IT认证电子书

质　量　更　高　　服　务　更　好

半年免费升级服务

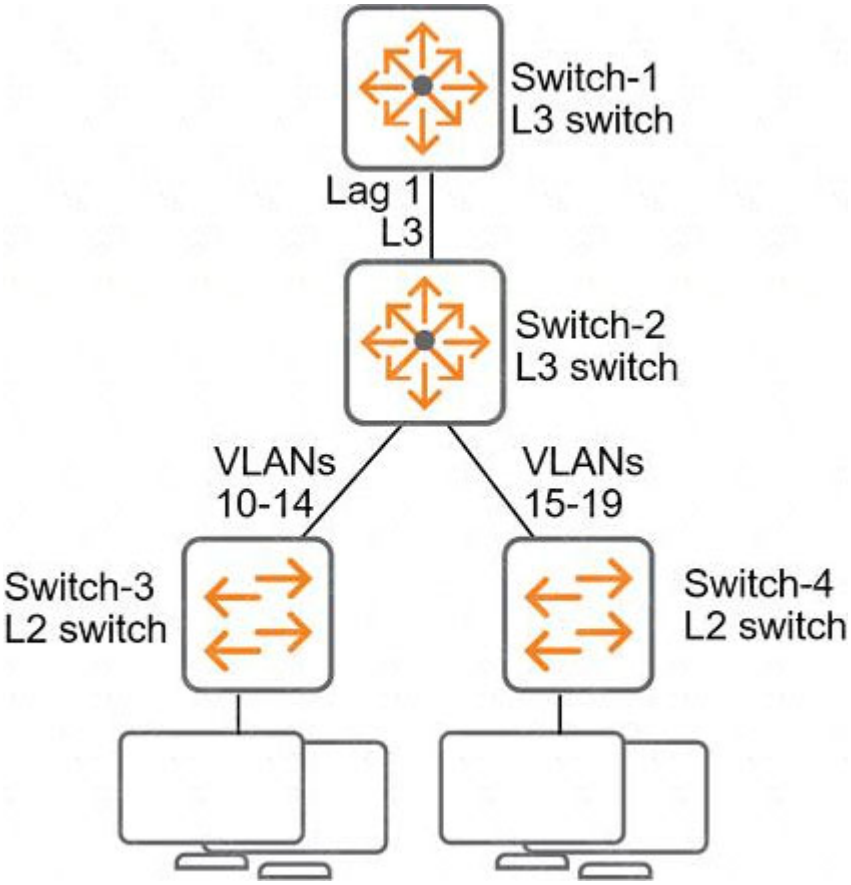
http://www.itrenzheng.com

Exam : **HPE7-A02**

Title : Aruba Certified Network Security Professional Exam

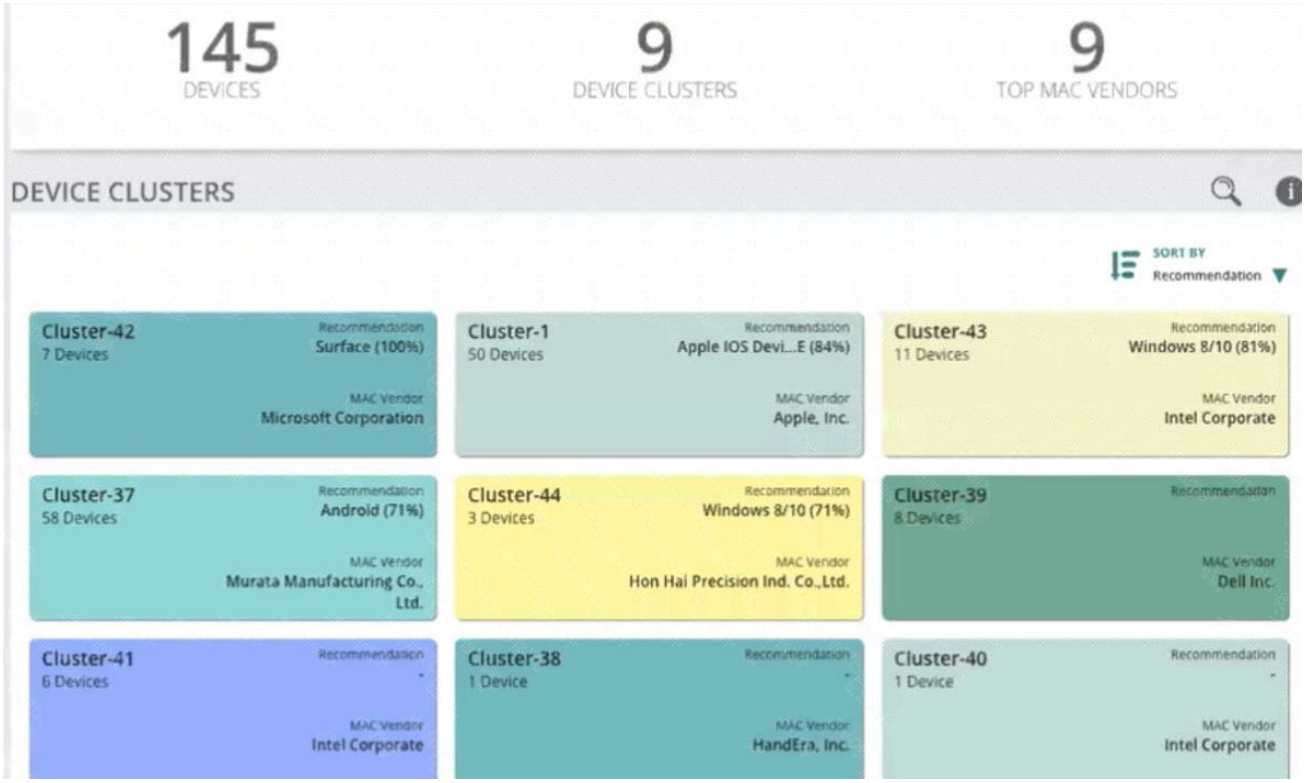
Version : DEMO

1.Refer to the exhibit.



All of the switches in the exhibit are AOS-CX switches.
What is the preferred configuration on Switch-2 for preventing rogue OSPF routers in this network?
A. Disable OSPF entirely on VLANs 10-19.
B. Configure OSPF authentication on VLANs 10-19 in password mode.
C. Configure OSPF authentication on Lag 1 in MD5 mode.
D. Configure passive-interface as the OSPF default and disable OSPF passive on Lag 1.
Answer: C
Explanation:
To prevent rogue OSPF routers in the network shown in the exhibit, the preferred configuration on Switch-2 is to configure OSPF authentication on Lag 1 in MD5 mode. This setup enhances security by ensuring that only routers with the correct MD5 authentication credentials can participate in the OSPF routing process. This method protects the OSPF sessions against unauthorized devices that might attempt to introduce rogue routing information into the network.
1. OSPF Authentication: Implementing MD5 authentication on Lag 1 ensures that OSPF updates are secured with a cryptographic hash. This prevents unauthorized OSPF routers from establishing peering sessions and injecting potentially malicious routing information.
2. Secure Communication: MD5 authentication provides a higher level of security compared to simple password authentication, as it uses a more robust hashing algorithm.
3. Applicability: Lag 1 is the primary link between Switch-1 and Switch-2, and securing this link helps protect the integrity of the OSPF routing domain.

2.Refer to Exhibit.



A company is using HPE Aruba Networking ClearPass Device Insight (CPDI) (the standalone application). In the CPDI interface, you go to the Generic Devices page and see the view shown in the exhibit.

What correctly describes what you see?

A. Each cluster is a group of unclassified devices that CPDI's machine learning has discovered to have similar attributes.

B. Each cluster is a group of devices that match one of the tags configured by admins.

C. Each cluster is all the devices that have been assigned to the same category by one of CPDI's built-in system rules.

D. Each cluster is a group of devices that have been classified with user rules, but for which CPDI offers different recommendations.

Answer: A

Explanation:

In HPE Aruba Networking ClearPass Device Insight (CPDI), the clusters shown in the exhibit represent groups of unclassified devices that CPDI's machine learning algorithms have identified as having similar attributes. These clusters are formed based on observed characteristics and behaviors of the devices, helping administrators to categorize and manage devices more effectively.

1.Machine Learning: CPDI uses machine learning to analyze device attributes and group them into clusters based on similarities.

2.Unclassified Devices: These clusters typically represent devices that have not yet been explicitly classified by admins but share common attributes that suggest they belong to the same category.

3.Management: This clustering helps in simplifying the process of managing and applying policies to groups of similar devices.

3.You have installed an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch to monitor a particular function.
Which additional step must you complete to start the monitoring?
A. Reboot the switch.
B. Enable NAE, which is disabled by default.
C. Edit the script to define monitor parameters.
D. Create an agent from the script.
Answer: D
Explanation:
After installing an HPE Aruba Networking Network Analytic Engine (NAE) script on an AOS-CX switch, the additional step required to start the monitoring is to create an agent from the script. The agent is responsible for executing the script and collecting the monitoring data as defined by the script parameters.
1. Script Installation: Installing the script provides the logic and parameters for monitoring.
2. Agent Creation: Creating an agent from the script activates the monitoring process, allowing the NAE to begin tracking the specified function.
3. Operational Step: This step ensures that the monitoring logic is applied and the data collection starts as per the script's configuration.

4.A company has HPE Aruba Networking gateways that implement gateway IDS/IPS. Admins sometimes check the Security Dashboard, but they want a faster way to discover if a gateway starts detecting threats in traffic.
What should they do?
A. Use Syslog to integrate the gateways with HPE Aruba Networking ClearPass Policy Manager (CPPM) event processing.
B. Integrate HPE Aruba Networking ClearPass Device Insight (CPDI) with Central and schedule hourly reports.
C. Set up email notifications using HPE Aruba Networking Central's global alert settings.
D. Set up Webhooks that are attached to the HPE Aruba Networking Central Threat Dashboard.
Answer: C
Explanation:
For a faster way to discover if a gateway starts detecting threats in traffic, admins should set up email notifications using HPE Aruba Networking Central's global alert settings. This setup ensures that the security team is promptly informed via email whenever the IDS/IPS on the gateways detects any threats, allowing for immediate investigation and response.
1.Email Notifications: By configuring email notifications, admins can receive real-time alerts directly to their inbox, reducing the time to discover and react to security incidents.
2.Global Alert Settings: HPE Aruba Networking Central's global alert settings allow for customization of alerts based on specific security events and thresholds, providing flexibility in monitoring and response.
3.Proactive Monitoring: This proactive approach ensures that the security team is always aware of potential threats without the need to constantly check the Security Dashboard manually.

5.A company uses HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server to authenticate managers on its AOS-CX switches. You want to assign managers to groups on the AOS-CX

switch by name.
How do you configure this setting in a CPPM TACACS+ enforcement profile?
A. Add the Shell service and set autocmd to the group name.
B. Add the Shell service and set priv-lvl to the group name.
C. Add the Aruba: Common service and set Aruba-Admin-Role to the group name.
D. Add the Aruba: Common service and set Aruba-Priv-Admin-User to the group name.
Answer: C
Explanation:
To assign managers to groups on the AOS-CX switch by name using HPE Aruba Networking ClearPass Policy Manager (CPPM) as a TACACS+ server, you should add the Aruba service to the TACACS+ enforcement profile and set the Aruba-Admin-Role to the group name. This configuration ensures that the appropriate administrative roles are assigned to managers based on their group membership, allowing for role-based access control on the AOS-CX switches.