

300-615^{Q&As}

Troubleshooting Cisco Data Center Infrastructure (DCIT)

Pass Cisco 300-615 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.leads4pass.com/300-615.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Cisco
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



QUESTION 1

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

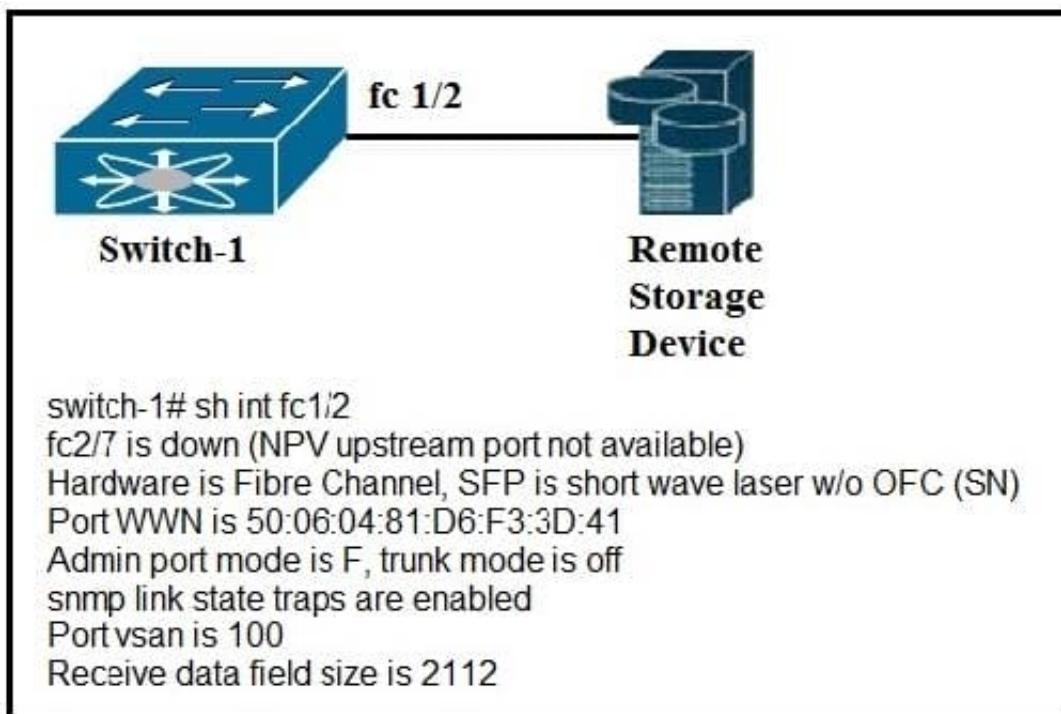
A network engineer needs to capture traffic from the VMs that utilize the IOM host interface Eth1/1/23 of a Cisco UCS B-Series chassis. A traffic analyzer is used to get traffic captured from the Eth1/4 interface of the subordinate fabric interconnect. The network engineer notices that traffic is not 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 1/2 of the primary fabric interconnect
- C. Span the traffic from the Eth 1/4 of the subordinate fabric interconnect
- D. Span the traffic from the Eth 1/4 of the primary fabric interconnect

Correct Answer: B

QUESTION 2

Refer to the exhibit.



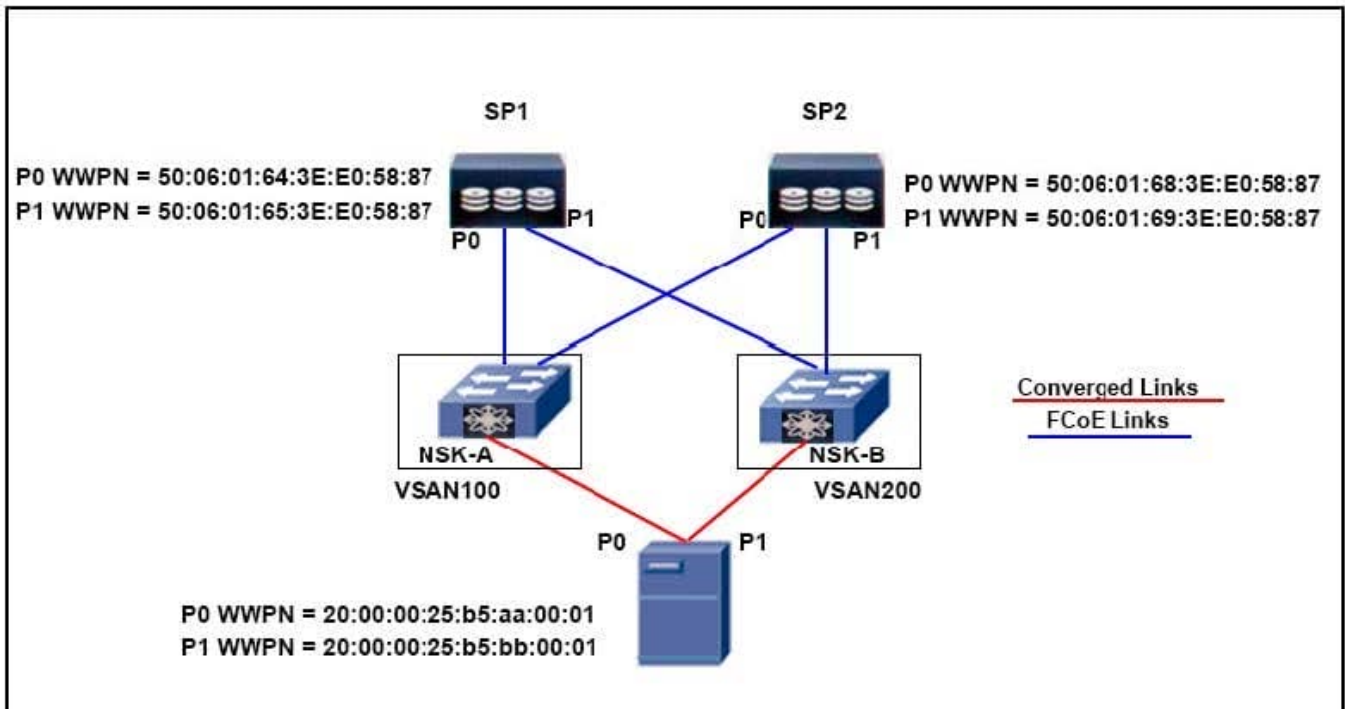
A remote device connected to fc 1/2 fails to come online. Which do you configure to resolve the issue?

- A. remote and local ports to be in the correct VSAN
- B. local switch for NPV
- C. remote device for NPIV
- D. port on remote device as an f-port-channel

Correct Answer: A

QUESTION 3

DRAG DROP Refer to the exhibit.



```

!!!! VSAN100-ZONING
zone name host1_hba0- SP1 vsan 100
  member pwn 20:00:00:25:b5:aa:00:01

zone name host1_hba0_SP2 vsan 100
  member pwn 50:06:01:68:3E:E0:E0:58:87

!!!! VSAN200-ZONING
zone name host1_hba1- SP1 vsan 200
  member pwn 50:06:01:65:3E:E0:58:87

zone name host1_hba1_SP2 vsan 200
  member pwn 20:00:00:25:b5:bb:00:01
    
```

Boot Order				
Name	vNIC/v...	Type	WWN	LUN N...
SAN Primary	hba0	Primary		
San Target Primary		Primary	50:06:01:64:3E:E0:58:87	0
SAN Target Secondary		Secondary	50:06:01:64:3E:E0:58:87	0
SAN Secondary	hba1	Secondary		
San Target Primary		Primary	50:06:01:68:3E:E0:58:87	0
SAN Target Secondary		Secondary	50:06:01:69:3E:E0:58:87	0

Boot from SAN fails. The host fails to detect the LUNs. You must resolve the issue. Drag and drop the WWPNs on the left to the correct zones on the right.

Select and Place:

50:06:01:69:3E:E0:58:87	host1_hb0_SP1 vsan 100
20:00:00:25:b5:aa:00:01	host1_hba1_SP1 vsan 200
50:06:01:64:3E:E0:58:87	host1_hba0_SP2 vsan 100
20:00:00:25:b5:bb:00:01	host1_hba1_SP2 vsan 200

Correct Answer:

	50:06:01:64:3E:E0:58:87
	20:00:00:25:b5:aa:00:01
	20:00:00:25:b5:bb:00:01
	50:06:01:69:3E:E0:58:87

QUESTION 4

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 prevents 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.

Correct Answer: D

QUESTION 5

Refer to the exhibit.

Schedule Node Upgrade

Group Type: Switch vPod

Upgrade Group Name: DC_Lab

Target Firmware Version: aci-n900-dk9.14.2.2a.b

Ignore Compatibility
 Check:

Graceful Maintenance:

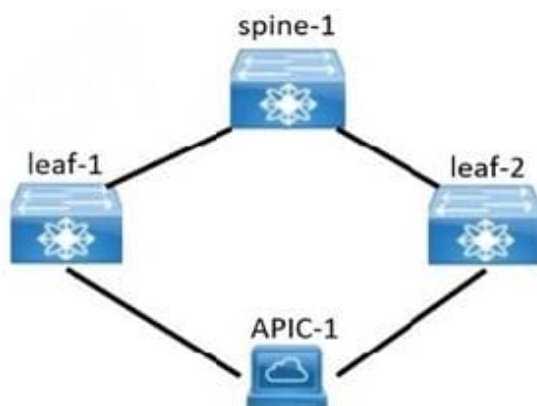
Run Mode: Do not pause on failure and do not wait on cluter health Pause upon upgrade failure

Upgrade Start Time: Now Schedule For Later

Node Selection: Range Manual

All Nodes

Selected	ID	Name	Role	Model	Current Firmware	Target Firmware	Status
<input checked="" type="checkbox"/>	Pod1/101	leaf-1	leaf	N9K-C9396PX	4.1(1k)		Not Scheduled
<input checked="" type="checkbox"/>	Pod1/101	leaf-2	leaf	N9K-C9396PX	4.1(1k)		Not Scheduled
<input checked="" type="checkbox"/>	Pod1/201	spine-1	spine	N9K-C9508	4.1(1k)		Not Scheduled



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

Correct Answer: BD

Reference: https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ts/guide/UCSTroubleshooting/UCSTroubleshooting_chapter_0100.html

QUESTION 6

A Cisco Nexus Series interface is 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.

Correct Answer: B

QUESTION 7

When the engineer runs the command, this error is received:

```
opsengineer@wkst1:/home/auto/bash_scripts$ curl -s -b cookie_file_39916907.txt -X GET -k
192.15.132.101/api/node/class/Tenant.json {"totalCount": "1", "imdata":[{"error":{"attributes":{"code": "400", "text":
"Requestfailed, (output omitted)}}}]}
```

Which action resolves the issue?

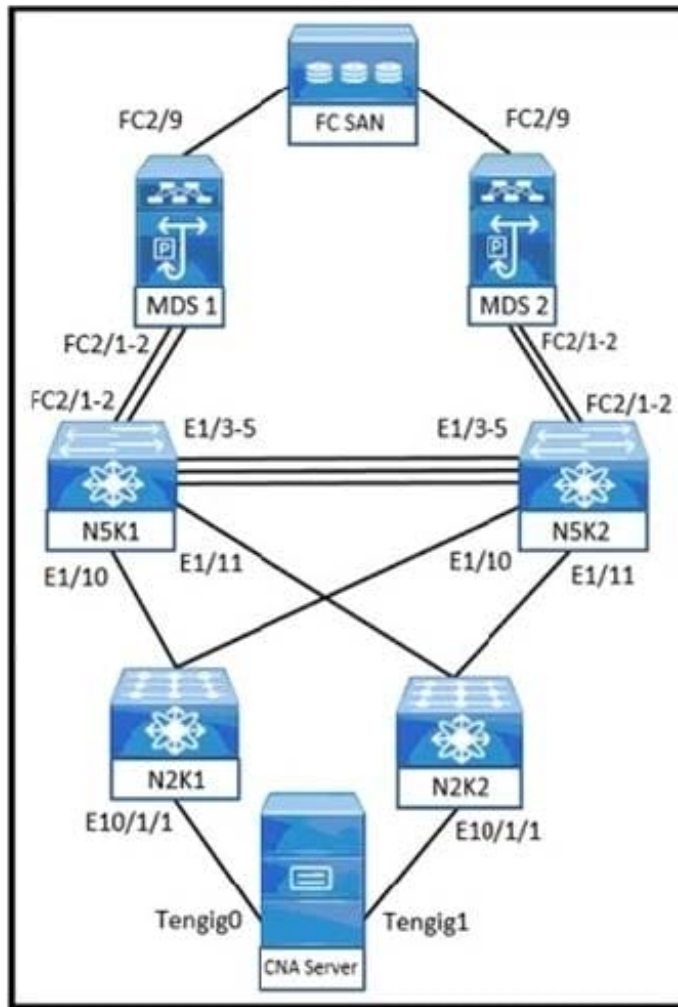
- A. Regenerate the API token object
- B. Modify the URI to 192.15.132.101/api/node/class/fvTenant.json
- C. Add the -c class Tenant flag to the cURL command
- D. Change the HTTP verb to POST

Correct Answer: B

Reference: <https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2019/pdf/DEVNET-2000.pdf>

QUESTION 8

Refer to the exhibit.



```
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
```

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

Correct Answer: D

Reference: https://www.cisco.com/c/en/us/td/docs/switches/datacenter/nexus5000/sw/troubleshooting/guide/N5K_Troubleshooting_Guide/n5K_ts_fcoe.html

QUESTION 9

Which control plane is used according to this output?

```
N7K-A# show l2route evpn mac-ip all
Topology ID Mac Address Prod Host IP Next Hop(s)
-----
200 2010.0000.0010 HMM 209.165.202.139 N/A
200 2425.1245.7411 BGP 209.165.202.140 10.1.1.56
```

- A. flood-and-learn MAC address learning
- B. BGP EVPN
- C. flood-and-learn IP address learning
- D. VXLAN OAM

Correct Answer: B

QUESTION 10

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

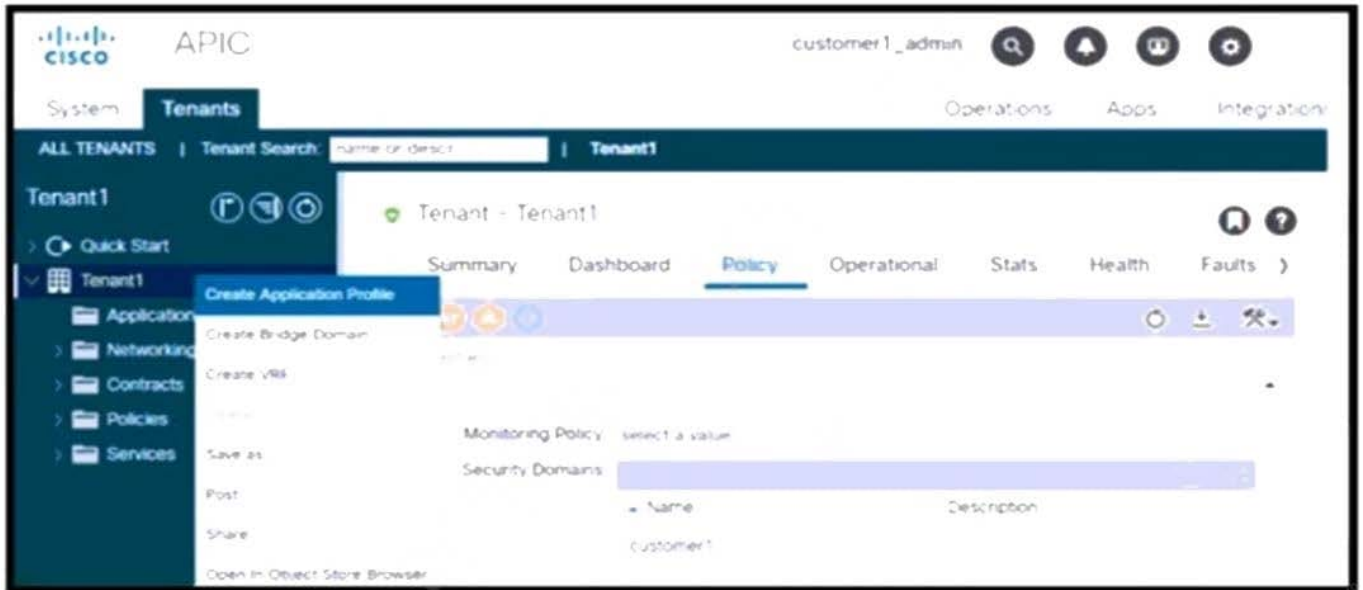
switch port. The server fails to send the FC traffic to the fabric. Which action resolves the issue?

- 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.

Correct Answer: B

QUESTION 11

Refer to the exhibit.



The Cisco ACI fabric is configured with RADIUS realm as the default authentication method. The customer1_admin user is configured with the read-all role but still can create new objects in Tenant1. Which Cisco AV pair must be used to resolve the issue?

- A. shell:domains=customer1/read-all/, customer1//read-all
- B. shell:domains=customer1/access-admin/
- C. shell:domains=customer1//admin
- D. shell:domains=customer1/tenant-admin/

Correct Answer: A

QUESTION 12

Refer to the exhibit.

```
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
```

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. 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

Correct Answer: B

QUESTION 13

Refer to the exhibit.

```
SW-1
Nexus1# show hsrp
Vlan13 - Group 13 (HSRP-V1) (IPv4)
  Local state is Active, priority 90 (Cfged 90), may preempt
  Forwarding threshold(for vPC), lower: 1 upper: 90
  Hellotime 3 sec, holdtime 10 sec
Authentication text "cisco123"
Virtual mac address is 0000.0c07.ab0d (Default MAC)
10 state changes, last state change never
IP redundancy name is hsrp-Vlan13-13 (default)

SW-2
interface vlan13
no ip redirects
ip address 10.82.82.2/24
hsrp 13
no preempt
priority 80
ip 10.82.82.1
no shutdown
```

A recent configuration change removes the HSRP adjacency between the SW-1 and SW-2 Cisco Nexus switches. The change causes the servers on this subnet to lose Internet access. Which action restores the connectivity of all servers on VLAN 13?

- A. Set the HSRP password on SW-2.
- B. Set the HSRP priority to 70 on SW-1.
- C. Disable HSRP IP redirects on SW-1.
- D. Activate HSRP preempt on SW-2.

Correct Answer: A

QUESTION 14

Refer to the exhibit.


```
switch# show scheduler logfile
Job Name : back-cfg Job Status: Failed (1)
Schedule Name : daily User Name : operator
Completion time: Fri Jan 1 1:00:01 2019
----- Job Output -----
`cli var name timestamp 2019-01-01-01.00.00`
`copy running-config bootflash:/${HOSTNAME}-cfg.${timestamp}`
`copy bootflash:/switch-cfg.2019-01-01-01.00.00 tftp://10.10.10.5/ vrf management `
copy: cannot access file '/bootflash/switch-cfg.2019-01-01-01.00.00'
=====
Job Name : back-cfg Job Status: Success (0)
Schedule Name : daily User Name : admin
Completion time: Fri Jan 2 1:00:01 2019
----- Job Output -----
`cli var name timestamp 2019-01-02-01.00.00`
`copy running-config bootflash:/switch-cfg.2019-01-02-01.00.00`
`copy bootflash:/switch-cfg.2019--01-02-01.00.00 tftp://10.10.10.5/ vrf management
`
Connection to Server Established.
[ ] 0.50KBTrying to connect to tftp server.....
[##### ] 24.50KB
TFTP put operation was successful
=====
```

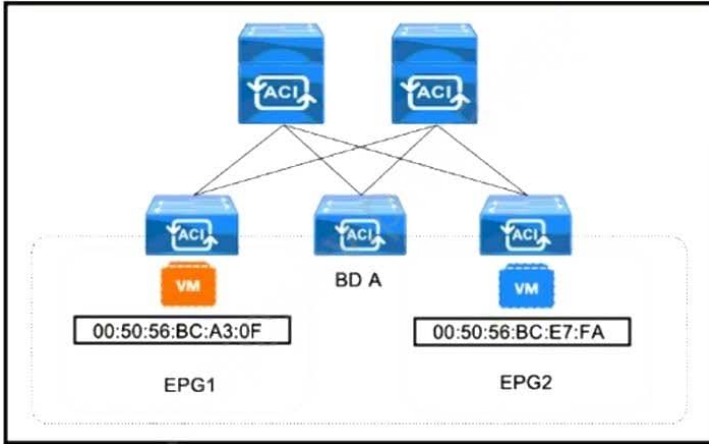
The scheduler job fails to run. Which action resolves the issue?

- A. Change the file name.
- B. Configure the authentication credentials.
- C. Configure the authentication credentials.
- D. Change the TFTP server address.

Correct Answer: D

QUESTION 15

Refer to the exhibit.



```

LEAF101# show system internal epm endpoint mac 00:50:56:BC:A3:0F LEAF103# show system internal epm endpoint mac 00:50:56:BC:E7:FA
MAC : 0050.56bc.a30f ::: Num IPs : 0                               MAC : 0050.56bc.e7fa ::: Num IPs : 0
Vlan id : 63 ::: Vlan vnid : 12308 ::: VRF name : C1:C1           Vlan id : 62 ::: Vlan vnid : 12340 ::: VRF name : C1:C1
BD vnid : 16514960 ::: VRF vnid : 3112963                         BD vnid : 16678783 ::: VRF vnid : 3112963
Phy If : 0x16000005 ::: Tunnel If : 0                             Phy If : 0x16000005 ::: Tunnel If : 0
Interface : port-channel6                                         Interface : port-channel6
Flags : 0x80004805 ::: sclass : 32783 ::: Ref count : 4          Flags : 0x80004805 ::: sclass : 16395 ::: Ref count : 4
EP Create Timestamp : 09/10/2021 03:53:12.422438                 EP Create Timestamp : 09/10/2021 03:51:14.222070
EP Update Timestamp : 09/10/2021 03:55:34.206922                 EP Update Timestamp : 09/10/2021 03:55:34.206823
EP Flags : local|vPC|MAC|sclass|timer|                             EP Flags : local|vPC|MAC|sclass|timer|

LEAF101# show zoning-rule scope 3112963 | grep 16395
| 4249 | 16395 | 0 | implicit | uni-dir | enabled | 3112963 | | deny_log | grp_src_any_any_deny(18) |
| 4250 | 0 | 16395 | implicit | uni-dir | enabled | 3112963 | | deny_log | grp_any_dest_any_deny(19) |
| 4254 | 16395 | 32783 | default | bi-dir | enabled | 3112963 | all_traffic | permit | src_dst_any(9) |
| 4255 | 32783 | 16395 | default | uni-dir-ignore | enabled | 3112963 | all_traffic | permit | src_dst_any(9) |
    
```

The connectivity fails between endpoints from different EPGs that use the same bridge domain. All endpoints are on the same subnet configured under the shared bridge domain. Which action resolves the issue?

- A. Enable unicast routing on the bridge domain.
- B. Configure a contract between the EPGs.
- C. Set the preferred group option on the VRF.
- D. Attach the same bridge domain to the EPGs.

Correct Answer: B