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.geekcert.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 would like to allow only the AD users with the "Manager" title from the "HQ" location to Onboard their personal devices. Any other AD users should not be authorized to pass beyond the initial device provisioning page.

Which Onboard service will you use to implement this requirement?

A. Onboard CP login service

B. Onboard Authorization service

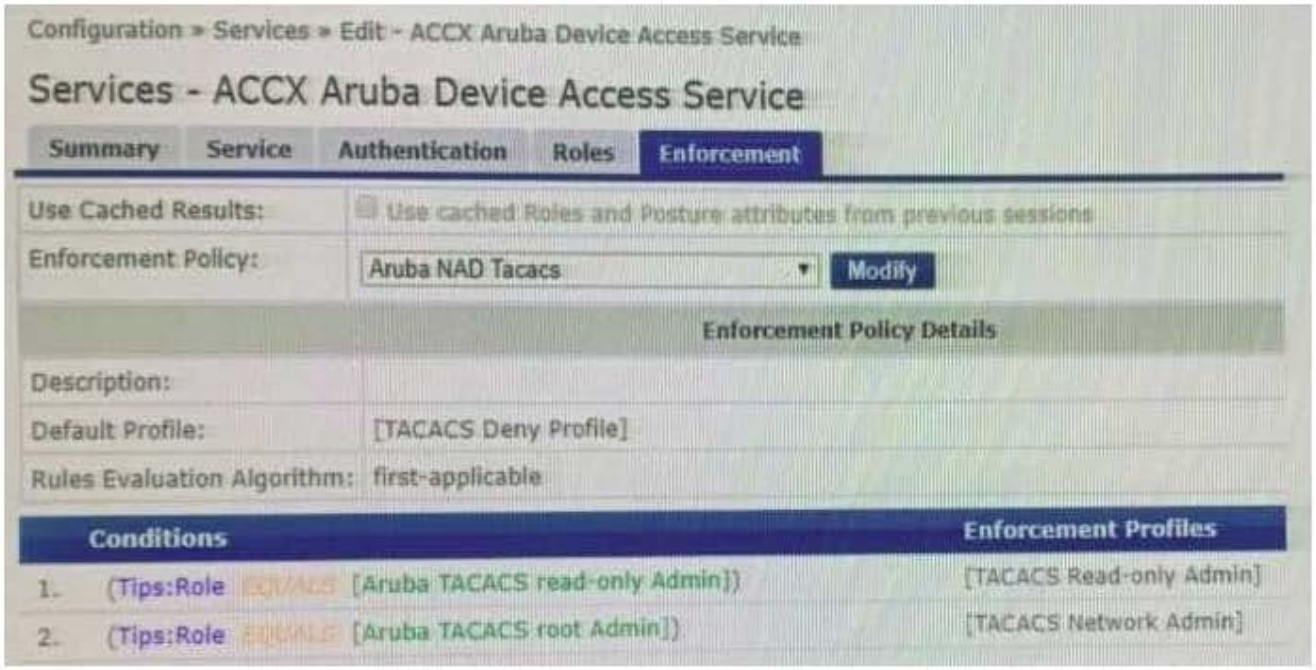
C. Onboard Provisioning service

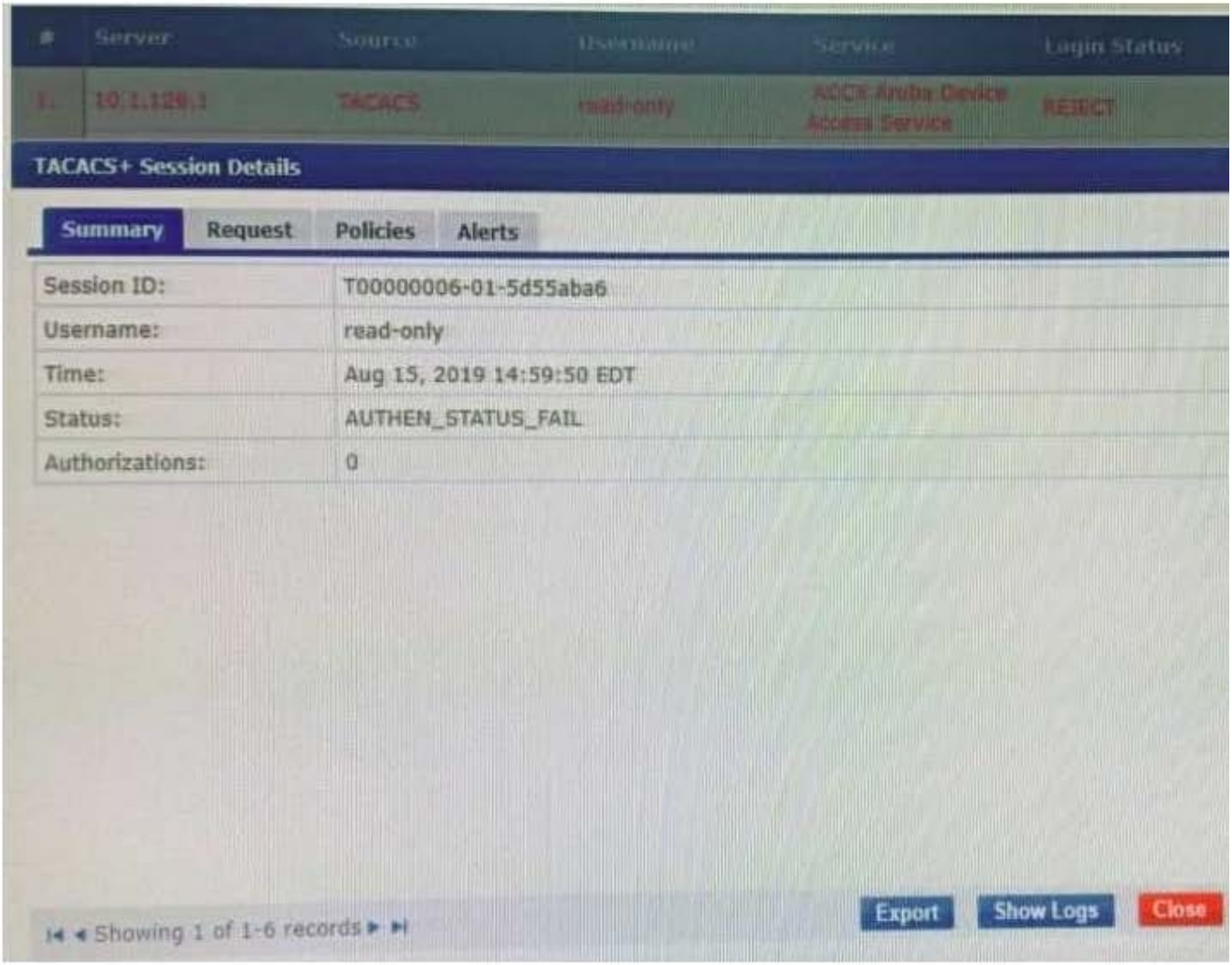
D. Onboard Pre-Auth service

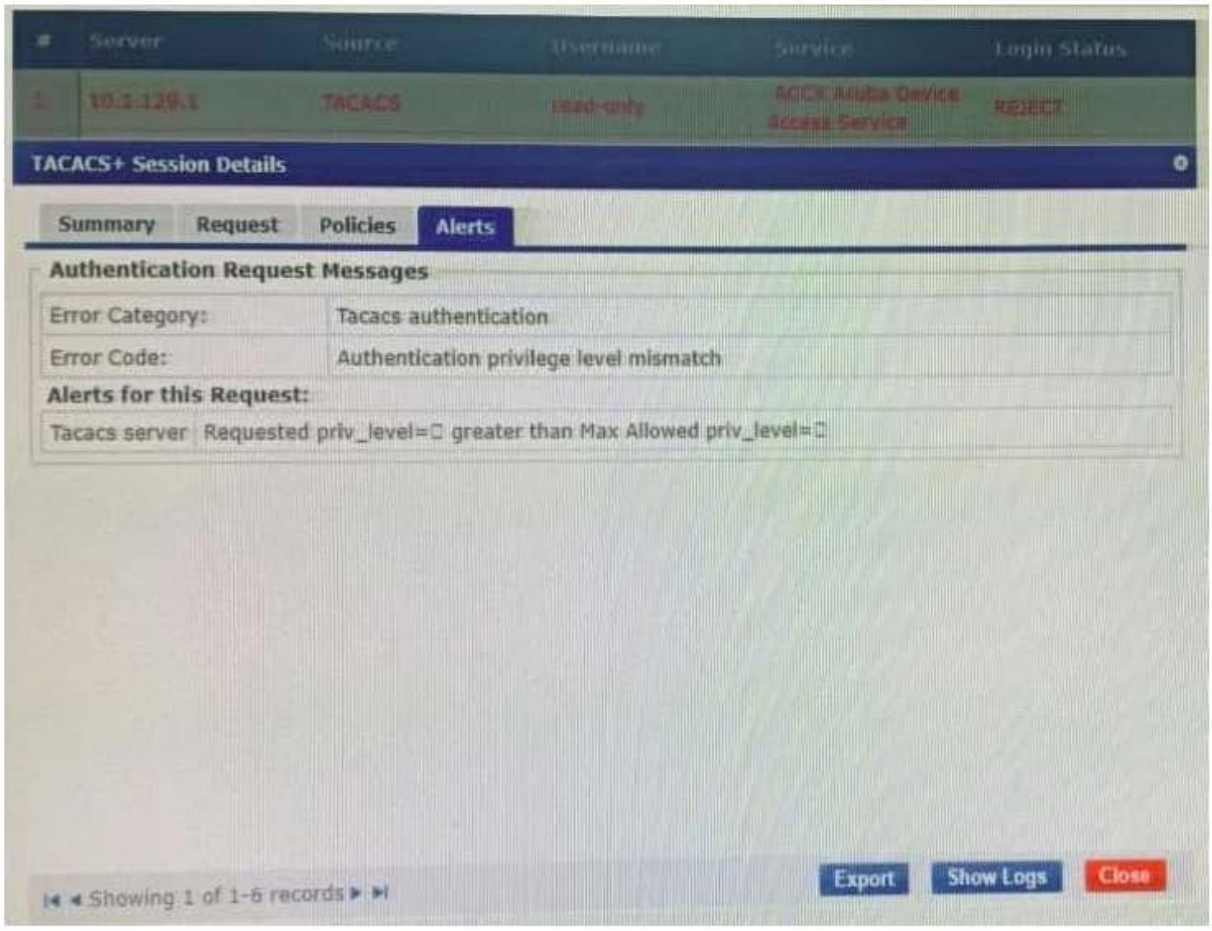
Correct Answer: A

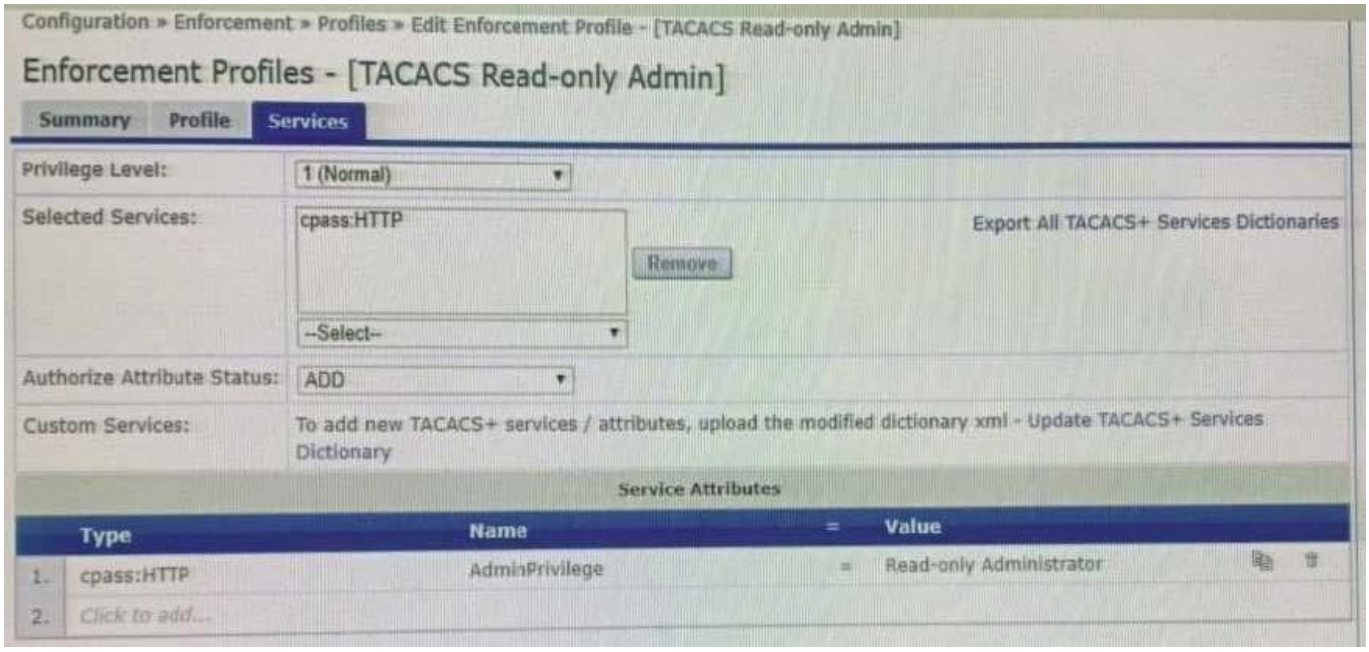
QUESTION 2

Refer to the exhibit:


Configuration » Services » Edit - ACCX Aruba Device Access Service
Services - ACCX Aruba Device Access Service
Summary
Service
Authentication
Roles
Enforcement
Use Cached Results:
Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:
Aruba NAD Tacacs
Modify
Enforcement Policy Details
Description:
Default Profile:
[TACACS Deny Profile]
Rules Evaluation Algorithm:
first-applicable
Conditions
Enforcement Profiles
1. (Tips:Role [Aruba TACACS read-only Admin])
[TACACS Read-only Admin]
2. (Tips:Role [Aruba TACACS root Admin])
[TACACS Network Admin]


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Session ID:
T00000006-01-5d55aba6
Username:
read-only
Time:
Aug 15, 2019 14:59:50 EDT
Status:
AUTHEN_STATUS_FAIL
Authorizations:
0
Showing 1 of 1-6 records
Export
Show Logs
Close


Server
Source
Username
Service
Login Status
TACACS
read-only
REJECT
TACACS+ Session Details
Summary
Request
Policies
Alerts
Authentication Request Messages
Error Category:
Tacacs authentication
Error Code:
Authentication privilege level mismatch
Alerts for this Request:
Tacacs server
Requested priv_level=□ greater than Max Allowed priv_level=□
Showing 1 of 1-6 records
Export
Show Logs
Close



A customer is trying to configure a TACACS Authentication Service for administrative access to the Aruba Controller, During testing the authentication is not successful.

Given the screen shot what could be the reason for the Login status REJECT?

A. The password used by the administrative user, user is wrong.

B. The Enforcement profile is not designed to be used on Aruba Controller.

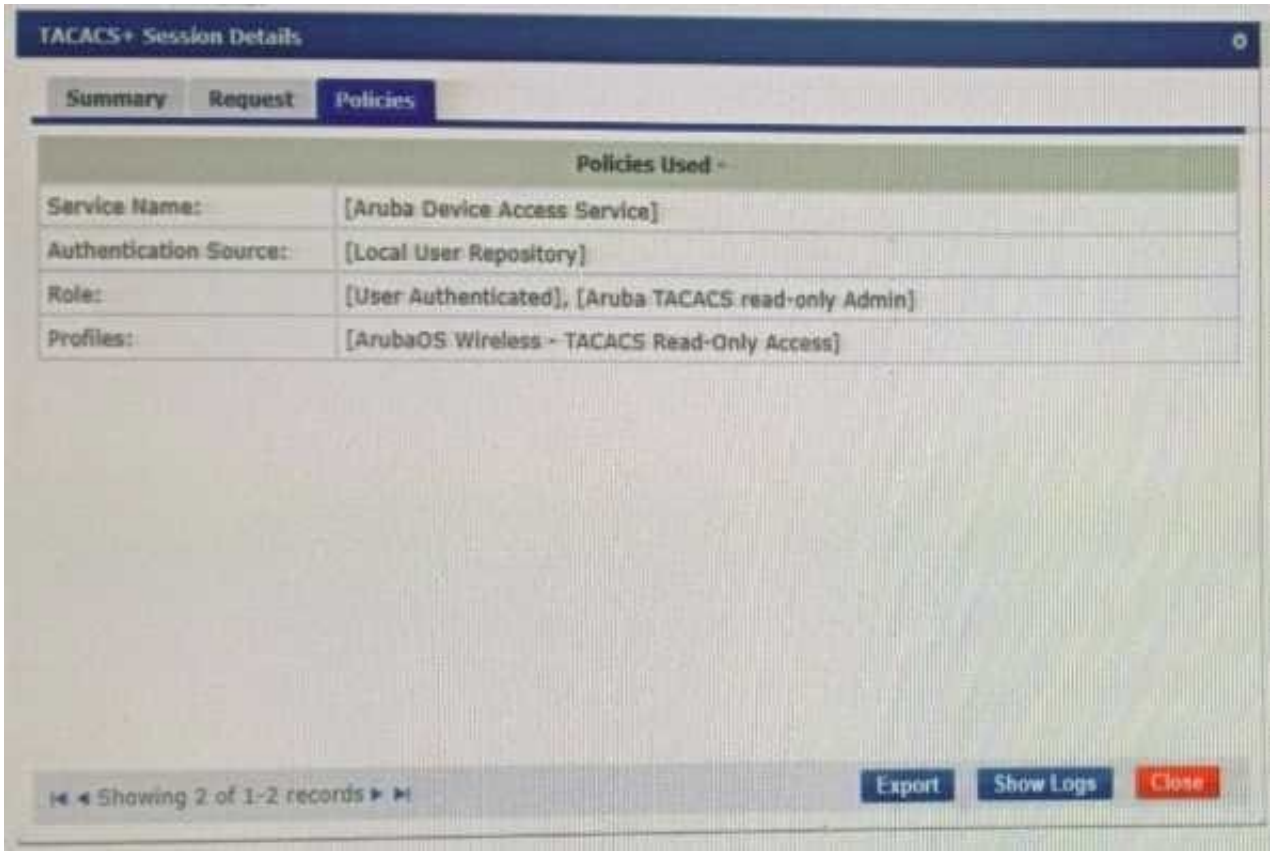
C. The Read-only Administrator role does not exist on the Controller.

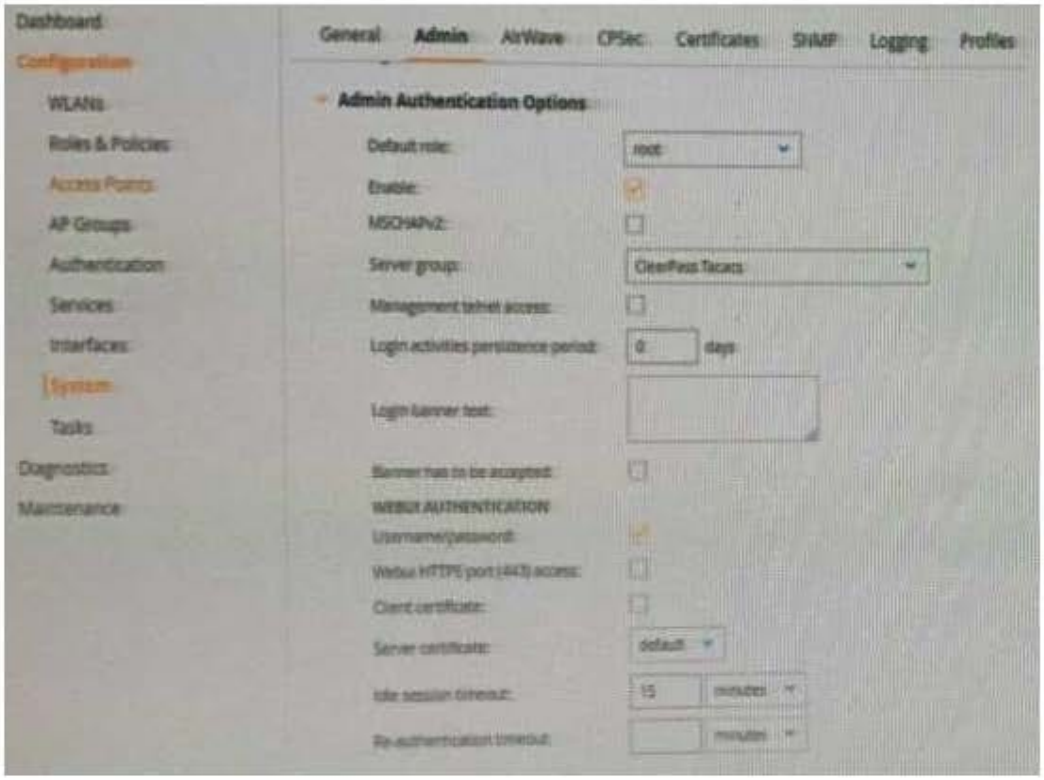
D. The Enforcement profile used is not a TACACS profile.

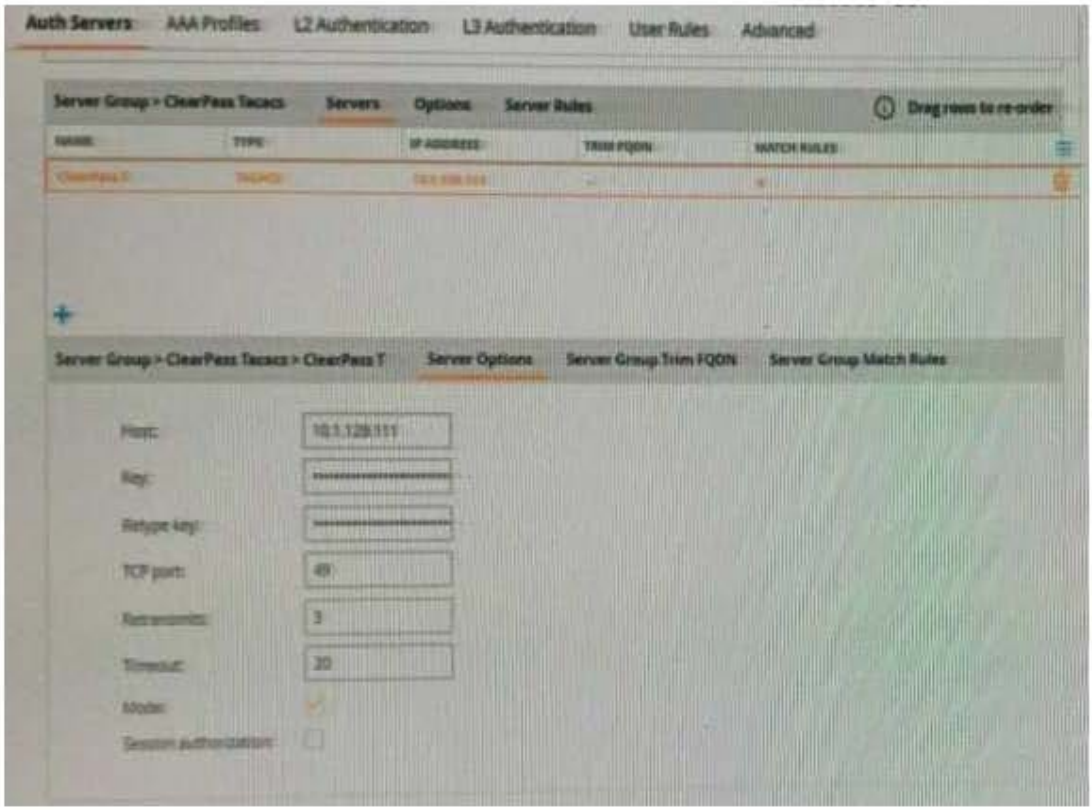
Correct Answer: A

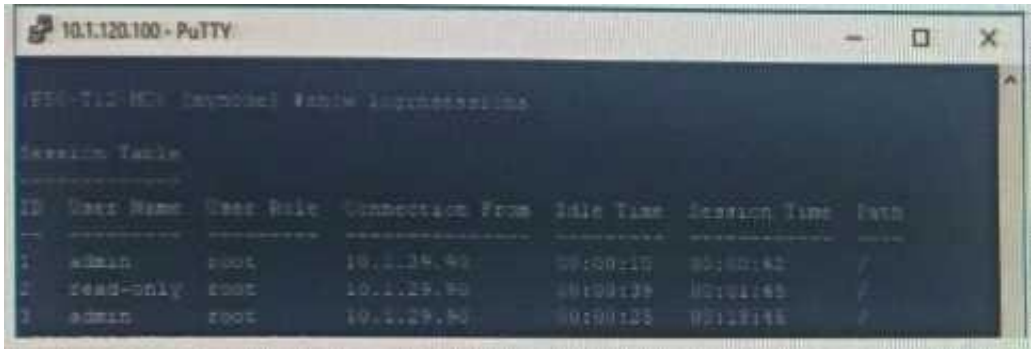
QUESTION 3

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:
MSCHAPv2:
Server group:
ClearPass Tacacs
Management telnet access:
Login activities persistence period:
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:
minutes
Re-authentication timeout:
minutes


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
TRIM FQDN
MATCH RULES
Server Group > ClearPass Tacacs > ClearPass T
Server Options
Server Group Trim FQDN
Server Group Match Rules
Host:
10.1.128.111
Key:
Retype key:
TCP port:
49
Retransmits:
3
Timeout:
20
Mode:
Session authentication:



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 Controllers Admin Authentication Options Default role is mapped to toot.

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 TACAC$ authentication server Is not configured for Session authorization

Correct Answer: CE

QUESTION 4

How does the RadSec improve the RADIUS message exchange? (Select two.)

A. It can be used on an unsecured network or the Internet.

B. It builds a TTLS tunnel between the NAD and ClearPass.

C. Only the NAD needs to trust the ClearPass Certificate.

D. It encrypts the entire RADIUS message.

E. It uses UDP to exchange the radius packets.

Correct Answer: DE

QUESTION 5

What is the Open SSID (otherwise referred to as Dual SSID) Onboard deployment service workflow?

A. OnBoard Pre-Auth Application service, OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

B. OnBoard Pre-Auth RADIUS service. OnBoard Authorization Application service. OnBoard Provisioning RADIUS service

C. OnBoard Authorization Application service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

D. OnBoard Authorization RADIUS service, OnBoard Pre-Auth Application service, OnBoard Provisioning RADIUS service

Correct Answer: C