Fortinet

Exam Questions FCSS_NST_SE-7.4

FCSS - Network Security 7.4 Support Engineer

NEW QUESTION 1
Exhibit.

```
# diagnose automation test HAFailOver
automation test failed(1). stitch:HAFailOver
```

Refer to the exhibit, which shows the output of diagnose automation test. What can you observe from the output? (Choose two.)

A. The automation stitch test is not being logged.
B. The automation stitch test failed but the HA failover was successful.
C. An HA failover occurred.
D. The test was unsuccessful.

Answer: AD

NEW QUESTION 2
Refer to the exhibit, which shows a partial output of the fssod daemon real-time debug command.

```
# diagnose debug application fssod -1
# diagnose debug enable
[fsso_svr.c:save_result:579] event_id=4768, logon=bobby, domain=FSSO workstation=, ip=10.124.2.90 port=49215, time=1372061722
```

What two conclusions can you draw Itom the output? (Choose two.)

A. The workstation with IP 10.124.2.90 will be polled frequently using TCP port 445 to see if the user is still logged on.
B. The logon event can be seen on the collector agent installed on Windows.
C. FSSO is using DC agent mode to detect logon events.
D. FSSO is using agentless polling mode to detect logon events.

Answer: AD

NEW QUESTION 3
Exhibit.

```
FGT # diagnose debug rating
Locale       : english

Service      : Web-filter
Status       : Enable
License      : Contract

Service      : Antispam
Status       : Disable

Service      : Virus Outbreak Prevention
Status       : Disable

Num. of servers : 1
Protocol        : https
Port            : 443
Anycast         : Enable
Default servers : Included

-=- Server List (Mon May  1 03:47:52 2023) -=-

IP                                   Weight    RTT Flags   TZ   FortiGuard-requests  Curr Lost Total Lost           Updated Time
64.26.151.37                             10     45          -5                262432         0        846 Mon May  1 03:47:43 2023
64.26.151.35                             10     46          -5                329072         0       6806 Mon May  1 03:47:43 2023
66.117.56.37                             10     75          -5                 71638         0        275 Mon May  1 03:47:43 2023
65.210.95.240                            20     71          -8                 36875         0         92 Mon May  1 03:47:43 2023
209.22.147.36                            20     103 DI      -8                 34784         0       1070 Mon May  1 03:47:43 2023
208.91.112.194                           20     107 D       -8                 35170         0       1533 Mon May  1 03:47:43 2023
                                                            0                  33728         0        120 Mon May  1 03:47:43 2023
                                                            1                  33797         0        192 Mon May  1 03:47:43 2023
                                                            9                  33754         0        145 Mon May  1 03:47:43 2023
                                                           -5                  26410     26226      26227 Mon May  1 03:47:43 2023
```

Refer to the exhibit, which shows the output of a diagnose command. What can you conclude about the debug output in this scenario?

A. The first server provided to FortiGate when it performed a DNS query looking for a list of rating servers, was 121.111.236.179.
B. There is a natural correlation between the value in the FortiGuard-requests field and the value in the Weight field.
C. FortiGate used 64.26.151.37 as the initial server to validate its contract.
D. Servers with a negative TZ value are less preferred for rating requests.

Answer: B

NEW QUESTION 4
Exhibit.

```
… name_ip_match: failed to connect to workstation: <Workstation Name> (192.168.1.1)
… failed to connect to registry: WORKSTATION02 (192.168.12.232)
```

Refer to the exhibit, which shows two entries that were generated in theFSSO collectoragent logs.
What three conclusions can you draw from these log entries? {Choose three.)

A. Remote registry is not running on the workstation.
B. The user's status shows as "not verified" in the collector agent.
C. DNS resolution is unable to resolve the workstation name.
D. The FortiGate firmware version is not compatible with that of the collector agent.
E. A firewall is blocking traffic to port 139 and 445.

Answer: ABE

NEW QUESTION 5
Exhibit.

```
NGFW-1 # get sys ha status
HA Health Status: OK
Model: FortiGate-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:1:25
Cluster state change time: 2023-04-18 12:07:47
Primary selected using:
   <2023/04/18 12:07:47> FGVM010000077649 is selected as the primary because its override priority is larger than peer member
FGVM010000077650.
ses_pickup: disable
override: disable
Configuration Status:
    FGVM010000077649(updated 4 seconds ago): in-sync
    FGVM010000077650(updated 1 seconds ago): out-of-sync
System Usage stats:
    FGVM010000077649(updated 4 seconds ago):
        sessions=166, average-cpu-user/nice/system/idle=1%/0%/0%/99%, memory=45%
    FGVM010000077650(updated 1 seconds ago):
        sessions=3, average-cpu-user/nice/system/idle=0%/0%/0%/100%, memory=44%
HBDEV stats:
    FGVM010000077649(updated 4 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=167663/567/0/0, tx=262623/656/0/0
    FGVM010000077650(updated 1 seconds ago):
        port7: physical/1000auto, up, rx-bytes/packets/dropped/errors=271373/680/0/0, tx=176013/592/0/0
Primary     : NGFW-1          , FGVM010000077649, HA cluster index = 1
Secondary   : NGFW-2          , FGVM010000077650, HA cluster index = 0
number of vcluster: 1
vcluster 1: work 169.254.0.2
Primary: FGVM010000077649, HA operating index = 0
Secondary: FGVM010000077650, HA operating index = 1
```

Refer to theexhibit,which shows the output of getsystem ha status. NGFW-1 and NGFW-2 have been up for a week.
Which two statements about the output are true? (Choose two.)

A. If a configuration change is made to the primary FortiGate at this time, the secondary will initiate a synchronization reset.
B. If port 7 becomes disconnected on the secondary, both FortiGate devices will elect itself as primary.
C. If FGVM...649 is reboote
D. FGVM...650 will become the primary and retain that role, even after FGVM...649 rejoins the cluster.
E. If no action is taken, the primary FortiGate will leave the cluster because of the current sync status.

Answer: BC

NEW QUESTION 6
Exhibit 1.

```
config system global
    set snat-route-change disable
end
```

```
config router static
    edit 1
        set gateway 10.200.1.254
        set priority 5
        set device "port1"
    next
    edit 2
        set gateway 10.200.2.254
        set priority 10
        set device "port2"
    next
end
```

Exhibit 2.

```
FGT # diagnose sys session list
session info: proto=6 proto_state=01 duration=600 expire=3179 timeout=3600 flags=00000000
sockflag=00000000 sockport= av_idx=0 use=4
origin-shaper=
reply-shaper=
per_ip_shaper=
class_id=0 ha_id=0 policy_dir=0 tunnel=/ vlan cos=0/255
state=log may_dirty npu f00
statistic (bytes/packets/allow_err): org=3208/25/1 reply=11144/29/1 tuples=2
tx speed (Bps/kbps): 0/0 rx speed (Bps/kbps): 0/0
orgin->sink: org pre->post, reply pre->post dev=4->2/2->4 gwy=10.200.1.254/10.0.1.10
hook=post dir=org act=snat 10.0.1.10:64907->54.239.158.170:80(10.200.1.1:64907)
hook=pre dir=reply act=dnat 54.239.158.170:80->10.200.1.1:64907(10.0.1.10:64907)
pos/ (before, after) 0/(0,0), 0/(0,0)
src_mac=b4:f7:a1:e9:91:97
misc=0 policy_id=1 auth_info=0 chk_client_info=0 vd=0
serial=00317c56 tos=ff/ff app_list=0 app=0 url_cat=0
rpdb_link_id = 00000000
dd_type=0 dd_mode=0
npu_state=0x000c00
npu info: flag=0x00/0x00, offload=0/0, ips_offload=0/0, epid=0/0, ipid=0/0, vlan=0x0000/0x0000
vlifid=0/0, vtag in=0x0000/0x0000 in_npu=0/0, out_npu=0/0, fwd_en=0/0, qid=0/0
no_ofld_reason:
```

Refer to the exhibits, which show the configuration on FortiGate and partial internet session information from a user on the internal network.
An administrator would like to lest session failover between the two service provider connections.
Which two changes must the administrator make to force this existing session to immediately start using the other interface? (Choose two.)

A. Change the priority of the port! static route to 11.
B. Change the priority of the port2 static route to 5.
C. Configure unsetsnat-route-change to return it to the default setting.
D. Configure setsnat-route-change enable.

Answer: AD

NEW QUESTION 7
Refer to the exhibit, which shows a truncated output of a real-time LDAP debug.

```
# diagnose debug application fnbamd -1
# diagnose debug enable
    fnbamd_fsm.c[1274] handle_req-Rcvd auth req 8781845 for jsmith in Lab opt=27 prot=0
    fnbamd_ldap.c[637] resolve_ldap_FQDN-Resolved address 10.10.181.10, result 10.10.181.10
    fnbamd_ldap.c[232] start_search_dn-base:'DC=TAC,DC=ottawa,DC=fortinet,DC=com' filter:sAMAccountName=jsmith
    fnbamd_ldap.c[1351] fnbamd_ldap_get_result-Going to SEARCH state
    fnbamd_fsm.c[1833] poll_ldap_servers-Continue pending for req 8781845
    fnbamd_ldap.c[266] get_all_dn-Found DN 1:CN=John Smith,CN=Users,DC=TAC,DC=ottawa,DC=fortinet,DC=com
```

What two conclusions can you draw from the output? (Choose two.)

A. The name of the configured LDAP server is Lab.
B. The user is authenticating using CN=John Smith.
C. FortiOS is able to locate the user in step 3 (Bind Request) of the LDAP authentication process.
D. FortiOS is performing the second step (Search Request) in the LDAP authentication process.

Answer: BD

NEW QUESTION 8
Refer to the exhibit,which shows the output of getrouter info ospf neighbor.

```
Spoke1 # get router info ospf neighbor

OSPF process 0, VRF 0:
Neighbor ID     Pri   State           Dead Time   Address       Interface
0.0.0.1           1   Full/DR         00:00:39    10.10.2.1     wan1
0.0.0.3           1   Full/DROther    00:00:37    10.10.3.2     wan2
0.0.0.10         c1   Full/ -         00:00:36    172.16.1.2    ToHub
```

What can you conclude from the command output?

A. The network type connecting the local Fortigate and OSPF neighbor 0.0.0.10 is point-to- point.
B. All neighbors are in area 0.0.0.0.
C. The local FortiGate is the BDR.
D. The local FortiGate is not a DROther.

Answer: A

NEW QUESTION 9
Which two statements about an auxiliary session ate true? (Choose two.)

A. With the auxiliary session selling disabled, only auxiliary sessions are offloaded.
B. With the auxiliary session setting enable
C. ECMP traffic is accelerated to the NP6 processor.
D. With the auxiliary session setting enable
E. Iwo sessions are created in case of routing change.
F. With the auxiliary session setting disabled, for each traffic pat
G. FortiGate uses the same auxiliary session.

Answer: BC

NEW QUESTION 10
Refer to the exhibit.

```
# diagnose sys top
Run Time:  0 days, 0 hours and 18 minutes
0U, 0N, 1S, 95I, 0WA, 0HI, 0SI, 0ST; 16063, 12523F
          pyfcgid      248      S       2.9      3.8   9
           newcli      251      R       0.1      1.0   5
  merged_daemons      185      S       0.1      0.7   6
          miglogd      177      S       0.0      6.8   0
          pyfcgid      249      S       0.0      3.0   2
          pyfcgid      246      S       0.0      2.8   5
          reportd      197      S       0.0      2.7   2
          cmdbsvr      113      S       0.0      2.4   7
```

Which three pieces of information does the diagnose sys top command provide? (Choose three.)

A. The miglogd daemon is running on CPU core ID 0.
B. The diagnose sys top command has been running for 18 minutes.
C. The miglogd daemon would be on top of the list, if the administrator pressed m on the keyboard.
D. The cmdbsvr process is occupying 2.4% of the total user memory space.
E. If the neweli daemon continues to be in the R state, it will need to be manually restarted.

Answer: ABD

NEW QUESTION 10
.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questons and Answers in PDF Format

FCSS_NST_SE-7.4 Practice Exam Features:

* FCSS_NST_SE-7.4 Questions and Answers Updated Frequently

* FCSS_NST_SE-7.4 Practice Questions Verified by Expert Senior Certified Staff

* FCSS_NST_SE-7.4 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* FCSS_NST_SE-7.4 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year