Prepare Smart for Success Free Fortinet NSE6_FMG_AD-7.6 Exam Questions and Answers

Ready to pass faster? Grab free and updated Fortinet NSE 6 - FortiManager 7.6 Administrator exam PDF questions now. Get authentic NSE6_FMG_AD-7.6 dumps packed with verified answers and secure your certification success with PrepBolt NSE6_FMG_AD-7.6 exam pdf questions and answers.

Thank you for Downloading NSE6_FMG_AD-7.6 exam PDF Demo

https://prepbolt.com/NSE6_FMG_AD-7.6.html

Question 1

Question Type: MultipleChoice

An administrator suspects that the Collector Agent is not forwarding login events to FortiGate.

What is the most effective troubleshooting step?

Options:

A- Verify if DC agent is enabled on the FortiGate.
B- Restart the domain controller to refresh authentication services.
C- Verify if FortiGate is set to use LDAP authentication instead of FSSO.
D- Check if TCP port 8000 is open between the collector agent and FortiGate.

Answer:

D

Explanation:

This point is not covered in the uploaded FortiManager 7.6 study guide, so the answer is based on Fortinet's official FSSO documentation. Fortinet documents that in FSSO Collector Agent deployments, the FortiGate connects to the Collector Agent on TCP port 8000 by default, and if a different port is not configured, that is the port that must be reachable. Fortinet also explains that the DC agents monitor user logon events and pass the information to the Collector Agent, which stores the information and sends it to the FortiGate.

So, when login events are not reaching FortiGate, the most effective first troubleshooting step is to verify connectivity on TCP 8000 between the Collector Agent and FortiGate. Options A, B, and C are less direct and do not test the actual transport path used by the Collector Agent to send FSSO information to FortiGate.

Question 2

Question Type: MultipleChoice

Refer to Exhibits:

HA configuration

```
HQ-NGFW-1 # config system ha

HQ-NGFW-1 (ha) # show
config system ha
    set group-id 5
    set group-name "Training"
    set mode a-p
    set password ENC a4fbyqY4iPexFmAnZgzDY
    set hbdev "port7" 0
    set session-pickup enable
    set override disable
    set priority 200
    set monitor "port1"
    set memory-based-failover enable
    set memory-failover-threshold 70
    set memory-failover-monitor-period 50
    set memory-failover-sample-rate 10
    set memory-failover-flip-timeout 60
end
```

HQ-NGFW-1 System Performance output

```
HQ-NGFW-1 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 1837868k used (90%), 104146k free (5.1%), 100062k freeable (4.9%)
Average network usage: 19/2 kbps in 1 minute, 19/4 kbps in 10 minutes, 19/3 kbps in 30 minutes
Maximal network usage: 36/18 kbps in 1 minute, 58/86 kbps in 10 minutes, 58/87 kbps in 30 minutes
Average sessions: 21 sessions in 1 minute, 22 sessions in 10 minutes, 21 sessions in 30 minutes
Maximal sessions: 22 sessions in 1 minute, 28 sessions in 10 minutes, 28 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 22 hours, 50 minutes
```

HQ-NGFW-2 System Performance output

```
HQ-NGFW-2 # get system performance status
CPU states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU0 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
CPU1 states: 0% user 0% system 0% nice 100% idle 0% iowait 0% irq 0% softirq
Memory: 2042076k total, 993836k used (48.7%), 690352k free (33.8%), 357888k freeable (17.5%)
Average network usage: 26/18 kbps in 1 minute, 25/18 kbps in 10 minutes, 24/18 kbps in 30 minutes
Maximal network usage: 91/27 kbps in 1 minute, 92/27 kbps in 10 minutes, 92/32 kbps in 30 minutes
Average sessions: 9 sessions in 1 minute, 9 sessions in 10 minutes, 9 sessions in 30 minutes
Maximal sessions: 11 sessions in 1 minute, 11 sessions in 10 minutes, 13 sessions in 30 minutes
Average session setup rate: 0 sessions per second in last 1 minute, 0 sessions per second in last 10 minutes
Maximal session setup rate: 0 sessions per second in last 1 minute, 1 sessions per second in last 10 minutes
Average NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Maximal NPU sessions: 0 sessions in last 1 minute, 0 sessions in last 10 minutes, 0 sessions in last 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 10 days, 10 hours, 50 minutes
```

An administrator has observed the performance status outputs on an HA cluster for 55 seconds.

Which FortiGate is the primary?

Options:

A- HQ-NGFW-2 with the parameter memory-failover-threshold setting

B- HQ-NGFW-2 with the parameter priority setting

C- HQ-NGFW-1 with the parameter memory-failover-flip-timeout setting

D- HQ-NGFW-1 with the parameter override setting

Answer:

A

Explanation:

The correct answer is A. This conclusion comes from the HA settings shown in the exhibit plus Fortinet's HA behavior. In the exhibit, HQ-NGFW-1 has memory-based-failover enabled, memory-failover-threshold 70, memory-failover-monitor-period 50, and its memory usage is about 90%, while HQ-NGFW-2 is about 48.7%. Fortinet's official documentation states that memory-failover-threshold is the memory percentage that triggers failover, and memory-failover-monitor-period is the duration high memory must persist before failover occurs. It also states that if utilization stays above the threshold for the entire monitor period, a failover is triggered, and the peer becomes primary. (Fortinet Document Library)

Because the condition was observed for 55 seconds, which is longer than the configured 50-second monitor period, the cluster would fail over from HQ-NGFW-1 to HQ-NGFW-2 due to the memory-failover-threshold condition. The priority setting does not explain this result here, because override is disabled, and flip-timeout governs subsequent memory-based failovers, not the initial trigger. (Fortinet Document Library)

=========

Question 3

Question Type: MultipleChoice

FortiGate is integrated with FortiAnalyzer and FortiManager.

When creating a firewall policy, which attribute must an administrator include to enhance functionality and enable log recording on FortiAnalyzer and FortiManager?

Options:

A- Policy ID
B- Log ID
C- Universally Unique Identifier
D- Sequence ID

Answer:

C

Explanation:

The correct answer is C. The uploaded FortiManager 7.6 Administrator Lab Guide gives the exact extract: ''FortiManager will update the universally unique identifiers (UUID) without deleting other configurations'' and ''UUIDs on both FortiGate and FortiManager are critical for ensuring the unique identification, consistency, and correct management of firewall policies across multiple devices and configurations. They provide a reliable and immutable reference for policies.''

The same source also shows administrators enabling UUIDs in Traffic Log on FortiGate log settings, which supports the logging and policy-correlation use case with FortiAnalyzer/FortiManager.

So the attribute that improves policy identification and logging correlation is the Universally Unique Identifier, not Policy ID, Log ID, or Sequence ID.

=========

Question 4

Question Type: MultipleChoice

An administrator assigned the Training global policy package to the Branches policy package in ADOM1. Later, the administrator created a new policy package named Remotes on ADOM1.

What should the administrator do to sync the Training global policy package with the Remotes policy package in ADOM1?

Options:

A- Manually add and assign the Remotes policy package to the Training global policy package
B- Use the automatically install policies to ADOM devices method to sync from the Training global policy package to the Remotes policy package
C- Assign the Training global policy package to the Remotes policy package
D- Unassign the Training policy package and reassign it to all policy packages within ADOM1

Answer:

C

Explanation:

The correct answer is C. The FortiManager 7.6 Administrator Study Guide explicitly says: ''You must explicitly assign global policy packages to specific ADOMs'' and ''you can even pick specific policy packages in individual ADOMs that you want to apply the global policies to.'' The study guide also

explains the assignment workflow: ''This slide shows the steps to assign a global policy package to an ADOM policy package'' and ''First, add the required ADOMs as targets. Second, assign the global policy package to the ADOMs.''

Because Remotes is a newly created policy package, it does not inherit the earlier assignment automatically. The administrator must explicitly assign the Training global policy package to the Remotes policy package. Automatic install does not create that assignment, and unassigning all packages is unnecessary.

Question 5

Question Type: MultipleChoice

An administrator upgrades FortiManager with workspace mode per ADOM enabled to the latest version but notices that the ADOM versions did not change.

Why were the ADOMs not upgraded?

Options:

A- The administrator did not run the database integrity check before performing the upgrade.
B- FortiManager does not automatically upgrade ADOMs after a firmware upgrade.
C- A FortiManager process task is stuck and blocking the ADOM upgrade, so the administrator must fix it.
D- A user had all ADOMs locked before the upgrade, which stopped them from being upgraded.

Answer:

B

Explanation:

The correct answer is B. The FortiManager 7.6 Administrator Study Guide gives the exact extract: ''Also note when you upgrade the FortiManager firmware version the existing ADOMs are not automatically upgraded.'' This directly explains why the administrator saw the FortiManager upgrade complete while the ADOM versions remained unchanged.

The same section also explains that ADOM upgrades are a separate action: ''You can upgrade an ADOM in System Settings > ADOMs'' and ''Can upgrade to one version higher at a time.'' In addition, the guide recommends: ''upgrade all devices first, and then upgrade the ADOM.''

So the issue is not workspace mode, locked ADOMs, or a stuck task. The ADOMs simply require their own manual upgrade step after the FortiManager firmware upgrade.

Question 6

Question Type: MultipleChoice

What are two outcomes of ADOM revisions? Choose two answers.

Options:

A- ADOM revisions can save the current state of the entire ADOM.
B- ADOM revisions do not increase the size of configuration backups.
C- ADOM revisions can save the current state of all policy packages and objects for an ADOM.
D- ADOM revisions appear in the Install Policy and Package Settings section of the install wizard.

Answer:

A, C

Explanation:

The correct answers are A and C. The FortiManager 7.6 Administrator Study Guide states: ''An ADOM revision creates a snapshot of all policy and object configurations for the ADOM''. The lab guide says the same thing in practical terms: ''An ADOM revision creates a snapshot of the policy and object configuration for the ADOM'' and that these revisions are useful for comparing differences and reverting to a previous revision.

Because the revision is a snapshot of the ADOM's policy-and-object state, it saves the current ADOM policy/object state, which supports A and directly proves C. B is false because the study guide warns: ''ADOM revisions can significantly increase the size of the configuration backup files.'' D is not supported by the uploaded sources.

=========

Thank You for trying NSE6_FMG_AD-7.6 PDF Demo

To try our NSE6_FMG_AD-7.6 practice exam software visit link below

https://prepbolt.com/NSE6_FMG_AD-7.6.html

Start Your NSE6_FMG_AD-7.6 Preparation

Use Coupon “SAVE50” for extra 50% discount on the purchase of Practice Test Software. Test your NSE6_FMG_AD-7.6 preparation with actual exam questions.