and ensure that normal CLI behavior is preserved after the automation fires.

NEW QUESTION: 19
Refer to the exhibit.

```
event manager applet Script_1
event cli match "administratively down"
action 1.0 cli local tclsh Config.tcl
```

An EEM applet must be used to run a Python file called " Config " that enables all administratively disabled interfaces. The script fails to run as expected. Which command resolves the issue?
A. action 1.0 cli local python Config.py
B. action 1.0 cli local tclsh Config
C. action 1.0 cli local tclsh Script_1
D. action 1.0 cli local python Script_1.py
Answer: A (LEAVE A REPLY)

The selected option, action 1.0 cli local python Config.py, is correct for the automation path described. Cisco NX-OS requires precision in EEM applets, scheduler jobs, Guest Shell operations, and REST/NX-API syntax.
The affected element is EEM; therefore, the fix must be applied to the component that actually executes the action. For EEM, that means a valid event detector and explicit actions, with event-default when the matched CLI command should continue. For Guest Shell and Bash, DNS, proxy, resource allocation, and reboot behavior are local to the Linux container. For REST calls, the class name, method, authentication, and XML
/JSON structure must match the APIC or NX-OS object model. The distractors usually change the switch globally or alter an unrelated command. Cisco DCIT automation troubleshooting confirms the fix by checking the returned error, then rerunning the exact job, script, or API operation in the same context.

NEW QUESTION: 20
Refer to the exhibit.

```
vrf context management
 ip name-server 4.2.2.2
 ip route 0.0.0.0/0 192.168.30.2

interface mgmt0
 ip address dhcp
 vrf member management

N9K-Core# ping google.com vrf management
PING google.com (216.58.209.238): 56 data bytes
64 bytes fron 216.58.209.238: icmp_seq=0 ttl=127 time=151.982 ms
64 bytes fron 216.58.209.238: icmp_seq=1 ttl=127 time=136.198 ms
64 bytes fron 216.58.209.238: icmp_seq=2 ttl=127 time=224.796 ms
64 bytes fron 216.58.209.238: icmp_seq=3 ttl=127 time=148.458 ms
64 bytes fron 216.58.209.238: icmp_seq=4 ttl=127 time=129.98 ms

- - - google.com ping statistics - - -
5 packets transmitted, 5 packets received, 0.00% packet loss
round-trip min/avg/max = 129.98/158.282/224.796 ms
```

A network engineer has connected the Nexus switch management port to the Internet using DHCP to allow the Guest shell running on the switch to download Python packages. The engineer can ping google.com successfully from the Nexus switch, but the Guest shell failed to download any Python packages. Which action resolves the problem?
A. Update the Python packages on the Cisco Nexus switch directly.
B. Manually configure DNS in the Guest shell, even if it is claimed on the Cisco Nexus switch through DHCP.
C. Manually configure NTP in the Guest shell.
D. Connect Guest shell to data plane interfaces to be able to connect to the networks outside the Cisco Nexus switch.
Answer: B (LEAVE A REPLY)
Manually configure DNS in the Guest shell, even if it is claimed on the Cisco Nexus switch through DHCP is the required fix because the automation failure is caused by execution context, syntax, or resource state around Guest Shell, Cisco Nexus. On Cisco Nexus switches, automation is not a single feature; EEM policies, CLI actions, Guest

Shell Linux commands, REST payloads, and scheduled jobs are evaluated by different subsystems. A script can fail even while the switch itself has connectivity or the command works interactively. The selected answer supplies the missing requirement, such as the correct event/action, DNS or resource setting, API URI, payload format, feature enablement, or reboot needed for a Guest Shell change to take effect. The other choices address adjacent features but do not satisfy the failing subsystem. After applying the fix, the engineer should verify the policy registration, job result, API response code, or Guest Shell runtime state and confirm that the intended command is no longer blocked or silently ignored.

NEW QUESTION: 21
Refer to the exhibit.

```
Error Message    PORT-7-IF_DOWN_DOMAIN_OVERLAP_ISOLATION: Interface [chars] is down
```

An engineer troubleshoots an issue invoking where some Cisco MDS 9000 Series Switches fail to be discovered by other MDS switches in the VSAN. The engineer receives the error message shown Which action resolves the issue?
A. Assign a new alias to port 7 and reset the port worldwide name.
B. Move port 7 to VSAN 1 to remove the port from isolation
C. Assign a new domain ID to the isolated switch
D. Restart the domain manager and reset port 7
Answer: C (LEAVE A REPLY)
The selected resolution is Assign a new domain ID to the isolated switch because the failure is in the Fibre Channel/FCoE control path around MDS, VSAN. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 22
Refer to the exhibit.

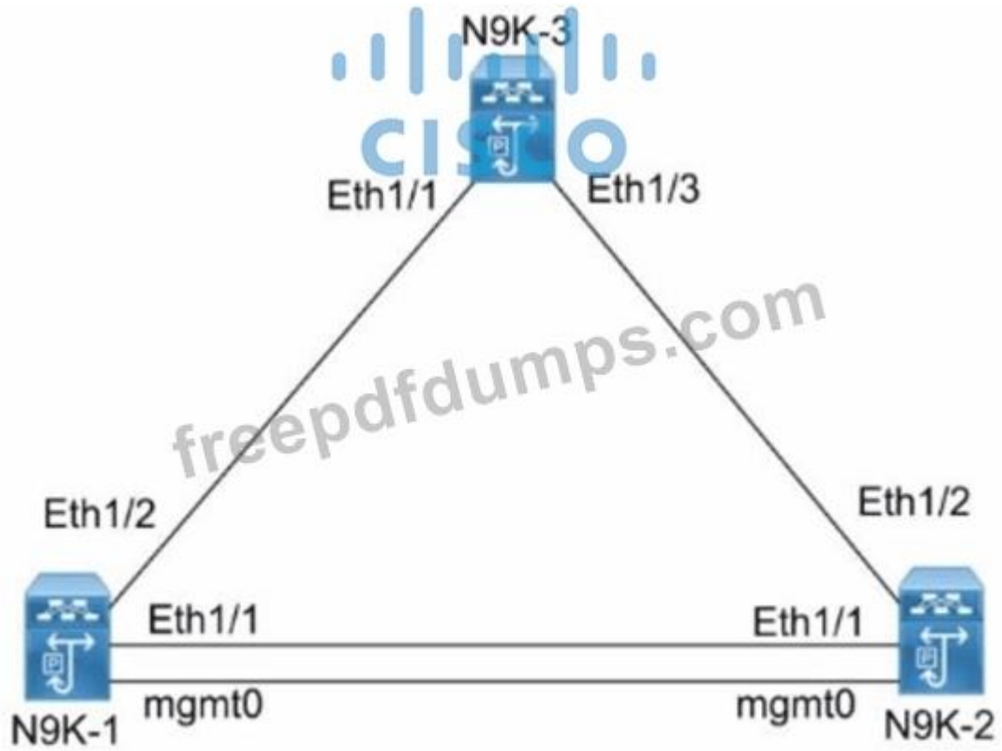
A Postman call to a Cisco APIC fails. The access credentials were confirmed to be configured as expected.
Which action resolves the issue?
A. Change operation type to POST
B. Modify the protocol to HTTP

C. Change the IP address to a domain name
D. Modify the target protocol type to XML
Answer: A (LEAVE A REPLY)
Change operation type to POST resolves the problem because the symptom is specific to the automation subsystem handling APIC, Postman. Nexus automation failures are frequently caused by a missing EEM event statement, absent event-default action, invalid REST path, incorrect JSON or XML syntax, Guest Shell DNS/resource settings, or a scheduler feature that is not enabled. The selected answer corrects that execution prerequisite. The wrong options may make sense for normal switch forwarding, but they do not repair the automation control path. Cisco documentation treats Guest Shell as a separate Linux environment and EEM as a policy engine that can intercept CLI events; both must be validated from their own operational state. A proper verification is to confirm the policy is registered, run the job or API call again, review the response or syslog output, and ensure that normal CLI behavior is preserved after the automation fires.

NEW QUESTION: 23

Refer to the exhibit. A network engineer creates an EEM script to trigger an SNMP notification when a user enters configuration mode, but the trap is not received when the condition is met. Which action resolves the issue?
A. Append action 2.0 event-default to the script
B. Append action 2.0 cli "conf t" to the script
C. Modify snmp-trap strdata "Configuration changed" to syslog msg Configuration changed
D. Modify cli match "conf t" to "snmp match "conf t"
Answer: A (LEAVE A REPLY)
The correct answer is Append action 2.0 event-default to the script. Cisco NX-OS automation features are context-sensitive: Guest Shell, Bash, EEM, scheduler, NX-API, REST calls, and Python scripts each run with their own parser, privilege model, environment, and resource limits. The scenario involves EEM, SNMP, and the selected action corrects the missing execution condition. Cisco documentation for Nexus programmability states that Guest Shell resources and networking must be configured inside the Guest Shell context, EEM applets require a valid event statement and event-default when the intercepted CLI command must continue, and API calls must target the correct managed object or class. The alternative answers either operate in the wrong context, omit a required trigger/action, or correct a parameter unrelated to the failure. Validation should include running the command manually in the same context, checking logs or return codes, and confirming that the automation completes without blocking the normal NX-OS operation it observes.

NEW QUESTION: 24
Refer to the exhibit.




```
N9K-2(config)# interface mgmt0
N9K-2(config-if)# ip address 10.90.90.5/24
N9K-2(config)# feature vpc
N9K-2(config)# feature lacp
N9K-2(config)# vpc domain 100
N9K-2(config)# interface Po100
N9K-2(config-if)# switchport mode trunk
N9K-2(config-if)# vpc peer-link
N9K-2(config)# interface E1/1
N9K-2(config-if)# channel-group 100 mode active
N9K-2(config-if)# int E1/2
N9K-2(config-if)# channel-group 2 mode active
```

```
N9K-3(config)# feature lacp
N9K-3(config)# interface E1/1
N9K-3(config-if)# channel-group 9 mode active
N9K-3(config-if)# int E1/3
N9K-3(config-if)# channel-group 9 mode active

N9K-3(config)# show port-channel summary
Flags:  D - Down        P - Up in port-channel (members)
        I - Individual  H - Hot-standby (LACP only)
        s - Suspended   r - Module-removed
        b - BFD Session Wait
        S - Switched    R - Routed
        U - Up (port-channel)
        p - Up in delay-lacp mode (member)
        M - Not in use. Min-links not met
--------------------------------------------------------------------------------
Group Port-       Type     Protocol  Member Ports
      Channel
--------------------------------------------------------------------------------
9     Po2(SU)     Eth      LACP      Eth1/2(P)    Eth1/3(s)
```

Which action must be taken to change the interface Eth1/3 on N9K-3 from suspended to up in the port channel?

A. Change channel-group 9 mode from active to passive on N9K-3.

B. Add peer-keepalive source and destination under vPC domain 100 for N9K-1 and N9K-2.

C. Change channel-group ID from 9 to 2 on N9K-3.

D. Add vPC number under interface port-channel 2 for N9K-1 and N9K-2.

Answer: (SHOW ANSWER)

Cisco troubleshooting logic supports Change channel-group ID from 9 to 2 on N9K-3 as the required fix. In this question the symptoms point to vPC, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state

machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.

NEW QUESTION: 25
An engineer upgrades Cisco UCS firmware from release 3. 1(2) to release 3. 1(3) using Auto Install. Both fabric interconnects go offline during the software upgrade installation and issue multiple F SM retries in the DeployPollActivate stage. Which set of actions resolves the issue?
A. Fix the rights to 666 with the debug plugin on the primary fabric interconnet Save the current configuration on the running fabric interconnect.
Continue the upgrade on both fabric interconnects.
B. Enable the management interface monitoring policy on the fabric interconnects. Initiate a configuration backup on both fabric interconnects.
Commit the pending fabric interconnect reboot activity.
C. Acknowledge the error and reboot the primary fabric interconnect. Clear the default firmware version and upload a new one.
Restart the upgrade process manually.
D. Clear the startup version of the default infrastructure and server pack. Remove the service pack from the subordinate node.
Upgrade with the Force attribute through Auto Install.
Answer: D (LEAVE A REPLY)
The selected answer, the selected actions, follows Cisco UCS operational logic. UCS Manager is policy- driven, so troubleshooting must determine whether the problem is caused by hardware discovery, service profile association, firmware activation, boot order, storage presentation, or management integration. The scenario points to UCS, firmware, Auto Install, fabric interconnect; that is why the selected action fixes the root condition rather than merely restarting the server. The wrong options either affect a different policy, require unnecessary disruption, or assume that physical connectivity alone is sufficient. Cisco documentation for UCS server boot and firmware management stresses that boot policies must include the correct target details, firmware workflows must complete their FSM stages, and hardware changes often require acknowledgement or re-acknowledgement before UCS Manager uses the new inventory. After remediation, the engineer should confirm that the UCS fault is cleared, the server association or discovery state is complete, and the operating system or management service can use the intended path.

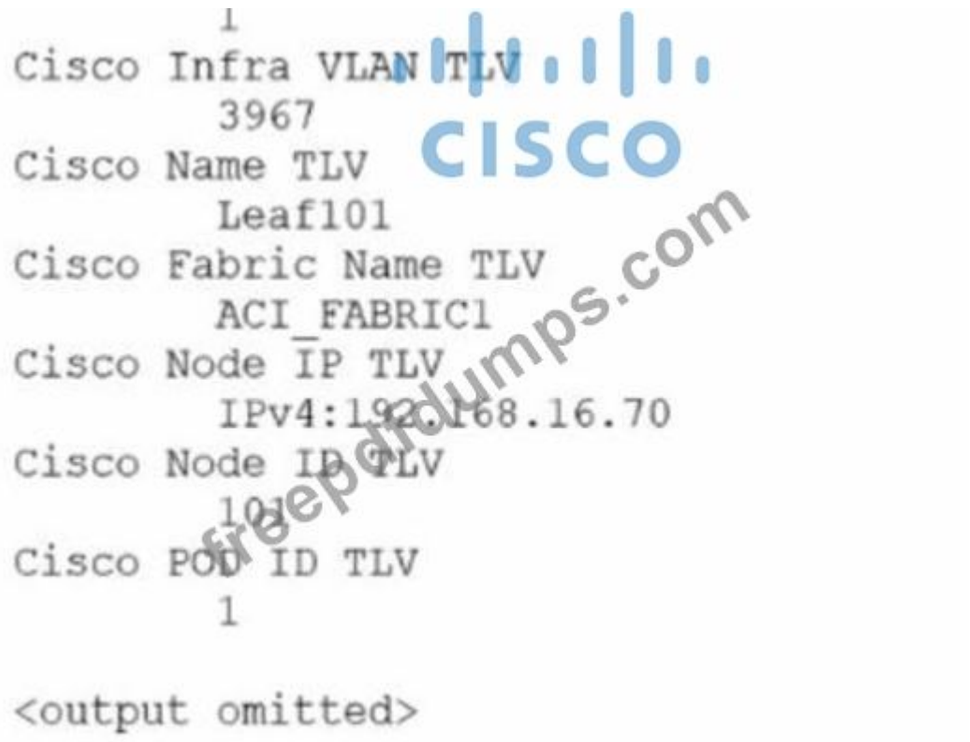
NEW QUESTION: 26
Refer to the exhibit.

```
UCS-1-A# connect nxos
UCS-1-A(nx-os)# show flogi database
^
% Invalid command at '^' marker.
UCS-1-A(nx-os)#
```

An administrator directly connects a Fibre Channel storage array to ports 1 through 4 on a Cisco UCS 6454 Fabric Interconnect. The administrator configures a service profile to boot directly from the new Fibre Channel storage array, but the service profile fails to boot. When the administrator checks the output of the show flogi database command on the fabric interconnect, it shows the output presented in the exhibit. Which action resolves the issue?
A. Configure the Zoning Type in vHBA Initiator Group as Multiple Initiator Single Target.
B. Configure the fabric interconnects in Fibre Channel switch mode.
C. Configure the Zoning Type in vHBA Initiator Group as Multiple Initiator Multiple Target.
D. Configure the fabric interconnects in Fibre Channel end-host mode
Answer: B (LEAVE A REPLY)
Configure the fabric interconnects in Fibre Channel switch mode is the correct fix under Cisco SAN troubleshooting practice. The issue described involves FLOGI, UCS, service profile, vHBA, fabric interconnect, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database.

MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

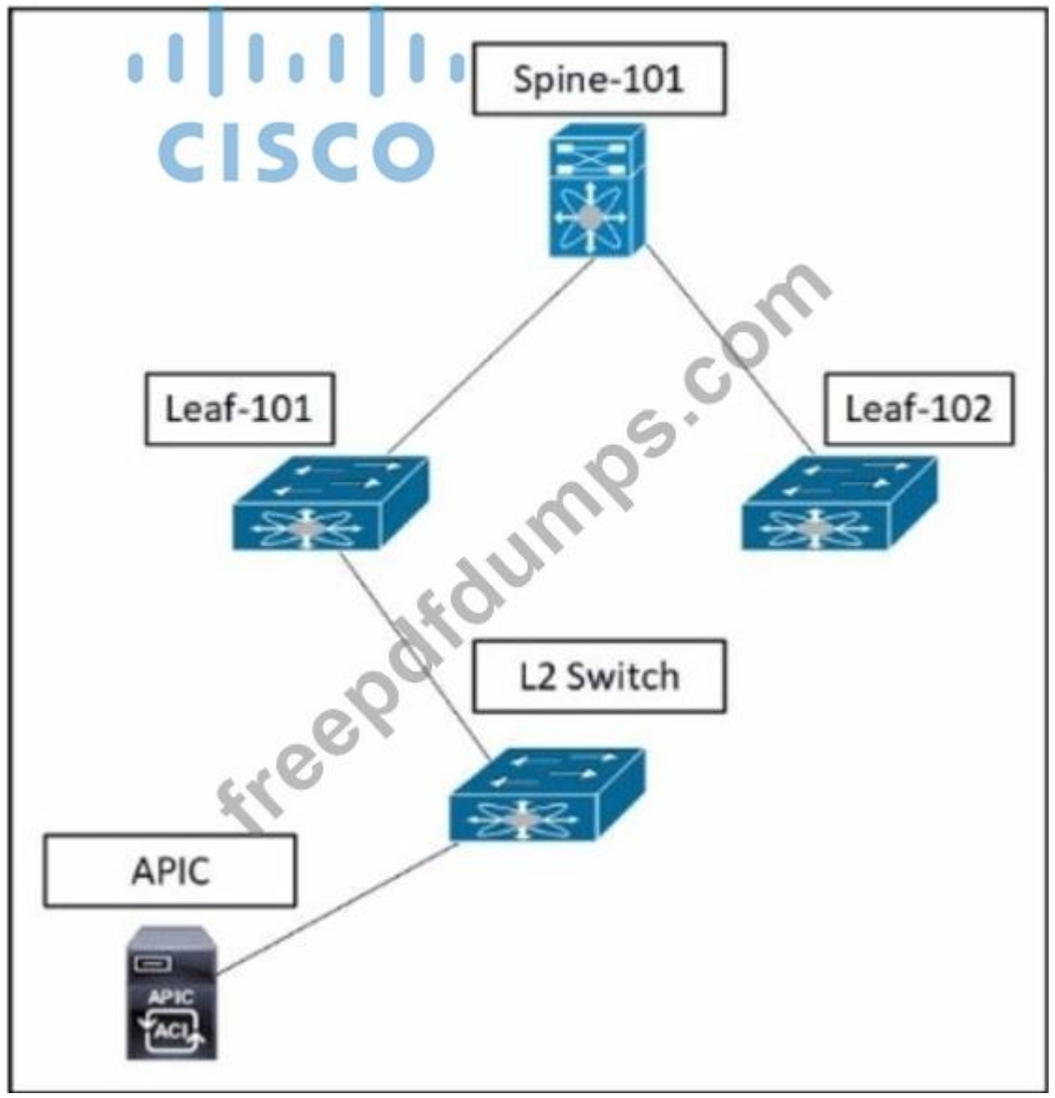
NEW QUESTION: 27
Refer to the exhibit.



A newly deployed Cisco APIC1 fails to discover a Cisco Nexus Series Switch. Which configuration resolves the issue?
A. Leaf101#(config)# no boot nxos
Leaf101# copy running-config startup-config
Leaf101# reload
B. APIC1# acidiag touch clean
APIC1# acidiag touch setup
APIC1# acidiag reboot
C. Leaf101# setup-clean-config.sh
Leaf101# reload
D. APIC1# acidiag restart mgmt
PIC1# acidiag reboot
Answer: C (LEAVE A REPLY)
Leaf101# setup-clean-config.sh Leaf101# reload is the valid corrective action because the failure described is a protocol or fabric state problem, not a generic connectivity issue. For Cisco Nexus, Cisco troubleshooting expects the engineer to compare both endpoints of the relationship: vPC peers must agree on consistency parameters, HSRP peers must exchange hellos in the same VLAN and version context, OSPF/BGP peers must match the attributes required for stable adjacency, and VXLAN EVPN must advertise the correct host or prefix information. The selected option restores that required state. The other options either operate on the wrong layer, change a value that is not used to form the relationship, or would make the peer relationship less deterministic. A clean validation is to inspect the control-plane table first, then verify the forwarding

table, and finally test end-to-end traffic. This is the Cisco-preferred approach because it avoids random changes and confirms that the fabric is forwarding based on correct protocol state.

NEW QUESTION: 28



Refer to the exhibit. An engineer is troubleshooting an issue with the Cisco ACI fabric discovery. During the Cisco APIC initialization, the infra VLAN was set to 4, and the TEP pool was configured to use subnet
11.0.0.0/16. Which action resolves the issue?

A. Connect the Layer 2 switch to Leaf-101 and Leaf-102.

B. Connect the Cisco APIC directly to Leaf-101.

C. Set the Enable LLDP flag on Cisco APIC CIMC.

D. Set the TEP pool to subnet 10.0.0.0/16.

Answer: B (LEAVE A REPLY)

Connect the Cisco APIC directly to Leaf-101 is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving ACI, APIC, LLDP, CIMC must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct

vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 29

Refer to the exhibit.

```
Cisco VIC iSCSI, Boot Driver Version 2.0 (1w)
(C) 2010 Cisco Systems, Inc.
Initialize error 1
```

An engineer is configuring boot from iSCSI on a Cisco UCS B-Series Blade Server, but the LUN fails to mount. Which action resolves the issue?

A. Statically configure the target information in the Boot Policy.

B. Configure an MTU size of 9000 on the appliance port.

C. Configure a QoS policy on the vNIC.

D. Set a connection timeout value of 250 in the iSCSI Adapter Policy.

Answer: (SHOW ANSWER)

Statically configure the target information in the Boot Policy is the correct fix under Cisco SAN troubleshooting practice. The issue described involves UCS, vNIC, iSCSI, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 30

```
1  mdsswitch# show port-security database active
2  ---------------------------------------------------------------------------
3
4  VSAN        Logging-in Entity              Logging-in Point        (Interface)     Learnt
5  ---------------------------------------------------------------------------
6
7
8
9  1           20:00:00:ee:ab:1e:ae:76(pwwn)  20:00:00:10:9b:5b:f0:70(fc1/4)          Yes
10
11
12 [Total 1 Entries]
```


Refer to the exhibit. A SAN engineer must enforce the port security configuration database in Fibre Channel fabric that uses Cisco MDS 9000 Switches. Port security is enabled on the VSAN to which the port belongs.

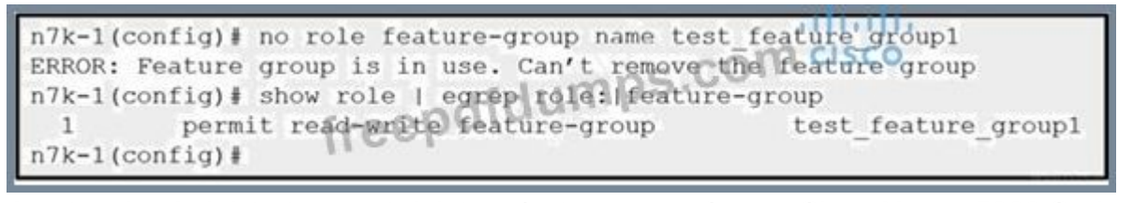
However, the rogue host can still log in to the fabric. Which Cisco MDS command resolves the issue?

A. Option A
B. Option B
C. Option C
D. Option D
Answer: (SHOW ANSWER)
The correct answer is Option A. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV/NPIV, or port-security policy. This question focuses on MDS, VSAN, port security, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator- to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 31
After upgrading a client's fabric interconnect to the latest version, an engineer discovers that the appliance has lost its entire configuration. Which two locations should an engineer check to confirm that the appliance had backed up the configuration prior to the upgrade in order to retrieve the lost configuration? (Choose two.)
A. Equipment FSM page, InternalBackup stage
B. Service profiles page, InternalBackup stage
C. Admin page, PollInternalBackup stage
D. Equipment FSM page, PollInternalBackup stage
E. Admin page, InternalBackup stage.
Answer: A,D (LEAVE A REPLY)
The correct action is Equipment FSM page, InternalBackup stage; Equipment FSM page, PollInternalBackup stage. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves fabric interconnect, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.

NEW QUESTION: 32

Refer to the exhibit.



A network administrator must delete a feature group from a Cisco Nexus 5000 Series Switch. Which action resolves the issue?

A. Detach the association with the no rule command within the role configuration mode

B. Detach the association with the no role command within the feature-group configuration mode

C. Detach the association with the no rule command within the feature-group configuration

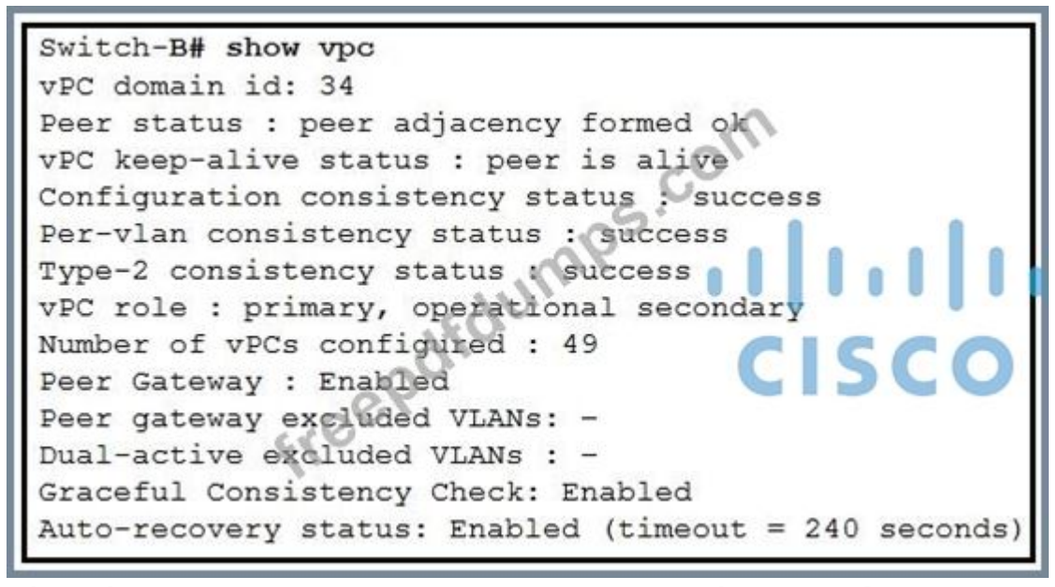
D. Detach the association with the no role command within the role configuration mode

Answer: B (LEAVE A REPLY)

Cisco troubleshooting logic supports Detach the association with the no role command within the feature- group configuration mode as the required fix. In this question the symptoms point to Cisco Nexus, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.

NEW QUESTION: 33

Refer to the exhibit.

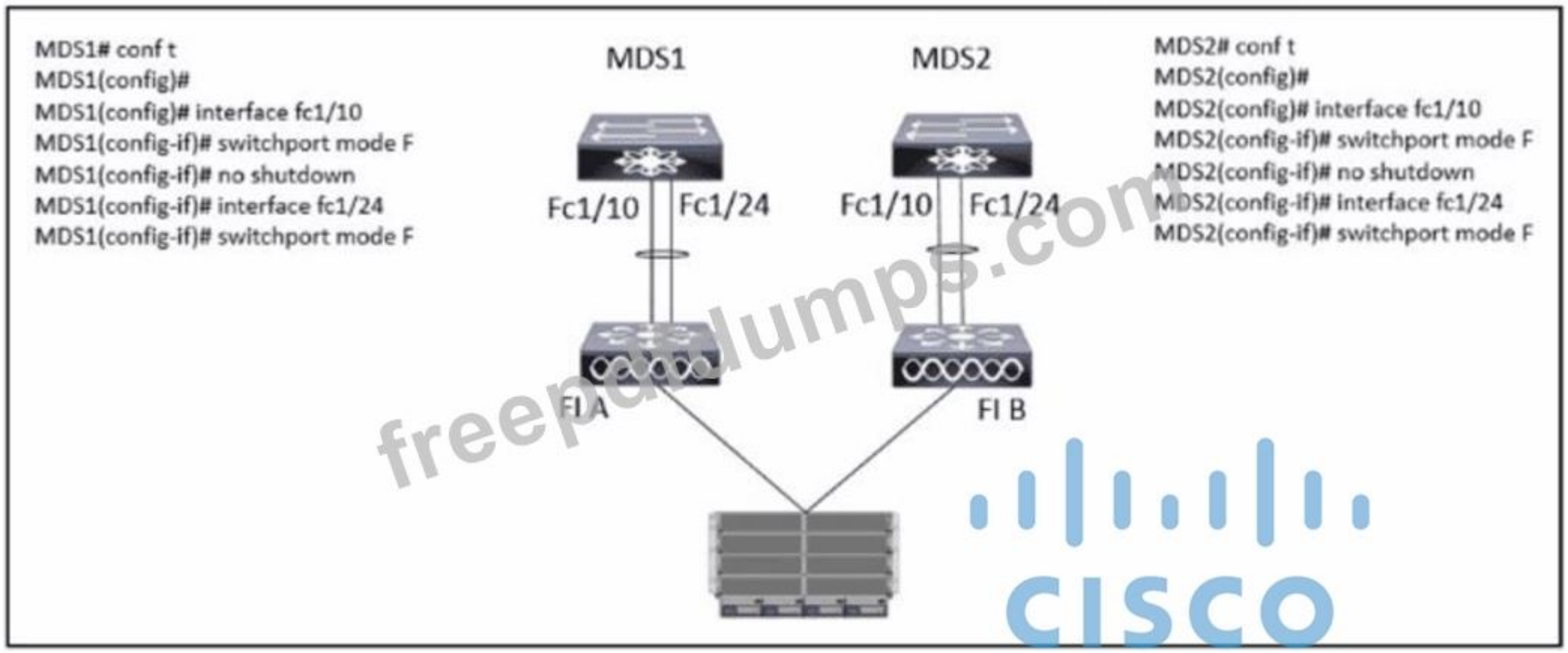


After a failover occurs, which two actions must be performed on Switch-B to manually preempt the operational primary role back to Switch-A? (Choose two.)

A. Configure the local vPC role priority to have a lower value than Switch-A.

B. Configure the local vPC role priority to have a higher value than Switch-A.
C. Disable and then re-enable the vPC peer-keepalive link.
D. Configure the local vPC role priority to have the same value as Switch-A.
E. Disable and then re-enable the vPC peer link.
Answer: B,E (LEAVE A REPLY)
Cisco troubleshooting logic supports Configure the local vPC role priority to have a higher value than Switch- A; Disable and then re-enable the vPC peer link as the required fix. In this question the symptoms point to vPC, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages.
That sequence proves that the network fabric is fixed, not merely restarted.

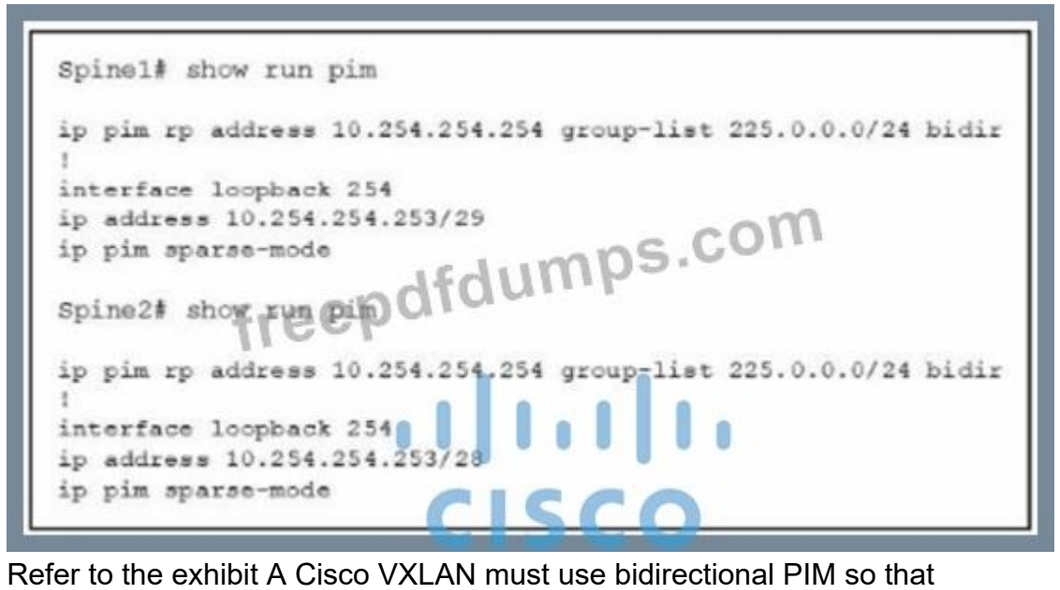
NEW QUESTION: 34



Refer to the exhibit A Cisco UCS system (ails to access the storage array. Which two actions taken on both MDS switches resolve the issue? (Choose two.) Configure a port channel with both interfaces as members
A. Change the switch port mode to an E port
B. Enable the (port-channel trunk feature
C. Issue the no shutdown command on interface fct ' 24
D. Replace the SFPs on interswitch links
Answer: A,C (LEAVE A REPLY)
The selected resolution is Change the switch port mode to an E port; Issue the no shutdown command on interface fct ' 24 because the failure is in the Fibre Channel/FCoE control path around MDS, UCS. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security

entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 35



Refer to the exhibit A Cisco VXLAN must use bidirectional PIM so that
*Spine2 is the active RP for multicast group 225 0 0 0V24
*Loopback 254 is used as a logical interface for PIM configuration
After configuration was applied, Spine1 became the active RP for multicast group 225.0.0.0/24 instead of Spine2. Which action resolves the issue?

A. Configure the IP pim ssm range 232.0.0.08 on Spme1
B. Delete the bidir keyword from ip pim rp address command on Spine1
C. Change the IP address of Loopback 254 to 10 254 254 254 on Spine2
D. Modify the subnet mask of Loopback 254 to ' 30 on Spine2

Answer: (SHOW ANSWER)

Cisco troubleshooting logic supports Modify the subnet mask of Loopback 254 to ' 30 on Spine2 as the required fix. In this question the symptoms point to VXLAN, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.

NEW QUESTION: 36

An attempt to use a global vNIC redundancy template pair results in a service profile that fails to apply.
Which action resolves the issues?

A. Create the peer names before creating the templates.
B. Assign the secondary template first, and then set the peer name.
C. Assign both templates simultaneously.

D. Assign the primary template first, and then set the peer name.
Answer: D (LEAVE A REPLY)
Assign the primary template first, and then set the peer name is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving service profile, vNIC must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 37
A server fails to boot from the operating system after a RAID1 cluster migration. The RAID remains in an inactive state during and after a service profile association. Which action resolves the issue?
A. Configure the SAN boot target in the service profile.
B. Configure the SAN boot target to any configuration mode.
C. Use a predefined local disk configuration policy.
D. Remove the local disk configuration policy.
Answer: C (LEAVE A REPLY)
Use a predefined local disk configuration policy is the correct fix under Cisco SAN troubleshooting practice.
The issue described involves service profile, SAN boot, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE /LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 38
Refer to the exhibit.

```
switch(config)# show system internal bloggerd info log-dump-info
------------------------------------------------------------
Log Dump config is READY
Log Dump is DISABLED for ALL application services in the switch
Exceptions to the above rule (if any) are as follows:
------------------------------------------------------------
Module     | VDC         | SAP                          | Enabled?
------------------------------------------------------------
1          | 1           | 351 (MTS_SAP_ACLMGR     ) | Enabled
------------------------------------------------------------
------------------------------------------------------------
Log Dump Throttle Switch-Wide Config:
------------------------------------------------------------
Log Dump Throttle                                        : ENABLED
Minimum buffer rollover count (before throttling)        : 5
Maximum allowed rollover count per minute                : 1
------------------------------------------------------------
```

```
switch# show system internal sysmgr service name aclmgr
Service "aclmgr" ("aclmgr", 80):
        UUID = 0x182, PID = 653, SAP = 351
        State: SRV_STATE_HANDSHAKED (entered at time Thu Feb  22 11:10:41 2024).
        Restart count: 1
        Time of last restart: Thu Feb  22 11:10:39 2024.
        The service never crashed since the last reboot.
        Tag = N/A
        Plugin ID: 0
```

An engineer failed to disable the log file retention for the ACL Manager service. Which code snippet resolves the issue?

A. no bloggerd log-dump aclmgr 80

B. no bloggerd log-dump pid 653

C. no bloggerd log-dump sap 351

D. no bloggerd log-dump vdc 1

Answer: (SHOW ANSWER)

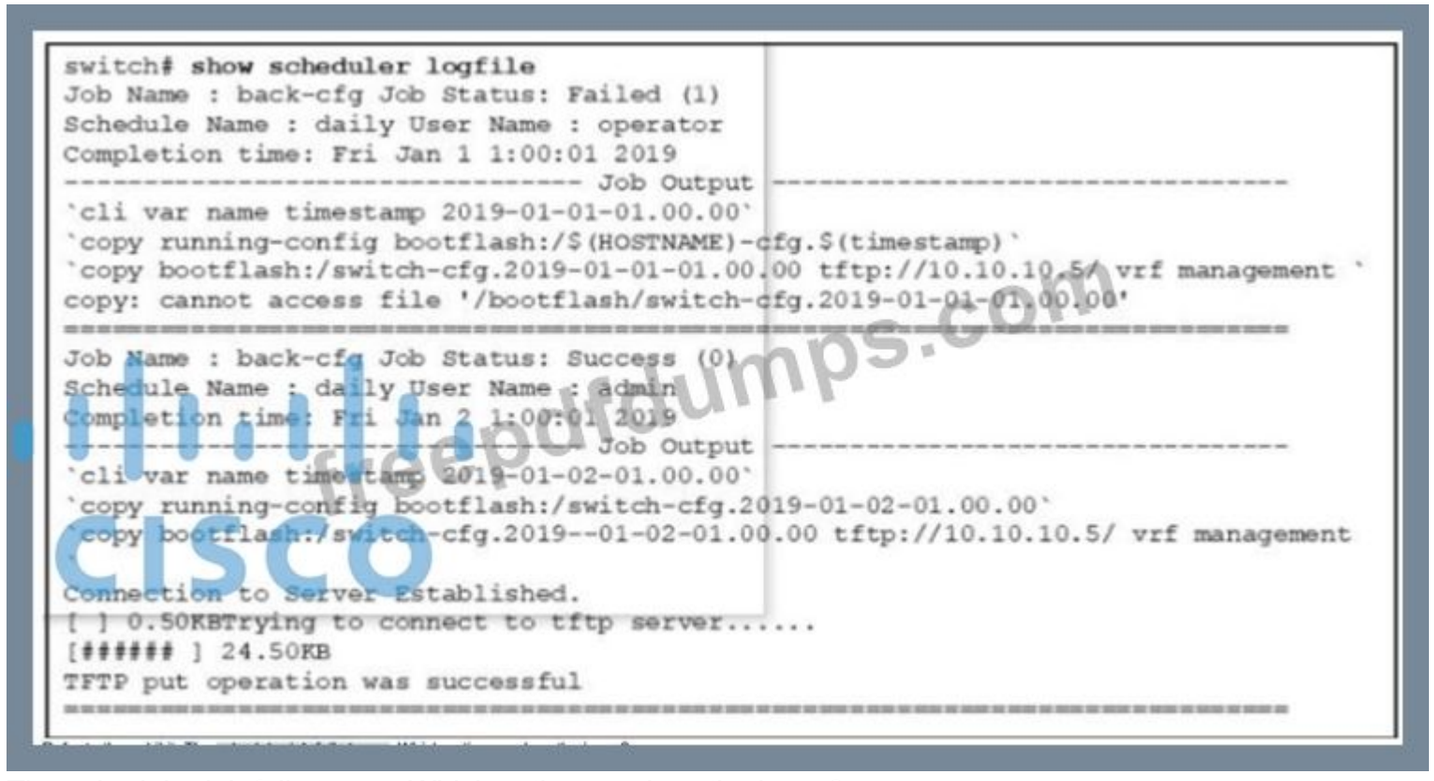
The correct remediation is no bloggerd log-dump sap 351. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on ACL, Manager, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as

state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 39
Refer to the exhibit.

The OTV overlay is deployed in multicast mode. After an unexpected reload of N7K-SITE1-OTV1, the network administrator observed that on N7K-SITE1-OTV2 the OTV site adjacency went into the partial state.
Which
action resolves the issue?
A. Configure the Site-Identifier on N7K-SITE1-OTV1 to 0002.0002.0002.
B. Enable IP IGMP version 3 on the join interface on N7K-SITE1-OTV1.
C. Change the Site-VLAN on N7K-SITE1-OTV2 to VLAN 1.
D. Modify the multicast data-group on N7K-SITE1-OTV1 to match N7K-SITE1-OTV2.
Answer: D (LEAVE A REPLY)
The answer is Modify the multicast data-group on N7K-SITE1-OTV1 to match N7K-SITE1-OTV2 because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references OTV; those technologies fail in predictable ways when required parameters do not match or when the required control-plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer- gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post-change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 40
Refer to the exhibit.



The scheduler job fails to run. Which action resolves the issue?
A. Change the file name.
B. Configure the authentication credentials.
C. Change the TFTP server address.
D. Configure the RBAC authentication.
Answer: A (LEAVE A REPLY)
The correct answer is Change the file name. Cisco NX-OS automation features are context-sensitive: Guest Shell, Bash, EEM, scheduler, NX-API, REST calls, and Python scripts each run with their own parser, privilege model, environment, and resource limits. The scenario involves RBAC, and the selected action corrects the missing execution condition. Cisco documentation for Nexus programmability states that Guest Shell resources and networking must be configured inside the Guest Shell context, EEM applets require a valid event statement and event-default when the intercepted CLI command must continue, and API calls must target the correct managed object or class. The alternative answers either operate in the wrong context, omit a required trigger/action, or correct a parameter unrelated to the failure. Validation should include running the command manually in the same context, checking logs or return codes, and confirming that the automation completes without blocking the normal NX-OS operation it observes.

NEW QUESTION: 41
Refer to the exhibit.

```
serverteam Cleartext-Password := "<password>"

Cisco-avpair = "shell:domains = user/admin/,common//read-
all(16000)"
```

An engineer is investigating a role mapping issue on a switch. The users report that they cannot view the IP addresses under the tenant "corp". Which action resolves the issue?

A. Add the users to the RADIUS server.

B. Update the UNIX ID.

C. Configure the correct secret password between the APIC and the RADIUS server.

D. Add the updated avpair to include/corp/admin/

Answer: (SHOW ANSWER)

The correct answer is Add the updated avpair to include/corp/admin/. Cisco management and operations troubleshooting focuses on control-plane services such as RBAC, AAA, certificates, SNMP, firmware packages, centralized management registration, fault workflows, and node lifecycle state. This item references APIC, RADIUS, so the selected action fixes the management dependency rather than the data-plane symptom. Cisco platforms often allow basic reachability while a higher-level integration still fails because of time synchronization, certificate trust, role mapping, authorization attributes, feature state, or incomplete lifecycle cleanup. The other options either modify forwarding behavior, adjust the wrong credential or role, or bypass the required operational workflow. The engineer should validate the fix by confirming the management session or registration, checking the relevant fault or audit log, and confirming that the user, node, or integration has the expected role and operational status. This is consistent with Cisco DCIT emphasis on operational evidence before and after the change.

NEW QUESTION: 42

```
N5K-1# show running-config aaa all
!
version 7.0(2)N2(1)
logging level aaa 5
aaa authentication login default group radius
aaa authentication login console group radius
aaa authorization ssh-publickey default local
aaa authorization ssh-certificate default local
aaa accounting default local
aaa user default-role
aaa authentication login default fallback error local
aaa authentication login console fallback error local
aaa authentication login error-enable
no aaa authentication login mschap enable
no aaa authentication login mscapv2 enable
no aaa authentication login chap enable
```

Refer to the exhibit. A functioning trunk port Ethernet1/48 exists between two identical Cisco Nexus 5000 Series Switches. The interfaces on the switches support the MACsec feature and are configured identically.

To enable manual MACsec, an engineer adds the configuration shown in the exhibit to both sides of the trunk.

The trunk port stops functioning. Which action should be taken to resolve the issue?

A. Disable and then enable the port

B. Enable the license for the trunk ports to support MACsec

C. Lower the MTU value to less than 9216 bytes

D. Configure the PMK with a length of 2048 bytes

Answer: A (LEAVE A REPLY)

The correct answer is Disable and then enable the port. Cisco management and operations troubleshooting focuses on control-plane services such as RBAC, AAA, certificates, SNMP, firmware packages, centralized management registration, fault workflows, and node lifecycle state. This item references Cisco Nexus, so the selected action fixes the management dependency rather than the data-plane symptom. Cisco platforms often allow basic reachability while a higher-level integration still fails

because of time synchronization, certificate trust, role mapping, authorization attributes, feature state, or incomplete lifecycle cleanup. The other options either modify forwarding behavior, adjust the wrong credential or role, or bypass the required operational workflow. The engineer should validate the fix by confirming the management session or registration, checking the relevant fault or audit log, and confirming that the user, node, or integration has the expected role and operational status. This is consistent with Cisco DCIT emphasis on operational evidence before and after the change.

NEW QUESTION: 43
A server administrator attempts to change the Cisco IMC KVM certificate to one signed by a private CA, but the certificate is not being accepted. What can cause this process to fail?
A. using a certificate with a password-protected private key
B. RSA encryption being used in the generation of the certificate.
C. AES encryption being used in the generation of the certificate.
D. public IP addres of the Cisco IMC not being included in the SAN.
Answer: A (LEAVE A REPLY)
using a certificate with a password-protected private key is the correct fix under Cisco SAN troubleshooting practice. The issue described involves Cisco IMC, certificate, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE
/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 44
Refer to the exhibit.

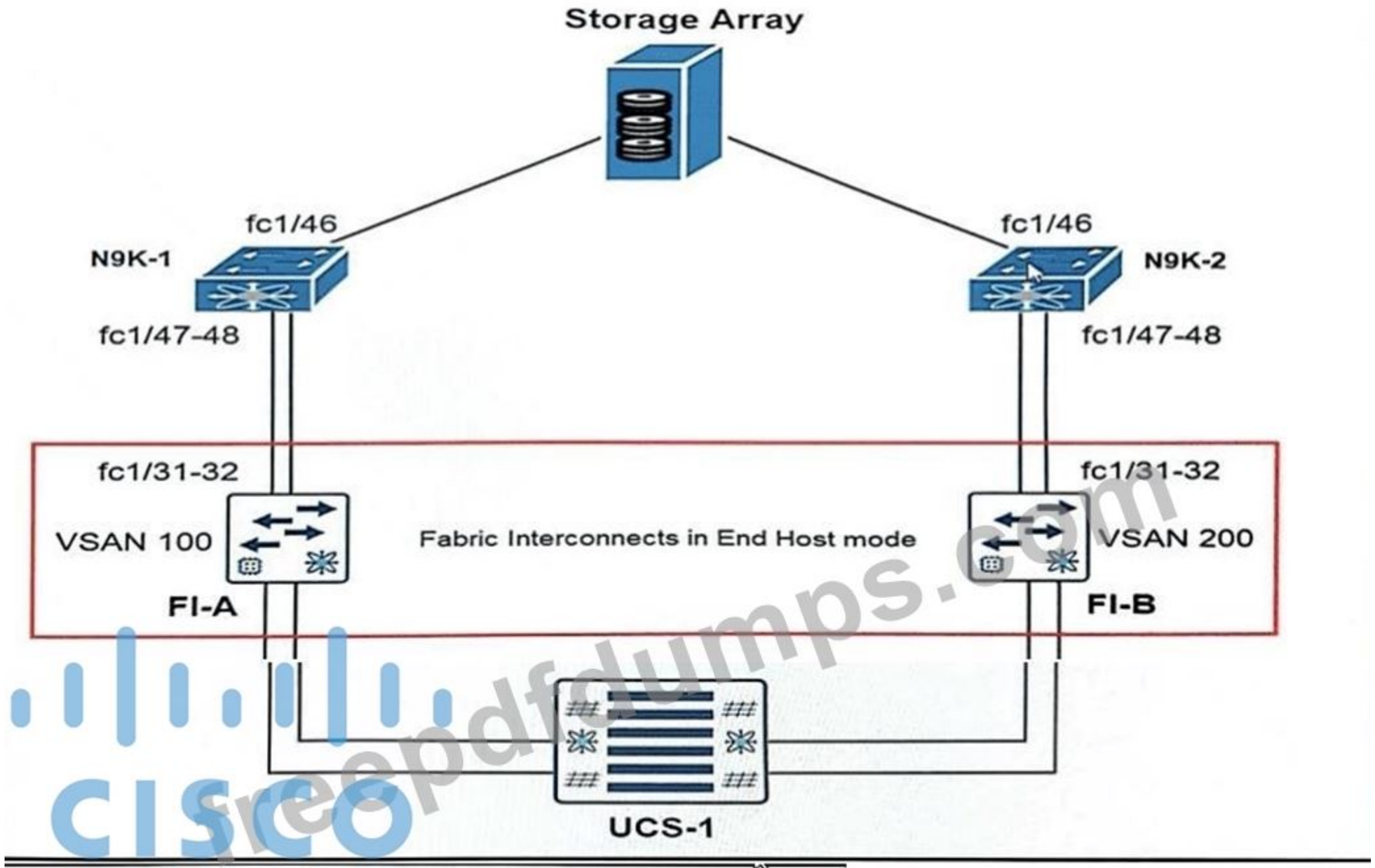
```
n7k-1# show ip ospf neighbors
 OSPF Process ID 1 VRF default
 Total number of neighbors: 2
 Neighbor ID     Pri State            Up Time  Address         Interface
 198.18.5.1        1 EXSTART/BDR      00:00:11 198.18.5.1      Eth2/1
 128.0.0.3         1 FULL/BDR         01:01:04 198.18.6.2      Eth2/2
```

A network engineer configures OSPF protocol between two Cisco Nexus 7000 Series Switches. The OSPF neighbors fail to synchronize OSPF databases. Which action resolves the issue?
A. Match the OSPF area between the two devices.
B. Configure the IP addresses of the interface in the same subnet.
C. Change the OSPF area type to 2 on n7k-1.
D. Set the same MTU values on both sides of the link.
Answer: D (LEAVE A REPLY)
The answer is Set the same MTU values on both sides of the link because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references OSPF, Cisco Nexus; those technologies fail in predictable ways when required parameters do not match or when the required control-plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational

table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host- route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post- change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 45
A network engineer finds an error that says, " BIOS failed power-on self-test. " When the engineer checks the console, they discover that the Cisco UCS Blade firmware upgrade process stopped at the " Configuring and testing memory " stage.
Which set of actions resolves the issue?
A. 1. Add the CIMC firmware on a server.
2. Initialize the CIMC firmware on a server.
B. 1. Update the BIOS firmware on a server.
2. Activate the BIOS firmware on a server
C. 1. Create a new host firmware package.
2. Assign the host firmware package to the service profile template.
D. 1. Upgrade the firmware on an adapter.
2. Enable the firmware on an adapter.
Answer: B (LEAVE A REPLY)
1. Update the BIOS firmware on a server. 2. Activate the BIOS firmware on a server is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure.
Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS, CIMC, firmware, service profile must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 46




```
N9K-1#
!
feature fcoe
slot 1
 port 44-48 type fc
!
vsan database
 vsan 100
 vsan 100 interface fc1/46-48
!
interface fc1/46-48
 no shutdown
!
```

```
N9K-1# show flogi database interface fc1/47-48
--------------------------------------------------------------------------
INTERFACE VSAN    FCID      PORT NAME                 NODE NAME
--------------------------------------------------------------------------
```

Refer to the exhibit. UCS- 1 fails to connect to the storage array. Which action resolves the issue?

A. Set the FI-A mode to FC End Host mode.

B. Enable N9K-1 mode to N-Port ID Virtualization.

C. Configure N-Port ID Virtualization on FI-A.

D. Implement N-Port Virtualization on N9K-1.

Answer: B (LEAVE A REPLY)

The selected resolution is Enable N9K-1 mode to N-Port ID Virtualization because the failure is in the Fibre Channel/FCoE control path around UCS. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 47

Refer to the exhibit.

```
MDS-1#
zoneset name ESX vsan 10
 zone name ESX01_B vsan 10
 * fcid 0x010a0e [pwwn 20:00:00:25:b5:aa:41:ba]
   fcid 0x840001 [pwwn 52:4a:93:7e:47:1d:ce:02]
   fcid 0x840021 [pwwn 52:4a:93:7e:47:1d:ce:06]
VSAN 10:
FCID    TYPE PWWN           (VENDOR)    FC4-TYPE:FEATURE
0x840041  N   52:4a:93:7e:47:1d:ce:04         scsi-fcp:target
0x840061  N   52:4a:93:7e:47:1d:ce:08         scsi-fcp:target
0x010a0e  N   20:00:00:25:b5:aa:41:ba         scsi-fcp:init
VSAN 20:
FCID    TYPE PWWN           (VENDOR)    FC4-TYPE:FEATURE
0x840001  N   52:4a:93:7e:47:1d:ce:02         scsi-fcp:target
0x840021  N   52:4a:93:7e:47:1d:ce:06         scsi-fcp:target
FI-A /org/service-profile #
vHBA:
    Name: vHBA1
    Fabric ID: B
    Dynamic WWPN: 20:00:00:25:B5:BB:41:BA
    Equipment: sys/chassis-1/blade-1/adaptor-1/host-fc-1
    Template Name: vHBA_SAN_B
    Oper Nw Templ Name: org-root/san-conn-templ-vHBA_SAN_B
    Adapter Policy: Windows
    Oper Adapter Policy: org-root/fc-profile-Windows
vHBA Template:
    Name                  Type              Fabric ID
    --------------------- ----------------- ---------
    vHBA_SAN_B            Updating Template B
FI-B(nxos)#
-------------------------------------------------------------------------------
INTERFACE VSAN FCID           PORT NAME               NODE NAME       EXTERNAL
-------------------------------------------------------------------------------
vfc2981   10   0x010a0e 20:00:00:25:b5:bb:41:ba 20:00:00:25:b5:a4:00:c9 San-po111
```

A blade that is connected to FI-B fails to boot from a SAN LUN. The boot policy is configured to boot by using vHBA1 as the SAN Primary. Which set of actions resolves the issue?

A. * Set ESX01_B zone to VSAN 20.
* Create a new vHBA and assign VSAN 20.

B. * vHBA1 to VSAN 20 in Service Profile.
* VMware Adapter Policy on vHBA1.

C. *Apply VMware Adapter Policy on vHBA1
*Change vHBA1 to VSAN 20 in Service Profile

D. * Set ESX01_B zone to VSAN 20.
* Change vHBA1 to VSAN 20 in Service Profile

Answer: D (LEAVE A REPLY)

The selected resolution is * Set ESX01_B zone to VSAN 20. * Change vHBA1 to VSAN 20 in Service Profile because the failure is in the Fibre Channel/FCoE control path around VSAN, service profile, vHBA. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as

fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 48

```
VTEP1# show vpc consistency-parameters vni
Legend:
Type 1 : vPC will be suspended in case of mismatch
Name                        Type      Local Value            Peer Value
--------------- ---- -------------------- --------------------
-
Nve1 Adm St, Src Adm St,    1       Up, Up,                Up, Up,
Sec IP, Host Reach, VMAC            192.168.100.100, CP,   192.168.100.100, CP,
Adv, SA,mcast l2, mcast             FALSE, Disabled,       FALSE, Disabled,
l3, IR BGP,MS Adm St, Reo           0.0.0.0, 0.0.0.0,      0.0.0.0, 0.0.0.0,
                                    Disabled, Down,        Disabled, Down,
                                    0.0.0.0                0.0.0.0
Nve1 Vni, Mcast, Mode,      1       1011, 239.0.11.1,      1011, 239.0.11.1,
Type, Flags                         Mcast, L2, None        Mcast, L2, None
Nve1 Vni, Mcast, Mode,      1       1010, 239.0.10.0,      1010, 239.0.10.0,
Type, Flags                         Mcast, L2, None        Mcast, L2, None
Nve1 Vni, Mcast, Mode,      1       50020, 0.0.0.0, n/a,   50020, 0.0.0.0, n/a,
Type, Flags                 -       L3, L3VNI              L3, L3VNI
Allowed VLANs               -       1,15,89-120            1,5,88-120
```

Refer to the exhibit. A VXLAN fabric is configured on Cisco Nexus 9000 Series Switches but the traffic is dropped on VLAN 88 between VTEP1 and VTEP2. Which configuration resolves the issue?

A. Add VLAN 88 using switchport trunk allowed VLAN add 88 on VTEP2.

B. Enable VLAN 88 using no shutdown on VTEP2.

C. Add VLAN 88 using switchport trunk allowed VLAN add 88 on VTEP1.

D. Enable VLAN 88 using no shutdown on VTEP1.

Answer: C (LEAVE A REPLY)

The correct remediation is Add VLAN 88 using switchport trunk allowed VLAN add 88 on VTEP1. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on VXLAN, Cisco Nexus, Nexus 9000, Cisco Nexus 9000, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF.

This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 49

Refer to the exhibit. A network engineer is troubleshooting a Cisco Nexus 5000 Series Switch. The interface between the server and the switch is nonoperational and is expected to operate at 10 Gbps. The drain rate of the interface is 3 Mbps. Which action resolves the issue?

A. Configure pause error-disable recovery

B. Enable link level pause on the interface

C. Reset priority flow counters

D. Set priority flow control pause

Answer: A (LEAVE A REPLY)

Configure pause error-disable recovery is the required SAN-side correction. In Cisco storage fabrics, symptoms such as isolated ports, missing targets, failed zone merges, vFC down state, or inaccessible LUNs are rarely solved by changing a random endpoint setting. The engineer must validate the FC control-plane dependency associated with Cisco Nexus: VSAN assignment, trunk allowance, FSPF parameters, fcdomain uniqueness, NPIV support, NPV uplink behavior, DCBX/LLDP negotiation, and active zoning. The selected answer is the one that restores that dependency. Other choices may be valid operational commands in a different failure, but they do not address the precise point where fabric membership or access control is broken. Cisco guidance is to verify the active database and the operational database separately because a configured object is not necessarily active in the fabric. Post-remediation checks should include interface state, VSAN status, FLOGI/PLOGI, zoneset membership, and target visibility from the initiator.

NEW QUESTION: 50

An engineer attempts to register Cisco UCS Manager to Cisco UCS Central, but the registration fails. The engineer can ping Cisco UCS Central from UCS Manager. Which two actions must the engineer attempt to resolve the problem? (Choose two.)

A. Synchronize the date and time to NTP for Cisco UCS Central and the Cisco UCS domains.

B. Apply the UCS Central license to UCS Central.

C. Place Cisco UCS Manager on the same subnet as Cisco UCS Central.

D. Allow port 443 between Cisco UCS Manager and Cisco UCS Central.

E. Allow port 9443 between Cisco UCS Manager and Cisco UCS Central.

Answer: A,D (LEAVE A REPLY)

The selected answer, Synchronize the date and time to NTP for Cisco UCS Central and the Cisco UCS domains; Allow port 443 between Cisco UCS Manager and Cisco UCS Central, follows Cisco UCS operational logic. UCS Manager is policy-driven, so troubleshooting must determine whether the problem is caused by hardware discovery, service profile association, firmware activation, boot order, storage presentation, or management integration. The scenario points to UCS, UCS Manager, UCS Central; that is why the selected action fixes the root condition rather than merely restarting the server. The wrong options either affect a different policy, require unnecessary disruption, or assume that physical connectivity alone is sufficient. Cisco documentation for UCS server boot and firmware management stresses that boot policies must include the correct target details, firmware workflows must complete their FSM stages, and hardware changes often require acknowledgement or re-acknowledgement before UCS Manager uses the new inventory. After remediation, the engineer should confirm that the UCS fault is cleared, the server association or discovery state is complete, and the operating system or management service can use the intended path.

NEW QUESTION: 51
An engineer is investigating traffic loss on a Cisco UCS B-Series blade server. The engineer discovers high rates of RX CRC STOMPED errors on the fabric interconnect ports to which the server traffic is pinned Which action resolves the issue?
A. Update the firmware version on the virtual interface card adapter
B. Configure the VLANs on the fabric interconnect
C. Change the flow control settings on the I/O module.
D. Change the cables to fix physical connections
Answer: D (LEAVE A REPLY)
Change the cables to fix physical connections is correct because the failure is tied to the UCS managed state of UCS, firmware, fabric interconnect. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations.
A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table. If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

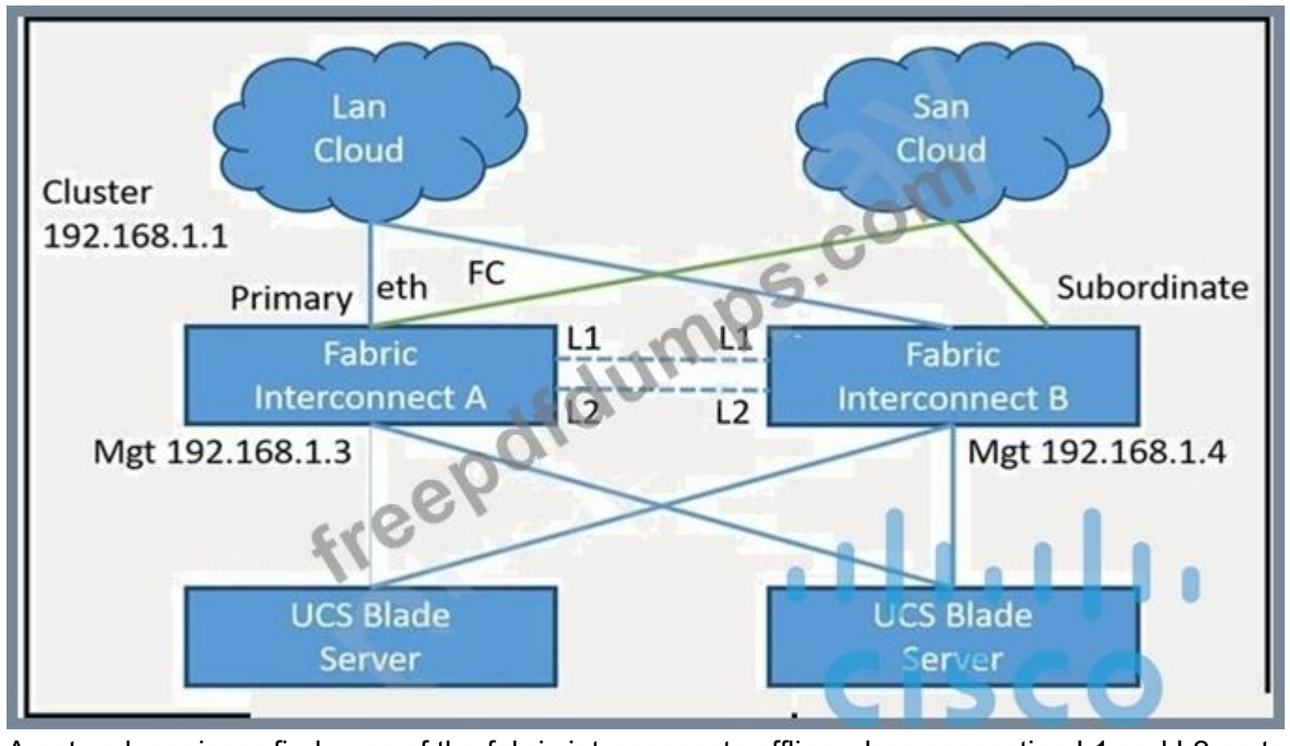
NEW QUESTION: 52
Refer to the exhibit.

```
Booting kickstart image: bootflash:/installables/switch/ucs-6100-k9-kickstart.4
.1.2.N2.1.1l.bin....Loader Version pr-1.3

loader> dir
bootflash:
  lost+found
  ucs-6100-k9-kickstart.4.1.3.N2.1.1l.bin
  ucs-6100-k9-system. 4.1.3.N2.1.1l.bin
  sysdebug
  chassis.img
  nuova-sim-mgmt-nsg.0.1.0.001.bin
  pnuos
  installabels
  mts.log
  vdc_2
  vdc_3
  vdc_4
  distributables
  initial_setup.log
  tmp
  .tmp-kickstart
  .tmp-system

loader>
```


A Cisco UCS Fabric Interconnect fails during the upgrade process. The working images of the fabric interconnect are stored on the bootflash. Which set of commands recovers the fabric interconnect?
A. loader > dir

loader > boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)# init system
switch(boot)# reload
switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
B. loader > dir
loader > boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)# copy ics-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.001.bin switch(boot)# boot ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
C. loader > dir
loader > boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)# init system
switch(boot)# reload
switch(boot)# boot ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
D. loader > dir
loader > boot ucs-6300-k9-kickstart.5.0.2.N1.3.02d56.bin
switch(boot)# copy ics-manager-k9.1.4.1k.bin nuova-sim-mgmt-nsg.0.1.001.bin switch(boot)# load ucs-6300-k9-system.5.0.2.N1.3.02d56.bin
Answer: D (LEAVE A REPLY)
The correct action is the selected command set. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves UCS, fabric interconnect, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.

NEW QUESTION: 53
Refer to the exhibit.



A network engineer finds one of the fabric interconnects offline when connecting L1 and L2 ports on both fabric interconnects. Which action resolves the issue?

A. 1. Connect to Fabric Interconnect B.
2. Verify the cluster status and HA election.
3. Validate Fabric Interconnect B hardware issues.

B. 1. Connect to Fabric Interconnect A.
2. Verify the cluster status and HA election.
3. Validate Fabric Interconnect A hardware issues.

C. 1. Connect Fabric Interconnect B and change the role to primary.
2. Reboot Fabric Interconnect B.
3. Add the Fabric Interconnect A as subordinate fabric to the cluster.

D. 1. Connect Fabric Interconnect B and execute "Erase configuration"
2. Reboot Fabric Interconnect B.
3. Add the subordinate Fabric Interconnect to the cluster.

Answer: D (LEAVE A REPLY)

The selected answer, 1. Connect Fabric Interconnect B and execute "Erase configuration" 2. Reboot Fabric Interconnect B. 3. Add the subordinate Fabric Interconnect to the cluster, follows Cisco UCS operational logic. UCS Manager is policy-driven, so troubleshooting must determine whether the problem is caused by hardware discovery, service profile association, firmware activation, boot order, storage presentation, or management integration. The scenario points to fabric interconnect; that is why the selected action fixes the root condition rather than merely restarting the server. The wrong options either affect a different policy, require unnecessary disruption, or assume that physical connectivity alone is sufficient. Cisco documentation for UCS server boot and firmware management stresses that boot policies must include the correct target details, firmware workflows must complete their FSM stages, and hardware changes often require acknowledgement or re-acknowledgement before UCS Manager uses the new inventory. After remediation, the engineer should confirm that the UCS fault is cleared, the server association or discovery state is complete, and the operating system or management service can use the intended path.

NEW QUESTION: 54

Refer to the exhibit . customer reports that all Intra - EPG isolation stopped working within a bare - metal tenant . Postman is running on a machine to get information from the APIC in case of orchestration failure .
Which action resolves the issue ? .

```
<fvTenant name="Tenant_VOD" >
 <fvAp name="VOD">
   <fvAEPg name="IntraEPGDeny" pcEnfPref="unenforced">
     <fvEsBd tnPvEDName="bd_VOD" />
         <fvRsDonatt tDn="uni/phyDem_VOD" />
         <fvRsPathAtt
tDn="topology/ped-1/paths-1022/pathep-(eth1/22)"
          encap="vlan-10" primaryEncap-"vlan-110"
instrImedcy="immediate">
       </fvAEPg>
   </fvAp>
</fvTenant>
```


A. B . Match encap = " vlan -10 " and primaryEncap= " vlan-110 "
B. C . Modify the GET command to reference the valid path for the managed object
C. D . Change pcEnfPref = " unenforced " to pcEnfPref = " enforced " .
Answer: (SHOW ANSWER)
Remove primaryEncap= " vlan-110 " from the specific port path is the required fix because the automation failure is caused by execution context, syntax, or resource state around APIC, EPG, Postman. On Cisco Nexus switches, automation is not a single feature; EEM policies, CLI actions, Guest Shell Linux commands, REST payloads, and scheduled jobs are evaluated by different subsystems. A script can fail even while the switch itself has connectivity or the command works interactively. The selected answer supplies the missing requirement, such as the correct event/action, DNS or resource setting, API URI, payload format, feature enablement, or reboot needed for a Guest Shell change to take effect. The other choices address adjacent features but do not satisfy the failing subsystem. After applying the fix, the engineer should verify the policy registration, job result, API response code, or Guest Shell runtime state and confirm that the intended command is no longer blocked or silently ignored.

NEW QUESTION: 55
Refer to the exhibit.

```
Test-5548-A# sh int fc2/12
sh int fc2/12 is down (NPV upstream port not available)
Hardware is Fibre Channel, SFP is short wave laser w/o OFC (SN)
Port WWN is 20:47:00:0d:ec:a4:3b:80
Admin port mode is F, trunk mode is off
snmp link state traps are enabled
Port vsan is 99
Receive data field Size is 2112
```

An engineer configures the server port on a Cisco Nexus 5000 Series Switch. The switch connects to an NPV edge switch port. The server fails to send the FC traffic to the fabric. Which action resolves the issue?

A. Enable the NPIV mode on the Cisco Nexus 5000 switch.

B. Match the VSAN membership on both ends of the connection.

C. Configure the BB_credit buffer on the uplink port.

D. Replace the SFP in slot fc2/12.

Answer: (SHOW ANSWER)

Enable the NPIV mode on the Cisco Nexus 5000 switch is the correct fix under Cisco SAN troubleshooting practice. The issue described involves VSAN, NPIV, NPV, Cisco Nexus, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 56

Refer to the exhibit. An engineer connected Switch_2 to Switch_1, but noticed that the Switch_2 Fibre Channel port that is destined to Switch_1 is down and isolated. Which two commands resolve this issue?

(Choose two.)
A. [ ] fcdomain restart disruptive vsan 5
B. [ ] fspf config vsan 5
C. [ ] fspf region 5 auto-reconfigure
D. [ ] fcdomain domain 23 static vsan 5
E. [ ] fcdomain priority 25 vsan 5
Answer: (SHOW ANSWER)
[ ] fcdomain restart disruptive vsan 5; [ ] fcdomain domain 23 static vsan 5 is the correct fix under Cisco SAN troubleshooting practice. The issue described involves VSAN, FSPF, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target.
The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 57
Refer to the exhibit.

During implementation of a Cisco UCS C-Series Server, an engineer receives the status that is shown in the exhibit. Which action resolves the issue.
A. Reconfigure the Drive Type from " Removable " to " Non-Removable "
B. Insert an SD card into SLOT-2
C. Configure the RAID that is associated with the card.

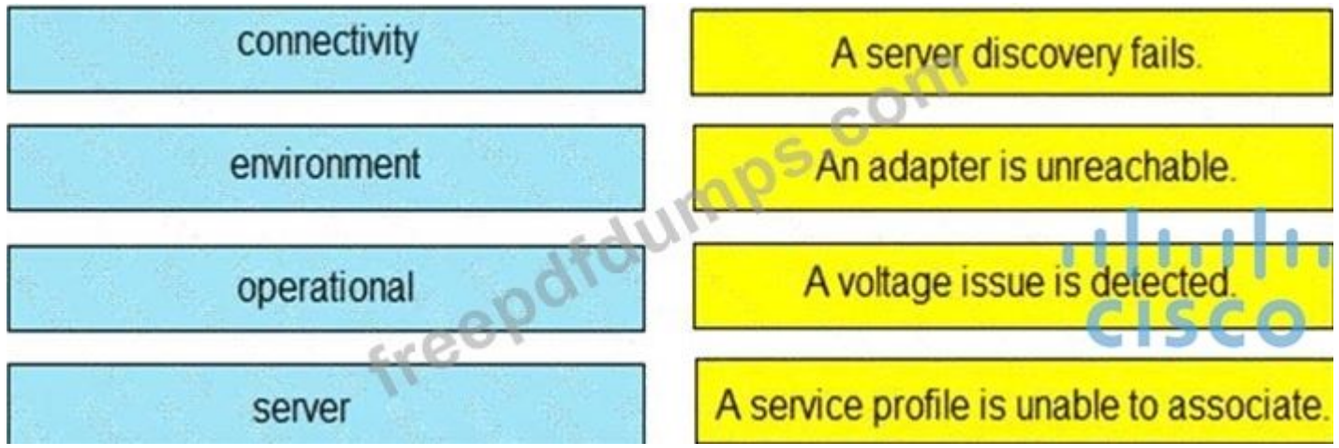
D. Set SLOT-1 Sync Mode to " Auto "

Answer: B (LEAVE A REPLY)

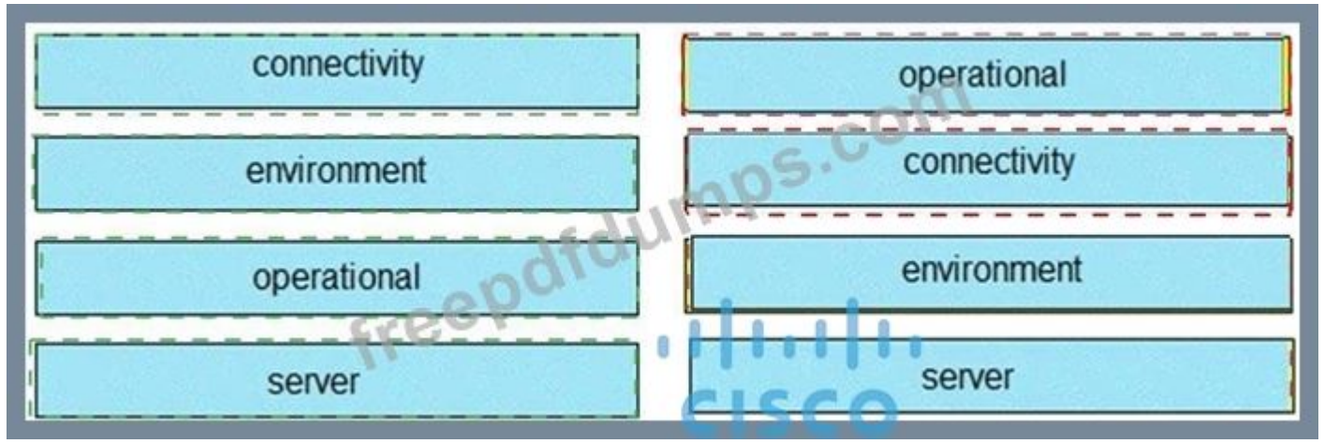
Insert an SD card into SLOT-2 is correct because the failure is tied to the UCS managed state of UCS. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table. If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

NEW QUESTION: 58

Drag and drop the Cisco UCS SNMP fault types from the left onto the correct issues on the right.

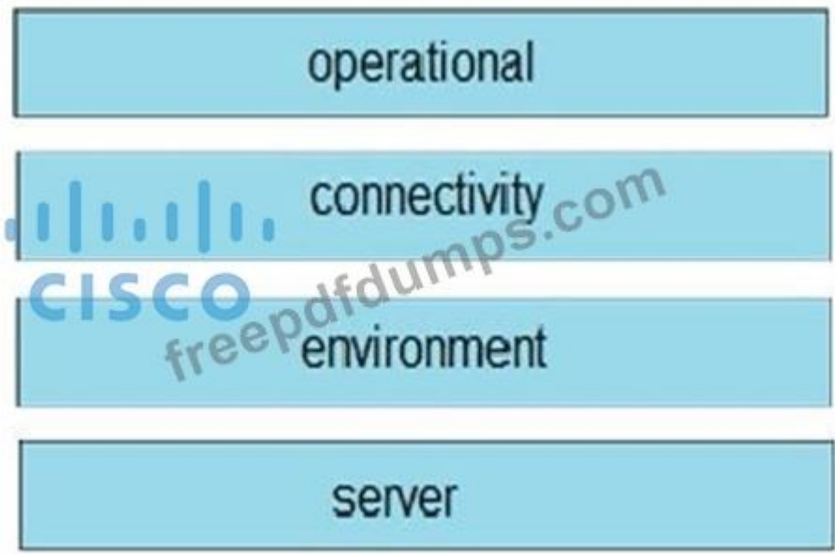


Answer:

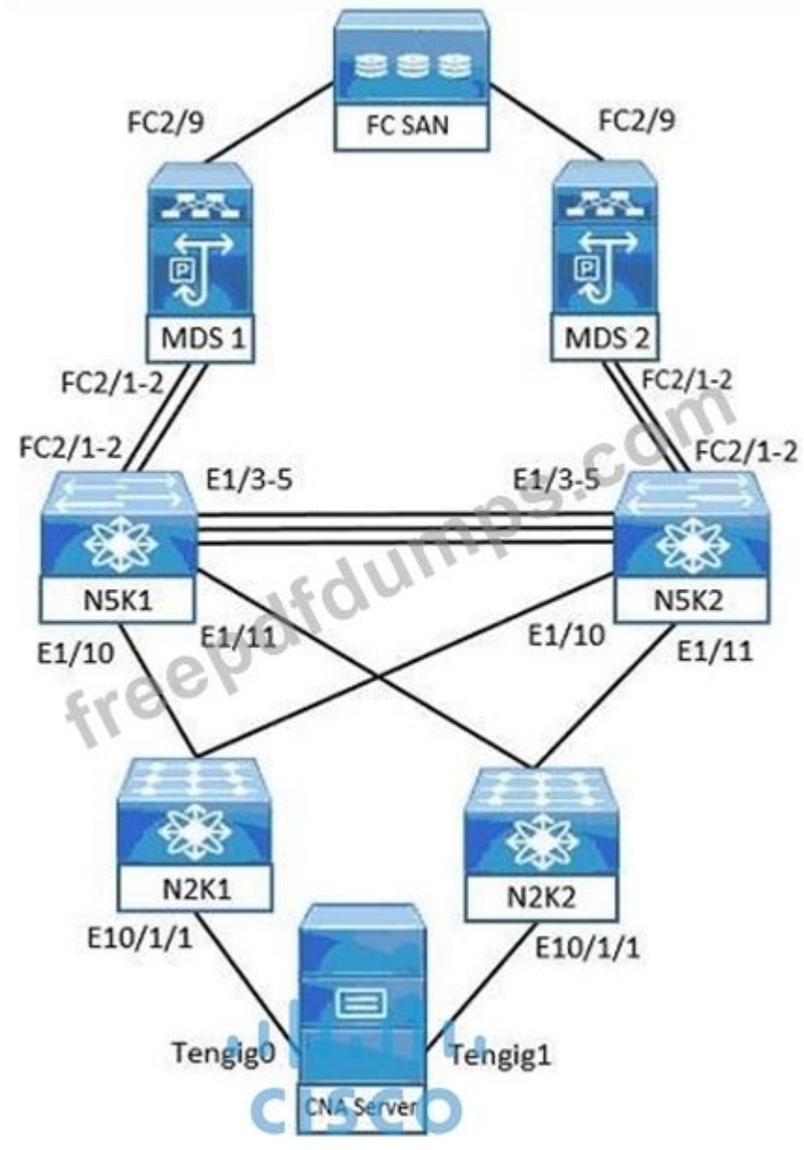


Explanation:

The correct action is the drag-and-drop mapping shown in the answer key. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves UCS, SNMP, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.



NEW QUESTION: 59
Refer to the exhibits.



N5K1 Config

```
feature fex
feature fcoe
vlan 10
vlan 1101
fcoe vsan 101
vsan database
vsan 101
interface fc2/1 - 2
switchport speed 2000
switchport mode E
switchport trunk
allowed vsan 101
no shutdown
!
interface Ethernet1/10
switchport mode fex-fabric
fex associate 101
```

```
interface Ethernet10/1/1
 switchport mode trunk
 switchport trunk native vlan 100
 switchport trunk allowed vlan 1101
 spanning-tree port type edge trunk
 no shutdown
!
interface vfc111
 bind interface Ethernet10/1/1
 switchport trunk allowed vsan 101
 no shutdown
!
vsan database
 vsan 101 interface vfc111
!
zone default-zone permit vsan 101
```

An engineer troubleshoots switch N5K1, which fails to receive traffic from the file server Which set of actions resolves this problem?

A. Bind native VLAN 10 with Ethemet1/10 and allow VSAN 101 in trunk configuration.

B. Assign native VLAN 10 with vfc111 and allow VLAN 1101 in trunk configuration.

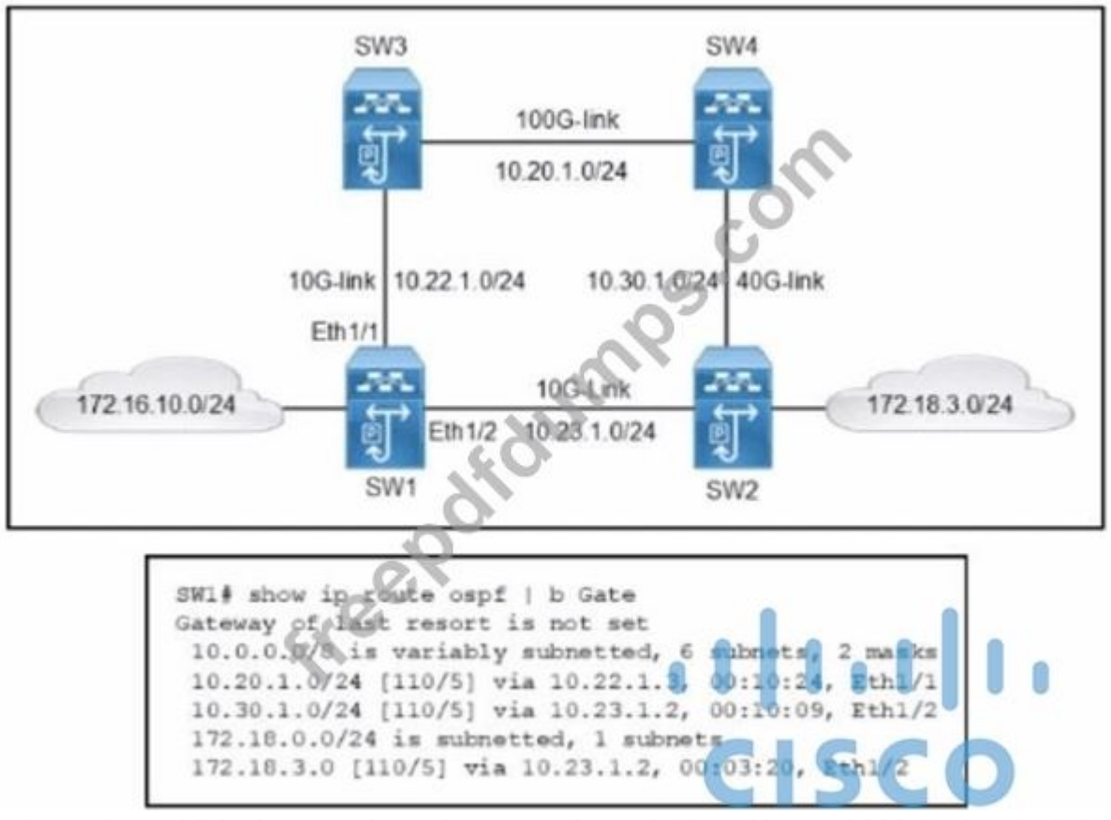
C. Bind native VLAN 10 with Ethemet10/1/1 and allow VLAN 10 in trunk configuration

D. Assign native VLAN 10 with fc2. ' I - 2 and allow VLAN 10 in trunk configuration.

Answer: C (LEAVE A REPLY)

Bind native VLAN 10 with Ethemet10/1/1 and allow VLAN 10 in trunk configuration is the correct fix under Cisco SAN troubleshooting practice. The issue described involves VSAN, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 60



Refer to the exhibit. A network engineer configured Cisco Nexus 9000 Series Switches to allow the traffic between 172.16.10.10/24 to 172.18.3.100/24 to pass through the 100G-link, but it fails. SW3 and SW4 are configured with the default OSPF configurations. Which configuration on SW1 resolves the issue?

A. interface eth1/1
ip ospf cost 1
B. interface eth1/1
auto-cost reference-bandwidth 10000
C. interface eth1/2
auto-cost reference-bandwidth 1000
D. interface eth1/2
ip ospf cost 5

Answer: (SHOW ANSWER)

The correct remediation is interface eth1/1 auto-cost reference-bandwidth 10000. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on OSPF, Cisco Nexus, Nexus 9000, Cisco Nexus 9000, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 61

An engineer must configure Linux hosts that are deployed on Cisco UCS B-Series Servers to boot from SAN.
The SAN boot policy is configured in Cisco UCS Manager, and the boot order is verified to be set as expected However, the Linux hosts fail to boot. Which action resolves the issue?

A. Remove all of the local storage that is installed
B. Delete and reconfigure the pWWN of the SAN boot target
C. Remove all of the ISO images that are mounted as a virtual CD-ROM
D. Delete and reconfigure the boot LUN
Answer: A (LEAVE A REPLY)
The selected resolution is Remove all of the local storage that is installed because the failure is in the Fibre Channel/FCoE control path around UCS, UCS Manager, SAN boot. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 62

```
<fvTenant name="PROD">
   <fvCtx name="Telco">
   <fvBD name="50-hssfepal1-sp-BD">
      <fvRsCtx tnFvCtxName="Telco">
      <fvSubnet ip="10.4.1.1/24">
   <fvBD>
<fvTenant>
```

Refer to the exhibit. An engineer must create a new bridge domain and VRF in the Cisco ACI fabric. After the data format encoding shown here is posted, nothing is created.
Which data format must be posted to resolve the issue?
A. < fvTenant name= " PROD " >
< fvCtx name= " Telco " / >
< fvBD name= " 50-hssfepal1-sp-BD " >
< fvRsCtx tnFvCtxName= " Telco " / >
< fvSubnet ip= " 10.4.1.1/24 " / >
< /fvTenant >
< /fvBD >
B. < fvTenant name= " PROD " >
< fvCtx name= " Telco " / >
< fvBD name= " 50-hssfepal1-sp-BD " >

< fvRsCtx tnFvCtxName= " Telco " / >
< fvSubnet ip= " 10.4.1.1/24 " / >
< /fvSubnet >
< /fvBD >
< /fvTenant >
C. < fvTenant name= " PROD " >
< fvCtx name= " Telco " / >
< fvBD name= " 50-hssfepal1-sp-BD " >
< fvRsCtx tnFvCtxName= " Telco " / >
< fvSubnet ip= " 10.4.1.1/24 " / >
< /fvBD >
< /fvTenant >
D. < fvTenant name= " PROD " >
< fvCtx name= " Telco " / >
< fvBD name= " 50-hssfepal1-sp-BD " >
< fvRsCtx tnFvCtxName= " Telco " / >
< fvSubnet ip= " 10.4.1.1/24 " / >
< /fvRsCtx >
< /fvCtx >
< /fvBD >
< /fvTenant >
Answer: C (LEAVE A REPLY)
Cisco troubleshooting logic supports < fvTenant name= " PROD " > < fvCtx name= " Telco " / > < fvBD name= " 50-hssfepal1-sp-BD " > < fvRsCtx tnFvCtxName= " Telco " / > < fvSubnet ip= " 10.4.1.1/24 " / > <
/fvBD > < /fvTenant > as the required fix. In this question the symptoms point to ACI, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.

NEW QUESTION: 63
One of Cisco Nexus Series interfaces has become errdisabled with the error message "DCX-No ACK in 100 PDUs". What is the cause of this error?
A. The host has not responded to the Control Sub-TLV DCBX exchanges of the switch.
B. The acknowledgement number in the server response has not incremented for 100 exchanges.
C. Cisco Discovery Protocol is disabled on the switch.
D. LLDP is disabled on the switch.
Answer: (SHOW ANSWER)
The correct remediation is The host has not responded to the Control Sub-TLV DCBX exchanges of the switch. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on DCBX, LLDP, Cisco Nexus, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC,

VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 64
Refer to the exhibit.

Debug messages from Router-A

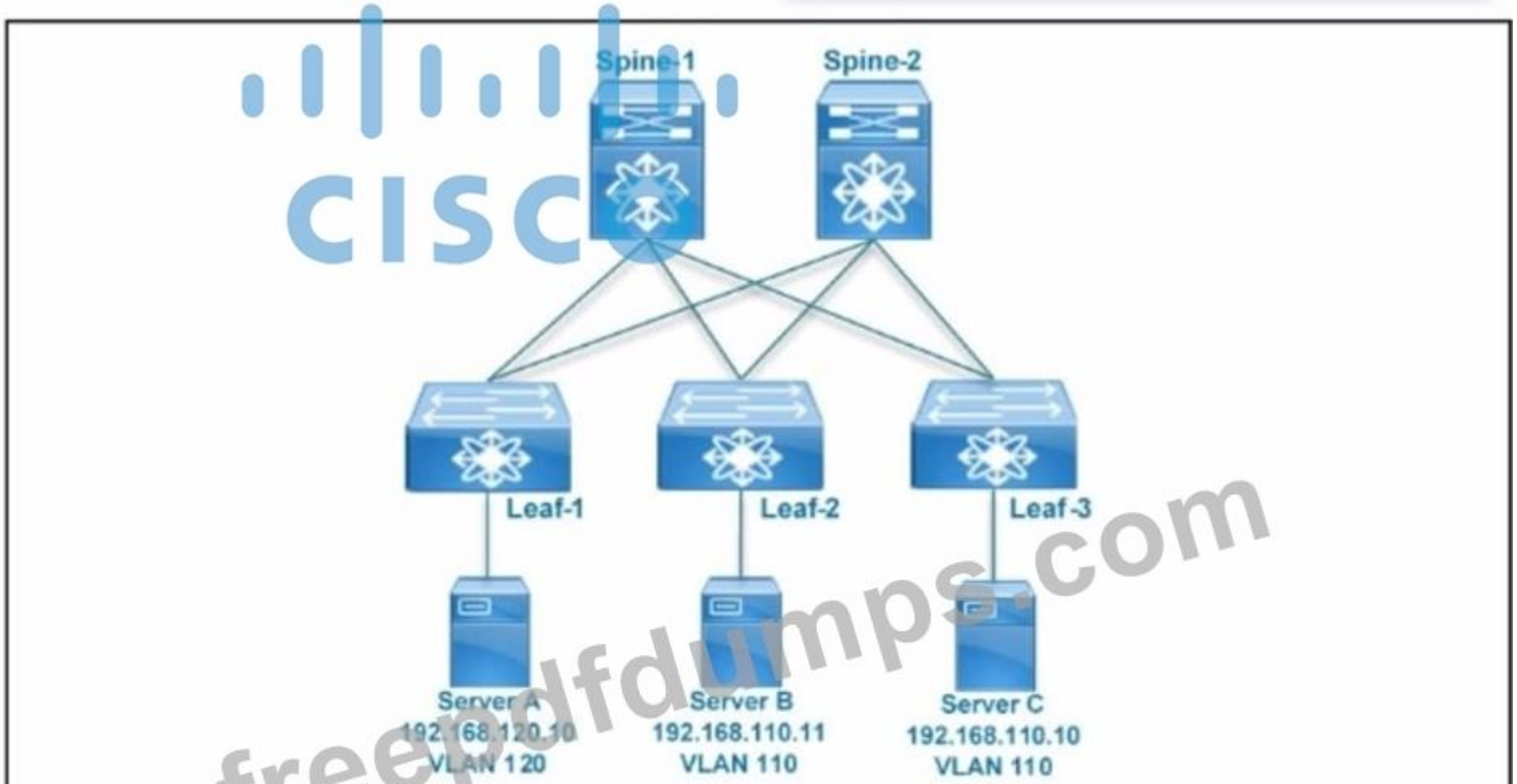
```
OSPF: Rcv DBD from 10.100.1.2 on GigabitEthernet0/1 seq 0x2124 opt 0x52 flag 0x2
     len 1452 mtu 2000 state EXSTART
OSPF: Nbr 10.100.1.2 has larger interface MTU
SPF: Send DBD to 10.100.1.2 on GigabitEthernet0/1 seq 0x9E6 opt 0x52 flag 0x7
     len 32
OSPF: Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1 [10]
OSPF: Send DBD to 10.100.1.2 on GigabitEtherenet0/1 seq 0x9E6 opt 0x52 flag 0x7
     len 32
OSPF Retransmitting DBD to 10.100.1.2 on GigabitEthernet0/1[11]
%OSPF-5-ADJCHG: Process 1, Nbr 10.100.1.2 on GigabitEthernet0/1 from EXSTART to
     DOWN, Neighbor Down: Too many retransmissions
```

Debug messages from Router-B

```
OSPF: Rev DBD from 10.100.100.1 on GigabitEthernet0/1 seq 0x89E opt 0x52 flag 0x
     len 32 mtu 1600 state EXCHANGE
OSPF: Nbr 10.100.100.1 has smaller inerface MTU
```

An OSPF adjacency between Router-A and Router-B cannot reach the FULL state. Which action resolves the issue?
A. Adjust the MTU on Router-A to 1600.
B. Disable the check of the MTU value.
C. Set the OSPF media type to point-to-point.
D. Adjust the MTU on Router-B to 1604.
Answer: B (LEAVE A REPLY)
The correct remediation is Disable the check of the MTU value. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on OSPF, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 65
Refer to the exhibit.




```
Leaf-3# show nve vni
Codes: CP - Control Plane          DP - Data Plane
       UC - Unconfigured           SA - Suppress ARP
       SU - Suppress Unknown Unicast
       Xconn - Crossconnect
       MS-IR - Multisite Ingress Replication
Interface VNI      Multicast-group   State Mode Type [BD/VRF]      Flags
--------- -------- ----------------- ----- ---- ------------------ -----
nve1      50110    239.0.0.110       Up    CP   L2 [110]
nve1      50120    239.0.0.120       Up    CP   L2 [120]
Leaf-3#
```


The VXLAN communication fails between Server A and Server C. Server A and Server B can communicate, but Server C can only reach Server B and its default gateway. Which action must be taken on Leaf-3 to resolve the issue?

A. Configure a tenant Layer 3 VNI.

B. Implement a VLAN 110 Layer 3 VNI.

C. Configure a Layer 2 VNI.

D. Implement a VLAN 120 Layer 2 VNI.

Answer: A (LEAVE A REPLY)

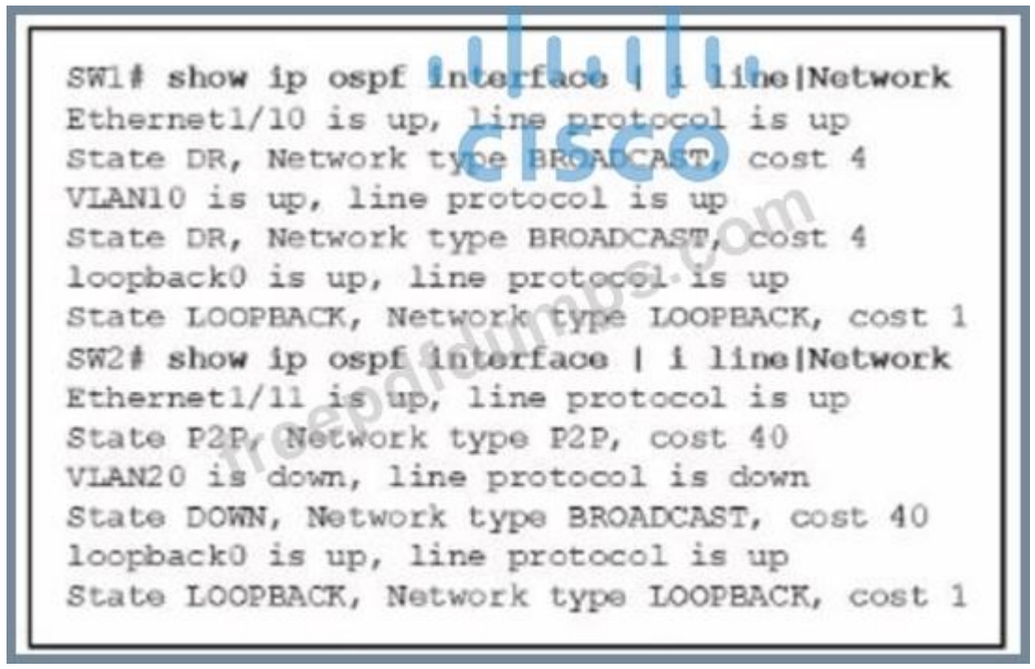
The answer is Configure a tenant Layer 3 VNI because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references VXLAN, VNI; those technologies fail in predictable ways when required parameters do not match or when the required control- plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post- change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 66
Refer to the exhibit.

```
sys/license/feature-ETH_PORT_ACTIVATION_PKG-cisco-1.0/inst-A/fault-F0670  license-
graceperiod-entered license for ETH_PORT_ACTIVATION_PKG on  fabric-interconnect A
has entered into the grace period
```

An engineer installed a UCS rack mount server and received this error after upgrade. Which action resolves the issue?
A. Copy the license file to the kernel module folder.
B. Enable disabled Ethernet ports.
C. Regenerate the modules map file.
D. Install the license on the fabric interconnect.
Answer: D (LEAVE A REPLY)
Install the license on the fabric interconnect is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS, fabric interconnect must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 67
Refer to the exhibit.



Two Cisco Nexus 9000 Series Switches fail to establish OSPF neighborship. Which action resolves the issue?

A. Enable interface VLAN 20 on SW2

B. Set cos1 of interface EthlM0 to 40

C. Configure Loopback0 as passive interface

D. Change interface 1/11 network type as Broadcast

Answer: D (LEAVE A REPLY)

The answer is Change interface 1/11 network type as Broadcast because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references OSPF, Cisco Nexus, Nexus 9000, Cisco Nexus 9000; those technologies fail in predictable ways when required parameters do not match or when the required control-plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post-change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 68

An FSM failed during an upgrade with the auto-install feature enabled. The engineer must remove the service pack from the subordinate fabric interconnect (FI) to recover the FIs. Which set of commands resolves the issue?

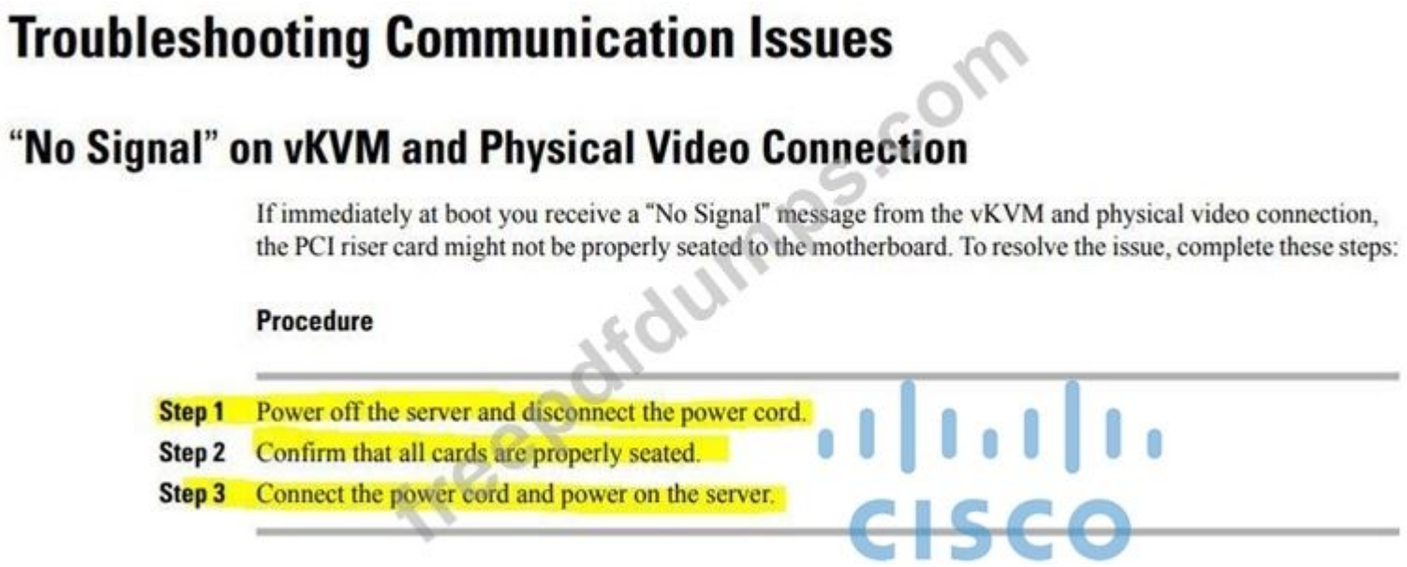
A. UCS-A# scope org
UCS-A/org # scope fw-infra-pack default
UCS-A /org/fw-infra-pack # set infra-bundle-version " "
UCS-A/org/fw-infra-pack* # commit-buffer

B. UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack
UCS-A# /fabric-interconnect* # commit-buffer

C. UCS-A# scope org
UCS-A/org # scope fw-infra-pack default

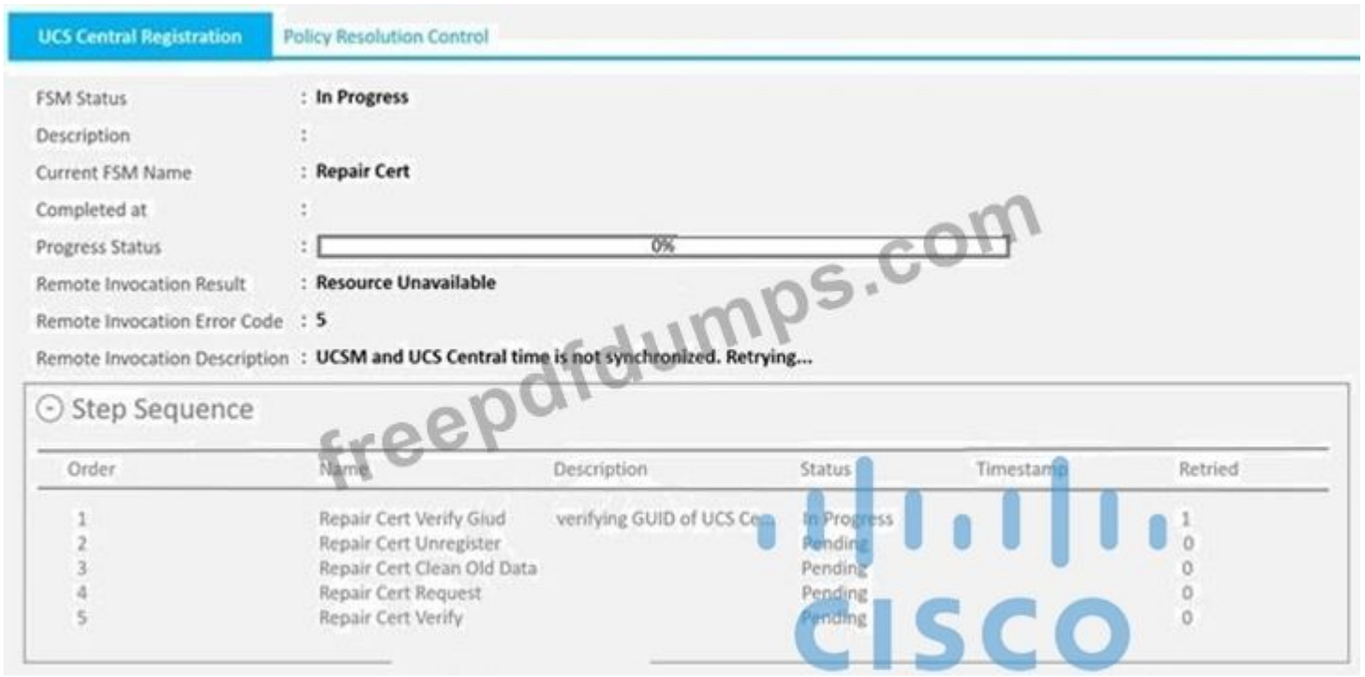
UCS-A /org/fw-infra-pack # set infra-bundle-version
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
D. UCS-A# scope fabric-interconnect b
UCS-A# /fabric-interconnect # remove service-pack security
UCS-A# /fabric-interconnect* # commit-buffer
Answer: D (LEAVE A REPLY)
UCS-A# scope fabric-interconnect b UCS-A# /fabric-interconnect # remove service-pack security UCS-A# /fabric-interconnect* # commit-buffer is correct because the failure is tied to the UCS managed state of UCS, fabric interconnect. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table. If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

NEW QUESTION: 69
During a boot process of a Cisco UCS C-Series Rack Server, an engineer receives a " No Signal " message from the vKVM and physical connection. Which set of steps resolves the issue?
A. 1- Disconnect the power cord
2- Confirm that all cards are properly seated
3- Connect the power cord and power on the server
B. 1- Power off the server and disconnect the power cord
2- Confirm that all cards are properly seated
3- Connect the power cord and power on the server
C. 1- Power off the server and disconnect the power cord
2- Confirm that all cards are available
3- Connect the power cord and power on the server
D. 1- Disconnect the power cord
2- Confirm that all cards are properly seated
3- Connect the power cord
Answer: B (LEAVE A REPLY)
1- Power off the server and disconnect the power cord 2- Confirm that all cards are properly seated 3- Connect the power cord and power on the server is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.



NEW QUESTION: 70

Refer to the exhibit.



The integration between Cisco UCS Manager and Cisco UCS Central failed. Which action resolves the issue?

A. Implement the consistent NTP source between the appliances

B. Implement the connectivity between the appliances through a firewall

C. Configure the certificate between the appliances

D. Configure the shared secret key between the appliances

Answer: A (LEAVE A REPLY)

Implement the consistent NTP source between the appliances is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS, UCS Manager, UCS Central, certificate must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot

failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 71
Refer to the exhibit.

A network engineer upgrades the firmware of a Cisco Fabric Interconnect from boot flash. During the process, the fabric interconnect reboots and displays the message shown in the exhibit. Which action resolves the issue?
A. Remove the service pack and upgrade through the auto-install procedure
B. Reset the I/O module and install the firmware image from the boot flash
C. Boot the kickstart image from boot flash and load the system image
D. Reload the switch and boot the kickstart image from the TFTP server
Answer: D (LEAVE A REPLY)
Reload the switch and boot the kickstart image from the TFTP server is correct because the failure is tied to the UCS managed state of firmware, fabric interconnect. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table.
If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

NEW QUESTION: 72
Refer to the exhibit.

An attempt to bind the Ethernet interface to vFC fails. Which action resolves the issue?

A. Add the FCoE VLAN to the allowed VLAN list.

B. Configure the FCoE VLAN that corresponds to the vFC VSAN as a private VLAN.

C. Configure the interface as a trunk port.

D. Configure the interface to use the native VLAN of the trunk port.

Answer: C (LEAVE A REPLY)

The correct answer is Configure the interface as a trunk port. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV/NPIV, or port-security policy. This question focuses on VSAN, FCoE, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator-to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 73

Refer to the exhibit.

A client configures an upgrade of its Cisco Nexus switches that are connected to the Cisco ACI controller, such that the switches are upgraded one at a time. After the upgrade is run, it is discovered that both Cisco Nexus switches were upgraded simultaneously. Which two actions ensure that the switches upgrade one at a time? (Choose two.)

A. Configure the *Do not pause on failure and do not wait on cluster health " Run Mode
B. Choose the ' Pause upon upgrade failure " Run Mode
C. Select the " Graceful Maintenance " checkbox
D. Place each leaf switch in a different upgrade group
E. Check the Ignore Compatibility " checkbox
Answer: (SHOW ANSWER)
The selected answer, Select the " Graceful Maintenance " checkbox; Place each leaf switch in a different upgrade group, follows Cisco UCS operational logic. UCS Manager is policy-driven, so troubleshooting must determine whether the problem is caused by hardware discovery, service profile association, firmware activation, boot order, storage presentation, or management integration. The scenario points to ACI, UCS, Cisco Nexus; that is why the selected action fixes the root condition rather than merely restarting the server.
The wrong options either affect a different policy, require unnecessary disruption, or assume that physical connectivity alone is sufficient. Cisco documentation for UCS server boot and firmware management stresses that boot policies must include the correct target details, firmware workflows must complete their FSM stages, and hardware changes often require acknowledgement or re-acknowledgement before UCS Manager uses the new inventory. After remediation, the engineer should confirm that the UCS fault is cleared, the server association or discovery state is complete, and the operating system or management service can use the intended path.

NEW QUESTION: 74
Refer to the exhibit.

```
ficl-mgmt-A# show cluster state
Cluster Id: 0xfe92119409cf1111-0x81a200defbec3111
A: UP, PRIMARY
B: UP, SUBORDINATE

ficl-mgmt-A(nxos)# show fex 1 detail | exclude Down
FEX: 1 Description: FEX0001   state: Online
   Pinning-mode: static    Max-links: 1
   Fabric port for control traffic: Eth1/4
   FCoE Admin: false
   FCoE Oper: true
   FCoE FEX AA Configured: false
   Fabric interface state:
      Eth1/1 - Interface Up. State: Active
      Eth1/2 - Interface Up. State: Active
      Eth1/3 - Interface Up. State: Active
      Eth1/4 - Interface Up. State: Active
   Fex Port        State   Fabric Port
     Eth1/1/1    Up       Eth1/1
```

Eth1/1/3	Up	Eth1/1
Eth1/1/5	Up	Eth1/2
Eth1/1/7	Up	Eth1/2
Eth1/1/9	Up	Eth1/3
Eth1/1/11	Up	Eth1/3
Eth1/1/13	Up	Eth1/4
Eth1/1/15	Up	Eth1/4
Eth1/1/17	Up	Eth1/1
Eth1/1/19	Up	Eth1/1
Eth1/1/21	Up	Eth1/2
Eth1/1/23	Up	Eth1/2
Eth1/1/33	Up	Eth1/4

A network engineer needs to capture traffic from the VMs that utilize the IOM host interface Eth1/1/23 of a Cisco UCS B-Series chassis. A traffic analyzer is used to get traffic captured from the Eth1/4 interface of the subordinate fabric interconnect. The network engineer notices that traffic is not captured on the traffic analyzer. Which action resolves the issue?

A. Span the traffic from the Eth 1/2 of the subordinate fabric interconnect.

B. Span the traffic from the Eth 1/4 of the subordinate fabric interconnect.

C. Span the traffic from the Eth 1/2 of the primary fabric interconnect.

D. Span the traffic from the Eth 1/4 of the primary fabric interconnect.

Answer: C (LEAVE A REPLY)

The correct action is Span the traffic from the Eth 1/2 of the primary fabric interconnect. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves UCS, fabric interconnect, IOM, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.

NEW QUESTION: 75

Refer to the exhibit.

```
switch# guestshell resize cpu 4
Note: System CPU share will be resized on Guest shell enable
```

After the configuration is performed, guestshell continues to use 2%CPU. Which action resolves the issue?

A. Resync the database

B. Recreate the guestshell

C. Reboot the guestshell

D. Reboot the switch

Answer: C (LEAVE A REPLY)

Reboot the guestshell resolves the problem because the symptom is specific to the automation subsystem handling After, CPU, Resync, Recreate. Nexus automation failures are frequently caused by a missing EEM event statement, absent event-default action, invalid REST path, incorrect JSON or XML syntax, Guest Shell DNS/resource settings, or a scheduler feature that is not enabled. The selected answer corrects that execution prerequisite. The wrong options may make sense for normal switch forwarding, but they do not repair the automation control path. Cisco documentation treats Guest Shell as a separate Linux environment and EEM as a policy engine that can intercept CLI events; both must be validated from their own operational state. A proper verification is to confirm the policy is registered, run the job or API call again, review the response or syslog output, and ensure that normal CLI behavior is preserved after the automation fires.

NEW QUESTION: 76
Refer to the exhibit.

```
F606263 [FSM:FAILED]: VMM Add-Controller FSM: comp/prov-VMware/ ctrlr-[RTPACILab]-
DCCCNP_Vcenter Failed to retrieve ServiceContent from the vCenter server
11.11.22.22(FSM:ifc:vmmmgr:CompCtrlrAdd)
F606351 [FSM:FAILED]: Task for updating comp:PolCont(TASK:ifc:vmmmgr:-
CompPolContUpdateCtrlrPol)
F16438 [FSM:STAGE:FAILED]: Establish connection Stage: comp/prov-VMware/ ctrlr-
[RTPACILab]- DCCCNP_Vcenter Failed to retrieve ServiceContent from the vCenter
server 11.11.22.22 (FSM-STAGE:ifc:vmmmgr:CompCtrlrAdd:Connect)
```

An engineer is configuring a VMM domain integration, but the operation fails to complete. Which two actions resolve the issue? (Choose two.)
A. Use a different device package.
B. Configure the route from virtual machine managerB management network to vCenter.
C. Update the VMware vCenter version to be compatible with the Cisco ACI release.
D. Change the VMware vCenter access credentials.
E. Change VMware vCenter IP address.
Answer: D,E (LEAVE A REPLY)
Cisco troubleshooting logic supports Change VMware vCenter IP address as the required fix. In this question the symptoms point to ACI, VMM, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.

NEW QUESTION: 77
Refer to the exhibit.

After an unexpected reload of the Cisco Nexus 9000 Series Switch, the network administrator noticed that one of the Software Maintenance Upgrades (SMU) images is inactive. The engineer must ensure that the package remains active after the switch is reloaded in the future. Which action accomplishes this goal?

A. Commit the package using the install commit command.

B. Save the running configuration after activating the package.

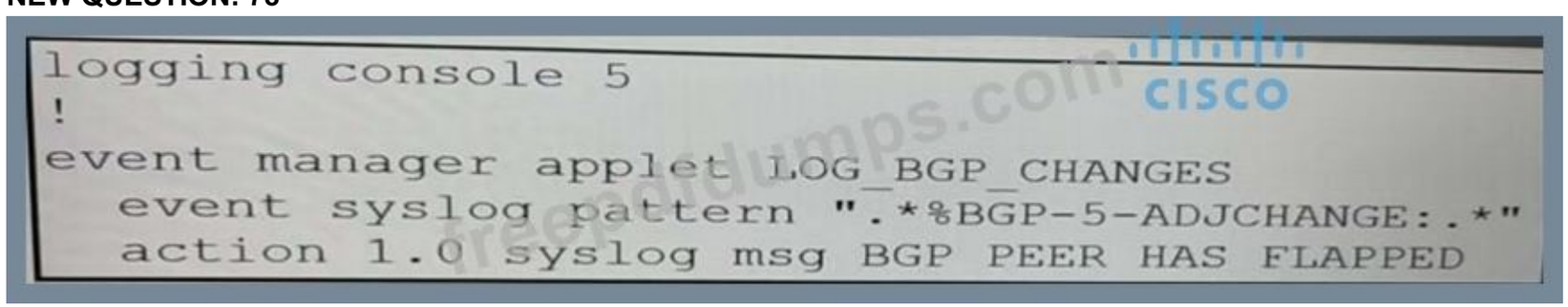
C. Deactivate and uninstall the active core package.

D. Copy the SMU package file on the bootflash.

Answer: A (LEAVE A REPLY)

Commit the package using the install commit command is the valid corrective action because the failure described is a protocol or fabric state problem, not a generic connectivity issue. For Cisco Nexus, Nexus
9000, Cisco Nexus 9000, Cisco troubleshooting expects the engineer to compare both endpoints of the relationship: vPC peers must agree on consistency parameters, HSRP peers must exchange hellos in the same VLAN and version context, OSPF/BGP peers must match the attributes required for stable adjacency, and VXLAN EVPN must advertise the correct host or prefix information. The selected option restores that required state. The other options either operate on the wrong layer, change a value that is not used to form the relationship, or would make the peer relationship less deterministic. A clean validation is to inspect the control-plane table first, then verify the forwarding table, and finally test end-to-end traffic. This is the Cisco- preferred approach because it avoids random changes and confirms that the fabric is forwarding based on correct protocol state.

NEW QUESTION: 78



Refer to the exhibit The EEM applet must generate a syslog message whena BGP adjacency flaps. This message must be displayed to the console of the switch. However, when a BGP adjacency failure is simulated, no syslog message is displayed. Which action resolves the issue?

A. Add the event-default action statement.

B. Modify the policy to use the snmp trap action.

C. Adjust the policy to match an SNMP OID.

D. Set the logging priority to Wamings.

Answer: D (LEAVE A REPLY)

The correct answer is Set the logging priority to Wamings. Cisco NX-OS automation features are context- sensitive: Guest Shell, Bash, EEM, scheduler, NX-API, REST calls, and Python scripts each run with their own parser, privilege model, environment, and resource limits. The scenario involves BGP, EEM, SNMP, and the selected action corrects the missing execution condition. Cisco documentation for Nexus programmability states that Guest Shell resources and networking must be configured inside the Guest Shell context, EEM applets require a valid event statement and event-default when the intercepted CLI command must continue, and API calls must target the correct managed object or class. The alternative answers either operate in the wrong context, omit a required trigger/action, or correct a parameter unrelated to the failure. Validation should include running the command manually in the same context, checking logs or return codes, and confirming that the automation completes without blocking the normal NX-OS operation it observes.

NEW QUESTION: 79

Refer to the exhibit.

```
POST
http://10.1.1.51/api/mo/uni.xml

<infraAccPortP name="vepa">
        <infraHPortS name="pselc" type="range">
            <infraPortBlk name="blk"
                fromCard="1" toCard="1" fromPort="1" toPort="10">
            </infraPortBlk>
            <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-
VepaPortG" />
        </infraHPortS>
 </infraAccPortP>
```


An engineer uses a REST API to map the interface selector with ports 1/1 to 1/20 to an interface profile. The script fails with a 400 response status code. Which action resolves the problem?

A. Permit user access to the requested resource.

B. Post the script using the HTTPS method.

C. Add a content-length header to the request.

D. Run the script again with valid authentication values.

Answer: D (LEAVE A REPLY)

Run the script again with valid authentication values is the required fix because the automation failure is caused by execution context, syntax, or resource state around REST API. On Cisco Nexus switches, automation is not a single feature; EEM policies, CLI actions, Guest Shell Linux commands, REST payloads, and scheduled jobs are evaluated by different subsystems. A script can fail even while the switch itself has connectivity or the command works interactively. The selected answer supplies the missing requirement, such as the correct event/action, DNS or resource setting, API URI, payload format, feature enablement, or reboot needed for a Guest Shell change to take effect. The other choices address adjacent features but do not satisfy the failing subsystem. After applying the fix, the engineer should verify the policy registration, job result, API response code, or Guest Shell runtime state and confirm that the intended command is no longer blocked or silently ignored.

NEW QUESTION: 80
You have an ACI environment with three APICs, two spine switches, and four-leaf switches. You wipe and reboot all APICs first then leaf and spine switches one-by-one and successfully go through the Initial Setup dialogue on the APIC 1 CIMC KVM console. When you log in to the APIC1 WebGUI, you notice that you do not see any directly connected leaf switches being discovered under Fabric > Inventory > Fabric Membership.
What is the cause of the issue?
A. The leaf nodes were not erased properly, which caused a fabric parameters mismatch with the APIC1.
B. Rebooting the APICs and the leaf and spine switches after wiping them is not required.
C. You forgot to enter the TEP Pool value during the Initial Setup dialogue on APIC1.
D. The same Fabric Name value should be used before after wiping all devices.
Answer: A (LEAVE A REPLY)
The leaf nodes were not erased properly, which caused a fabric parameters mismatch with the APIC1 is correct because the failure is tied to the UCS managed state of ACI, APIC, CIMC. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table. If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

NEW QUESTION: 81
A Cisco Nexus Dashboard consists of a single master node and three worker nodes, and the dashboard is integrated with a Cisco ACI Multi-Site fabric. An engineer notices that the Cisco ACI site is unavailable on the Nexus Dashboard. Which action resolves the issue?
A. Export APIC configuration before the site is onboarded.
B. Replace the master and worker nodes.
C. Reregister the site in the Nexus Dashboard GUI.
D. Re-add a different master node to the physical cluster.
Answer: C (LEAVE A REPLY)
Reregister the site in the Nexus Dashboard GUI is correct because the failure is an operations-plane condition involving ACI, APIC, Nexus Dashboard, Cisco Nexus. In Cisco data center products, management functions depend on more than IP connectivity. AAA servers must return the correct attributes, RBAC must map users to the correct security domain or role, certificates must be trusted and valid for the access method, and firmware or registration workflows must satisfy documented prerequisites such as NTP and required ports.
The selected answer corrects that dependency. The distractors are not root-cause fixes because they either target a different subsystem or change a setting that would not influence the observed login, registration, warning, or fault. After the change, validation should include a successful login or registration test, review of the audit/fault record, and confirmation that the expected administrative scope is enforced. That approach matches Cisco operational troubleshooting for DCIT environments.

NEW QUESTION: 82
Refer to the exhibit.

An engineer troubleshoots the HSRP configuration and notes that the remote end uses HSRP version 1. The engineer sets the local HSRP to version 1, but the problem continues. Which action resolves the issue?

A. Change the local group number to 255 or less and request that the remote data center matches the group member in its configuration.

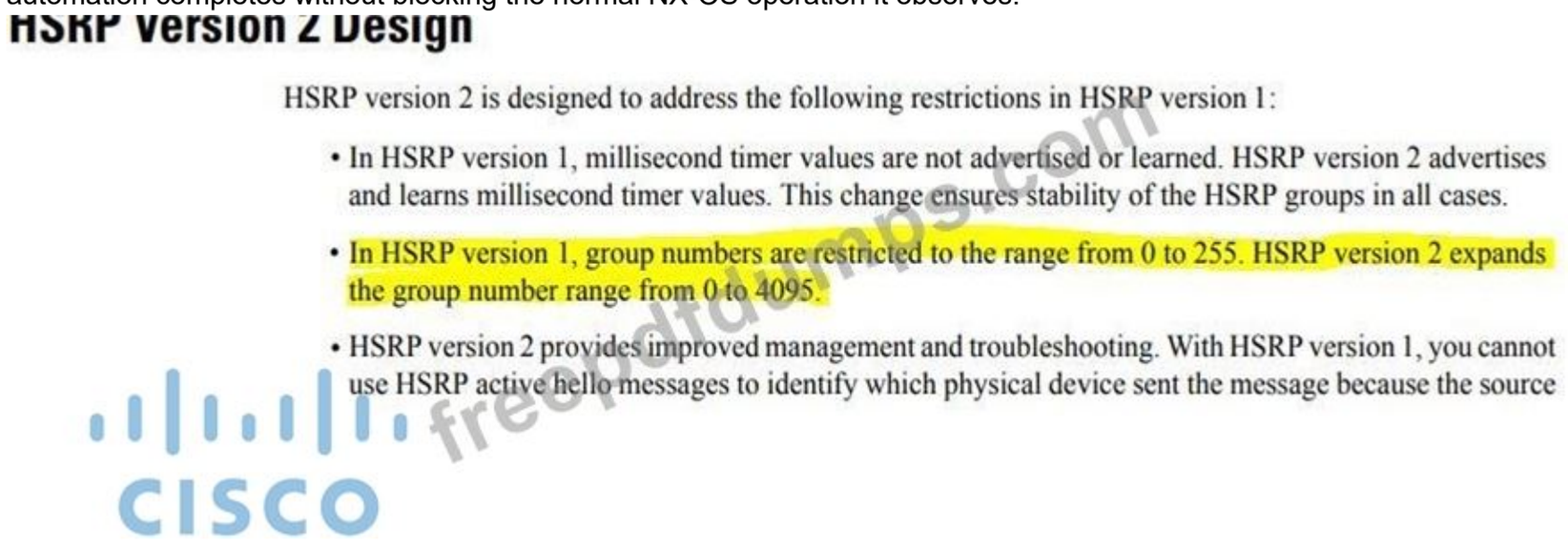
B. Set the local group number as 300 in the remote data center configuration

C. Run version 1 and version 2 HSRP on VLAN300 in the local data center.

D. Reduce the priority of the local HSRP to below 100 to force the local HSRP to standby and then change the version to version 1.

Answer: A (LEAVE A REPLY)

The correct answer is Change the local group number to 255 or less and request that the remote data center matches the group member in its configuration. Cisco NX-OS automation features are context-sensitive: Guest Shell, Bash, EEM, scheduler, NX-API, REST calls, and Python scripts each run with their own parser, privilege model, environment, and resource limits. The scenario involves HSRP, and the selected action corrects the missing execution condition. Cisco documentation for Nexus programmability states that Guest Shell resources and networking must be configured inside the Guest Shell context, EEM applets require a valid event statement and event-default when the intercepted CLI command must continue, and API calls must target the correct managed object or class. The alternative answers either operate in the wrong context, omit a required trigger/action, or correct a parameter unrelated to the failure. Validation should include running the command manually in the same context, checking logs or return codes, and confirming that the automation completes without blocking the normal NX-OS operation it observes.



NEW QUESTION: 83

Your client reports that many flaps and server cluster disconnects occur in their data center. While troubleshooting the issue, you discover a network attack hitting their Cisco Nexus 7000 Series Switches and determine that the source IP addresses are spoofed. Which first-line security solution resolves this issue?

A. Dynamic ARP Inspection

B. Unicast RPF

C. IP Source Guard

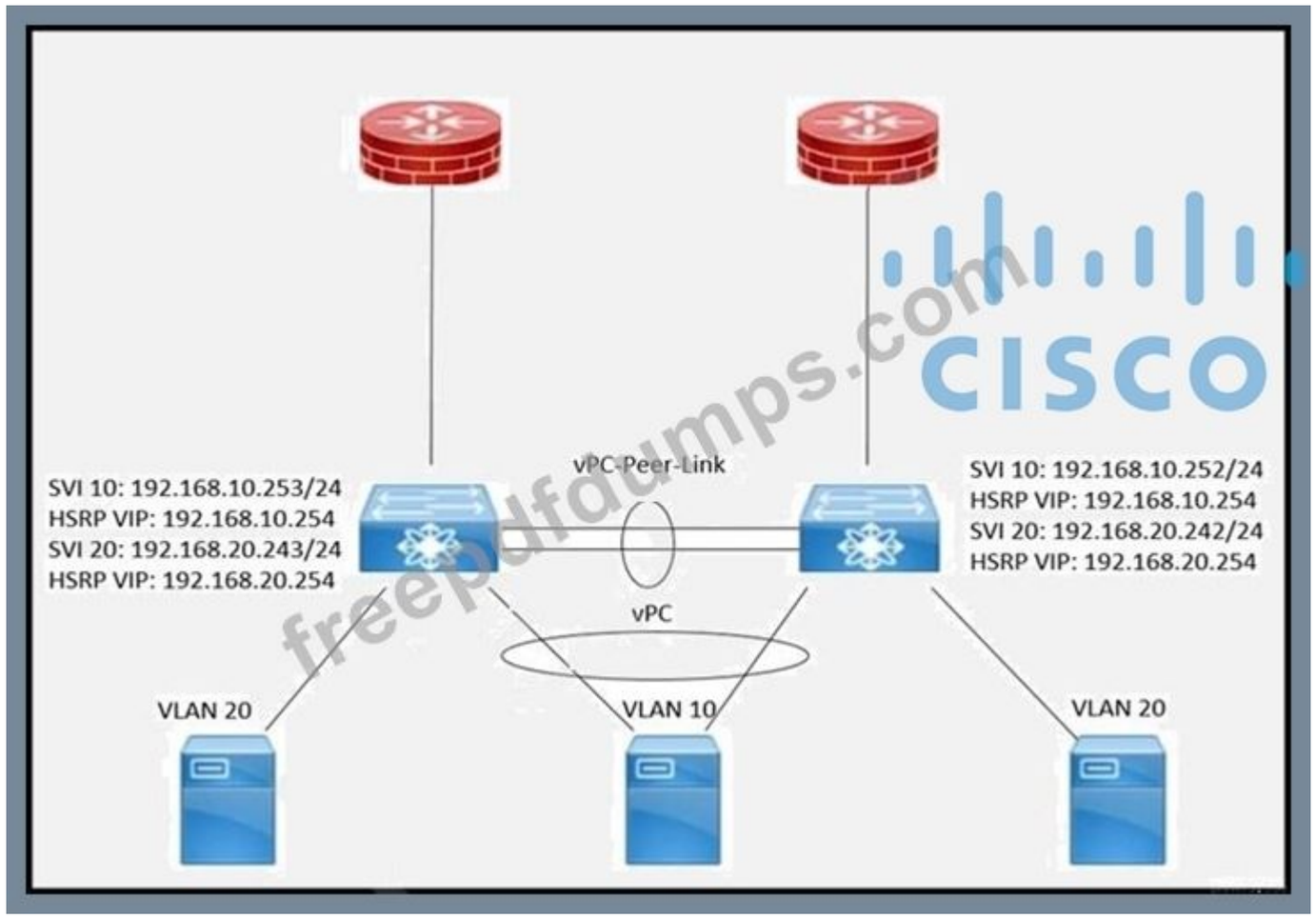
D. Storm Control

Answer: B (LEAVE A REPLY)

The answer is Unicast RPF because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references Unicast RPF, Dynamic ARP Inspection, IP Source Guard, Storm Control, Cisco Nexus; those technologies fail in predictable ways when required parameters do not match or when the required control-plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because they touch related features, but they do not resolve the specific failure condition. Post-change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 84

Refer to the exhibit.



An engineer discovers that if the vPC peer link goes down, half of the devices in VLAN 20 experience connectivity issues with the external networks Which action resolves the issue?

A. Configure a dedicated Layer 3 link between vPC peers

B. Allow non-vPC VLANs on a second trunk between the two vPC peers
C. Add the non-vPC SVIs in the dual-active exclude VLAN list
D. Exclude the non-vPC VLANs from vPC peer link
Answer: A (LEAVE A REPLY)
The correct remediation is Configure a dedicated Layer 3 link between vPC peers. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on vPC, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state- dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC
/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 85
A network engineer experiences the error "DDR3_P1_B1_ECC" when upgrading Cisco UCS firmware.
Which action resolves the issue?
A. Reset the DIMM
B. Reset the BMC firmware
C. Reflash the controller firmware
D. Reflash the DIMM
Answer: A (LEAVE A REPLY)
Reset the DIMM is correct because the failure is tied to the UCS managed state of UCS, firmware. In Cisco UCS, policies are not advisory; they are the source from which fabric interconnects program adapters, boot targets, server identity, firmware, and external integrations. A mismatch between the policy and the actual hardware or upstream storage/network state can cause boot, discovery, KVM, firmware, or connectivity failures. The selected action addresses the object that UCS Manager uses to build the final operational configuration. The distractors either solve a different fault domain or bypass the policy model. A disciplined DCIT validation sequence is to check the fault code, the FSM history, the equipment inventory, the service profile association, and the relevant adapter or boot table. If those states are correct after the change, the UCS component should return to operable service without unnecessary reconfiguration.

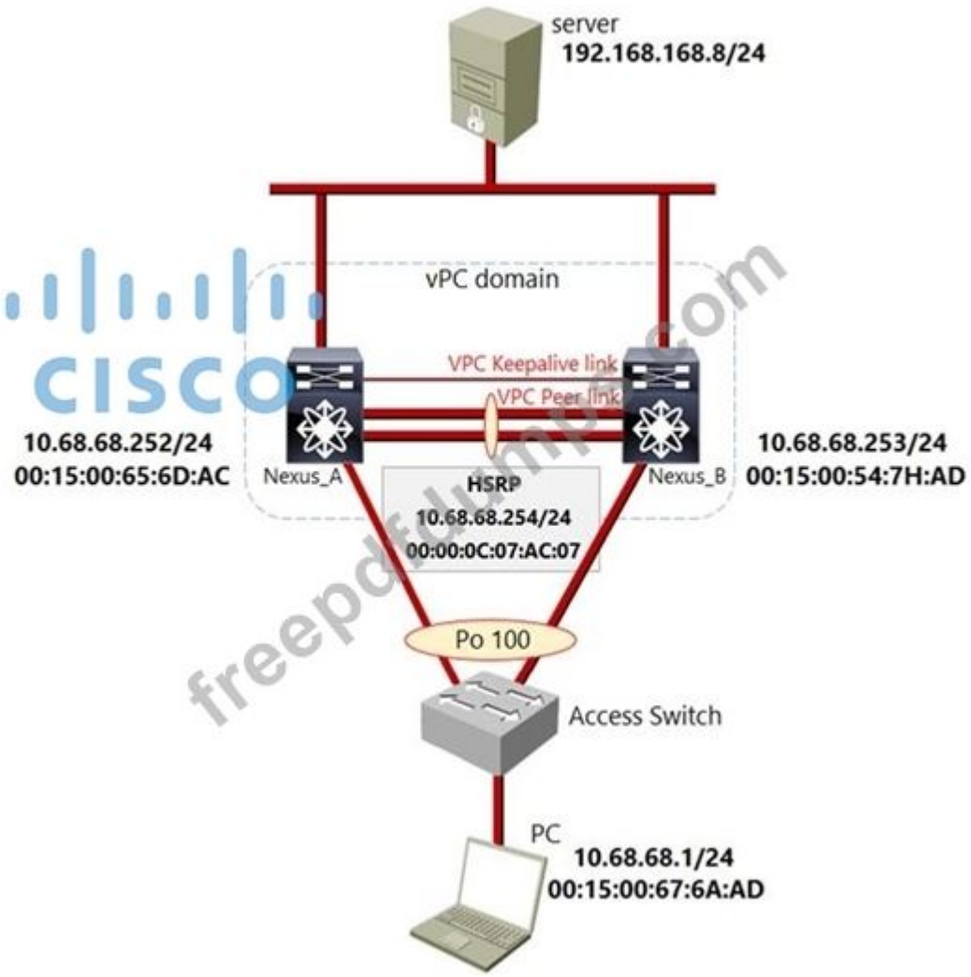
NEW QUESTION: 86
Cisco Unified Computing System Manager raises a critical error message that indicates that the system has overlapping Ethernet and FCoE VLANs. All of the Ethernet traffic on the overlapping VLANs drops. Which action resolves the issue?
A. Modify the VLAN assignment to vNICs.
B. Change the PIN groups on the vHBAs.
C. Modify the FCoE VLAN.
D. Set the FCoE VLAN as the native VLAN on server uplinks.
Answer: C (LEAVE A REPLY)
The selected resolution is Modify the FCoE VLAN because the failure is in the Fibre Channel/FCoE control path around FCoE. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting

therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 87
An engineer is troubleshooting a fabric discovery failure. Which two requirements must an engineer verify about switch connectivity to solve the problem? (Choose two.)
A. A Cisco APIC must be attached to a spine node only.
B. A Cisco APIC must be attached to leaf nodes.
C. Spine nodes must connect to other spine nodes.
D. A Cisco APIC must be dual-attached to two separate spine nodes.
E. Leaf nodes must connect to spine nodes only.
Answer: B,E (LEAVE A REPLY)
The correct remediation is A Cisco APIC must be attached to leaf nodes; Leaf nodes must connect to spine nodes only. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on APIC, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state-dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data- plane policy.

NEW QUESTION: 88
An engineer is troubleshooting a custom AV pair that was created by a client on an external authentication server to map a read-only role for a specific security domain. Which AV pair solves the problem?
A. shell:domains=Security_Domain_1//Read_Role_1|Read_Role_2
B. shell:domains=Security_Domain_1/Write_Role_1|Read_Role_2
C. shell=Security_Domain_1/Read_Role_1|Read_Role_2
D. shell:domains=Security_Domain_1/Read_Role_1|Read_Role_2
Answer: D (LEAVE A REPLY)
The correct answer is shell:domains=Security_Domain_1/Read_Role_1|Read_Role_2. Cisco management and operations troubleshooting focuses on control-plane services such as RBAC, AAA, certificates, SNMP, firmware packages, centralized management registration, fault workflows, and node lifecycle state. This item references the affected data-center component, so the selected action fixes the management dependency rather than the data-plane symptom. Cisco platforms often allow basic reachability while a higher-level integration still fails because of time synchronization, certificate trust, role mapping, authorization attributes, feature state, or incomplete lifecycle cleanup. The other options either modify forwarding behavior, adjust the wrong credential or role, or bypass the required operational workflow. The engineer should validate the fix by confirming the management session or registration, checking the relevant fault or audit log, and confirming that the user, node, or integration has the expected role and operational status. This is consistent with Cisco DCIT emphasis on operational evidence before and after the change.

NEW QUESTION: 89
Refer to the exhibit.



A PC belongs to VLAN 68 The user experiences a large amount of packet loss when communicating with hosts that are outside of VLAN 68. Which action resolves the problem?

A. Replace HSRP with GLBP

B. Enable the peer-gateway feature

C. Remove the HSRP configuration

D. Configure ip arp synchronization on both switches.

Answer: B (LEAVE A REPLY)

Enable the peer-gateway feature is correct because the failure is an operations-plane condition involving HSRP. In Cisco data center products, management functions depend on more than IP connectivity. AAA servers must return the correct attributes, RBAC must map users to the correct security domain or role, certificates must be trusted and valid for the access method, and firmware or registration workflows must satisfy documented prerequisites such as NTP and required ports. The selected answer corrects that dependency. The distractors are not root-cause fixes because they either target a different subsystem or change a setting that would not influence the observed login, registration, warning, or fault. After the change, validation should include a successful login or registration test, review of the audit/fault record, and confirmation that the expected administrative scope is enforced. That approach matches Cisco operational troubleshooting for DCIT environments. The final check is to document the before-and-after state so the remediation is tied to a repeatable Cisco troubleshooting symptom rather than an assumed fix.

NEW QUESTION: 90

```
switch-1# show fspf vsan 200 interface port-channel 200
FSPF interface port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 40 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT
Statistics counters :
Number of packets received : LSU 3 LSA 3 Hello 136 Error packets 3
Number of packets transmitted : LSU 3 LSA 3 Hello 182 Retransmitted LSU 0
Number of times inactivity timer expired for the interface = 0

switch-2# show fspf vsan 200 interface san-port-channel 200
FSPF interface san-port-channel 200 in VSAN 200
FSPF routing administrative state is active
Interface cost is 125
Timer intervals configured, Hello 20 s, Dead 80 s, Retransmit 5 s
FSPF State is INIT
Statistics counters :
Number of packets received : LSU 3 LSA 3 Hello 185 Error packets 169
Number of packets transmitted : LSU 3 LSA 3 Hello 139 Retransmitted LSU 0
Number of times inactivity timer expired for the interface = 24
```


Refer to the exhibit. VSAN traffic is not routed as expected. Which action should be taken to resolve the issue?

A. Reset the error packet counter
B. Configure the hello timer to match the neighbor
C. Configure the FSPF dead interval with a value higher than 80 seconds
D. Reset the inactivity timer on switch-2

Answer: B (LEAVE A REPLY)

The correct answer is Configure the hello timer to match the neighbor. Cisco MDS and Nexus SAN troubleshooting is driven by fabric state: the host and target must be in the correct VSAN, must complete FLOGI/PLOGI where applicable, and must be permitted by active zoning, fcdomain, FSPF, NPV/NPIV, or port-security policy. This question focuses on VSAN, FSPF, so the selected action fixes the dependency that prevents the initiator, target, or inter-switch link from becoming usable. Cisco documentation emphasizes checking VSAN membership, active zonesets, correct port mode, fabric binding, device-alias consistency, and the relevant FC databases before changing unrelated server settings. The distractors either target a different database, use the wrong port role, or would not cause the observed Fibre Channel state to change. After the fix, the engineer should confirm the interface state, FLOGI database, name-server entries, zoneset activation, and successful initiator-to-target reachability with tools such as fcping or fabric show commands.

NEW QUESTION: 91

Refer to the exhibit.

The cURL command fails to complete. Which action resolves the problem?

A. Remove " .json\ " from the URL.

B. Include -p " password " in the command.

C. Add -H " X-Auth-Token " to the command.

D. Change " .json " to " .xml " at the end of the URL.

Answer: (SHOW ANSWER)

The correct answer is Include -p " password " in the command. Cisco NX-OS automation features are context- sensitive: Guest Shell, Bash, EEM, scheduler, NX-API, REST calls, and Python scripts each run with their own parser, privilege model, environment, and resource limits. The scenario involves The, Remove, URL, Include, and the selected action corrects the missing execution condition. Cisco documentation for Nexus programmability states that Guest Shell resources and networking must be configured inside the Guest Shell context, EEM applets require a valid event statement and event-default when the intercepted CLI command must continue, and API calls must target the correct managed object or class. The alternative answers either operate in the wrong context, omit a required trigger/action, or correct a parameter unrelated to the failure.

Validation should include running the command manually in the same context, checking logs or return codes, and confirming that the automation completes without blocking the normal NX-OS operation it observes.

NEW QUESTION: 92

Refer to the exhibit.

A Cisco ACI fabric has a VPC policy group toward the external switch. These objects exist inside the fabric:
port channel policy LACP_Active_NoControl
NetFlow monitor policy NetFlow_POL
port channel member policy transmit rate as fast
The engineer must set the LACP timeout to 1 second. However, the engineer notices that the LACP timeout is set to 30 seconds on the CLI. Which action resolves the issue?

A. Add policy NetFlow_Pol to Synergy-18_Bay-3_MGMT_VPC_PolGrp.
B. Attach policy LACP_Active_NoControl to override policy.
C. Assign override policy LACP_fast to Eth1_9_IntSel.
D. Change port-channel member policy transmit rate to normal.

Answer: C (LEAVE A REPLY)

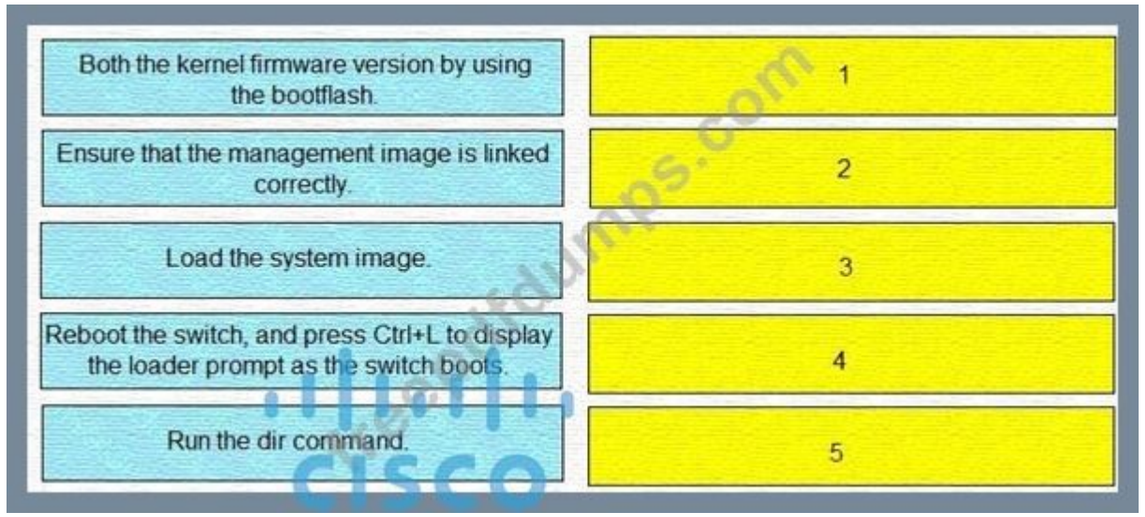
Assign override policy LACP_fast to Eth1_9_IntSel is the valid corrective action because the failure described is a protocol or fabric state problem, not a generic connectivity issue. For vPC, LACP, ACI, Cisco troubleshooting expects the engineer to compare both endpoints of the relationship: vPC peers must agree on consistency parameters, HSRP peers must exchange hellos in the same VLAN and version context, OSPF
/BGP peers must match the attributes required for stable adjacency, and VXLAN EVPN must advertise the correct host or prefix information. The selected option restores that required state. The other options either operate on the wrong layer, change a value that is not used to form the relationship, or would make the peer relationship less deterministic. A clean validation is to inspect the control-plane table first, then verify the forwarding table, and finally test end-to-end traffic. This is the Cisco-preferred approach because it avoids random changes and confirms that the fabric is forwarding based on correct protocol state.

NEW QUESTION: 93
Refer to the exhibit.

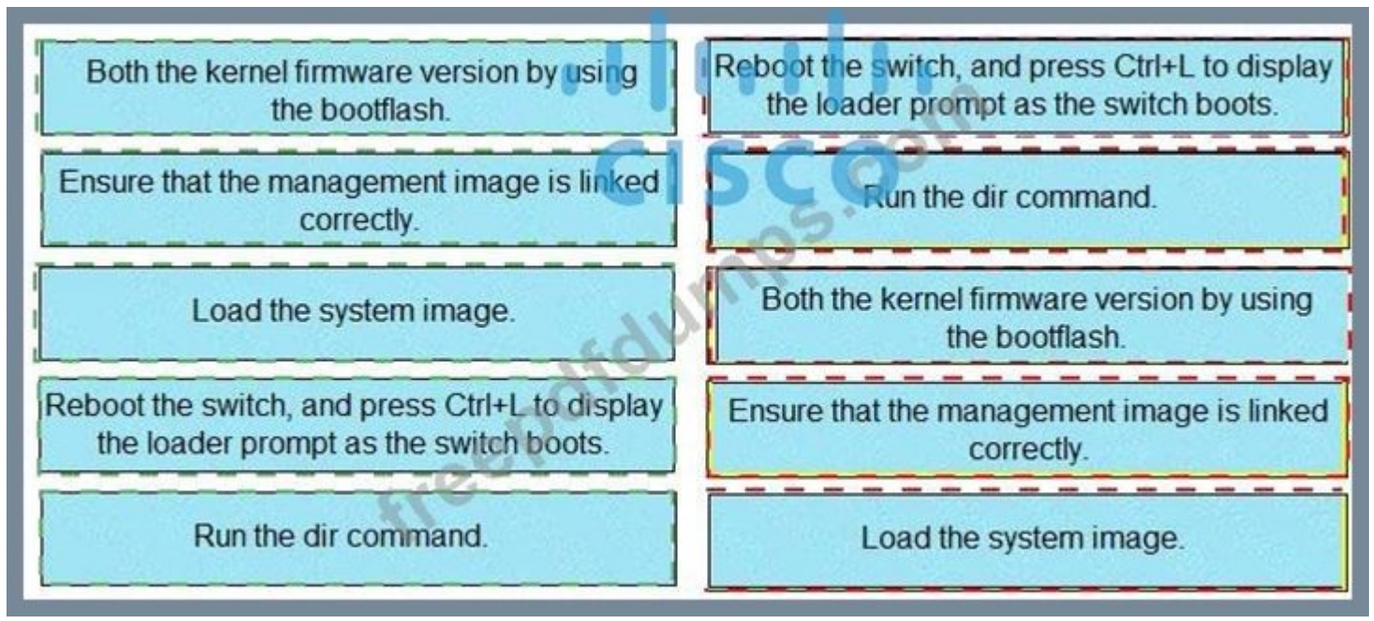
```
bash-4.3# docker run -d -p 69:69/udp -it cisco/tftp
Unable to find image cisco/tftp:latest' locally
docker: Error response from daemon: Get ttps://registry-
1.docker.io/v2/: dial tcp: lookup registry-1.docker.io on
[::1]:53: dial udp [::1]:53: connect: cannot assign requested
address.
```

An engineer is experiencing a problem when running a Docker container inside the Cisco Nexus 9000 bash shell. Which action resolves the issue?
A. Add a new nameserver
B. Connect to bash as a different user
C. Change VRF to management
D. Configure the mgmt0 interface
Answer: (SHOW ANSWER)
The selected option, Add a new nameserver, is correct for the automation path described. Cisco NX-OS requires precision in EEM applets, scheduler jobs, Guest Shell operations, and REST/NX-API syntax. The affected element is Bash, Cisco Nexus, Nexus 9000, Cisco Nexus 9000; therefore, the fix must be applied to the component that actually executes the action. For EEM, that means a valid event detector and explicit actions, with event-default when the matched CLI command should continue. For Guest Shell and Bash, DNS, proxy, resource allocation, and reboot behavior are local to the Linux container. For REST calls, the class name, method, authentication, and XML/JSON structure must match the APIC or NX-OS object model.
The distractors usually change the switch globally or alter an unrelated command. Cisco DCIT automation troubleshooting confirms the fix by checking the returned error, then rerunning the exact job, script, or API operation in the same context.

NEW QUESTION: 94
A firmware upgrade on a fabric interconnect fails. A bootflash contains a valid image. Drag and drop the recovery steps from the left onto the correct order on the right.



Answer:



Explanation:

The correct action is the drag-and-drop mapping shown in the answer key. Cisco UCS troubleshooting depends on the relationship between policy, inventory discovery, firmware state, and server identity. The question involves firmware, fabric interconnect, so the selected option fixes the UCS component or policy that directly controls the failure. In UCS Manager, service profiles, vNIC/vHBA templates, boot policies, firmware packages, server pools, adapters, fabric interconnects, and I/O modules are applied through a managed model; a server can fail even when basic IP reachability exists if the relevant policy is incomplete or the hardware inventory has not been acknowledged correctly. The distractors typically change an unrelated object, force a disruptive recovery without fixing the policy, or apply to a different UCS mode. Cisco guidance is to verify faults, FSM stage, inventory status, association status, and the specific boot or connectivity policy before taking action. After the remediation, validate that the fault clears, the FSM completes, and the server or fabric component returns to the expected operable state.

Reboot the switch, and press Ctrl+L to display the loader prompt as the switch boots.

Run the dir command.

Both the kernel firmware version by using the bootflash.

Ensure that the management image is linked correctly.

Load the system image.

NEW QUESTION: 95

```
vrf context BLUE
  address-family ipv4 unicast
  route-target export 65000:65000
vrf context RED
  address-family ipv4 unicast
  route-target import 65000:65000
!
interface Vlan1000
  no shutdown
  vrf member RED
  no ip redirects
  ip address 10.10.1.254/24
!
ip prefix-list RED_TO_BLUE_PL seq 5 permit 10.10.1.254/24
!
route-map RED_TO_BLUE_RM permit 10
  match ip address RED_TO_BLUE_PL
  set community 65500:65000
!
router bgp 65000
  log-neighbor-changes
  address-family ipv4 unicast
  vrf RED
    router-id 10.255.255.255
    address-family ipv4 unicast
      redistribute direct route-map RED_TO_BLUE_RM
!
```

Refer to the exhibit. The expected routes are not being leaked as expected from VRF RED to VRF BLUE.
Which action resolves the issue?

A. Include the " le 32 " knob under the RED_TO_BLUE_ACL prefix list.
B. Change the route targets under the VRFs.
C. Configure VRF BLUE under the BGP configuration.
D. Set the community to 65000:65000 under the route map.
Answer: D (LEAVE A REPLY)
Set the community to 65000:65000 under the route map is the valid corrective action because the failure described is a protocol or fabric state problem, not a generic connectivity issue. For BGP, Cisco troubleshooting expects the engineer to compare both endpoints of the relationship: vPC peers must agree on consistency parameters, HSRP peers must exchange hellos in the same VLAN and version context, OSPF
/BGP peers must match the attributes required for stable adjacency, and VXLAN EVPN must advertise the correct host or prefix information. The selected option restores that required state. The other options either operate on the wrong layer, change a value that is not used to form the relationship, or would make the peer relationship less deterministic. A clean validation is to inspect the control-plane table first, then verify the forwarding table, and finally test end-to-end traffic. This is the Cisco-preferred approach because it avoids random changes and confirms that the fabric is forwarding based on correct protocol state.

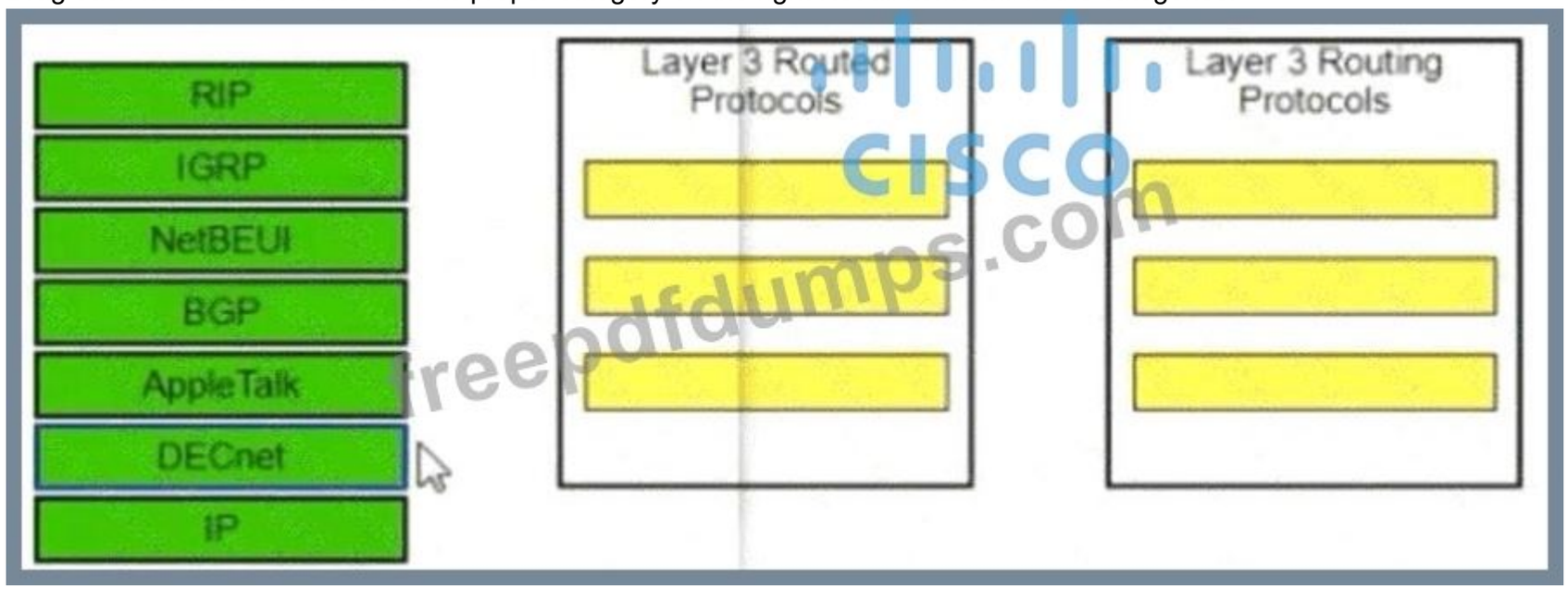
NEW QUESTION: 96

```
adapter 1/1/1 (fls):1# lunlist
vnic : 10 lifid: 5
- FLOGI State : flogi est (fc_id 0x8f0050)
- PLOGI Sessions
- WWNN 50:0a:08:88:87:49:10:14 WWPN 50:0a:08:88:87:49:10:14 fc_id 0x500000
- LUN's configured (SCSI Type, Version, Vendor, Serial No.)
LUN ID : 0x0000000000000001 access failure
- REPORT LUNs Query Response
- Nameserver Query Response
```

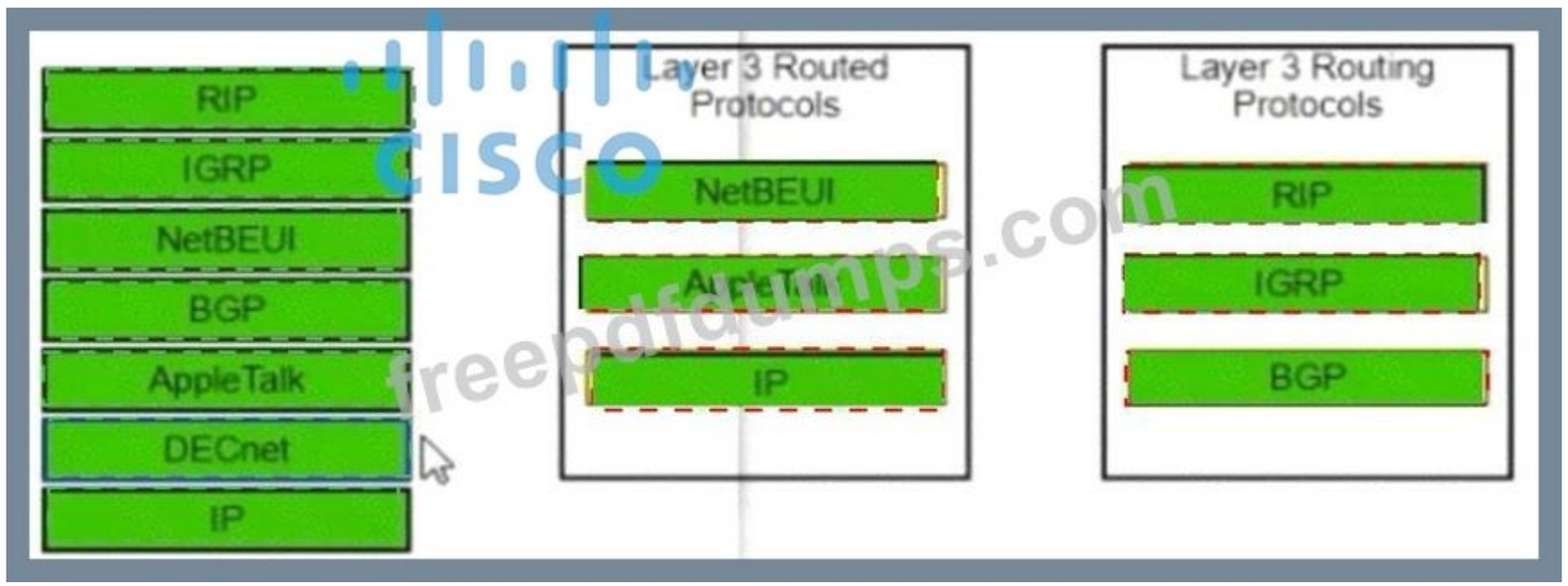
Refer to the exhibit A network engineer fails to boot a Cisco UCS blade from SAN The data center uses Cisco UCS B-Series blades with the end-host mode configured on Cisco UCS fabric interconnects The storage administrator reports no issues with the array Winch action resolves the issue?
A. Change zoning on the Cisco UCS side.
B. Modify zoning on the upstream switch.
C. Unmask the LUN on the storage array
D. Remove the LUN ID from the boot policy
Answer: (SHOW ANSWER)
Remove the LUN ID from the boot policy is the correct fix under Cisco SAN troubleshooting practice. The issue described involves UCS, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 97

Drag each item listed on the left to its proper category on the right Not all items will fit the categories.



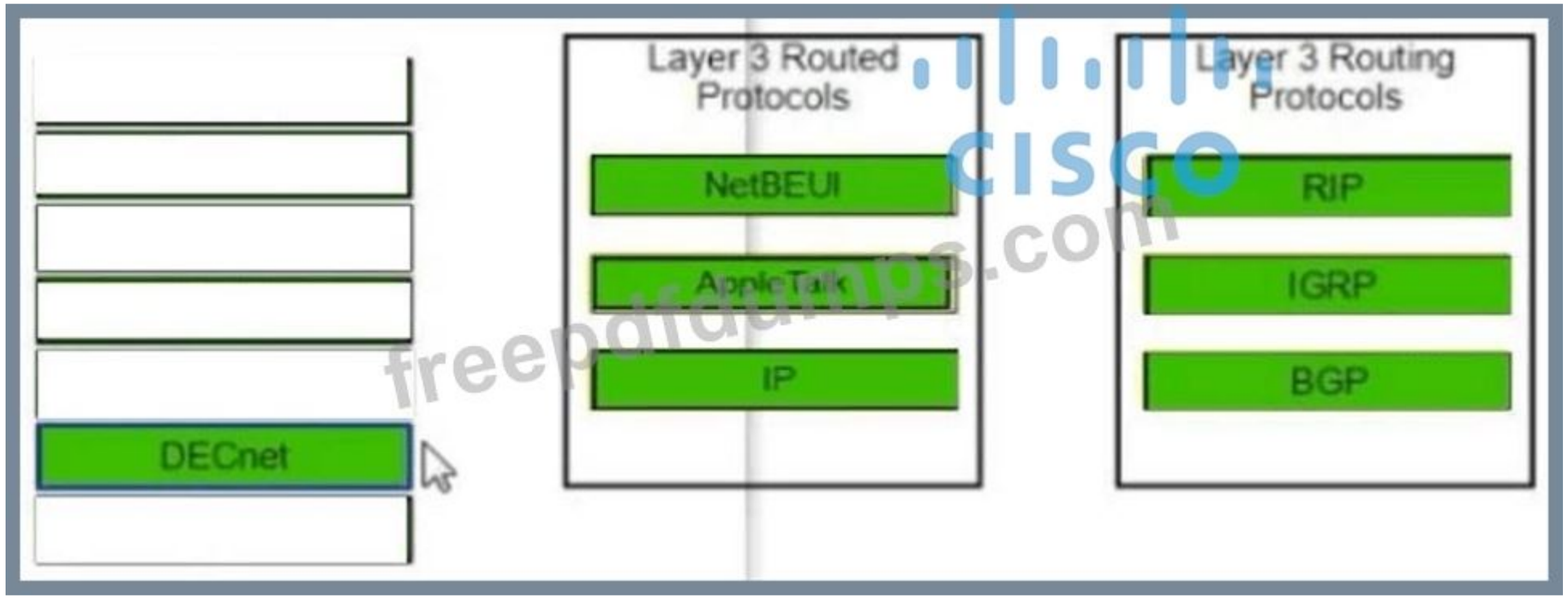
Answer:



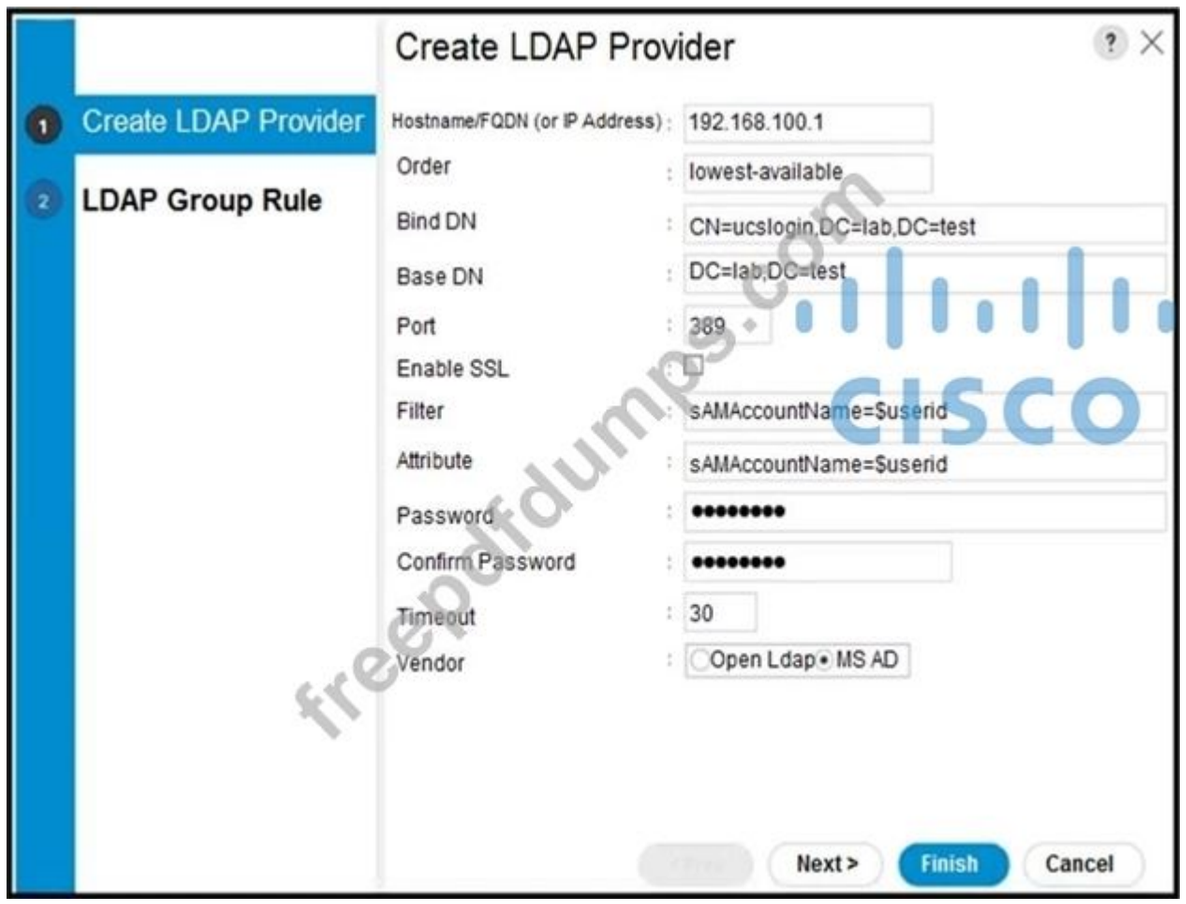
Explanation:

Cisco troubleshooting logic supports the drag-and-drop mapping shown in the answer key as the required fix.

In this question the symptoms point to DRAG, DROP, Drag, Not, and the defect is best handled by correcting the exact control-plane or consistency condition. Nexus platforms can show interfaces or peers as configured while still refusing to forward traffic if a vPC Type-1 parameter, VLAN allowance, MTU, HSRP version, EVPN route, or routing attribute is wrong. Cisco methodology is to avoid broad resets unless the state machine is stuck; instead, correct the mismatched parameter and verify that the resulting operational state becomes stable. The other choices do not remove the root cause, or they modify a setting that is not used by the failing protocol exchange. After the change, the engineer should review the peer status, route or MAC table, and counters for drops or inconsistency messages. That sequence proves that the network fabric is fixed, not merely restarted.



NEW QUESTION: 98



Refer to the exhibit. A network engineer configures an authentication domain through an LDAP provider on the Cisco UCS Manager for users from different companies to log into their respective organizations created in the UCS Manager. The engineer tests the configuration and notices that any user has login access to any organization in the UCS Manager. Which action should be taken to resolve the issue?

A. Configure the Filter field with sAMAccountName=$company

B. Configure the Attribute field with the company
C. Configure the Attribute field with sAMAccountName=$company
D. Configure the Filter field with the company
Answer: A (LEAVE A REPLY)
Configure the Filter field with sAMAccountName=$company is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS, UCS Manager, LDAP must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 99
An engineer must place a Cisco UCS B-Series Server in a single server pool in Cisco UCS Manager. The engineer creates a qualification policy, but the server is still seen in multiple pools. Which two actions resolve the issue? (Choose two.)
A. Select the Server Pool Policy Qualification from the qualification drop-down menu in the Server Pool Policy
B. Select the Server Pool Policy from the qualification drop-down menu in the Server Pool Policy Qualification
C. Set the operating system qualifier inside the Server Pool Policy Qualification
D. Set the number of vNICs qualifier inside the Server Pool Policy.
E. Set the storage capacity qualifier inside the Server Pool Policy Qualification.
Answer: A,C (LEAVE A REPLY)
the selected actions is the appropriate UCS remediation because the symptom maps to a specific managed object rather than a generic server failure. Cisco UCS abstracts hardware through service profiles and policies; therefore, issues involving UCS, UCS Manager must be corrected where UCS Manager programs the adapter, boot target, firmware, management certificate, pool qualification, or fabric interconnect state. The selected answer restores that programming path. The other options may appear plausible, but they do not correct the object that UCS uses to derive operational state. For example, boot failures require the correct vHBA/iSCSI target and LUN policy, discovery issues require the proper physical and management path, and firmware failures require the documented recovery action for the failed FSM stage. The correct validation is to inspect the associated fault, confirm inventory acknowledgment, verify the policy under the service profile or equipment tree, and then recheck boot or connectivity behavior after the FSM completes.

NEW QUESTION: 100
An engineer is troubleshooting a failed DCBX exchange between a server and a Cisco Nexus switch. Which action allows DCBX to successfully negotiate?
A. Enable ETS
B. Enable PFC.
C. Enable Cisco Discovery Protocol.
D. Enable LLDP.
Answer: D (LEAVE A REPLY)
The answer is Enable LLDP because Cisco Nexus and ACI forwarding depends on exact agreement between the devices participating in the feature. The scenario references DCBX, LLDP, Cisco Nexus; those technologies fail in predictable ways when required parameters do not match or when the required control- plane advertisement is absent. In DCIT troubleshooting, the engineer should identify the failed dependency, correct that dependency, and then verify the operational table that proves the fix. For example, vPC and EVPN checks focus on consistency, VNI/VRF bindings, peer-gateway behavior, and host-route advertisement; routing checks focus on neighbor state, MTU, timers, authentication, next-hop, and route preference. The selected answer addresses the dependency that blocks forwarding. The distractors are plausible because

they touch related features, but they do not resolve the specific failure condition. Post- change validation should include protocol state, learned endpoint or route entries, and a traffic test across the affected path.

NEW QUESTION: 101
A Cisco ACI fabric consists of three tenants User 1 must have permission to manage only the PROD tenant.
These configurations have already been completed *The security domain IbNANI has been created.
*User1 has been created with the " write " privilege level
*User1 has access to all leaf nodes
The configuration was deployed, but User1 still has access to all the other tenants. Which action resolves the issue?
A. Attach local user User1 to security domain all
B. Associate security domain TENANT to tenant PROD
C. Enable the restricted domain under security domain TFNANT
D. Add local user User1 to the RBAC node rule
Answer: B (LEAVE A REPLY)
Associate security domain TENANT to tenant PROD is correct because the failure is an operations-plane condition involving ACI, RBAC. In Cisco data center products, management functions depend on more than IP connectivity. AAA servers must return the correct attributes, RBAC must map users to the correct security domain or role, certificates must be trusted and valid for the access method, and firmware or registration workflows must satisfy documented prerequisites such as NTP and required ports. The selected answer corrects that dependency. The distractors are not root-cause fixes because they either target a different subsystem or change a setting that would not influence the observed login, registration, warning, or fault.
After the change, validation should include a successful login or registration test, review of the audit/fault record, and confirmation that the expected administrative scope is enforced. That approach matches Cisco operational troubleshooting for DCIT environments.

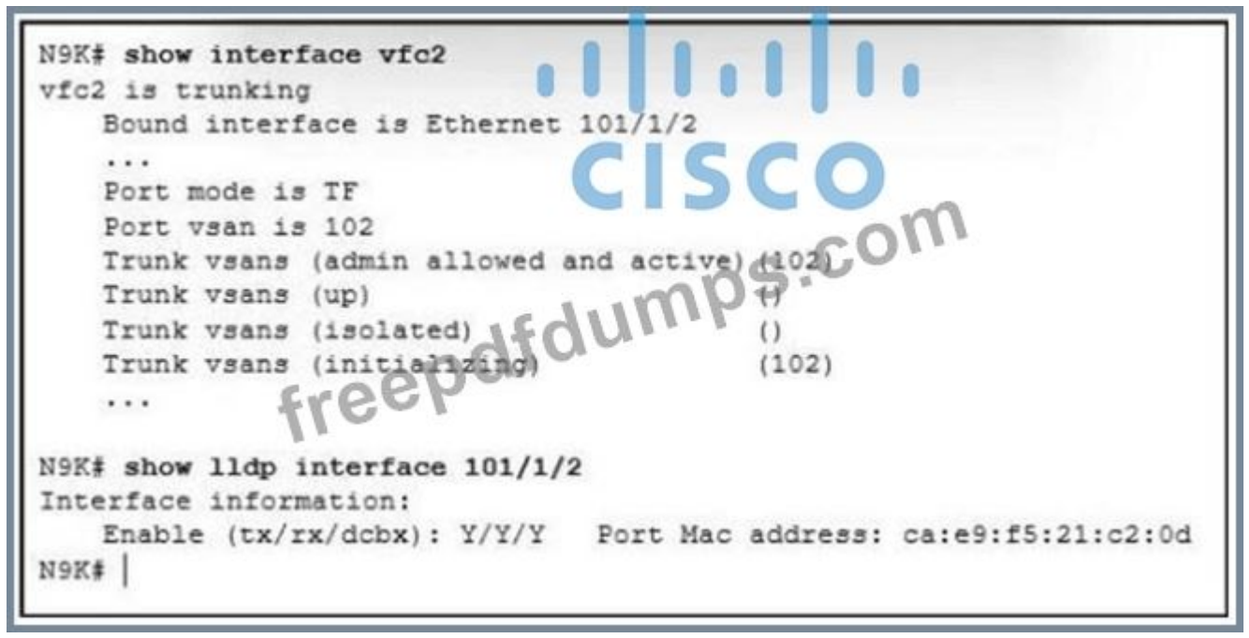
NEW QUESTION: 102
Refer to the exhibit.

```
ACME-5K-A(config-vsan-db) # sh int fc2/16

fc2/16 is down (Inactive)
     Port description is UplinkTo_MDS-A_1/6
     Hardware is Fibre Channel, SFP is short wave laser
w/o OFC (SN)
     Port WWN is 20:50:00:2a:6a:98:bc:80
     Admin port mode is E, trunk mode is auto
     snmp link state traps are enabled
     Port vsan is 1
     Receive data field Size is 2112
     Beacon is turned off
```

The connection between a Cisco Nexus 5548UP switch and a Cisco MDS switch fails to initialize. What is the cause of the issue?
A. VSAN 1 is suspended.
B. The SFP is unsupported.
C. Trunk mode must be activated.
D. The interface is in an incorrect mode.
Answer: A (LEAVE A REPLY)

The selected resolution is VSAN 1 is suspended because the failure is in the Fibre Channel/FCoE control path around MDS, VSAN, Cisco Nexus. Cisco MDS and Nexus platforms separate configuration from operational state: a VSAN, zone, vFC binding, device alias, or port-security entry can exist in configuration but still fail if it is not active, correctly merged, or allowed on the link. The correct option addresses the fabric condition that prevents communication. The incorrect options are technically adjacent but would not repair the specific dependency; for example, changing unrelated databases or resetting ports without correcting policy leaves the same failure to recur. Cisco SAN troubleshooting therefore starts with port role and VSAN checks, then confirms fabric services such as fcdomain, FSPF, zoning, fabric binding, and name-server information. The expected validation is that the port becomes operational, the initiator and target appear in the appropriate databases, and permitted zone members can communicate.

NEW QUESTION: 103
Refer to the exhibit.



The FCoE traffic fails to traverse the vfc2 interface. The VSAN 102 is configured for vfc2. Which action resolves the issue?
A. Enable LLDP on the interface vfc2
B. Activate DCBX on the N9K switch
C. Activate DCBX on the interface e101/1/2
D. Enable LLDP on the neighbor switch
Answer: D (LEAVE A REPLY)
Enable LLDP on the neighbor switch is the correct fix under Cisco SAN troubleshooting practice. The issue described involves VSAN, FCoE, DCBX, LLDP, where the operating state depends on the correct combination of port type, VSAN, fabric service, and access-control database. MDS and Nexus SAN features do not infer missing policy: if the active zoneset, fabric-binding database, fcdomain, NPIV setting, or FCoE
/LLDP negotiation is wrong, the link may come up physically but the initiator will not reach the target. The selected answer corrects the missing or mismatched element. The remaining choices either act at the wrong layer, change a non-causal parameter, or provide only a temporary reset. After applying the fix, a proper Cisco validation path is to review show interface, show flogi database, show fcns database, show zoneset active, and any isolation or merge-failure logs. That confirms the storage network is operationally consistent.

NEW QUESTION: 104

```
Nexus# show running-config | section role

role feature-group name Group1
  feature radius
role name User1
  rule 4 deny read-write feature-group Group1
  rule 3 permit read
  rule 2 deny read-write
  rule 1 deny command clear users

Nexus(config)# no role feature-group name Group1
ERROR: Feature group is in use. Can't remove the feature group
```


Refer to the exhibit.

An engineer must delete the feature-group role on the Cisco Nexus 9000 Series Switch but the CLI rejects the command Which command set resolves the issue?

A. rote name User1
rule 4 permit read-write feature-group Group1

B. role name User1 no rule 4

C. role name User
no rule 1

D. role name User1
rule1 permit read-write feature-group Group1

Answer: B (LEAVE A REPLY)

The correct remediation is role name User1 no rule 4. In Cisco data center troubleshooting, the first priority is to isolate whether the failure is caused by the underlay, overlay control plane, first-hop gateway behavior, or a consistency parameter. This item is centered on Cisco Nexus, Nexus 9000, Cisco Nexus 9000, so the selected action targets the condition that prevents normal forwarding rather than masking the symptom. Cisco Nexus and ACI guidance treats vPC, VXLAN EVPN, OTV, OSPF, BGP, HSRP, and LACP issues as state- dependent technologies: a neighbor, peer, VLAN, VNI, multicast group, timer, MTU, or policy mismatch can leave the protocol partially operational while traffic is still dropped. The rejected alternatives either change unrelated attributes, introduce a new inconsistency, or affect only a secondary behavior. The operational check after applying the fix should be to confirm adjacency or peer state, validate the relevant route/MAC
/endpoint table, and test traffic in the affected VLAN or VRF. This aligns with Cisco DCIT network troubleshooting methodology for isolating control-plane state before changing data-plane policy.

NEW QUESTION: 105

A Fibre Channel interface on a Cisco Nexus 5000 Series Switch receives bit errors, and the switch disables the interface. A temporary workaround must be implemented before the root cause is identified. Which action does an engineer take to prevent this issue from reoccurring?

A. Verify that the SFPs are supported.

B. Change the SFP to operate at 4 Gbps instead of 2 Gbps.

C. Run the shutdown and then no shutdown command on the interface.

D. Run the switchport ignore bit-errors command on the interface.

Answer: (SHOW ANSWER)

Run the switchport ignore bit-errors command on the interface is the required SAN-side correction. In Cisco storage fabrics, symptoms such as isolated ports, missing targets, failed zone merges, vFC down state, or inaccessible LUNs are rarely solved by changing a random endpoint setting. The engineer must validate the FC control-plane dependency associated with Cisco Nexus: VSAN assignment, trunk allowance, FSPF parameters, fcdomain uniqueness, NPIV support, NPV uplink behavior, DCBX/LLDP negotiation, and active zoning. The selected answer is the one that restores that dependency. Other choices may be valid operational commands in a different failure, but they do not address the precise point where fabric membership or access control is broken. Cisco guidance is to verify the active database and the operational database separately because a configured object is not necessarily active in the fabric. Post-remediation checks should include interface state, VSAN status, FLOGI/PLOGI, zoneset membership, and target visibility from the initiator.