



HPE6-A68^{Q&As}

Aruba Certified ClearPass Professional (ACCP) V6.7

Pass HP HPE6-A68 Exam with 100% Guarantee

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

<https://www.geekcert.com/hpe6-a68.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

Refer to the exhibit.

Monitoring » Event Viewer

Event Viewer

Filter: Source contains RADIUS [Go] [Clear Filter]

#	Source	Level	Category
1.	RADIUS	ERROR	Authentication

System Event Details

Source	RADIUS
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	May 09, 2013 23:29:31 UTC
Level	ERROR
Category	Authentication
Action	Unknown
Timestamp	May 09, 2013 23:29:31 UTC
Description	Received packet from 10.8.10.100 with invalid Message-Authenticator! (Shared secret is incorrect.)

[Close]

The ClearPass Event Viewer displays an error when a user authenticates with EAP-TLS to ClearPass through an Aruba Controller Wireless Network. What is the cause of this error?

- A. The controller's shared secret used during the certificate exchange is incorrect.
- B. The NAS source interface IP is incorrect.
- C. The client sent an incorrect shared secret for the 802.1X authentication.
- D. The controller used an incorrect shared secret for the RADIUS authentication.
- E. The client's shared secret used during the certificate exchange is incorrect.

Correct Answer: D

QUESTION 2

Refer to the exhibit.



Monitoring & Reporting » Live Monitoring » Access Tracker

Access Tracker

Jul 12, 2012 10:26:39 PDT

Data Filter: [All Requests] Server: Clearpass6 (10.254.1.176)

Date Range: Last 1 day before Today

Filter: Type contains [] + Go Clear Filter Show 10 records

Server	Type	User	Service Name	Login	Date
10.254.1.176	RADIUS	BC705A065CF0		REJECT	2012/07/12

Request Details

Summary Input Output Alerts

Error Code: 204

Error Category: Authentication failure

Error Message: Failed to classify request to service

Alerts for this Request

RADIUS Service Categorization failed

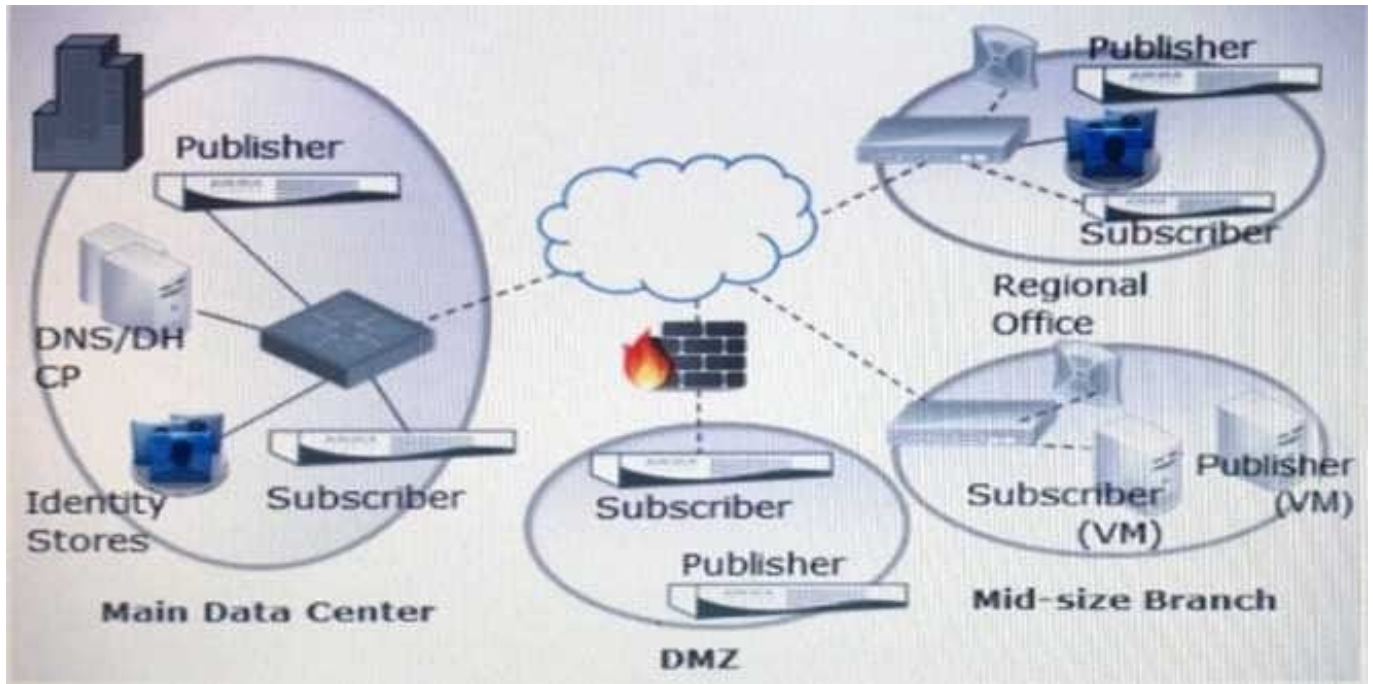
What can be concluded from the Access Tracker output shown?

- A. The client used incorrect credentials to authenticate to the network.
- B. ClearPass does not have a service enabled for MAC authentication.
- C. The client MAC address is not present in the Endpoints table in the ClearPass database.
- D. The RADIUS client on the Windows server failed to categorize the service correctly.
- E. The client wireless profile is incorrectly setup.

Correct Answer: B

QUESTION 3

Refer to the exhibit.



A customer wants to enable Publisher redundancy.

Based on the network topology diagram shown, which node should the network administrator configure as the standby Publisher for the Publisher in the main data center?

- A. Subscriber in the main data center
- B. Publisher in the regional office
- C. Any of the other three Publishers
- D. Publisher in the mid-size branch
- E. Publisher in the DMZ

Correct Answer: A

ClearPass Policy Manager allows you to designate one of the subscriber nodes in a cluster to be the Standby Publisher, thereby providing for that subscriber node to be automatically promoted to active Publisher status in the event that the Publisher goes out of service. This ensures that any service degradation is limited to an absolute minimum.

References: http://www.arubanetworks.com/techdocs/ClearPass/Aruba_DeployGd_HTML/Content/5%20Cluster%20Deployment/Standby_publisher.htm

QUESTION 4

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:

1.
system update (for patches)
2.
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 5

In a single SSID Onboarding, which method can be used in the Enforcement Policy to distinguish between a provisioned device and a device that has not gone through the Onboard workflow?

- A. Active Directory Attributes
- B. Network Access Device used
- C. Endpoint OS Category
- D. Onguard Agent used
- E. Authentication Method used

Correct Answer: E

[HPE6-A68 PDF Dumps](#)

[HPE6-A68 Exam Questions](#)

[HPE6-A68 Braindumps](#)