NSE4_FGT-7.2$^{Q\&As}$

Fortinet NSE 4 - FortiOS 7.2

QUESTION 1

An administrator needs to increase network bandwidth and provide redundancy.

What interface type must the administrator select to bind multiple FortiGate interfaces?

A. VLAN interface

B. Software Switch interface

C. Aggregate interface

D. Redundant interface

Correct Answer: C

An aggregate interface is a logical interface that combines two or more physical interfaces into one virtual interface1. An aggregate interface can increase network bandwidth and provide redundancy by distributing traffic across multiple physical interfaces using a load balancing algorithm1. An aggregate interface can also support link aggregation control protocol (LACP) to negotiate the link aggregation settings with the connected device1.

Reference: https://forum.fortinet.com/tm .aspx?m=120324
https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/567758/aggregation-and-redundancy

QUESTION 2

You have enabled logging on a FortiGate device for event logs and all security logs, and you have set up logging to use the FortiGate local disk. What is the default behavior when the local disk is full?

A. No new log is recorded after the warning is issued when log disk use reaches the threshold of 95%.

B. No new log is recorded until you manually clear logs from the local disk.

C. Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

D. Logs are overwritten and the only warning is issued when log disk use reaches the threshold of 95%.

Correct Answer: C

config log disk setting

set diskfull [overwrite | nolog]

Action to take when disk is full. The system can overwrite the oldest log messages or stop logging when the disk is full. (default --> overwrite)

config log memory global-setting

set full-first-warning-threshold {integer}

Log full first warning threshold as a percent. (default --> 75) Reference:

https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/421620/config-log-disk- setting https://docs.fortinet.com/document/fortigate/7.2.5/cli-reference/418620/config-log-memory- global-setting

Logs are overwritten and the first warning is issued when log disk use reaches the threshold of 75%.

This is true because this is the default behavior of FortiGate when logging to the local disk. The local disk is the internal storage of FortiGate that can be used to store event logs and security logs. When the local disk is full, FortiGate will

overwrite the oldest logs with the newest ones, and issue warnings at different thresholds of disk usage. The first warning is issued when log disk use reaches 75%, the second warning is issued when log disk use reaches 85%, and the final

warning is issued when log disk use reaches 95%. The administrator can configure these thresholds and the action to take when the disk is full using the CLI command config log disk setting1

QUESTION 3

Which two configuration settings are synchronized when FortiGate devices are in an active- active HA cluster? (Choose two.)

A. FortiGuard web filter cache

B. FortiGate hostname

C. NTP

D. DNS

Correct Answer: CD

In the 7.2 Infrastructure Guide (page 306) the list of configuration settings that are NOT synchronized includes both \\'FortiGate host name\\' and \\'Cache\\'

QUESTION 4

A network administrator has enabled full SSL inspection and web filtering on FortiGate. When visiting any HTTPS websites, the browser reports certificate warning errors. When visiting HTTP websites, the browser does not report errors.

What is the reason for the certificate warning errors?

A. The matching firewall policy is set to proxy inspection mode.

B. The certificate used by FortiGate for SSL inspection does not contain the required certificate extensions.

C. The full SSL inspection feature does not have a valid license.

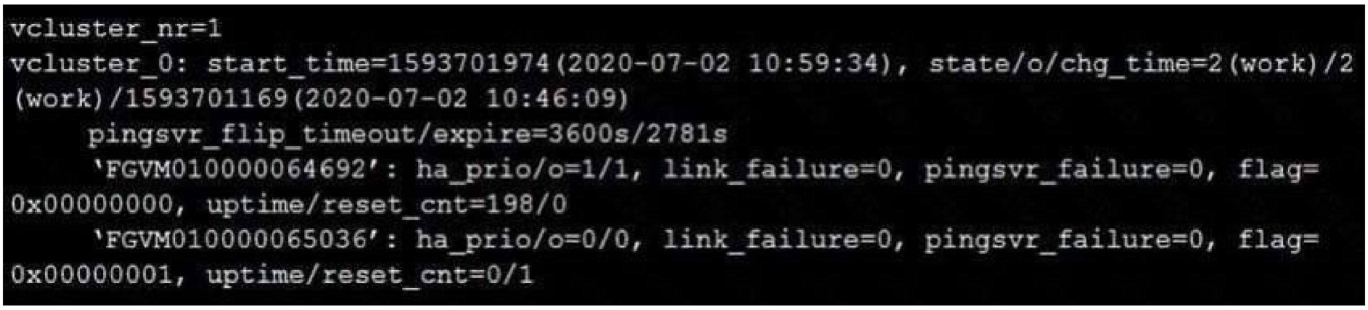
D. The browser does not trust the certificate used by FortiGate for SSL inspection.

Correct Answer: D

FortiGate Security 7.2 Study Guide (p.235): "If FortiGate receives a trusted SSL certificate, then it generates a temporary certificate signed by the built-in Fortinet_CA_SSL certificate and sends it to the browser. If the browser trusts the Fortinet_CA_SSL certificate, the browser completes the SSL handshake. Otherwise, the browser also presents a warning message informing the user that the site is untrusted. In other words, for this function to work as intended, you must import the Fortinet_CA_SSL certificate into the trusted root CA certificate store of your browser."

QUESTION 5

Refer to the exhibit.



```
vcluster_nr=1
vcluster_0: start_time=1593701974(2020-07-02 10:59:34), state/o/chg_time=2(work)/2
(work)/1593701169(2020-07-02 10:46:09)
     pingsvr_flip_timeout/expire=3600s/2781s
     'FGVM010000064692': ha_prio/o=1/1, link_failure=0, pingsvr_failure=0, flag=
0x00000000, uptime/reset_cnt=198/0
     'FGVM010000065036': ha_prio/o=0/0, link_failure=0, pingsvr_failure=0, flag=
0x00000001, uptime/reset_cnt=0/1
```

The exhibit displays the output of the CLI command: diagnose sys ha dump-by vcluster.

The override setting is enable for the FortiGate with SN FGVM010000064692.

Which two statements are true? (Choose two.)

A. FortiGate SN FGVM010000065036 HA uptime has been reset.

B. FortiGate devices are not in sync because one device is down.

C. FortiGate SN FGVM010000064692 is the primary because of higher HA uptime.

D. FortiGate SN FGVM010000064692 has the higher HA priority.

Correct Answer: AD

Study Guide

NSE4_FGT-7.2 Practice Test | NSE4_FGT-7.2 Exam Questions | NSE4_FGT-7.2 Braindumps