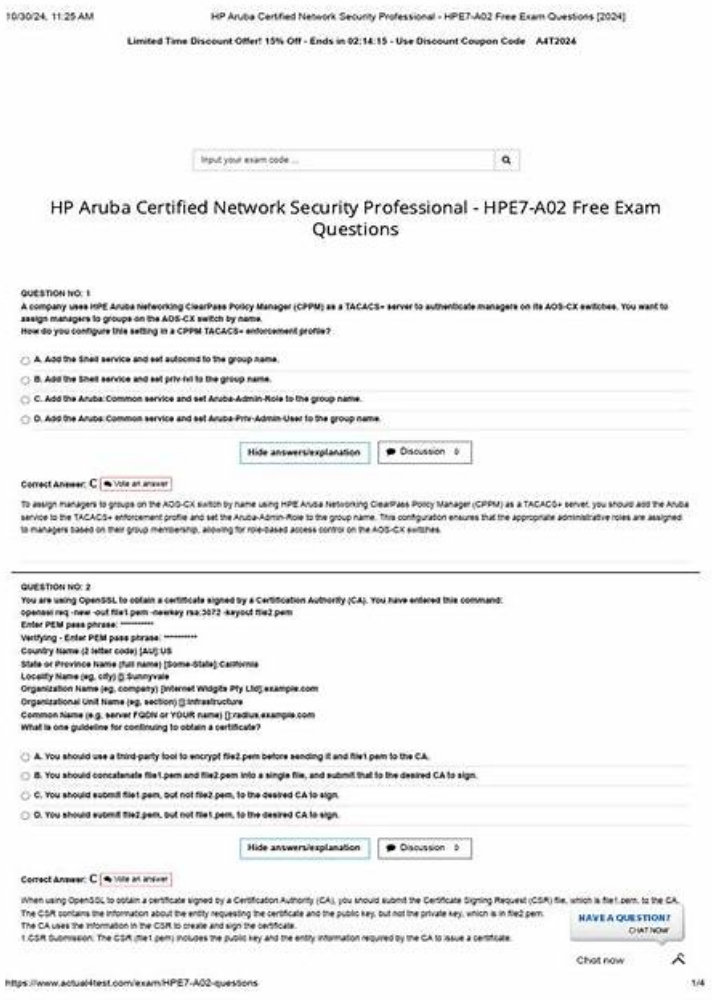
Valid Braindumps HPE7-A02 Ppt & HPE7-A02 Most Reliable Questions


10/30/24, 11:25 AM HP Aruba Certified Network Security Professional - HPE7-A02 Free Exam Questions [2024]

Limited Time Discount Offer! 15% Off - Ends in 02:14:15 - Use Discount Coupon Code A4T2024

Input your exam code ...

HP Aruba Certified Network Security Professional - HPE7-A02 Free Exam Questions

QUESTION NO: 1
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.

Hide answers/explanation Discussion 0

Correct Answer: C Vote an answer

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.

QUESTION NO: 2
You are using OpenSSL to obtain a certificate signed by a Certification Authority (CA). You have entered this command:
openssl req -new -out file1.pem -newkey rsa:3072 -keyout file2.pem
Enter PEM pass phrase: **********
Verifying - Enter PEM pass phrase: **********
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:Sunnyvale
Organization Name (eg, company) [Internet Widgits Pty Ltd]:example.com
Organizational Unit Name (eg, section) []:Infrastructure
Common Name (e.g. server FQDN or YOUR name) []:radius.example.com
What is one guideline for continuing to obtain a certificate?

A. You should use a third-party tool to encrypt file2.pem before sending it and file1.pem to the CA.
B. You should concatenate file1.pem and file2.pem into a single file, and submit that to the desired CA to sign.
C. You should submit file1.pem, but not file2.pem, to the desired CA to sign.
D. You should submit file2.pem, but not file1.pem, to the desired CA to sign.

Hide answers/explanation Discussion 0

Correct Answer: C Vote an answer

When using OpenSSL to obtain a certificate signed by a Certification Authority (CA), you should submit the Certificate Signing Request (CSR) file, which is file1.pem, to the CA. The CSR contains the information about the entity requesting the certificate and the public key, but not the private key, which is in file2.pem. The CA uses the information in the CSR to create and sign the certificate.
1 CSR Submission: The CSR (file1.pem) includes the public key and the entity information required by the CA to issue a certificate.

HAVE A QUESTION? CHAT NOW

Chat now

https://www.actual4test.com/exam/HPE7-A02-questions 1/4

P.S. Free 2026 HP HPE7-A02 dumps are available on Google Drive shared by Test4Engine: https://drive.google.com/open?id=1txKTZhiHJ486lg2-KGsBSLOh-iJ6Otia

Our company has successfully created ourselves famous brands in the past years, and all of the HPE7-A02 valid study guide materials from our company have been authenticated by the international authoritative institutes and cater for the demands of all customers at the same time. We are attested that the quality of the HPE7-A02 Test Prep from our company have won great faith and favor of customers. We persist in keeping creating the best helpful and most suitable HPE7-A02 study practice question for all customers.

HP HPE7-A02 Certification Exam is ideal for professionals who are looking to advance their careers in the field of network security. HPE7-A02 exam covers a range of topics including network security fundamentals, secure wireless design and configuration, firewall technologies, VPN technologies, and intrusion detection and prevention.

>> Valid Braindumps HPE7-A02 Ppt <<

HPE7-A02 Most Reliable Questions, New HPE7-A02 Test Question

Whatever HPE7-A02 Exam, you are taking; the study guides of Test4Engine are there to help you get through the exam without any hassle. The questions and answers are absolutely exam oriented, focusing only the most essential part of your exam syllabus. Thus they save your time and energy going waste in thumbing through the unnecessary details.

To be eligible for the HPE7-A02 exam, you must have a minimum of three years of experience in designing and implementing network security solutions in complex environments. You must also possess a thorough understanding of network security technologies, protocols, and methodologies. HPE7-A02 exam consists of 60 multiple-choice questions that you must answer within 90 minutes. To pass the exam, you must score a minimum of 70%. Achieving the HPE7-A02 Certification demonstrates your expertise in network security and validates your ability to design, implement, and troubleshoot secure network infrastructure solutions in complex enterprise environments.

HP Aruba Certified Network Security Professional Exam Sample Questions (Q41-Q46):

NEW QUESTION # 41
A company wants to use the HPE Aruba Networking ClearPass OnGuard agent to assign posture to clients.
How do you define the conditions by which a client receives a particular posture?

- A. Create rules within a WebAuth enforcement policy
- B. Create rules directly in a service's Posture tab
- C. Create the rules directly in a service's Enforcement tab
- D. Create rules within a posture policy

Answer: D

Explanation:
ClearPass OnGuard uses a Posture Policy object to define:
* Which checks are performed (e.g., AV installed, firewall status, patches)
* How the results map to posture tokens such as "Healthy," "Quarantined," etc.
The official OnGuard configuration workflow states that you must first "Define the posture policy", and that these posture policies contain the rules for evaluating health and determining posture tokens.
Service enforcement policies then consume the posture token (e.g., Tips:Posture = Healthy) but do not define the posture conditions themselves. The "Posture" tab on a service is used to enable posture and associate it with the posture policy; the detailed rules live in the posture policy object.
Therefore, posture logic is defined by creating rules within a posture policy # Option A.

NEW QUESTION # 42
You are configuring the HPE Aruba Networking ClearPass Device Insight Integration settings on ClearPass Policy Manager (CPPM). For which use case should you set the 'Tag Updates Action" to " apply for all tag updates"?

- A. When you plan to have CPPM issue CoAs for clients with new tags, but do not want to have to list those specific tags in the Device Integration settings in advance.
- B. When Device Insight tags are only used to identify dangerous devices, and you want to disconnect those devices without having to set up new rules in enforcement policies.
- C. When CPPM is gathering posture information for CPDI, and you want CPDI to always have access to the most up-to-date information.
- D. When the Device Insight integration poll interval is set to a relatively long interval but you still want CPPM to be informed quickly about devices' new tags.

Answer: A

Explanation:
* Tag Updates Action - "Apply for All Tag Updates":
* This setting ensures that all updated tags from Device Insight (CPDI) are applied dynamically.
* It is particularly useful when you want to trigger Change of Authorization (CoA) without explicitly predefining the tag values.
* Option D: Correct. This setting allows CPPM to issue CoAs automatically for updated tags without requiring prior configuration of specific tags.
* Option A: Incorrect. The setting is not directly related to reducing the poll interval latency.
* Option B: Incorrect. Disconnecting devices based on dangerous tags would require predefined enforcement rules.
* Option C: Incorrect. Posture information updates do not directly rely on this setting.

NEW QUESTION # 43

A company has been running Gateway IDS/IPS on its gateways in IDS mode for several weeks. The company wants to transition to IPS mode.
What is one step you should recommend?

- A. Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
- B. Change the mode on one gateway at a time to establish a smoother transition period.
- C. Consider applying a stricter IPS policy to minimize issues during the transition period.
- D. Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.

Answer: A

Explanation:
When transitioning from Intrusion Detection System (IDS) mode to Intrusion Prevention System (IPS) mode, it's critical to review and refine configurations to ensure legitimate traffic is not blocked. Here's the reasoning behind each option:
A: Disable traffic inspection and reboot before re-enabling traffic inspection with the new mode.
* Incorrect:
* Transitioning to IPS mode does not require a full reboot or disabling traffic inspection.
* This step is unnecessary and could lead to downtime that impacts network operations.
B: Change the mode on one gateway at a time to establish a smoother transition period.
* Incorrect:
* While a phased approach might help in some large deployments, it does not directly address the potential for legitimate traffic to be blocked by IPS mode.
* IPS operates in real-time, so misconfigured rules or policies need to be addressed before enabling IPS on any gateway.
C: Consider applying a stricter IPS policy to minimize issues during the transition period.
* Incorrect:
* A stricter IPS policy increases the likelihood of false positives, which could disrupt legitimate business-critical traffic.
* During the transition, the focus should be on minimizing disruptions by fine-tuning policies, not making them stricter.
D: Check for legitimate traffic that has been flagged as a threat and allow list the associated rules.
* Correct:
* In IDS mode, the system only detects and logs suspicious traffic but does not block it. Reviewing these logs for false positives allows the organization to fine-tune policies and allow list legitimate traffic before transitioning to IPS mode.
* By doing this, the company ensures that IPS mode will block actual threats while permitting legitimate traffic.
* This is a proactive step to prevent unnecessary disruptions to normal operations when IPS mode is enabled.
References
* HPE Aruba Gateway IDS/IPS Configuration Guide.
* Best Practices for Transitioning from IDS to IPS Modes in Aruba Networks.
* Aruba Network Threat Management Documentation.

NEW QUESTION # 44
You have configured an AOS-CX switch to implement 802.1X on edge ports. Assume ports operate in the default auth-mode. VoIP phones are assigned to the "voice" role and need to send traffic that is tagged for VLAN 12. Where should you configure VLAN 12?

- A. As the allowed trunk VLAN in the "voice" role (and not in the edge port settings).
- B. As the trunk native VLAN in the "voice" role (and not in the edge port settings).
- C. As the trunk native VLAN on edge ports and the trunk native VLAN on the "voice" role.
- D. As a trunk allowed VLAN on edge ports and the trunk native VLAN in the "voice" role.

Answer: A

Explanation:
* Voice Role VLAN Configuration:
* When VoIP phones are authenticated and assigned to the "voice" role, VLAN 12 should be explicitly defined as an allowed trunk VLAN within the role configuration.
* The VLAN configuration should be role-specific rather than on the edge port, as this ensures dynamic VLAN assignment based on authentication results.
* Option Analysis:
* Option A: Incorrect. Native VLANs are for untagged traffic, but VoIP traffic is tagged.
* Option B: Correct. VLAN 12 must be configured as the allowed trunk VLAN in the "voice" role to tag VoIP traffic correctly.
* Option C: Incorrect. Configuring VLAN 12 in both edge port and role settings is redundant and unnecessary.

* Option D: Incorrect. Native VLANs do not handle tagged traffic like VLAN 12 for VoIP phones.

NEW QUESTION # 45
Your company wants to implement Tunneled EAP (TEAP).
How can you set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificated-based authentication for clients using TEAP?

- A. For the service using TEAP, set the authentication source to an internal database.
- B. Select an EAP-TLS-type authentication method for the TEAP method's inner method.
- C. Create an authentication method named "TEAP" with the type set to EAP-TLS.
- D. Select a service certificate when you specify TEAP as a service's authentication method.

Answer: B

Explanation:
To set up HPE Aruba Networking ClearPass Policy Manager (CPPM) to enforce certificate-based authentication for clients using Tunneled EAP (TEAP), you need to select an EAP-TLS-type authentication method for TEAP's inner method. TEAP allows for a combination of certificate-based (EAP-TLS) and password-based (EAP-MSCHAPv2) authentication. By choosing EAP-TLS as the inner method, you ensure that the clients are authenticated using their certificates, thus enforcing certificate-based authentication within the TEAP framework.

NEW QUESTION # 46
.....

id=1txKTZhiHJ486lg2-KGsBSLOh-iJ6Otia