CCIE Data Center v3

Module 1# :Design V3

DEMO

1 of 32

Welcome to the Design Module

Please read all the available resources before starting the scenario by clicking 'Next item'

Q2 - List the recommended approaches to build a vPC peer-keepalive link in the descending order of preference, where preference 1 is most preferred and preference 3 is least preferred.

dedicated Layer 3 link or a port channel	Preference 1
vPC peer-keepalive link on top of vPC peer-link	Preference 2
mgmt0 interfaces	Preference 3
vPC peer-keepalive link routed over the Layer 3 infrastructure	

Answer

	dedicated Layer 3 link or a port channel
vPC peer-keepalive link on top of vPC peer-link	mgmt0 interfaces
	vPC peer-keepalive link routed over the Layer 3 infrastructure

Q3 – Which design changes must be implemented to meet customer requirements? *(Choose all that apply.)*

- Configure the vPC peer-gateway on both vPC switches.
- Configure the vPC primary switch with lower STP priority.
- Configure spanning-tree port type network on non-vPC p2p links.
- Implement spanning-tree pseudo-information for VLANs.
- Configure the vPC primary switch with higher STP priority.
- Configure the vPC peer-switch feature on both vPC switches.

Answer

- Configure the vPC peer-gateway on both vPC switches.
- Configure the vPC peer-switch feature on both vPC switches.

Q4-For each of the following configuration changes, indicate whether it fully addresses, partially addresses, or does not address the requirements.

Answer

Configuration Change	Does not address	Fully addresses	Partially addresses
Enable vPC ARP Sync on both DC1-N7K-1 and DC1-N7K-2 switches			●
Configure peer-router functionality in vPC domain			●
Configure orphan-port suspend on NAS-connected interfaces			●
Rely on default HSRP/VRRP operation for SVI in VLAN 220, with no additional vPC config	●		
Enable vPC peer-gateway on both DC1-N7K-1 and DC1-N7K-2 switches		●	
Increase peer-link bandwidth and monitor for congestion during failover events			●
Move NAS devices to a new VLAN and ensure only one SVI (on primary) is active at any time		●	

Q5-Choose the correct answer based on the customer project requirements.

Answer

- PIM SM

Q6- For each of these shared protocol capabilities, indicate which protocol offers more of an advantage over the other.

Answer

Protocol Capabilities	OSPF	BGP
Handling a large number of prefixes and AS domains		●
Traffic control between external sites or cloud regions	●	
Automatic neighbor discovery and adjacency formation		●
Path manipulation using attributes like Local Preference or MED		●
Convergence speed within a LAN or single broadcast domain	●	
Loop prevention using path history or route origin information		●
Support for route summarization at multiple hierarchy levels		●
Simplified topology analysis and route tracing through an LSDB	●	

Q7-Which configuration meets the requirements of the Xandar data center automation project?

- **configure terminal**
  feature scheduler
  scheduler job name cfg_backup_plan
  python bootflash:///scripts/cfg_backup.py
  exit
  scheduler schedule name cfg_backup_plan
  job name cfg_backup_plan
  time start now repeat 1:0:0
  end

  cfg_backup.py file:

  #!/bin/env python
  from cli import *
  from nxos import *
  import os
  import datetime

  fName = 'config_backup_' + str(datetime.date.today())
  res = cli("show run > bootflash:" + fName)

  msg = 'Configuration was backed up to ' + fName + ' on the bootflash'
  print msg

- **configure terminal**
  feature scheduler
  scheduler job name cfg_backup_plan
  python bootflash:///scripts/cfg_backup.py
  time start now repeat 24:0:0
  end

  cfg_backup.py file:

  #!/bin/env python
  from cli import *
  from nxos import *
  import os
  import datetime

  fName = 'config_backup_' + str(datetime.date.today())
  res = cli("show run > bootflash:" + fName)

  msg = 'Configuration was backed up to ' + fName + ' on the bootflash'
  py syslog(1, msg)

- **configure terminal**
  feature scheduler
  scheduler schedule name cfg_backup_plan
  python bootflash:///scripts/cfg_backup.py
  time start now repeat 1:0:0
  end

  cfg_backup.py file:

  #!/bin/env python
  from cli import *
  from nxos import *
  import os
  import datetime

  fName = 'config_backup_' + str(datetime.date.today())
  res = cli("show run > bootflash:" + fName)

  msg = 'Configuration was backed up to ' + fName + ' on the bootflash'
  print msg

Answer

- configure terminal
  feature scheduler
  scheduler job name cfg_backup_plan
  python bootflash:///scripts/cfg_backup.py
  exit
  scheduler schedule name cfg_backup_plan
  job name cfg_backup_plan
  time start now repeat 1:0:0
  end

  cfg_backup.py file:

  #!/bin/env python
  from cli import *
  from nxos import *
  import os
  import datetime

  fName = 'config_backup_' + str(datetime.date.today())
  res = cli("show run > bootflash:" + fName)

  msg = 'Configuration was backed up to ' + fName + ' on the bootflash'
  print msg

Q8-In the Xandar data center, CoPP can help with certain hardening requirements. Drag and drop the requirements that are supported by CoPP.

CoPP enforces limits on control-plane packet rates to prevent CPU overload.	Preference 1
CoPP policy can be customized, which allows administrators to set the permitted rate of traffic for different types of control plane traffic.	Preference 2
CoPP policies can be applied to both IPv4 and IPv6 control-plane traffic.	Preference 3
CoPP can increase the throughput of control plane traffic during peak periods.	
CoPP blocks all exception packets, such as a packet with IP options set, by default.	
Traffic going to mgmt0 gets restricted by CoPP.	
CoPP mitigates the effects of man-in-the-middle attacks.	
CoPP protects from malicious traffic transiting the switch.	
Dense CoPP policy is applied by default.	

Answer

	CoPP policy can be customized, which allows administrators to set the permitted rate of traffic for different types of control plane traffic.
	CoPP policies can be applied to both IPv4 and IPv6 control-plane traffic.
	CoPP enforces limits on control-plane packet rates to prevent CPU overload.
CoPP can increase the throughput of control plane traffic during peak periods.	
CoPP blocks all exception packets, such as a packet with IP options set, by default.	
Traffic going to mgmt0 gets restricted by CoPP.	
CoPP mitigates the effects of man-in-the-middle attacks.	
CoPP protects from malicious traffic transiting the switch.	
Dense CoPP policy is applied by default.	