TESTPASSPORT

QUESTIONS D'ENTRAÎNEMENT

UN MEILLEUR ACCOMPAGNEMENT

https://www.testpassport.fr

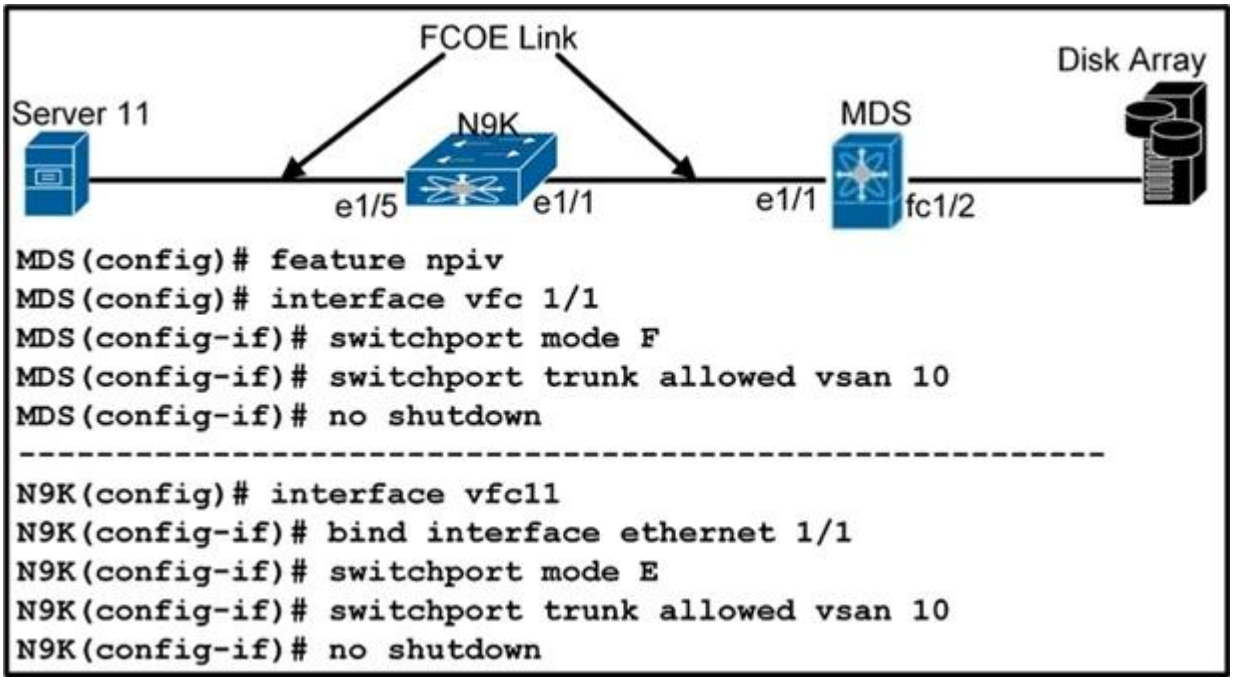
Mises à jour gratuites pendant un an

Exam : **300-615**

Title : Troubleshooting Cisco Data Center Infrastructure (DCIT)

Version : DEMO

1.Refer to the exhibit.



A network engineer is configuring the FCoE N_Port virtualization storage area network. After the initial implementation, server 11 fails to connect to the disk array.
Which action resolves the issue?
A. On MDS interface vfc 1/1, change switchport mode configuration to VF
B. On N9K interface vfc11, change switchport mode configuration to NP
C. On N9K interface vfc11 and MDS interface vfc 1/1, change switchport mode configuration to F
D. On N9K interface vfc11 and MDS interface vfc 1/1, change switchport mode configuration to E
Answer: D
Explanation:
On N9K interface vfc11 and MDS interface vfc 1/1, change switchport mode configuration to E 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 MDS, FCoE: 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.

2.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

Explanation:

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.

3.A Cisco UCS C125 M5 server is integrated with Cisco UCS Manager using direct connect mode. The adapter for the server is reported as "inoperable" inside Cisco UCS Manager.
Which action resolves the issue?

A. Match the adapter firmware to the Cisco UCS Manager version.
B. Connect the network cable to port 6 of the vNIC adapter.
C. Use a port expander with the vNIC adapter.
D. Reseat the adapter on the motherboard of the server.

Answer: D

Explanation:

The selected answer, Reseat the adapter on the motherboard of the server, 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, firmware, vNIC; 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.

4.A host connected to port Eth0/1 on the Cisco Nexus Series Switch received this error
*Mar 6 12 57 42 882 %PM-4-ERR DISABLE psecure-violation error detected on Eth0/1, putting Eth0/1 in err-disable state-Mar 6 12 57 42 882 %PORT_SECURITY-2-PSECURE_VIOLATION Security violation occurred, caused by MAC address a526 cc69 3503 on port EthernetO'1.
The server administrator concluded that the issue was caused by plugging the host in the wrong switch port and fixed the problem.
Which action must be taken to recover the port from the error?
A. Install ENHANCED_LAYER2_PKG license
B. Enable NET\V0RK_SERV1CES_PKG license.
C. Shut and no shut the interface Eth0/I.
D. Change the interface Eth0/1 mode to access
Answer: C
Explanation:
Shut and no shut the interface Eth0/I is correct because the failure is an operations-plane condition involving 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.

5.A request to activate the port security database is rejected.
Which action do you perform to investigate the cause of the issue?
A. Enable the auto-learning feature.
B. Use the force option to identify rejected devices.
C. Find conflicting entries between the active and configuration databases.
D. Verify that devices are fully attached to the active database.
Answer: B
Explanation:
Use the force option to identify rejected devices 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 port security: 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.