HPE6-A15 Q&As

Aruba Certified Clearpass Professional 6.5

Pass HP HPE6-A15 Exam with 100% Guarantee

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

https://www.leads4pass.com/hpe6-a15.html

100% Passing Guarantee
100% Money Back Assurance

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

QUESTION 1

A customer would like to deploy ClearPass with these requirements: every day, 100 employees need to authenticate with their corporate laptops using EAP-TLS every Friday, a meeting with business partners takes place and an additional 50 devices need to authenticate using Web Login Guest Authentication

What should the customer do regarding licenses? (Select two.)

A. When counting policy manager licenses, include the additional 50 business partner devices.

B. When counting policy manager licenses, exclude the additional 50 business partner devices.

C. Purchase Onboard licenses.

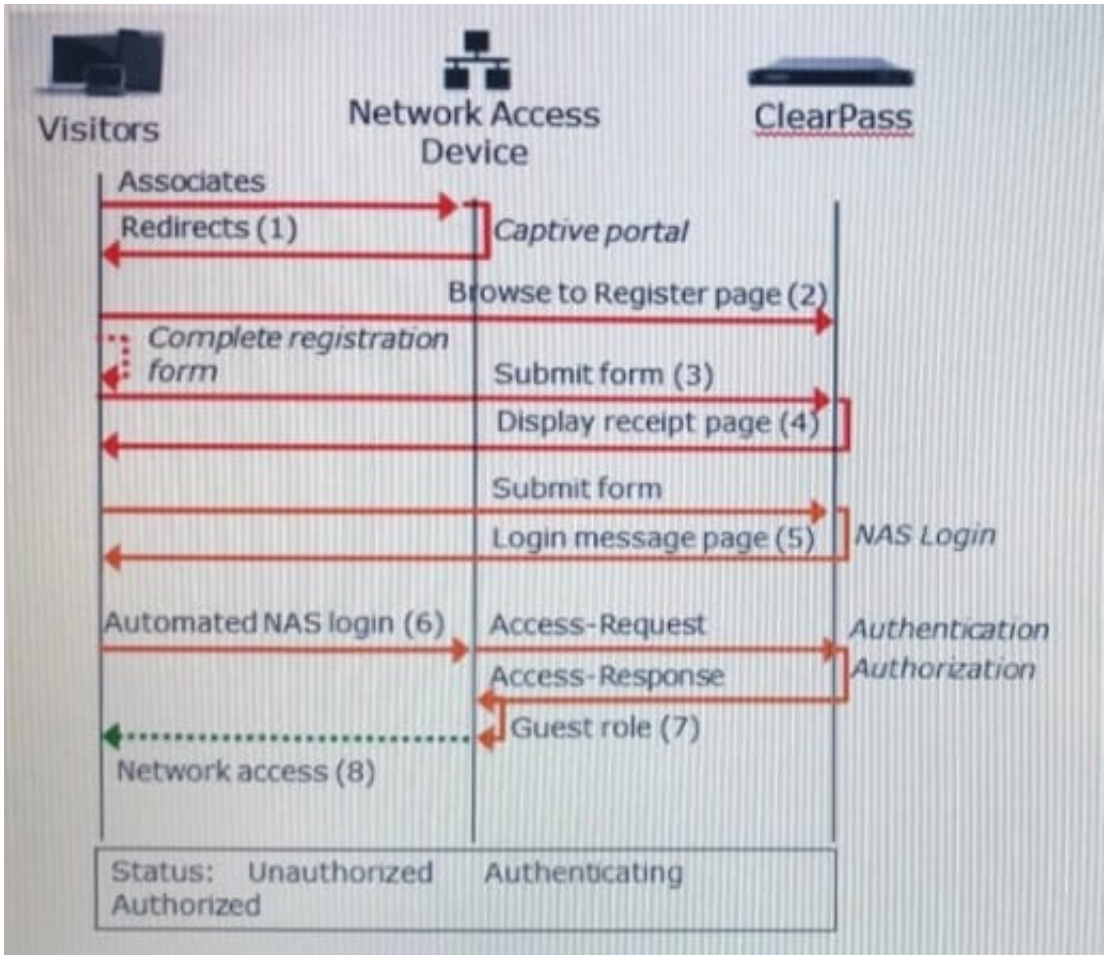
D. Purchase guest licenses.

E. Purchase Onguard licenses.

Correct Answer: AC

QUESTION 2

Refer to the exhibit.



Based on the guest Self-Registration with Sponsor Approval workflow shown, at which stage is an email request sent to the sponsor?

A. after `Guest Role (7)\\'

B. after `Login Message page (5)\\'

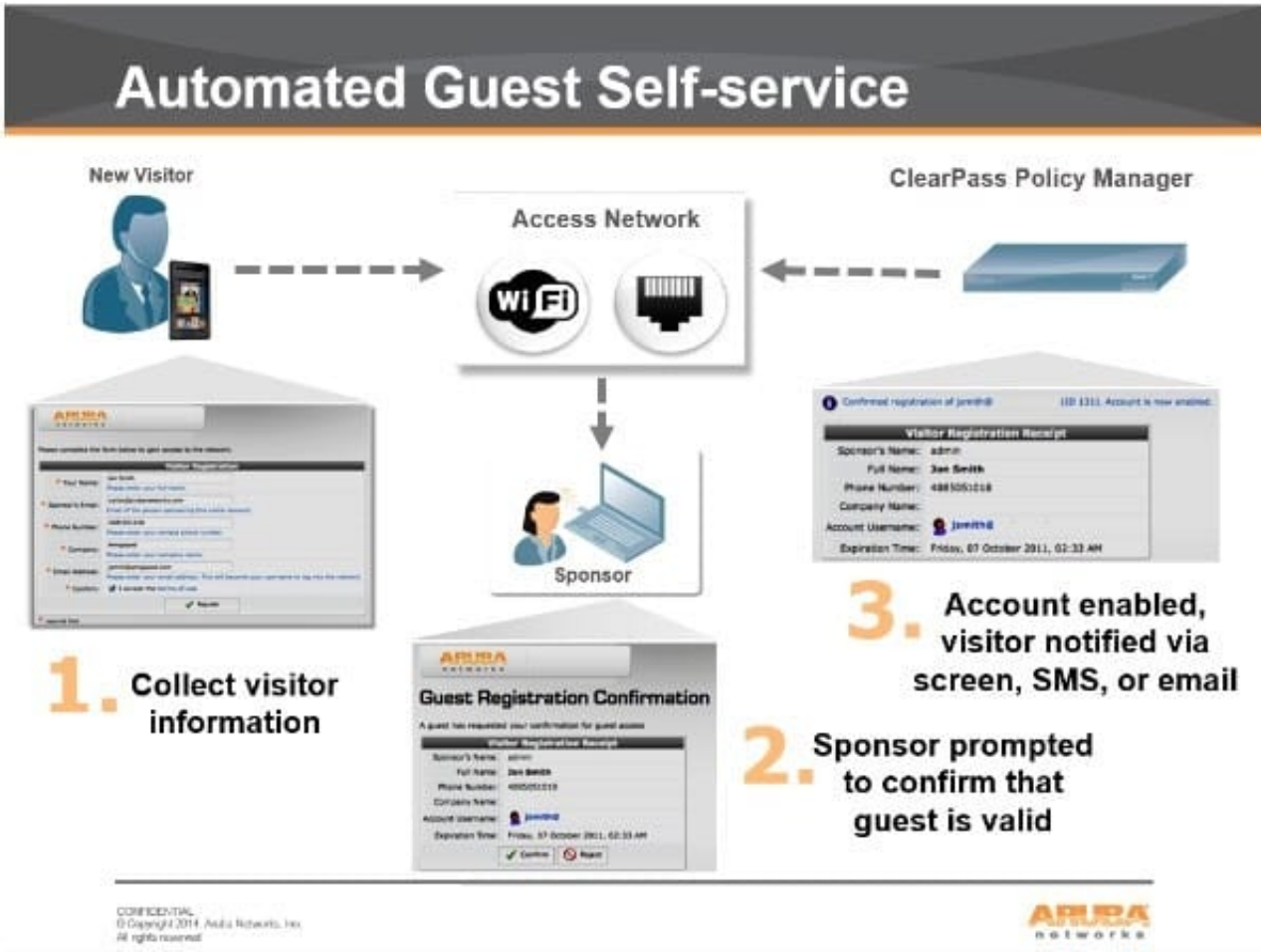
C. after `Submit form (3)\\'

D. after `Automated NAS login (6)\\'

E. after `Redirects (1)\\'

Correct Answer: C

There\\'s the Self Service part of provisioning one\\'s information. Then the sponsor/operator part to confirm that guest is valid. Then the enablement via the sponsor/operator clicking \\'confirm\\'.



References: https://community.arubanetworks.com/t5/Security/Guest-Captive-Portal-sponsor-approval-architecture/td-p/267625

QUESTION 3

What must be configured to enable RADIUS authentication with ClearPass on a network access device (NAD)? (Select two.)

A. the ClearPass server must have the network device added as a valid NAD

B. the ClearPass server certificate must be installed on the NAD

C. a matching shared secret must be configured on both the ClearPass server and NAD

D. an NTP server needs to be set up on the NAD

E. a bind username and bind password must be provided

Correct Answer: AC

QUESTION 4

An administrator enabled the Pre-auth check for their guest self-registration.

At what stage in the registration process in this check performed?

A. after the user clicks the login button and after the NAD sends an authentication request

B. after the user self-registers but before the user logs in

C. after the user clicks the login button but before the NAD sends an authentication request

D. when a user is re-authenticating to the network

E. before the user self-registers

Correct Answer: C

The Onboard template is designed for configuration that allows to perform checks before allowing Onboard provisioning for Bring Your Own Device (BYOD) use-cases. This service creates an Onboard Pre-Auth service to check the user\\'s credentials before starting the device provisioning process. This also creates an authorization service that checks whether a user\\'s device can be provisioned using Onboard.

QUESTION 5

A customer wants all guests who access a company\\'s guest network to have their accounts approved by the receptionist, before they are given access to the network. How should the network administrator set this up in ClearPass? (Select two.)

A. Enable sponsor approval confirmation in Receipt actions.

B. Configure SMTP messaging in the Policy Manager.

C. Configure a MAC caching service in the Policy Manager.

D. Configure a MAC auth service in the Policy Manager.

E. Enable sponsor approval in the captive portal authentication profile on the NAD.

Correct Answer: AD

A: Sponsored self-registration is a means to allow guests to self-register, but not give them full access until a sponsor (could even be a central help desk) has approved the request. When the registration form is completed by the guest/user, an on screen message is displayed for the guest stating the account requires approval.

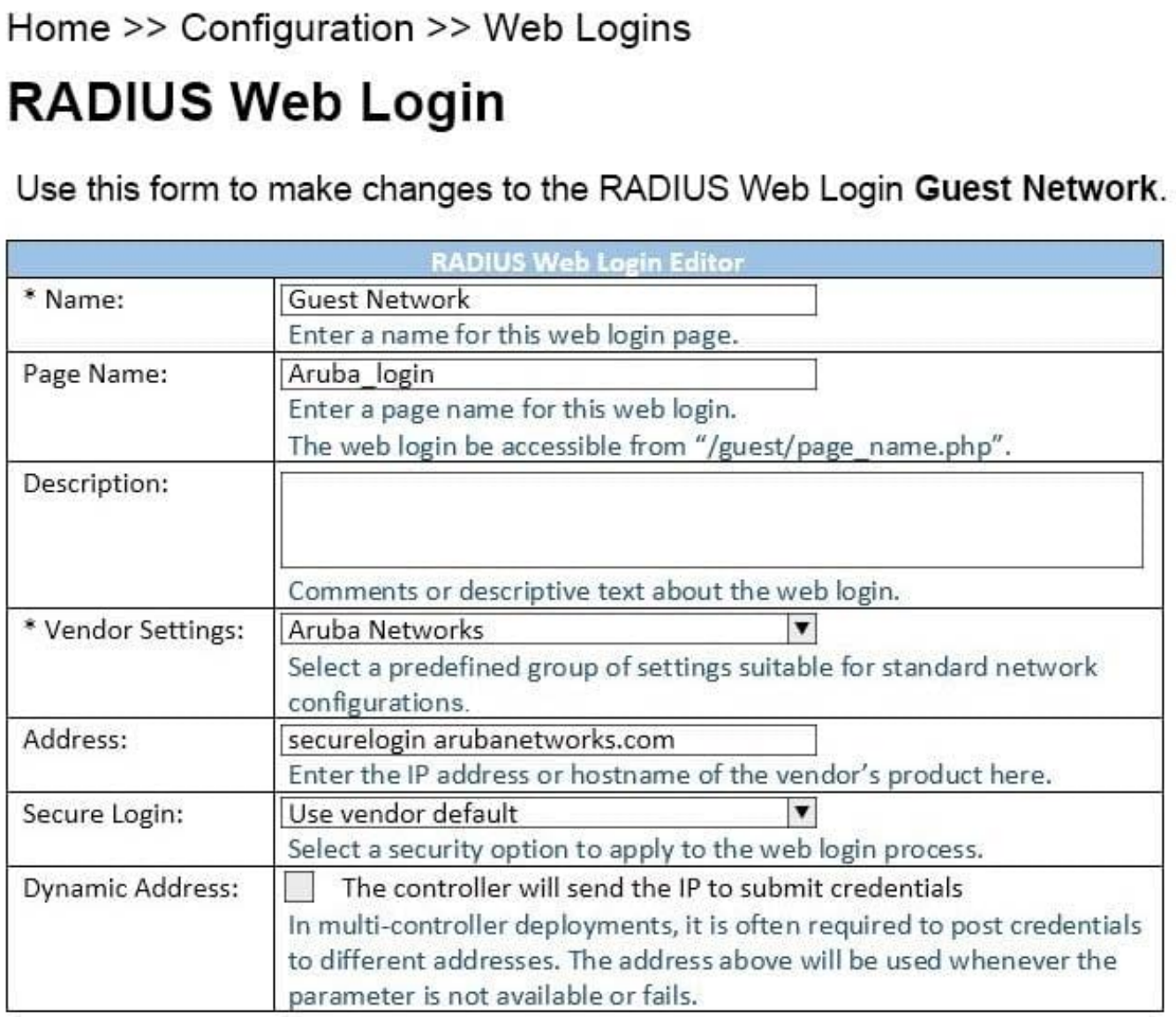
Guests are disabled upon registration and need to wait on the receipt page for the confirmation until the login button gets enabled.

D. Device Mac Authentication is designed for authenticating guest devices based on their MAC address.

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 94 https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 6

Refer to the exhibit.



When configuring a Web Login Page in ClearPass Guest, the information shown is displayed. What is the page name field used for?

A. for forming the Web Login Page URL

B. for Administrators to access the PHP page, but not guests

C. for Administrators to reference the page only

D. for forming the Web Login Page URL where Administrators add guest users

E. for informing the Web Login Page URL and the page name that guests must configure on their laptop wireless supplicant.

Correct Answer: A

The Page Name is an identifier page name that will appear in the URL -- for example, "/guest/page_name.php".

References: http://www.arubanetworks.com/techdocs/ClearPass/CPGuest_UG_HTML_6.5/Content/Configuration/CreateEditWebLogin.htm

QUESTION 7

Which use cases will require a ClearPass Guest application license? (Select two.)

A. Guest device fingerprinting

B. Guest endpoint health assessment

C. Sponsor based guest user access

D. Guest user self-registration for access

E. Guest personal device onboarding

Correct Answer: CD

QUESTION 8

Refer to the exhibit.

Based on the Enforcement Profile configuration shown, which statement accurately describes what is sent?

A. A limited access VLAN value is sent to the Network Access Device.

B. An unhealthy role value is sent to the Network Access Device.

C. A message is sent to the Onguard Agent on the client device.

D. A RADIUS CoA message is sent to bounce the client.

E. A RADIUS access-accept message is sent to the Controller

Correct Answer: C

The OnGuard Agent enforcement policy retrieves the posture token. If the token is HEALTHY it returns a healthy message to the agent and bounces the session. If the token is UNHEALTHY it returns an unhealthy message to the agent and bounces the session.

References: CLEARPASS ONGUARD CONFIGURATION GUIDE (July 2015), page 27

QUESTION 9

Why is a terminate session enforcement profile used during posture checks with 802.1x authentication?

A. To send a RADIUS CoA message from the ClearPass server to the client

B. To disconnect the user for 30 seconds when they are in an unhealthy posture state

C. To blacklist the user when they are in an unhealthy posture state

D. To force the user to re-authenticate and run through the service flow again

E. To remediate the client applications and firewall do that updates can be installed

Correct Answer: A

QUESTION 10

When a third party Mobile Device Management server is integrated with ClearPass, where is the endpoint information from the MDM server stored in ClearPass?

A. Endpoints repository

B. Onboard Device repository

C. MDM repository

D. Guest User repository

E. Local User repository

Correct Answer: A

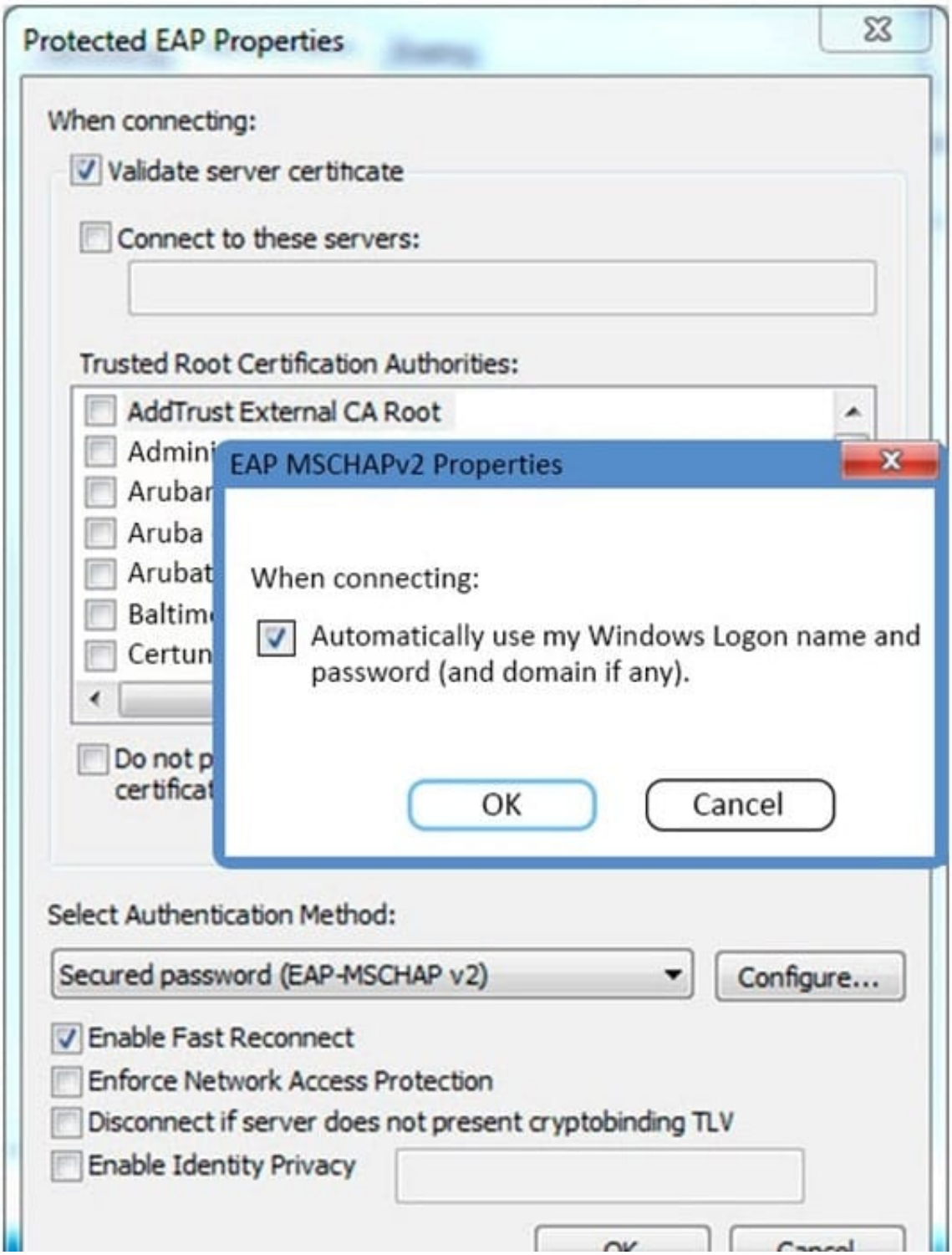
A service running in CPPM periodically polls MDM servers using their exposed APIs. Device attributes obtained from MDM are added as endpoint tags. Profiler related attributes are send to profiler which uses these attributes to derive final profile.

References: ClearPass Profiling TechNote (2014), page 23 https://community.arubanetworks.com/aruba/attachments/aruba/ForoenEspanol/653/1/ClearPass%20Profiling%20TechNote.pdf

QUESTION 11

Refer to the exhibit.

Based on the configuration of a Windows 802.1X supplicant shown, what will be the outcome when `Automatically use my Windows logon name and password\\' are selected?



A. The client will use machine authentication.

B. The client\\'s Windows login username and password will be sent inside a certificate to the Active Directory server.

C. The client\\'s Windows login username and password will be sent to the Authentication server.

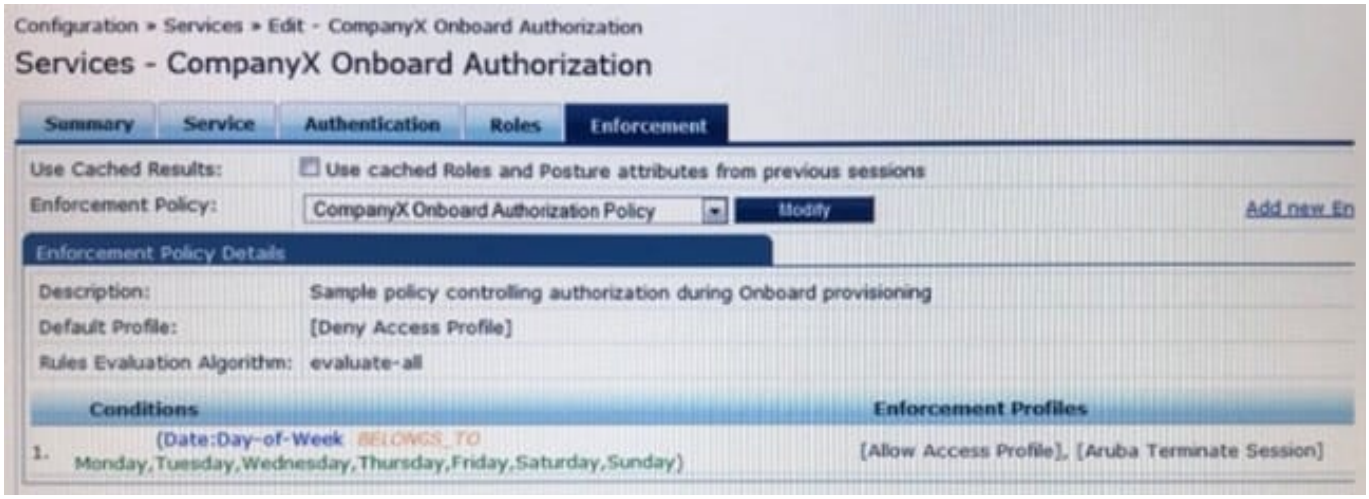
D. The client will need to re-authenticate every time they connect to the network.

E. The client will prompt the user to enter the logon username and password.

Correct Answer: C

QUESTION 12

Refer to the exhibit.



Based on the configuration of the Enforcement Profiles in the Onboard Authorization service shown, which Onboarding action will occur?

A. The device will be disconnected from the network after Onboarding so that an EAP-TLS authentication is not performed.

B. The device will be disconnected from and reconnected to the network after Onboarding is completed.

C. The device\\'s onboard authorization request will be denied.

D. The device will be disconnected after post-Onboarding EAP-TLS authentication, so a second EAP-TLS authentication is performed.

E. After logging in on the Onboard web login page, the device will be disconnected form and reconnected to the network before Onboard begins.

Correct Answer: B

QUESTION 13

Which CLI command is used to upgrade the image of a ClearPass server?

A. Image update

B. System upgrade

C. Upgrade image

D. Reboot

E. Upgrade software

Correct Answer: B

When logged in as appadmin, you can manually install the Upgrade and Patch binaries imported via the CLI using the following commands:

*

system update (for patches)

*

system upgrade (for upgrades)

References: ClearPass Policy Manager 6.5 User Guide (October 2015), page 564 https://community.arubanetworks.com/aruba/attachments/aruba/SoftwareUserReferenceGuides/52/1/ClearPass%20Policy%20Manager%206.5%20User%20Guide.pdf

QUESTION 14

A customer wants to implement Virtual IP redundancy, such that in case of a ClearPass server outage, 802.1x authentications will not be interrupted. The administrator has enabled a single Virtual IP address on two ClearPass servers.

Which statements accurately describe next steps? (Select two.)

A. The NAD should be configured with the primary node IP address for RADIUS authentication on the 802.1x network.

B. A new Virtual IP address should be created for each NAD.

C. Both the primary and secondary nodes will respond to authentication requests sent to the Virtual IP address when the primary node is active.

D. The primary node will respond to authentication requests sent to the Virtual IP address when the primary node is active.

E. The NAD should be configured with the Virtual IP address for RADIUS authentications on the 802.1x network.

Correct Answer: DE

In an Aruba network, APs are controlled by a controller. The APs tunnel all data to the controller for processing, including encryption/decryption and bridging/forwarding data. Local controller redundancy provides APs with failover to a backup controller if a controller becomes unavailable. Local controller redundancy is provided by running VRRP between a pair of controllers. The APs are then configured to connect to the "virtual-IP" configured for the VRRP instance.

References: http://www.arubanetworks.com/techdocs/ArubaOS_64x_WebHelp/Content/ArubaFrameStyles/VRRP/Redundancy_Parameters.htm

QUESTION 15

Which steps are required to use ClearPass as a TACACS+ Authentication server for a network device? (Select two.)

A. Configure a TACACS Enforcement Profile on ClearPass for the desired privilege level.

B. Configure a RADIUS Enforcement Profile on ClearPass for the desired privilege level.

C. Configure ClearPass as an Authentication server on the network device.

D. Configure ClearPass roles on the network device.

E. Enable RADIUS accounting on the NAD.

Correct Answer: AC

You need to make sure you modify your policy (Configuration ?Enforcement ?Policies ?Edit - [Admin Network Login Policy]) and add your AD group settings in to the corresponding privilege level.