



HPE6-A81^{Q&As}

Aruba Certified ClearPass Expert Written Exam

Pass HP HPE6-A81 Exam with 100% Guarantee

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

<https://www.passapply.com/hpe6-a81.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by HP Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers





QUESTION 1

A customer is planning to implement machine and user authentication on infrastructure with one Aruba Controller and a single ClearPass Server.

What should the customer consider while designing this solution? (Select three.)

- A. The Windows User must log off, restart or disconnect their machine to initiate a machine authentication before the cache expires.
- B. The machine authentication status is written in the Multi-master cache on the ClearPass Server for 24 hrs.
- C. Onboard must be used to install the Certificates on the personal devices to do the user and machine authentication.
- D. The Customer should enable Multi-Master Cache Survivability as the Aruba Controller will not cache the machine state.
- E. Machine Authentication only uses EAP TLS, as such a PKI infrastructure should be in place for machine authentication.
- F. The customer does not need to worry about Multi-Master Cache Survivability because the Controller will also cache the machine state.

Correct Answer: BCE

QUESTION 2

A customer is looking to implement a Web-Based Health Check solution with the following requirements:

for the HR user's client devices, check if a USB stick is mounted.

for the RandD user's client devices, check if the hard disk is fully encrypted.

The Web-Based Health Check service has been configured but the customer it is not sure how to design the Profile Policy.

How can be accomplished this customer request?

- A. create two Posture Policies and customize the OnGuard Agent (Persistent or Dissolvable) to select the correct SHV checks
- B. create one Posture Policy and define Rules Conditions that will apply different Tokens for each SHV check condition
- C. create two Posture Policies and use the Restrict by Roles option to filter for HR and RandD user roles and apply the correct SHV checks
- D. create one Posture Policy to check the HR users client devices and use the NAP Agent to check RandD users client devices

Correct Answer: A



QUESTION 3

Refer to the exhibit:

TACACS+ Session Details

Summary Request Policies

Policies Used -

| | |
|------------------------|--|
| Service Name: | [Aruba Device Access Service] |
| Authentication Source: | [Local User Repository] |
| Role: | [User Authenticated], [Aruba TACACS read-only Admin] |
| Profiles: | [ArubaOS Wireless - TACACS Read-Only Access] |

Showing 2 of 1-2 records

Export Show Logs Close



Dashboard

Configuration

- WLANs
- Roles & Policies
- Access Points
- AP Groups
- Authentication
- Services
- Interfaces
- System
- Tasks

Diagnostics

Maintenance

General Admin AirWave CPSec Certificates SNMP Logging Profiles

Admin Authentication Options

Default role: root

Enable: ☒

MSOAPV2: ☐

Server group: ClearPass Tacacs

Management telnet access: ☐

Login activities persistence period: 0 days

Login banner text:

Banner has to be accepted: ☐

WEBUI AUTHENTICATION

Username/password: ☒

Webui HTTPS port (443) access: ☐

Client certificate: ☐

Server certificate: default

Idle session timeout: 15 minutes

Re-authentication timeout:

Auth Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group > ClearPass Tacacs Servers Options Server Rules

Drag rows to re-order

| Name | Type | IP Address | Trust FQDN | Match Rules |
|-------------|--------|--------------|------------|-------------|
| ClearPass T | TACACS | 10.1.128.111 | - | - |

+ Add

Server Group > ClearPass Tacacs > ClearPass T Server Options Server Group Trust FQDN Server Group Match Rules

Host: 10.1.128.111

Key: [Redacted]

Retype key: [Redacted]

TCP port: 49

Retransmits: 3

Timeout: 20

Mode: ☒

Session authentication: ☐



| ID | User Name | User Role | Connection From | Idle Time | Session Time | Path |
|----|-----------|-----------|-----------------|-----------|--------------|------|
| 1 | admin | root | 10.1.29.90 | 00:00:10 | 00:00:42 | / |
| 2 | read-only | root | 10.1.29.90 | 00:00:10 | 00:01:45 | / |
| 3 | admin | root | 10.1.29.90 | 00:00:10 | 00:01:45 | / |

A customer has configured the Aruba Controller for administrative authentication using ClearPass as a TACACS server. During testing, the read-only user is getting the root access role. What could be a possible reason for this behavior? (Select two.)

- A. The Controller's Admin Authentication Options Default role is mapped to root.
- B. The ClearPass user role associated to the read-only user is wrong
- C. The Controller Server Group Match Rules are changing the user role
- D. The read-only enforcement profile is mapped to the root role
- E. On the Controller, the TACACS authentication server is not configured for Session authorization

Correct Answer: CE

QUESTION 4

Refer to the exhibit: A customer has configured a Guest Self registration page for their Cisco Wireless network with the settings shown. What should be changed in order to successfully authenticate guests users?



Home » Configuration » Pages » Self-Registrations

Customize Self-Registration (Admin-GuestCiscoSelfReg)

Use this form to make changes to the self-registration instance Admin-GuestCiscoSelfReg.

| Customize Self-Registration | |
|---|--|
| Login Options controlling logging in for self-registered guests. | |
| Enabled: | <input checked="" type="checkbox"/> Enable guest login to a Network Access Server |
| * Vendor Settings: | Cisco Systems <small>Select a predefined group of settings suitable for standard network configurations.</small> |
| Login Method: | Controller-initiated — Guest browser performs HTTP form submit <small>Select how the user's network login will be handled. Server-initiated logins require the user's MAC address to be available, usually from the captive portal redirection process.</small> |
| * IP Address: | 1.1.1.1 <small>Enter the IP address or hostname of the vendor's product here.</small> |
| Secure Login: | <input checked="" type="checkbox"/> Use vendor default <small>Select a security option to apply to the web login process.</small> |
| Dynamic Address: | <input type="checkbox"/> The controller will send the IP to submit credentials. <small>In multi-controller deployments, it is often required to post credentials to different addresses made available as part of the original redirection. The address above will be used whenever the parameter is not available or fails the requirements below.</small> |
| Username Suffix: | <input type="text"/> <small>The suffix is automatically appended to the username before logging into the NAS.</small> |
| Default Destination Options for controlling the destination clients will redirect to after login. | |
| * Default URL: | <input type="text"/> <small>Enter the default URL to redirect clients. Please ensure you prepend "http://" for any external domain.</small> |
| Override Destination: | <input checked="" type="checkbox"/> Force default destination for all clients <small>If selected, the client's default destination will be overridden regardless of its value.</small> |
| <input type="button" value="Save Changes"/> <input type="button" value="Save and Continue"/> | |

| CISCO | |
|---|---|
| MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT | |
| Management | |
| Summary | |
| SNMP | |
| HTTP-HTTPS | |
| Telnet-SSH | |
| Serial Port | |
| Local Management | |
| Users | |
| User Sessions | |
| HTTP-HTTPS Configuration | |
| HTTP Access | <input checked="" type="checkbox"/> Enabled |
| HTTPS Access | <input checked="" type="checkbox"/> Enabled |
| WebAuth SecureWeb | <input type="checkbox"/> Disabled |
| HTTPS Redirection | <input type="checkbox"/> Disabled |
| Web Session Timeout | 30 Minutes |
| Current Certificate | |

- A. Secure Login should use HTTP
- B. Change the Vendor Settings to Airespace Networks
- C. Change the IP Address to the Cisco Controller DNS name



D. Login Method should be Controller-initiated - using HTTPs form submit

Correct Answer: C

QUESTION 5

A corporate ClearPass Cluster with two servers located at a single site, has both Management and Data port IP addresses configured. The Management port IPs are in the DataCenter networks subnet, while the Data port IPs are in the DMZ. What is the difference between using one Virtual IP for the AAA traffic versus sending AAA requests to the physical IPs for each server? (Select two.)

- A. The failover can be accomplished only by using Virtual IP.
- B. The Individual IPs can provide failover and load balancing.
- C. One Virtual IP can be used together with the individual server IPs for load balancing.
- D. By using the Virtual IP, the failover convergence is faster than using individual server IPs.
- E. Using the one Virtual IP can provide failover and load balancing.

Correct Answer: BE

[HPE6-A81 PDF Dumps](#)

[HPE6-A81 Exam Questions](#)

[HPE6-A81 Braindumps](#)