HP

Exam HPE6-A07

Aruba Certified ClearPass Associate 6.5

Verson: Demo

[Total Questions: 10]

Question No : 1

Which device verifies the Server certificate during the Over the air provisioning process?

A. Aruba Controller
B. Active Directory
C. ClearPass Onboard
D. Client
E. ClearPass Policy Manager

Answer: C

Question No : 2

What does a client need for it to perform EAP-TLS successfully? (Select two.)

A. Username and Password
B. Server Certificate
C. Pre-shared key
D. Certificate Authority
E. Client Certificate

Answer: B,E

Explanation:

Referencehttps://community.arubanetworks.com/t5/AAA-NAC-Guest-Access-BYOD/Binary-comparison-in-EAP-TLS-Authentication/ta-p/257857

Question No : 3

Which licenses are included in the built-in starter kit for ClearPass?

A. 10 ClearPass Guest licenses,10 ClearPass OnGuard licenses and 10 ClearPass Onboard licenses
B. 10 ClearPass Enterprise licenses

C. 25 ClearPass Policy Manager licenses
D. 25 ClearPass Profiler licenses
E. 25 ClearPass Enterprise licenses

Answer: E

Question No : 4

When Active Directory is added as an authentication source, what should the format be for the Active Directory bin DN?

A. admin.domain.com
B. domain.com\admin
C. domain.com
D. admin@domain.com
E. admin\domain.com

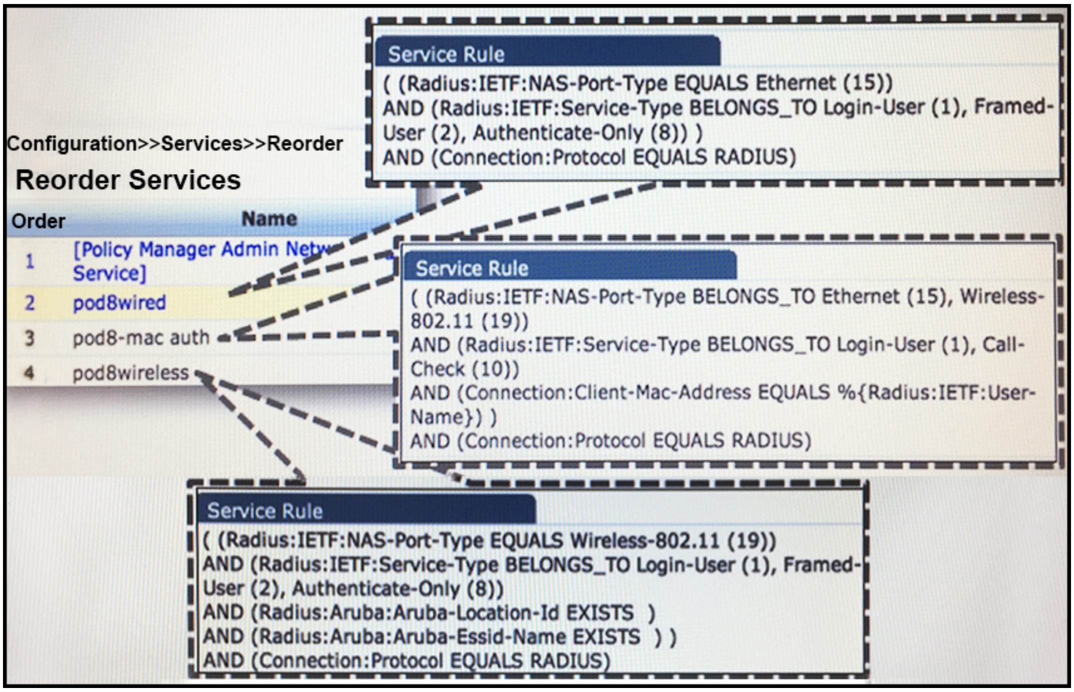
Answer: D

Explanation:

For Active Directory, the bind DN can also be in the administrator@domain format (for example,administrator@acme.com).

Referencehttp://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Auth/AuthSource_GenericLDAP.htm

Question No : 5



Configuration>>Services>>Reorder

Reorder Services

Order	Name
1	[Policy Manager Admin Netw Service]
2	pod8wired
3	pod8-mac auth
4	pod8wireless

Service Rule

((Radius:IETF:NAS-Port-Type EQUALS Ethernet (15))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8)))
AND (Connection:Protocol EQUALS RADIUS)

Service Rule

((Radius:IETF:NAS-Port-Type BELONGS_TO Ethernet (15), Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Call-Check (10))
AND (Connection:Client-Mac-Address EQUALS %{Radius:IETF:User-Name}))
AND (Connection:Protocol EQUALS RADIUS)

Service Rule

((Radius:IETF:NAS-Port-Type EQUALS Wireless-802.11 (19))
AND (Radius:IETF:Service-Type BELONGS_TO Login-User (1), Framed-User (2), Authenticate-Only (8))
AND (Radius:Aruba:Aruba-Location-Id EXISTS)
AND (Radius:Aruba:Aruba-Essid-Name EXISTS))
AND (Connection:Protocol EQUALS RADIUS)

Refer to the exhibit. A user connects to an Aruba Access Point wireless SSID named “secure-corporate” and performs an 802.1X authentication with ClearPass as the authentication server.

Based on this service configuration, which service will be triggered?

A. pod8-mac auth
B. Noservice will be triggered
C. pod8wireless
D. [Policy Manager Admin Network Service]
E. pod8wired

Answer: A

Question No : 6

An organization wants to have employees connect their own personal devices securely to the WLAN.

Which ClearPass feature can be used to accomplish this?

A. Enforcement
B. Guest
C. Profiling
D. Onboarding
E. Guest withself-registration

Answer: D

Explanation:

Referencehttp://www.arubanetworks.com/pdf/solutions/CS_ConsulateHealthCare.pdf

Question No : 7

Which additional service must be added to a ClearPass server to use the OnGuard Agent health checks for 802.1x authentication?

A. HTTP Posture Service
B. 802.1x Authentication
C. 802.1x Posture Service
D. 802.1x Enforcement policy
E. WebAuth Service

Answer: E

Explanation:

Referencehttp://community.arubanetworks.com/t5/Security/Clearpass-Onguard-implementation-and-documentation/td-p/121057

Question No : 8

Which type of ClearPass service is used to process health checks from the OnGuard agent?

A. WebAuth

B. RADIUS
C. TACACS
D. HTTP
E. AppAuth

Answer: A

Explanation:

Referencehttps://community.arubanetworks.com/aruba/attachments/aruba/aaa-nac-guest-access-byod/21122/1/OnGuard%20config%20Tech%20Note%20v1.pdf

Question No : 9

What is the purpose of the pre-auth check during guest authentication?

A. for the NAD device to do an internal authentication check before sending the credentials to ClearPass
B. for the NAD device to check that ClearPass is active before sending it the RADIUS request
C. for ClearPass to do aninternal authentication check before the NAS login happens
D. for the client device to do an internal sanity check before the NAS login occurs
E. for the client device to check that ClearPass is active before sending it the credentials

Answer: C

Explanation:

Explanation

The way NAS devices like wireless controllers do authentication on external captive portals only allowsstandard reject message handlinglike "authentication failed".The pre auth check allows CPPM to provide advanced error handling of a reject like "your time limit has been reached" before a user logs in. It is to do an end run around limited error handing of NAS devices on external captive portals.

Referencehttps://community.arubanetworks.com/t5/Security/why-use-pre-auth-check/m-p/93254

Question No : 10

What is Radius CoA used for?

A. to validate a host MAC against a white and a black list
B. to force the client to re-authenticate upon roaming to a new controller
C. to authenticate users or devices before granting them access to a network
D. to transmit messages to the NAD/NAS to modify a user’s session status
E. to apply firewall policies based on authentication credentials

Answer: B

Explanation:

Referencehttp://www.arubanetworks.com/techdocs/ClearPass/Aruba_CPPMOnlineHelp/Content/CPPM_UserGuide/Enforce/EPRADIUS_CoA.htm