HPE6-A77 Q&As

Aruba Certified ClearPass Expert Written

Pass HP HPE6-A77 Exam with 100% Guarantee

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

https://www.passapply.com/hpe6-a77.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

Which statements are true about Aruba downloadable user roles? (Select three.)

A. Can be applied only on ports or WLAN users authenticated by ClearPass.

B. Aruba downloadable user role are universally available across the environment

C. Aruba downloadable user role is a built in enforcement template in ClearPass

D. Downloadable role names must be defined in Aruba switch or controller

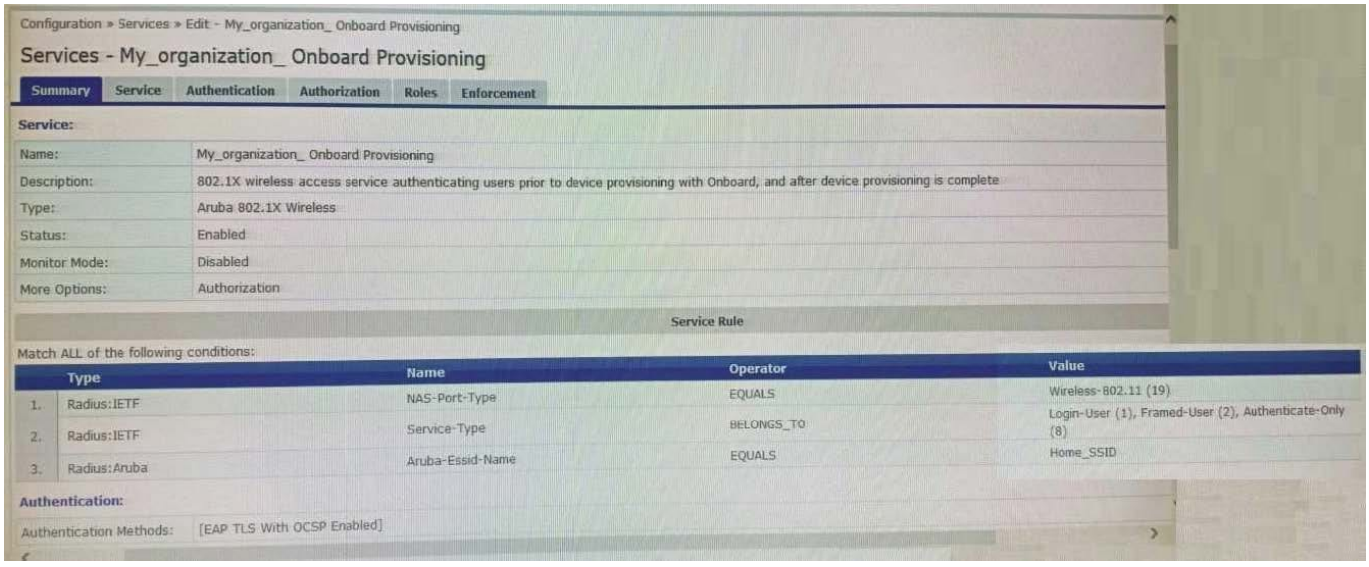
E. Can use these roles for other authentication methods not involving ClearPass

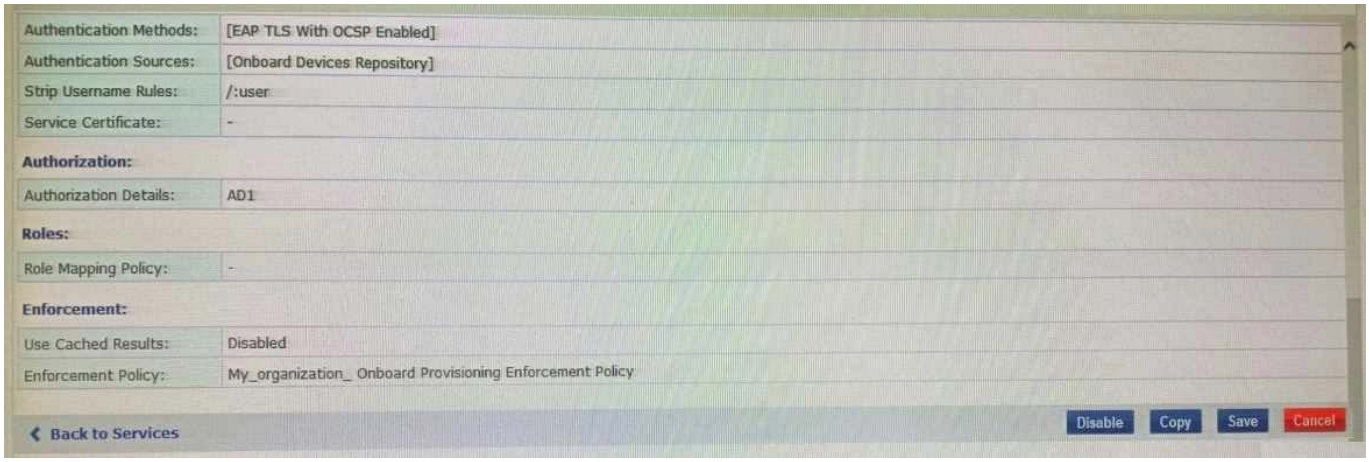
F. Administering downloadable user roles can be difficult for a large enterprise

Correct Answer: ADE

QUESTION 2

Refer to the exhibit: A customer has configured a service with the Onboard Devices Repository as an Authentication Source and an Active Directory Domain Server as an Authorization Source. What will happen if the client certificate is still valid and the user account associated with the certificate is disabled in Active Directory?





A. ClearPass will not process the request

B. Enforcement will apply the [Deny Access Profile]

C. ClearPass will redirect the client to Onboard again

D. ClearPass will block network access to the device

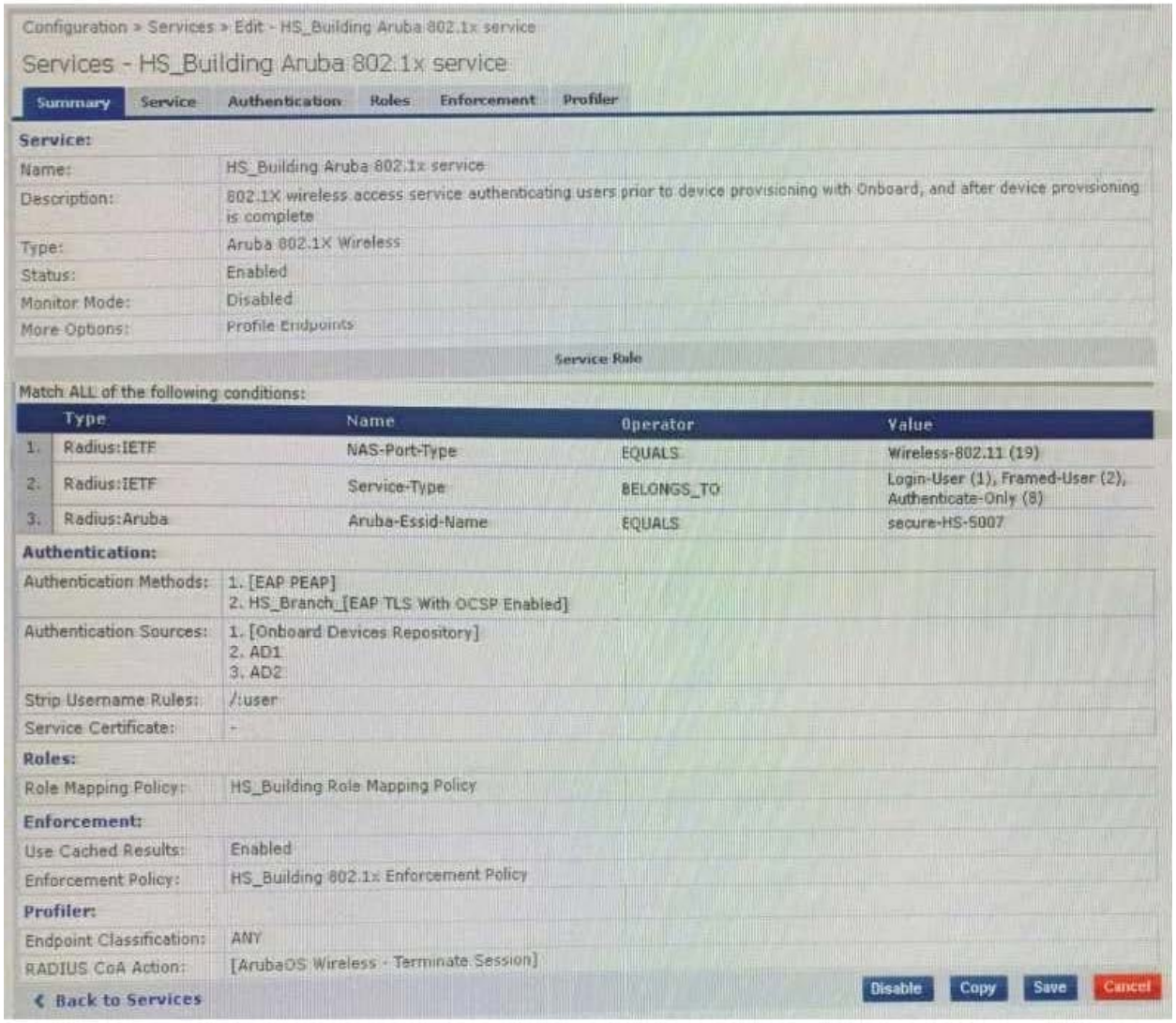
E. ClearPass will allow the device to access the network.

Correct Answer: D

QUESTION 3

Refer to the exhibit:


Request Details
Summary
Input
Output
Alerts
Login Status: REJECT
Session Identifier: R00000218-01-5d9db68b
Date and Time: Oct 09, 2019 06:29:34 EDT
End-Host Identifier: 78D29437BD68 (Computer / Windows / Windows 10)
Username: andy07
Access Device IP/Port: 10.1.70.100:0 (ArubaController / Aruba)
System Posture Status: UNKNOWN (100)
Policies Used -
Service: HS_Building Aruba 802.1x service
Authentication Method: EAP-PEAP,EAP-MSCHAPv2
Authentication Source: AD:AD1.aruba1.local
Authorization Source: AD1
Roles: [Other], [User Authenticated]
Enforcement Profiles: [Deny Access Profile]
Service Monitor Mode: Disabled
Online Status: Not Available
Showing 1 of 1-20 records
Show Configuration
Export
Show Logs
Close
Request Details
Summary
Input
Output
Alerts
Error Code: 206
Error Category: Authentication failure
Error Message: Access denied by policy
Alerts for this Request
RADIUS Applied 'Reject' profile



Configuration » Services » Edit - HS_Building Aruba 802.1x service

Services - HS_Building Aruba 802.1x service

Summary | Service | Authentication | Roles | Enforcement | Profiler

Service:

Name:	HS_Building Aruba 802.1x service
Description:	802.1X wireless access service authenticating users prior to device provisioning with Onboard, and after device provisioning is complete
Type:	Aruba 802.1X Wireless
Status:	Enabled
Monitor Mode:	Disabled
More Options:	Profile Endpoints

Service Rule

Match ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	EQUALS	Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Framed-User (2), Authenticate-Only (8)
3.	Radius:Aruba	Aruba-Essid-Name	EQUALS	secure-HS-5007

Authentication:

Authentication Methods:	1. [EAP PEAP] 2. HS_Branch_[EAP TLS With OCSP Enabled]
Authentication Sources:	1. [Onboard Devices Repository] 2. AD1 3. AD2
Strip Username Rules:	/:user
Service Certificate:	-

Roles:

Role Mapping Policy:	HS_Building Role Mapping Policy

Enforcement:

Use Cached Results:	Enabled
Enforcement Policy:	HS_Building 802.1x Enforcement Policy

Profiler:

Endpoint Classification:	ANY
RADIUS CoA Action:	[ArubaOS Wireless - Terminate Session]

« Back to Services

Disable | Copy | Save | Cancel


Configuration » Services » Edit - HS_Building Aruba 802.1x service
Services - HS_Building Aruba 802.1x service
Summary
Service
Authentication
Roles
Enforcement
Profiler
Role Mapping Policy:
HS_Building Role Mapping Policy
Modify
Add New Role Mapping Policy
Role Mapping Policy Details
Description:
Default Role:
[Other]
Rules Evaluation Algorithm:
first-applicable
Conditions
Role
1. (Connection:Client-Mac-Address BELONGS_TO_GROUP VIP User MAC)
VIP User
2. (Authorization:Corp SQL:MAC EXISTS)
Corp SQL Tablet
3. (Authorization:[Endpoints Repository]:Category EQUALS VoIP Phone)
IP Phone
4. (Authorization:[Endpoints Repository]:Category EQUALS SmartDevice)
Personal SmartDevice
5. (Authorization:[Endpoints Repository]:Category EQUALS Point of Sale devices)
Vending Machine
6. (Authorization:[Endpoints Repository]:Category EQUALS Printer) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS CANON INC.)
Printer
7. (Authorization:[Endpoints Repository]:Category EQUALS Network Camera) AND (Authorization:[Endpoints Repository]:MAC Vendor EQUALS Axis Communications AB)
IP Camera


Configuration » Services » Edit - HS_Building Aruba 802.1x service
Services - HS_Building Aruba 802.1x service
Summary
Service
Authentication
Roles
Enforcement
Profiler
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
HS_Building 802.1x Enforcement Policy
Modify
Add New Enforcement Policy
Enforcement Policy Details
Description:
Default Profile:
[Deny Access Profile]
Rules Evaluation Algorithm:
first-applicable
Conditions
Enforcement Profiles
1. (Endpoint:MDM Enabled EQUALS true)
Aruba Full Access Profile
2. (Authentication:OuterMethod EQUALS EAP-PEAP) AND (Tips:Role EQUALS Corp SQL Tablet)
Redirect to Aruba OnBoard Portal
3. (Authentication:OuterMethod EQUALS EAP-TLS) AND (Tips:Role EQUALS Corp SQL Tablet)
Aruba Full Access Profile
4. (Tips:Role EQUALS VIP User)
Aruba VIP Full Access Profile
5. (Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS HEALTHY (0))
Aruba Full Access Profile
6. (Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture EQUALS UNKNOWN (100))
Aruba Limited Access Profile, Redirect to Aruba Dissolvable_page Profile
7. (Tips:Role MATCHES_ALL [User Authenticated] [Machine Authenticated]) AND (Authentication:Source EQUALS AD1) AND (Tips:Posture NOT_EQUALS HEALTHY (0))
Redirect to Aruba Quarantine Profile

Your company has a postgres SQL database with the MAC addresses of the company-owned tablets You have configured a role mapping condition to tag the SQL devices. When one of the tablets connects to the network, it does not get the correct role and receives a deny access profile.

How would you resolve the issue?

A. Remove SQL condition from role mapping policy and add it under the enforcement policy conditions.

B. Edit the SQL authentication source niter attributes and modify the SQL server filter query.

C. Add the SQL server as an authentication source and map .t under the authentication tab in the service.

D. Enable authorization tab in the service and add the SQL server as an authorization source.

Correct Answer: B

QUESTION 4

You have recently implemented a serf-registration portal in ClearPass Guest to be used on a Guest SSID broadcast from an Aruba controller. Your customer has started complaining that the users are not able to reliably access the internet after clicking the login button on the receipt page. They tell you that the users will click the login button multiple times and alter about a minute they gain access. What could be causing this issue?

A. The self-registration page is configured with a 1 minute login delay.

B. The guest client is delayed getting an IP address from the DHCP server.

C. The guest users are assigned a firewall user role that has a rate limit.

D. The enforcement profile on ClearPass is set up with an lETF:session delay.

Correct Answer: A

QUESTION 5

Refer to the exhibit:

A customer with multiple Aruba Controllers has just installed a new certificate for "*.customerdomain com" on all Aruba Controllers. While testing the existing guest Self-Registration page the customer noticed that the logins are failing. While troubleshooting they are finding no entries in the Event Viewer or Access Tracker for the tests. Suspecting that the Aruba Controllers may not be properly posting the credentials from the guest browser, they open the NAS Vendor Settings for the Guest Self-Registration Page. From the screen shown, how can you fix the errors?

A. Change the "IP Address: field to" securelogin.customerdomain.com.

B. Change the "Secure Login:" field to "Use Vendor Default".

C. Change the "IP Address field to "captiveportal-login.customerdomain.com".

D. Add PTR records on the DNS server for "securelogin.arubanetworks.com".

Correct Answer: B