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.passapply.com/nse7_sac-6-2.html

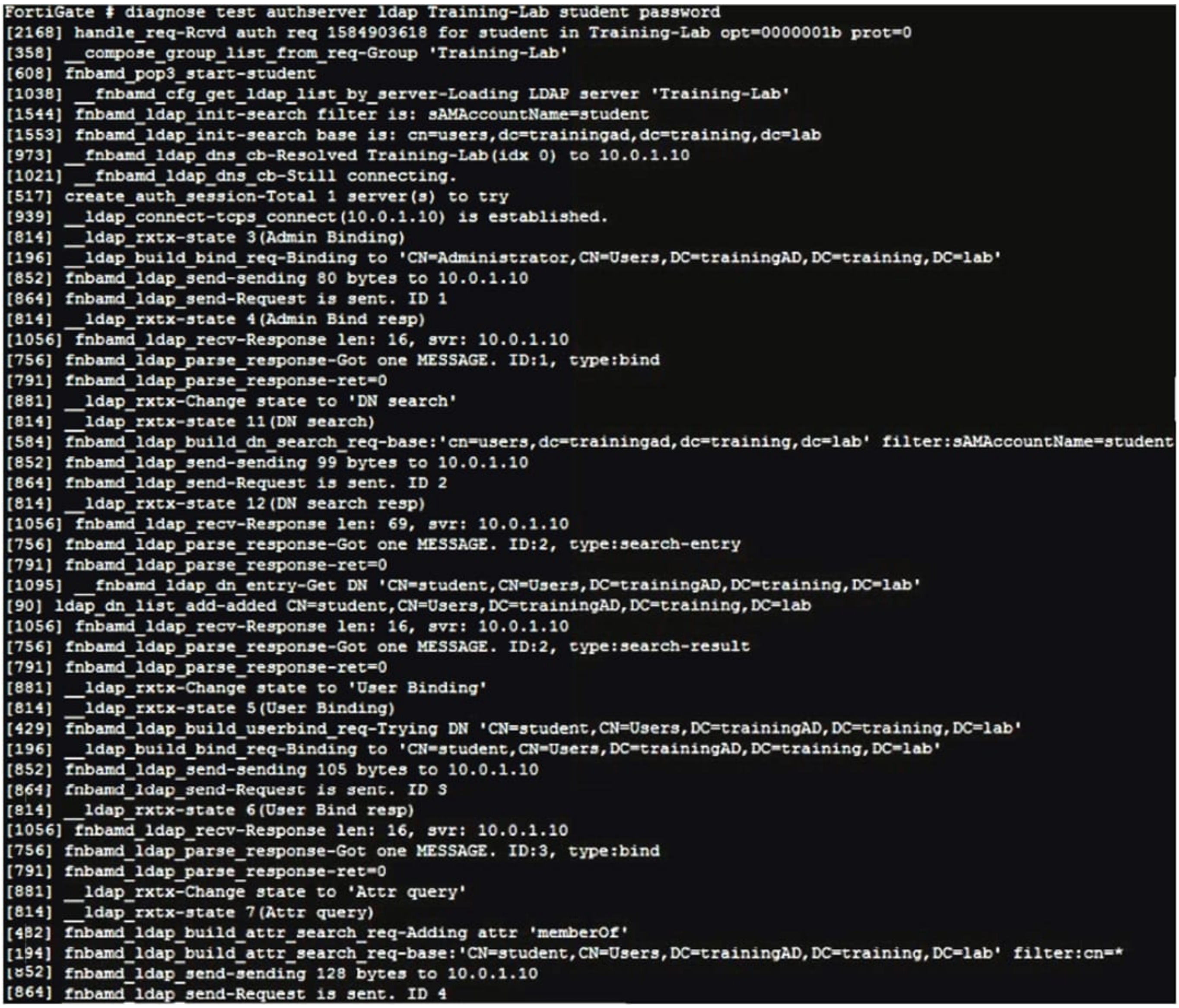
100% Passing Guarantee
100% Money Back Assurance

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

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_recv-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_recv-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_recv-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_recv-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.

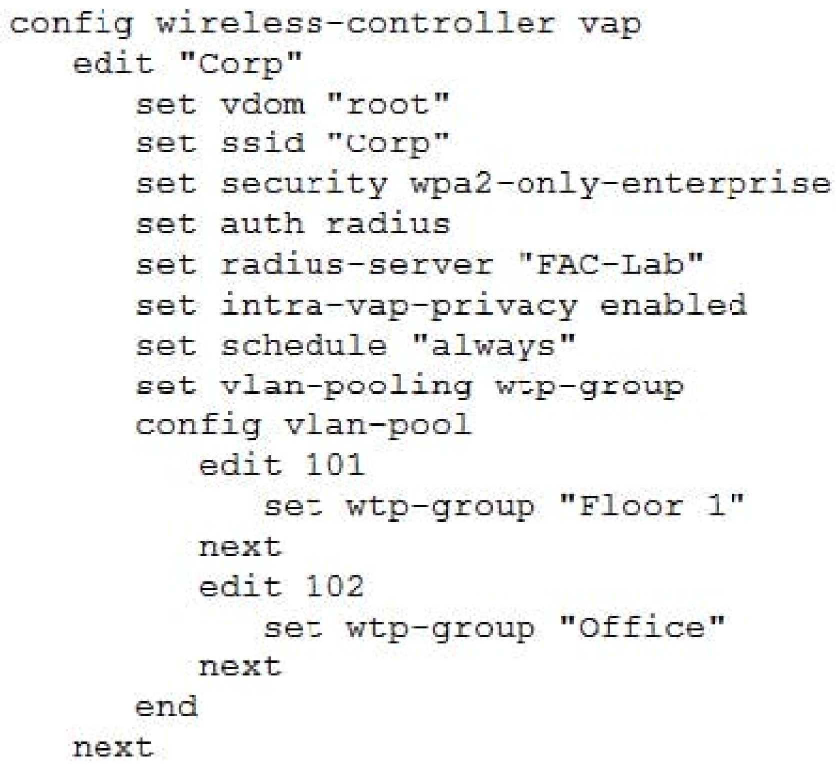
C. The LDAP server is configured to use regular bind.

D. The debug output shows multiple user authentications.

Correct Answer: BC

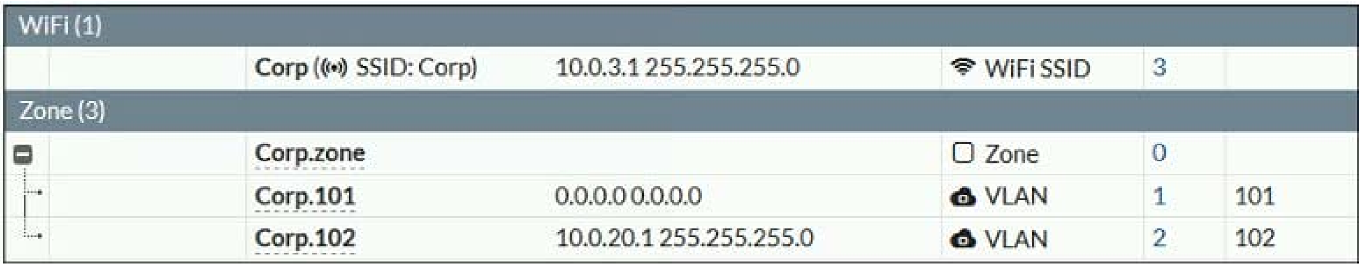
QUESTION 2

Refer to the exhibits.



```
config wireless-controller vap
   edit "Corp"
      set vdom "root"
      set ssid "Corp"
      set security wpa2-only-enterprise
      set auth radius
      set radius-server "FAC-Lab"
      set intra-vap-privacy enabled
      set schedule "always"
      set vlan-pooling wtp-group
      config vlan-pool
         edit 101
            set wtp-group "Floor 1"
         next
         edit 102
            set wtp-group "Office"
         next
      end
   next
```

Examine the VAP configuration and the WiFi zones table shown in the exhibits.



WiFi (1)						
		Corp ((•)) SSID: Corp)	10.0.3.1 255.255.255.0	WiFi SSID	3	
Zone (3)						
⊟		Corp.zone		□ Zone	0	
		Corp.101	0.0.0.0 0.0.0.0	VLAN	1	101
		Corp.102	10.0.20.1 255.255.255.0	VLAN	2	102

Which two statements describe FortiGate behavior regarding assignment of VLANs to wireless clients? (Choose two.)

A. FortiGate will load balance clients using VLAN 101 and VLAN 102 and assign them an IP address from the 10.0.3.0/24 subnet.

B. Clients connecting to APs in the Floor 1 group will not be able to receive an IP address.

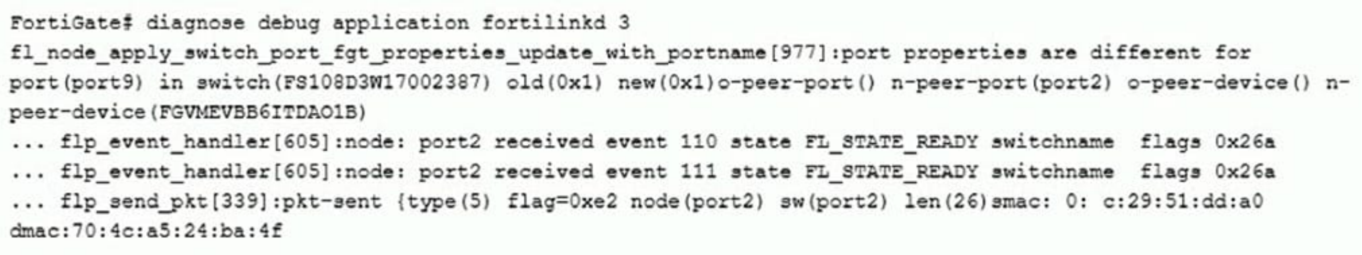
C. All clients connecting to the Corp SSID will receive an IP address from the 10.0.3.1/24 subnet.

D. Clients connecting to APs in the Office group will be assigned an IP address from the 10.0.20.1/24 subnet.

Correct Answer: BD

QUESTION 3

Examine the following output from the FortiLink real-time debug.



```
FortiGate# diagnose debug application fortilinkd 3
fl_node_apply_switch_port_fgt_properties_update_with_portname[977]:port properties are different for
port(port9) in switch(FS108D3W17002387) old(0x1) new(0x1)o-peer-port() n-peer-port(port2) o-peer-device() n-
peer-device(FGVMEVBB6ITDAO1B)
... flp_event_handler[605]:node: port2 received event 110 state FL_STATE_READY switchname  flags 0x26a
... flp_event_handler[605]:node: port2 received event 111 state FL_STATE_READY switchname  flags 0x26a
... flp_send_pkt[339]:pkt-sent {type(5) flag=0xe2 node(port2) sw(port2) len(26)smac: 0: c:29:51:dd:a0
dmac:70:4c:a5:24:ba:4f
```

Based on the output, what is the status of the communication between FortiGate and FortiSwitch?

A. FortiGate is unable to authorize the FortiSwitch.

B. FortiGate is unable to establish FortiLink tunnel to manage the FortiSwitch.

C. FortiGate is unable to located a previously managed FortiSwitch.

D. The FortiLink heartbeat is up.

Correct Answer: D

QUESTION 4

A wireless network in a school provides guest access using a captive portal to allow unregistered users to self-register and access the network. The administrator is requested to update the existing configuration to provide captive portal authentication through a secure connection (HTTPS) to protect and encrypt guest user credentials after they receive the login information when registered for the first time.

Which two changes must the administrator make to enforce HTTPS authentication? (Choose two.)

A. Provide instructions to users to use HTTPS to access the network.

B. Create a new SSID with the HTTPS captive portal URL.

C. Enable Redirect HTTP Challenge to a Secure Channel (HTTPS) in the user authentication settings

D. Update the captive portal URL to use HTTPS on FortiGate and FortiAuthenticator

Correct Answer: BD

QUESTION 5

What does DHCP snooping MAC verification do?

A. Drops DHCP release packets on untrusted ports

B. Drops DHCP packets with no relay agent information (option 82) on untrusted ports

C. Drops DHCP offer packets on untrusted ports

D. Drops DHCP packets on untrusted ports when the client hardware address does not match the source MAC address

Correct Answer: D

Reference: https://docs.fortinet.com/document/fortiswitch/6.4.2/administration-guide/335964/dhcpsnooping (note)