HP

HPE6-A69 Exam

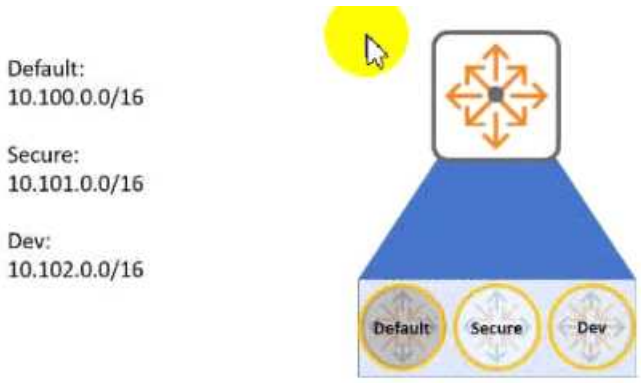
Aruba Certified Switching Expert Written

Questions & Answers
Demo

Version: 4.0

Question: 1

Refer to the exhibit.



Aruba CX 6300 switch has routes in three different VRFs as per the example above. The user needs to leak routes between VRF Secure and VRF Dev. and also between VRF default and VRF Dev
The customer Is not able to establish routing between directly connected networks 10.100.50.0/24 and 10.102.26.0/24 Which statement is true regarding the routing troubleshooting?

A. Multi-protocol BGP routing needs to be defined for route leaking
B. Route Distinguisher needs to be set to 1 for default VRF.
C. Route leaking is supported between non-default VRFs only
D. Route leaking between default and non-default VRFs is supported with Aruba CX 8400.

Answer: A

Explanation:

Question: 2

You have created an OSPF neighbor configuration with ArubaOS-CX 8320 VSX and a third-party switch The OSPF peering falls. In the event togs you see the following entries.
2020-10-28:03:14 20.371489|hpe-routlng|LOG_WARN|AMM|1/5jOSPFV2|OSPFV2iOSPF 268698624 Packet received with unexpected authentication type 2020-10-28:03:14.20.371503|hpe-routing|LOG_WARN|AMM|1/5|OSPFV2|OSPFV2|Expected authentication type = 0
Which statement is true about the above events?

A. The ArubaOS-CX switch requires plain-text authentication with OSPF.
B. The third-party switch should be configured with MD5 authentication
C. The ArubaOS-CX switch does not expect authentication with OSPF.
D. The third-party switch should be configured with key chain authentication

Answer: D

Explanation:

Question: 3

When applying me following access-list to an ArubaOS-CX 6300 switch:

```
10 permit tcp any RADIUS-SERVERS group WEB-PORTS log
20 permit udp any any group DHCP-PORTS log
30 permit udp any any group DNS-PORTS log
40 permit icmp any RADIUS-SERVERS log
50 deny tcp any MANAGEMENT-SERVERS log
60 deny icmp any MANAGEMENT-SERVERS count
70 permit udp any MANAGEMENT-SERVERS eq 162 count
80 permit udp any MANAGEMENT-SERVERS eq 69 log
```

How does this ACL behave on the selected switch? (Select two.)

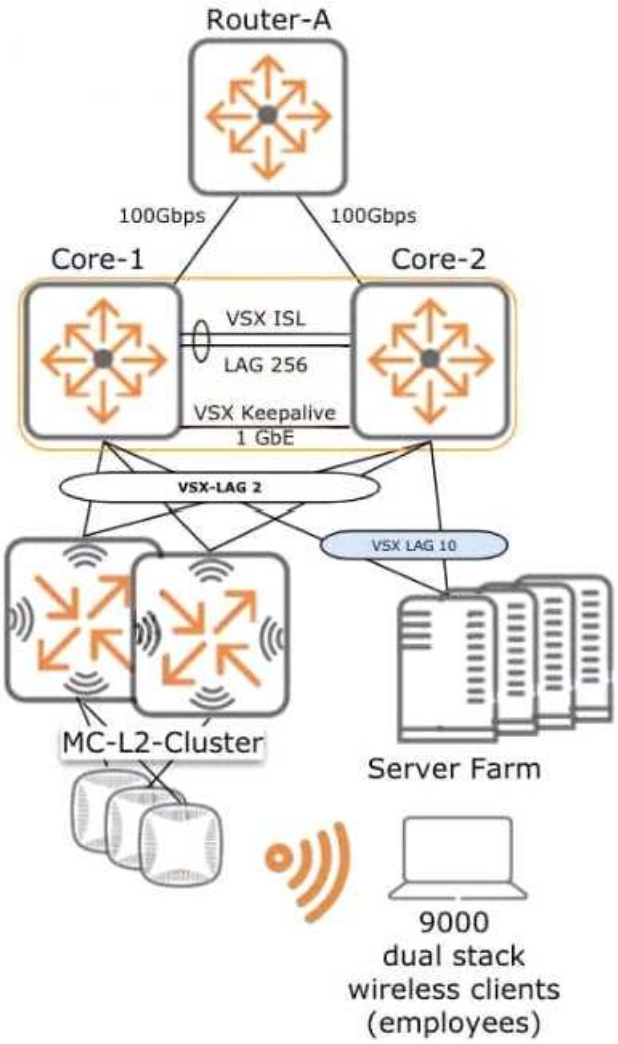
A. The mp traffic to MANAGEMENT-SERVERS group is logged to me event logs
B. The tftp traffic to MANAGEMENT-SERVERS group is not logged to the event logs.
C. The snmp-trap traffic to MANAGEMENT-SERVERS is logged to the event togs.
D. The denied tcp traffic to the MANAGEMENT-SERVERS group is logged to event logs.
E. The denied tcp traffic to the MANAGEMENT-SERVERS group is not logged to event logs

Answer: B, E

Explanation:

Question: 4

The customer is considering Implemented the following VSX configuration that will host an Aruba mobility cluster servicing 9000 dual stack employee devices.
The client's default gateways will be hosted on the VSX stack. The customer is seeking advice about how to ensure ArubaOS-CX VSX best practices have been applied.


Router-A
100Gbps
100Gbps
Core-1
Core-2
VSX ISL
LAG 256
VSX Keepalive
1 GbE
VSX-LAG 2
VSX LAG 10
MC-L2-Cluster
Server Farm
9000
dual stack
wireless clients
(employees)

```
Aggl# show vsx  status
VSX Operational State
---------------------
  ISL channel         : In-Sync
  ISL mgmt channel    : operational
  Config Sync Status  : in-sync
Attribute           Local              Peer
------------        --------           --------
ISL link            lag256             lag256
ISL version         2                  2
System MAC          02:01:00:00:00:00  02:01:00:00:00:00
Platform            8325               8325
Software Version    GL.10.05.0021      GL.10.05.0021
Device Role         primary            secondary
```

```
Aggl# show profiles available
Available profiles
------------------
 L3-agg   98304 L2 entries, 120000 Host entries (8190  unique overlay
          neighbors, 48638 unique underlay neighbors), 29696  Route entries
 L3-core  32768 L2 entries, 28000  Host entries (12286 unique overlay
          neighbors, 32766 unique underlay neighbors), 163796 Route entries
 Leaf     98304 L2 entries, 120000 Host entries (32766 unique overlay
          neighbors, 12286 unique underlay neighbors), 29696  Route entries
          (Default)
 Spine    32768 L2 entries, 28000  Host entries (12286 unique overlay
          neighbors, 32766 unique underlay neighbors), 163796 Route entries
```

```
Aggl# show profiles current
Current profile
---------------
L3-core
```

```
Agg-1# show vsx configuration keepalive
Keepalive Interface : 1/1/45
Keepalive VRF       : KA
Source IP Address   : 192.168.0.0
Peer IP Address     : 192.168.0.1
UDP Port            : 7678
Hello Interval      : 1 Seconds
Dead Interval       : 3 Seconds
```

What advice can you offer the customer? (Select two)

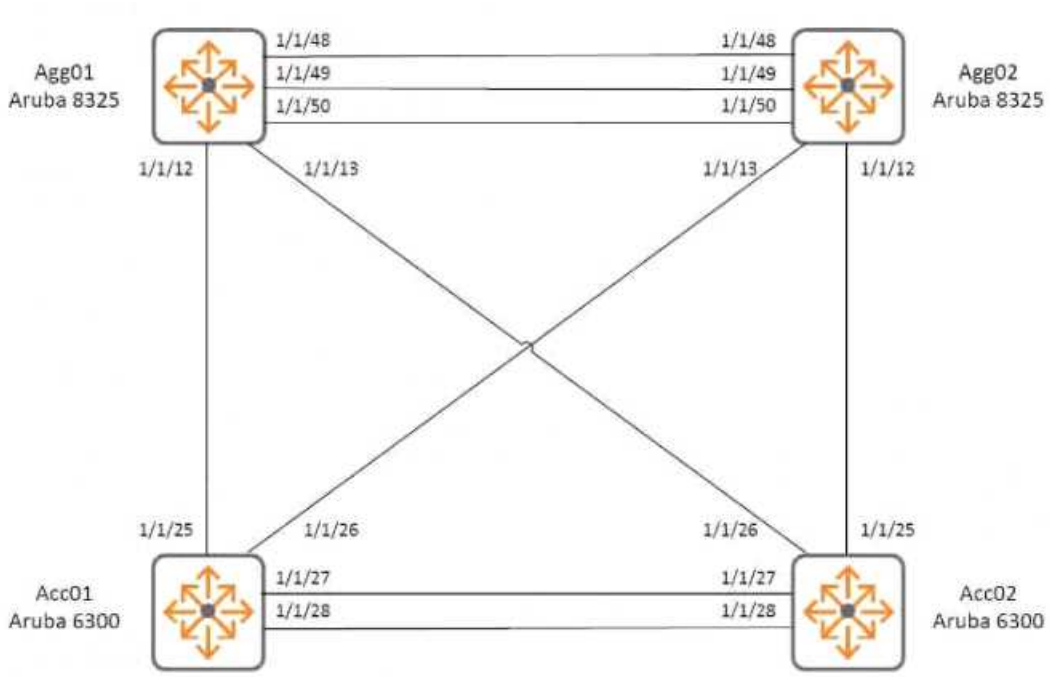
A. The ISL Bandwidth should be upgraded
B. Agg-1 and Agg-2's hardware forwarding table profile should be changed to "L3-agg''.
C. The -system-mac' of Agg-1 should be changed to an unused address from the unicast private address range
D. The vsx linkup-delay timer is unnecessarily high; it should be reduced to prevent excessive delay of packet forwarding when a VSX peer joins an existing master.
E. The Keepalive interface should be changed to interface LAG2 so there is redundancy through the mobility cluster.
F. The keepalive subnet is misconfigured, it has an inappropriate address on Agg-1.

Answer: BF

Explanation:

Question: 5

(Scenarios may contain multiple errors which may or may not Impact the solution > Refer to the exhibit.



An engineer has attempted to configure two pairs of switches in the referenced configuration it is required to implement VSX keep-alive at the aggregation layer.

The ports of the ArubaOS-CS 8325 switches used for Agg01 and Agg02 are populated as follows:

```
1/1/12 10G SFP+ LC SR 300m MMF Transceiver
1/1/13 10G SFP+ LC SR 300m MMF Transceiver
1/1/48 25G SFP28 5m DAC cable
1/1/49 100G QSFP28 5m DAC cable
1/1/50 100G QSFP28 5m DAC cable
```

The configuration of switch AGG01 includes:

```
!
!Version ArubaOS-CX GL.10.04.2000
!export-password: default
hostname Agg01
profile L3-agg
no usb
vrf KA
ntp server 10.77.77.77
ntp vrf mgmt
interface mgmt
    no shutdown
    ip static 10.177.177.70/24
    default-gateway 10.177.177.128
system interface-group 2 speed 10g
system interface-group 4 speed 25g
interface lag 1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 700-701
    lacp mode active
interface lag 2 multi-chassis
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed 700-701
    lag 1
 interface 1/1/48
    no shutdown
    vrf attach KA
    description VSX-KeepAlive
    ip address 192.168.20.1/30
 interface 1/1/49
    no shutdown
    mtu 9198
    lag 256
 interface 1/1/50
    no shutdown
    mtu 9198
    lag 256
 vsx
    system-mac 02:01:00:00:20:00
    inter-switch-link lag 256
    role primary
    keepalive peer 192.168.20.2 source 192.168.20.1
    linkup-delay-timer 600
    vsx-sync aaa acl-log-timer bfd-global bgp copp-policy dhcp-relay dhcp-server dhcp-
snooping dns icmp-tcp lldp loop-protect-global mac-lockout mclag-interfaces neighbor ospf
qos-global route-map sflow-global   snmp
ssh stp-global time vsx-global
ip dns server-address 10.25.110.250 vrf mgmt
https-server rest access-mode read-write
https-server vrf mgmt
```

VSX keep-alive is not working. Which modification should you make lo resolve the error condition?

A. Edit interface 1/1/48, adding the command "vpn-instance KA"
B. Modify the Interface lag 2 command, removing "multi-chassis"
C. Modify the Keepalive peer 192.168.20.2 source 192 168.20.1 command, adding "vrf KA"
D. Edit the vsx-sync command, adding "keep-alive"

Answer: B