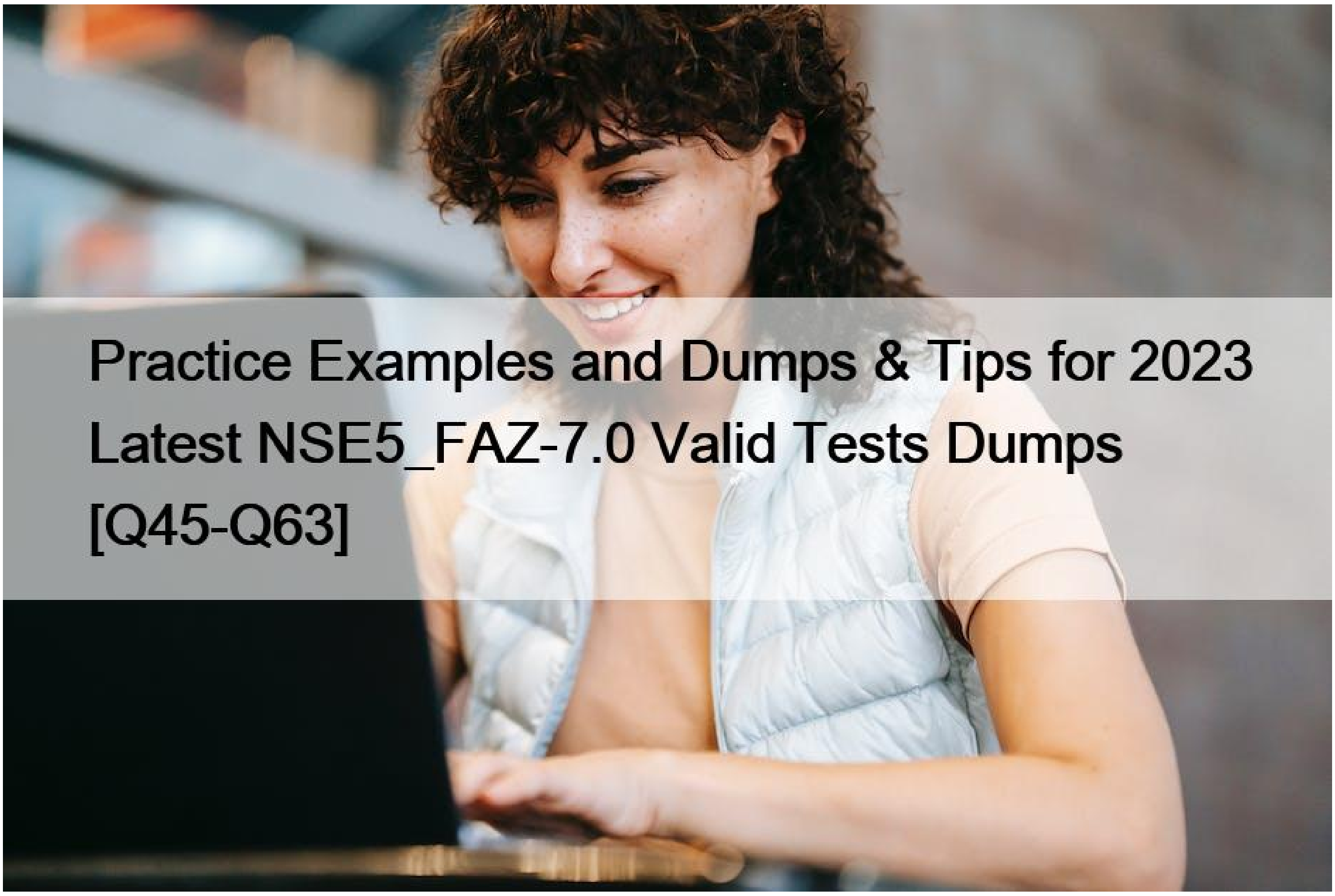
Practice Examples and Dumps & Tips for 2023 Latest NSE5_FAZ-7.0 Valid Tests Dumps [Q45-Q63


Practice Examples and Dumps & Tips for 2023
Latest NSE5_FAZ-7.0 Valid Tests Dumps
[Q45-Q63]

Practice Examples and Dumps & Tips for 2023 Latest NSE5_FAZ-7.0 Valid Tests Dumps
Latest [Dec 06, 2023] 100% Passing Guarantee - Brilliant NSE5_FAZ-7.0 Exam Questions PDF

Fortinet NSE5_FAZ-7.0 certification is suitable for network administrators, security analysts, and other IT professionals who want to demonstrate their expertise in managing and analyzing network security logs. Fortinet NSE 5 - FortiAnalyzer 7.0 certification is also beneficial for those who want to enhance their career prospects in the network security industry.

Fortinet NSE5_FAZ-7.0 certification is a valuable asset for security professionals looking to advance their careers in the cybersecurity industry. Fortinet NSE 5 - FortiAnalyzer 7.0 certification is recognized by industry leaders and employers worldwide, and it demonstrates the candidate's expertise in managing and analyzing security logs using FortiAnalyzer 7.0. Fortinet NSE 5 - FortiAnalyzer 7.0 certification can help professionals stand out in a competitive job market and can lead to higher salaries and better job opportunities.

NO.45 What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

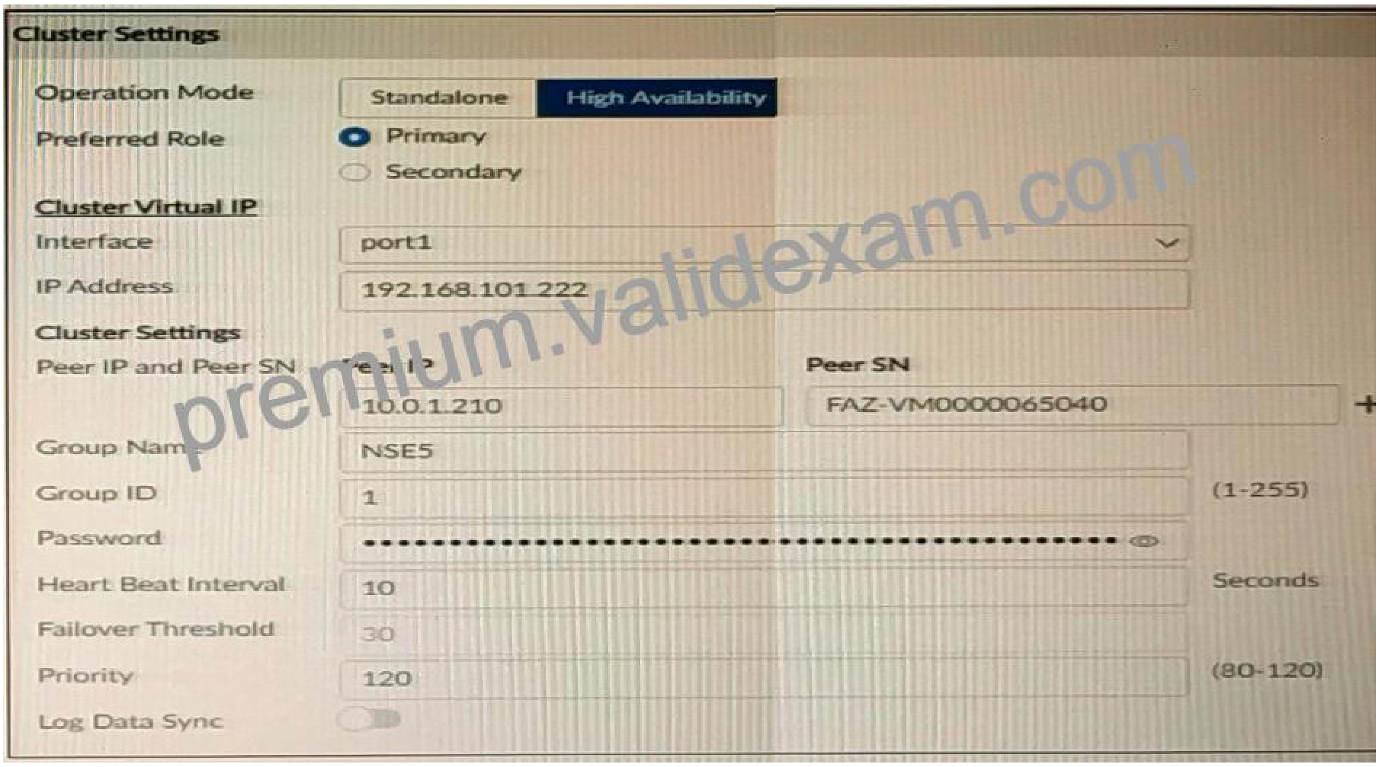
* Hot swap the disk.
* There is no need to do anything because the disk will self-recover.
* Run execute format disk to format and restart the FortiAnalyzer device.
* Shut down FortiAnalyzer and replace the disk
https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiManager%20devices%20that,to%20exchanging%20the%20hard%20disk.

If a hard disk on a FortiAnalyzer unit fails, it must be replaced. On FortiAnalyzer devices that support hardware RAID, the hard disk can be replaced while the unit is still running &#8211; known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NO.46 Why should you use an NTP server on FortiAnalyzer and all registered devices that log into FortiAnalyzer?
* To properly correlate logs
* To use real-time forwarding
* To resolve host names
* To improve DNS response times

NO.47 What remote authentication servers can you configure to validate your FortiAnalyzer administrator logons? (Choose three)
* RADIUS
* Local
* LDAP
* PKI
* TACACS+

NO.48 Refer to the exhibit.



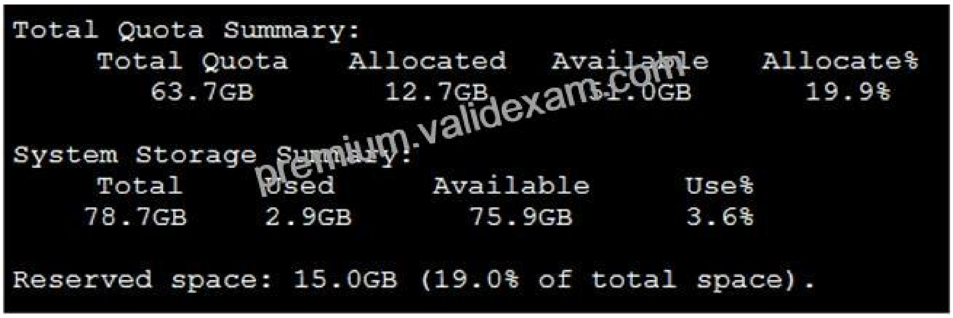
Cluster Settings

Operation Mode	Standalone	High Availability	
Preferred Role	● Primary ○ Secondary		
Cluster Virtual IP			
Interface	port1		
IP Address	192.168.101.222		
Cluster Settings			
Peer IP and Peer SN	Peer IP 10.0.1.210	Peer SN FAZ-VM0000065040	+
Group Name	NSE5		
Group ID	1		(1-255)
Password	••		
Heart Beat Interval	10		Seconds
Failover Threshold	30		
Priority	120		(80-120)
Log Data Sync	○		

The image displays the configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.

What can you conclude from the configuration displayed?
* This FortiAnalyzer will join to the existing HA cluster as the primary.
* This FortiAnalyzer is configured to receive logs in its port1.
* This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
* After joining to the cluster, this FortiAnalyzer will keep an updated log database.

NO.49 View the exhibit.



```
Total Quota Summary:
     Total Quota    Allocated   Available   Allocate%
       63.7GB         12.7GB      51.0GB      19.9%

System Storage Summary:
     Total      Used        Available      Use%
    78.7GB     2.9GB         75.9GB        3.6%

Reserved space: 15.0GB (19.0% of total space).
```

Why is the total quota less than the total system storage?
* 3.6% of the system storage is already being used.
* Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
* The oftpd process has not archived the logs yet
* The logfiled process is just estimating the total quota
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation

NO.50 An administrator fortinet, is able to view logs and perform device management tasks, such as adding and removing registered devices. However, administrator fortinet is not able to create a mall server that can be used to send email.

What could be the problem?
* Fortinet is assigned the Standard_ User administrator profile.
* A trusted host is configured.
* ADOM mode is configured with Advanced mode.
* Fortinet is assigned the Restricted_ User administrator profile.
* Super_User, which, like in FortiGate, provides access to all device and system privileges.

* Standard_User, which provides read and write access to device privileges, but not system privileges.

* Restricted_User, which provides read access only to device privileges, but not system privileges. Access to the Management extensions is also removed.

* No_Permissions_User, which provides no system or device privileges. Can be used, for example, to temporarily remove access granted to existing admins.

FortiAnalyzer_7.0_Study_Guide-Online page 42

NO.51 Which two purposes does the auto cache setting on reports serve? (Choose two.)

* It automatically updates the hcache when new logs arrive.
* It provides diagnostics on report generation time.
* It reduces the log insert lag rate.
* It reduces report generation time.
Reference:

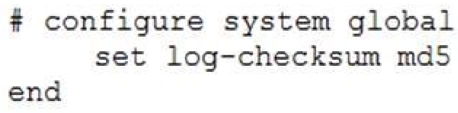
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/384416/how-auto-cache-works

https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/86926/enabling-auto-cache

NO.52 When working with FortiAnalyzer reports, what is the purpose of a dataset?
* To provide the layout used for reports
* To define the chart type to be used
* To retrieve data from the database
* To set the data included in templates
Reference:

Datasets: Structured Query Language (SQL) SELECT queries that extract specific data from the database

NO.53 What is the purpose of the following CLI command?

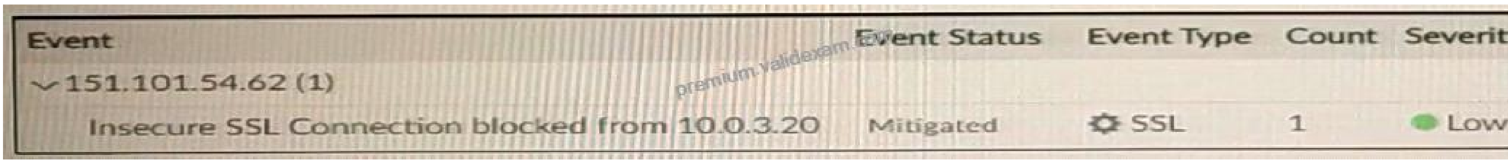


```
# configure system global
      set log-checksum md5
end
```

* To add a log file checksum
* To add the MD&#8217;s hash value and authentication code
* To add a unique tag to each log to prove that it came from this FortiAnalyzer
* To encrypt log communications
https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global

NO.54 What statements are true regarding FortiAnalyzer &#8216;s treatment of high availability (HA) dusters? (Choose two)
* FortiAnalyzer distinguishes different devices by their serial number.
* FortiAnalyzer receives logs from d devices in a duster.
* FortiAnalyzer receives bgs only from the primary device in the cluster.
* FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automaticaly discovers the other devices.

NO.55 Refer to the exhibit.



Event	Event Status	Event Type	Count	Severit
⌄151.101.54.62 (1)				
Insecure SSL Connection blocked from 10.0.3.20	Mitigated	⚙ SSL	1	● Low

Which statement is correct regarding the event displayed?

* The security risk was blocked or dropped.
* The security event risk is considered open.
* An incident was created from this event.
* The risk source is isolated.

NO.56 Which two actions should an administrator take to view Compromised Hosts on FortiAnalyzer? (Choose two.)
* Enable web filtering in firewall policies on FortiGate devices, and make sure these logs are sent to FortiAnalyzer.
* Make sure all endpoints are reachable by FortiAnalyzer.
* Enable device detection on an interface on the FortiGate devices that are connected to the FortiAnalyzer device.
* Subscribe FortiAnalyzer to FortiGuard to keep its local threat database up to date.
In order to configure IOC, you require the following:

* A one-year subscription to IOC. Note that FortiAnalyzer does include an evaluation license, but it is restrictive and only meant to give you an idea of how the feature works.

* A web filter services subscription on FortiGate device(s)

* Web filter policies on FortiGate device(s) that send traffic to FortiAnalyzer Compromised Hosts or Indicators of Compromise service (IOC) is a licensed feature.

To view Compromised Hosts, you must turn on the UTM web filter of FortiGate devices and subscribe your FortiAnalyzer unit to FortiGuard to keep its local threat database synchronized with the FortiGuard threat database. See Subscribing FortiAnalyzer to FortiGuard.

Ref : https://docs.fortinet.com/document/fortianalyzer/6.4.0/administration-guide/137635/viewing-compromised-hosts

NO.57 You have recently grouped multiple FortiGate devices into a single ADOM. System Settings > Storage Info shows the quota used.

What does the disk quota refer to?
* The maximum disk utilization for each device in the ADOM
* The maximum disk utilization for the FortiAnalyzer model
* The maximum disk utilization for the ADOM type
* The maximum disk utilization for all devices in the ADOM

NO.58 Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)
* ADOMs are enabled by default.
* ADOMs constrain other administrator&#8217;s access privileges to a subset of devices in the device list.
* Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
* All administrators can create ADOMs&#8211;not just the admin administrator.

NO.59 FortiAnalyzer reports are dropping analytical data from 15 days ago, even though the data policy setting for analytics logs is 60 days.

What is the most likely problem?
* Quota enforcement is acting on analytical data before a report is complete
* Logs are rolling before the report is run
* CPU resources are too high
* Disk utilization for archive logs is set for 15 days

NO.60 Which two statements are true regarding high availability (HA) on FortiAnalyzer? (Choose two.)

* FortiAnalyzer HA can function without VRRP. and VRRP is required only if you have more than two FortiAnalyzer devices in a cluster.
* FortiAnalyzer HA supports synchronization of logs as well as some system and configuration settings.
* All devices in a FortiAnalyzer HA cluster must run in the same operation mode: analyzer or collector.
* FortiAnalyzer HA implementation is supported by many public cloud infrastructures such as AWS, Microsoft Azure, and Google Cloud.

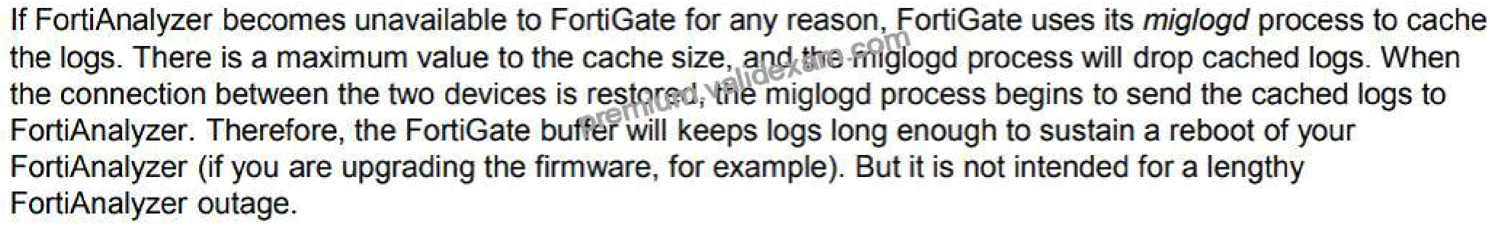
Reference:

FortiAnalyzer HA implementation works only in networks where Virtual Router Redundancy Protocol (VRRP) is permitted. Therefore it may not be supported by some public cloud infrastructures.

NO.61 You need to upgrade your FortiAnalyzer firmware.

What happens to the logs being sent to FortiAnalyzer from FortiGate during the time FortiAnalyzer is temporarily unavailable?

* FortiAnalyzer uses log fetching to retrieve the logs when back online
* FortiGate uses the miglogd process to cache the logs
* The logfiled process stores logs in offline mode
* Logs are dropped



If FortiAnalyzer becomes unavailable to FortiGate for any reason, FortiGate uses its *miglogd* process to cache the logs. There is a maximum value to the cache size, and the miglogd process will drop cached logs. When the connection between the two devices is restored, the miglogd process begins to send the cached logs to FortiAnalyzer. Therefore, the FortiGate buffer will keeps logs long enough to sustain a reboot of your FortiAnalyzer (if you are upgrading the firmware, for example). But it is not intended for a lengthy FortiAnalyzer outage.

NO.62 What is the recommended method of expanding disk space on a FortiAnalyzer VM?

* From the VM host manager, add an additional virtual disk and use the #execute lvm extend <disk number> command to expand the storage
* From the VM host manager, expand the size of the existing virtual disk
* From the VM host manager, expand the size of the existing virtual disk and use the # execute format disk command to reformat the disk
* From the VM host manager, add an additional virtual disk and rebuild your RAID array

https://kb.fortinet.com/kb/documentLink.do?externalID=FD40848

NO.63 What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server?

(Choose two.)

* SFTP, FTP, or SCP server
* Mail server
* Output profile
* Report scheduling

https://docs.fortinet.com/document/fortianalyzer/6.0.2/administration-guide/598322/creating-output-profiles

NSE5_FAZ-7.0 are Available for Instant Access: https://www.validexam.com/NSE5_FAZ-7.0-latest-dumps.html]