



NSE7_SAC-6.2^{Q&As}

Fortinet NSE 7 - Secure Access 6.2

Pass Fortinet NSE7_SAC-6.2 Exam with 100% Guarantee

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

https://www.pass4itsure.com/nse7_sac-6-2.html

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by Fortinet
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.

Examine the partial debug output shown in the exhibit.

```
FortiGate # diagnose test authserver ldap Training-Lab student password
[2168] handle_req-Rcvd auth req 1584903618 for student in Training-Lab opt=0000001b prot=0
[358] __compose_group_list_from_req-Group 'Training-Lab'
[608] fnbamd_pop3_start-student
[1038] __fnbamd_cfg_get_ldap_list_by_server-Loading LDAP server 'Training-Lab'
[1544] fnbamd_ldap_init-search filter is: sAMAccountName=student
[1553] fnbamd_ldap_init-search base is: cn=users,dc=trainingad,dc=training,dc=lab
[973] __fnbamd_ldap_dns_cb-Resolved Training-Lab(idx 0) to 10.0.1.10
[1021] __fnbamd_ldap_dns_cb-Still connecting.
[517] create_auth_session-Total 1 server(s) to try
[939] __ldap_connect-tcps_connect(10.0.1.10) is established.
[814] __ldap_rxtx-state 3(Admin Binding)
[196] __ldap_build_bind_req-Binding to 'CN=Administrator,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 80 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 1
[814] __ldap_rxtx-state 4(Admin Bind resp)
[1056] fnbamd_ldap_rcv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:1, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'DN search'
[814] __ldap_rxtx-state 11(DN search)
[584] fnbamd_ldap_build_dn_search_req-base:'cn=users,dc=trainingad,dc=training,dc=lab' filter:sAMAccountName=student
[852] fnbamd_ldap_send-sending 99 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 2
[814] __ldap_rxtx-state 12(DN search resp)
[1056] fnbamd_ldap_rcv-Response len: 69, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-entry
[791] fnbamd_ldap_parse_response-ret=0
[1095] __fnbamd_ldap_dn_entry-Get DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[90] ldap_dn_list_add-added CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab
[1056] fnbamd_ldap_rcv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:2, type:search-result
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'User Binding'
[814] __ldap_rxtx-state 5(User Binding)
[429] fnbamd_ldap_build_userbind_req-Trying DN 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[196] __ldap_build_bind_req-Binding to 'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab'
[852] fnbamd_ldap_send-sending 105 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 3
[814] __ldap_rxtx-state 6(User Bind resp)
[1056] fnbamd_ldap_rcv-Response len: 16, svr: 10.0.1.10
[756] fnbamd_ldap_parse_response-Got one MESSAGE. ID:3, type:bind
[791] fnbamd_ldap_parse_response-ret=0
[881] __ldap_rxtx-Change state to 'Attr query'
[814] __ldap_rxtx-state 7(Attr query)
[482] fnbamd_ldap_build_attr_search_req-Adding attr 'memberOf'
[194] fnbamd_ldap_build_attr_search_req-base:'CN=student,CN=Users,DC=trainingAD,DC=training,DC=lab' filter:cn=*
[852] fnbamd_ldap_send-sending 128 bytes to 10.0.1.10
[864] fnbamd_ldap_send-Request is sent. ID 4
```

Which two statements about the debug output are true? (Choose two.)

- A. The connection to the LDAP server timed out.
- B. The user authenticated successfully.
- C. The LDAP server is configured to use regular bind.
- D. The debug output shows multiple user authentications.

Correct Answer: BC



QUESTION 2

Refer to the exhibit showing certificate values.

Certificate Viewer: "fac.trainingad.training.lab"

General Details

Could not verify this certificate because the issuer is unknown.

Issued To

Common Name (CN)	fac.trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>
Serial Number	01:86:A4

Issued By

Common Name (CN)	trainingad.training.lab
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Period of Validity

Begins On	Thursday, October 17, 2019
Expires On	Tuesday, October 15, 2024

Fingerprints

SHA-256 Fingerprint	B5:42:6C:66:EF:87:25:D4:A7:9A:5F:83:3E:0D:6A:B2: ED:7F:18:0B:27:66:54:61:7B:B0:71:88:04:55:85:4E
SHA1 Fingerprint	0E:77:87:F4:C4:26:0E:60:85:8F:30:AD:CE:9E:06:B7:AC:1F:D4:07

Close

Wireless guest users are unable to authenticate because they are getting a certificate error while loading the captive portal login page. This URL string is the HTTPS POST URL guest wireless users see when attempting to access the network using the web browser:



`https://fac.trainingad.training.com/guests/login/?loginandpost=https://auth.trainingad.training.1ab:1003/fgtauthandmagic=000a038293d1f411andusermac=b8:27:eb:d8:50:02andapmac=70:4c:a5:9d:0d:28andapip=10.10.100.2anduserip=10.0.3.1andssid=Guest03andapname=PS221ETF18000148andbssid=70:4c:a5:9d:0d:30`

Which two settings are the likely causes of the issue? (Choose two.)

- A. The external server FQDN is incorrect.
- B. The FortiGate authentication interface address is using HTTPS.
- C. The wireless user's browser is missing a CA certificate.
- D. The user address is not in DDNS form.

Correct Answer: AC

QUESTION 3

Which statement correctly describes the quest portal behavior on FortiAuthenticator?

- A. Sponsored accounts cannot authenticate using guest portals.
- B. FortiAuthenticator uses POST parameters and a RADIUS client configuration to map the request to a guest portal for authentication.
- C. All guest accounts must be activated using SMS or email activation codes.
- D. All self-registered and sponsored accounts are listed on the local Users GUI page on FortiAuthenticator.

Correct Answer: A

QUESTION 4

An administrator is deploying APs that are connecting over an IPsec network. All APs have been configured to connect to FortiGate manually. FortiGate can discover the APs and authorize them. However, FortiGate is unable to establish CAPWAP tunnels to manage the APs.

Which configuration setting can the administrator perform to resolve the problem?

- A. Decrease the CAPWAP tunnel MTU size for APs to prevent fragmentation.
- B. Enable CAPWAP administrative access on the IPsec interface.
- C. Upgrade the FortiAP firmware image to ensure compatibility with the FortiOS version.
- D. Assign a custom AP profile for the remote APs with the set mpls-connectionoption enabled.

Correct Answer: B



QUESTION 5

Which two EAP methods can use MSCHAPV2 for client authentication? (Choose two.)

- A. PEAP
- B. EAP-TTLS
- C. EAP-TLS
- D. EAP-GTC

Correct Answer: AC

Reference: https://help.fortinet.com/fauth/3-3/Content/FortiAuthenticator%203_3%20Admin%20Guide/500/501_EAP.htm

[Latest NSE7_SAC-6.2 Dumps](#)

[NSE7_SAC-6.2 VCE Dumps](#)

[NSE7_SAC-6.2 Study Guide](#)