350-601^{Q&As}

Implementing and Operating Cisco Data Center Core Technologies (DCCOR)

Pass Cisco 350-601 Exam with 100% Guarantee

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

https://www.geekcert.com/350-601.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

Due to new regulatory requirements from a third party, organization ABC must enable two-factor authentication for the Cisco UCS environment. The requirement is also to provide redundancy if the authentication server goes offline. Which three authentication components must be enabled to meet this requirement? (Choose three.)

A. provider group

B. authentication domain

C. TACACS+

D. LDAP

E. local

Correct Answer: ABC

https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/ucs-manager/GUI-User-Guides/Admin-Management/3-2/b_Cisco_UCS_Admin_Mgmt_Guide_3_2/ b_Cisco_UCS_Admin_Mgmt_Guide_3_2_chapter_0101.html#concept_13D7B9B6F03E498A8E425BCF6C28CE59

Two-Factor Authentication

Cisco UCS Manager uses two-factor authentication for remote user logins, which adds a level of security to account logins. Two-factor authentication login requires a username, a token, and a password combination in the password field. You can provide a PIN, a certificate, or a token.

Two-factor authentication uses authentication applications that maintain token servers to generate one-time tokens for users during the login process and store passwords in the AAA server. Requests are sent to the token server to retrieve a vendor-specific attribute. Cisco UCS Manager expects the token server to integrate with the AAA server, therefore it forwards the request to the AAA server. The password and token are validated at the same time by the AAA server. Users must enter the token and password sequence in the same order as it is configured in the AAA server.

Two-factor authentication is supported by associating RADIUS or TACACS+ provider groups with designated authentication domains and enabling two-factor authentication for those domains. Two-factor authentication does not support IPM and is not supported when the authentication realm is set to LDAP, local, or none.

QUESTION 2

DRAG DROP

An engineer must configure HSPR protocol on two Cisco Nexus 9000 Series Switches running a virtual port channel. In addition, the HSRP implementation must meet these requirements:

It must allow more than 500 groups.

switch1 must act as the primary switch.

Both switches must use a user-defined hardware address.

Drag and drop the commands from the right to complete a configuration of the HSRP on the left. The commands are used more than once. Not all commands are used.

Select and Place:

Answer Area

3 / 7

```
! switch1

interface vlan300
ip 209.165.200.226/27
hsrp 300

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘

ip 209.165.200.225

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘


! switch2

interface vlan300
ip 209.165.200.227/27
hsrp 300

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘

ip 209.165.200.225

┌─────────────────────────────┐
│                             │
└─────────────────────────────┘
```

┌──────────────────────────────────┐
│ mac-address 6000.6000.6000   │
└──────────────────────────────────┘

┌──────────────────────────────────┐
│   hsrp version 1   │
└──────────────────────────────────┘

┌──────────────────────────────────┐
│   priority 255   │
└──────────────────────────────────┘

┌──────────────────────────────────┐
│   hsrp use-bia   │
└──────────────────────────────────┘

┌──────────────────────────────────┐
│   priority 100   │
└──────────────────────────────────┘

┌──────────────────────────────────┐
│   hsrp version 2   │
└──────────────────────────────────┘

Correct Answer:

Answer Area

```
! switch1

interface vlan300
ip 209.165.200.226/27
hsrp 300
        hsrp version 2

        priority 255
ip 209.165.200.225
  mac-address 6000.6000.6000


! switch2

interface vlan300
ip 209.165.200.227/27
hsrp 300
        hsrp version 2

        priority 100
ip 209.165.200.225
  mac-address 6000.6000.6000
```

```
mac-address 6000.6000.6000

hsrp version 1

priority 255

hsrp use-bia

priority 100

hsrp version 2
```

QUESTION 3

DRAG DROP

Drag and drop the keywords onto the URL request to collect all the subnets configured under tenant Production using a REST API. Not all options are used.

Select and Place:

```
https://{{apic_ip}}/api/ [            ] /uni/tn-Production.json?
[                    ] = [                    ] & [                    ]
= fvSubnet
```

target-subtree-class	query-target-filter
children	query-target
mo	class
subtree	

Correct Answer:

```
https://{{apic_ip}}/api/ [ mo            ] /uni/tn-Production.json?
[ query-target ] = [ target-subtree-class ] & [ subtree ]
= fvSubnet
```

	query-target-filter
children	
	class

QUESTION 4

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

A. Immediate Action

B. User Notification

C. User Acknowledge

D. Delayed Action

E. No Action

Correct Answer: CE

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

QUESTION 5

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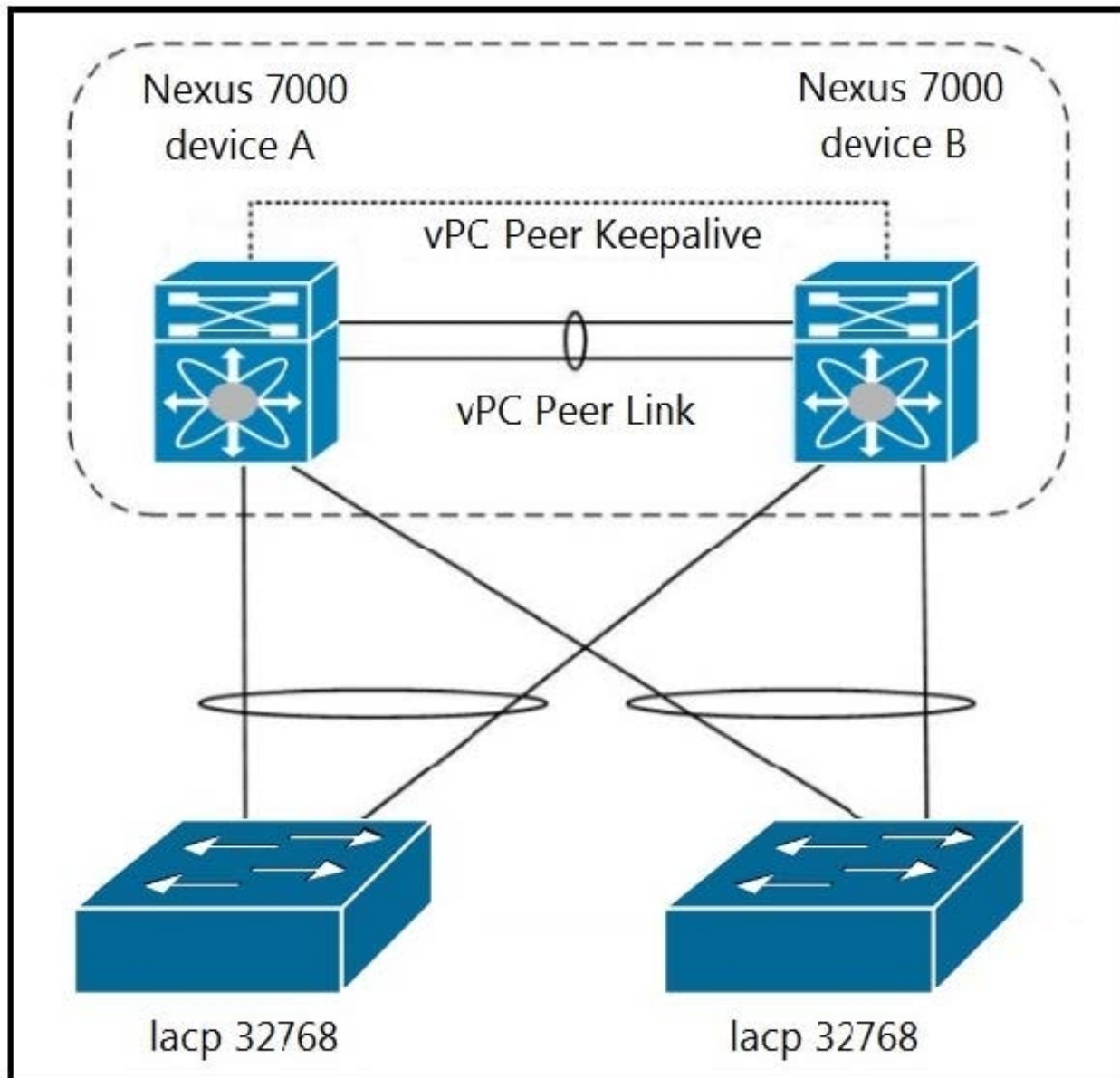
Which configuration ensure that the cisco Nexus 7000 series switches are the primary devices for LACP?

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

B. N7K_A(config-vpc-domain)# system-priority 32768 N7K_B(config-vpc-domain)# system-priority 32768

C. N7K_A(config-vpc-domain)# system-priority 100 N7K_B(config-vpc-domain)# system-priority 200

D. N7K_A(config-vpc-domain)# system-priority 4000 N7K_B(config-vpc-domain)# system-priority 4000

Correct Answer: D

A. Incorrect - role priority influences vPC primary/secondary election.

B. Incorrect - System priorities match however uses default values of lacp, would not ensure n7k\'s are primary devices.

C. Incorrect - vPC System priorities do not match between the peers, this config would result in vPC\\'s never coming up.

D. Correct - Defining a system priority of 4000 in vpc domain config ensures lacp priority for vPC\\'s would be 4000, the lower the number the more likely to become lacp master. What is the purpose and usage of the system priority command

under vpc configuration mode? The vpc quick config guide mentioned: "You should manually configure the vPC system priority when you are running Link Aggregation Control Protocol (LACP) to help ensure that the vPC peer devices are the

primary devices on LACP".

When you manually configure the system priority, ensure that you configure the same priority value on both vPC peer devices. If these values do not match, vPC will not come up.

350-601 PDF Dumps   350-601 Practice Test   350-601 Exam Questions