Updated Oct 04, 2023 Verified NSE5_FAZ-7.0 dumps Q&As - 100% Pass [Q17-Q35

Updated Oct 04, 2023 Verified NSE5_FAZ-7.0 dumps Q&As - 100% Pass [Q17-Q35]
Emerging Industry Leaders

Updated Oct 04, 2023 Verified NSE5_FAZ-7.0 dumps Q&As - 100% Pass
New 2023 Latest Questions NSE5_FAZ-7.0 Dumps - Use Updated Fortinet Exam

Fortinet NSE5_FAZ-7.0 (Fortinet NSE 5 - FortiAnalyzer 7.0) Certification Exam is designed for professionals who aim to validate their knowledge and skills in managing and analyzing logs and reports generated by Fortinet security appliances. FortiAnalyzer is a central logging and reporting solution that provides visibility and analysis of network activities, security events, and threat intelligence, enabling organizations to detect and respond to security incidents effectively. The NSE5_FAZ-7.0 exam measures the candidate's ability to configure and manage FortiAnalyzer devices, interpret and analyze logs and reports, and troubleshoot common issues.

NO.17 FortiAnalyzer uses the Optimized Fabric Transfer Protocok (OFTP) over SSL for what purpose?
* To upload logs to an SFTP server
* To prevent log modification during backup
* To send an identical set of logs to a second logging server
* To encrypt log communication between devices

NO.18 What is the purpose of a predefined template on the FortiAnalyzer?
- It can be edited and modified as required
- It specifies the report layout which contains predefined texts, charts, and macros
- It specifies report settings which contains time period, device selection, and schedule
- It contains predefined data to generate mock reports

Reference:

2300_Reports/0010_Predefined_reports.htm#:~:text=FortiAnalyzer%20includes%20a%20number%

20of,create%20and%2For%20build%20reports.&text=A%20template%20populates%20the%20Layout,that%

20is%20to%20be%20created.

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/2300_Reports/0010_Predefined_reports.htm

NO.19 What does the disk status Degraded mean for RAID management?
- One or more drives are missing from the FortiAnalyzer unit. The drive is no longer available to the operating system.
- The FortiAnalyzer device is writing to all the hard drives on the device in order to make the array fault tolerant.
- The FortiAnalyzer device is writing data to a newly added hard drive in order to restore the hard drive to an optimal state.
- The hard driveiIs no longer being used by the RAID controller

NO.20 On the RAID management page, the disk status is listed as Initializing.

What does the status Initializing indicate about what the FortiAnalyzer is currently doing?
- FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
- FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
- FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
- FortiAnalyzer is functioning normally

Reference:

8977-00505692583a/FortiAnalyzer-5.6.10-Administration-Guide.pdf (40)

NO.21 For which two SAML roles can the FortiAnalyzer be configured? (Choose two.)
- Principal
- Service provider
- Identity collector
- Identity provider

Reference:

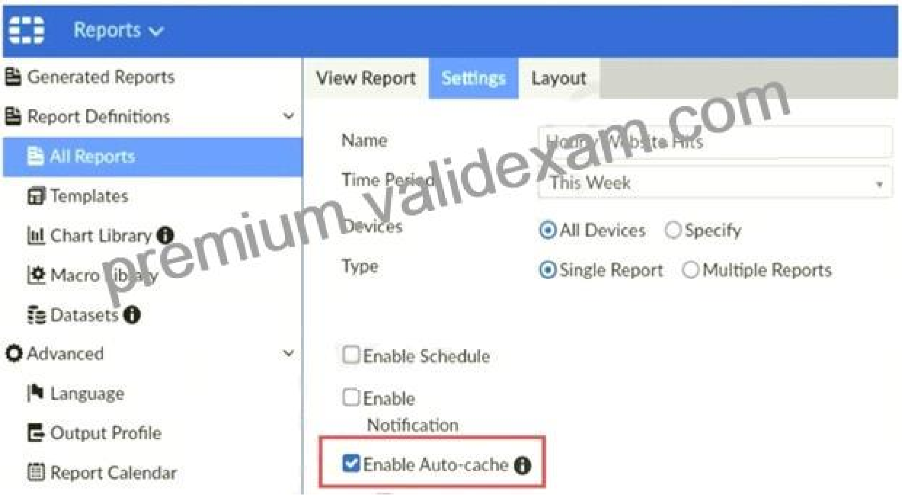
20the%20identity%20provider%20(IdP,external%20identity%20provider%20is%20available.

https://docs.fortinet.com/document/fortianalyzer/6.2.0/administration-guide/981386/saml-admin-authentication

NO.22 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.23 Refer to the exhibit.



Name Hourly Website Hits

Time Period This Week

Devices ● All Devices ○ Specify

Type ● Single Report ○ Multiple Reports

☐ Enable Schedule

☐ Enable Notification

☑ Enable Auto-cache

Which two statements are true regarding enabling auto-cache on FortiAnalyzer? (Choose two.)
* Report size will be optimized to conserve disk space on FortiAnalyzer.
* Reports will be cached in the memory.
* This feature is automatically enabled for scheduled reports.
* Enabling auto-cache reduces report generation time for reports that require a long time to assemble datasets.

NO.24 What can you do on FortiAnalyzer to restrict administrative access from specific locations?
* Configure trusted hosts for that administrator.
* Enable geo-location services on accessible interface.
* Configure two-factor authentication with a remote RADIUS server.
* Configure an ADOM for respective location.

NO.25 What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?
* Chart Builder
* Export to Report Chart
* Dataset Library
* Custom View
https://docs.fortinet.com/document/fortianalyzer/6.2.0/cookbook/989203/building-charts-with-chart-builder

NO.26 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.27 A play book contains five tasks in total. An administrator executed the playbook and four out of five tasks finished successfully, but one task failed. What will be the status of the playbook after its execution?

* Success
* Failed
* Running
* Upstream_failed

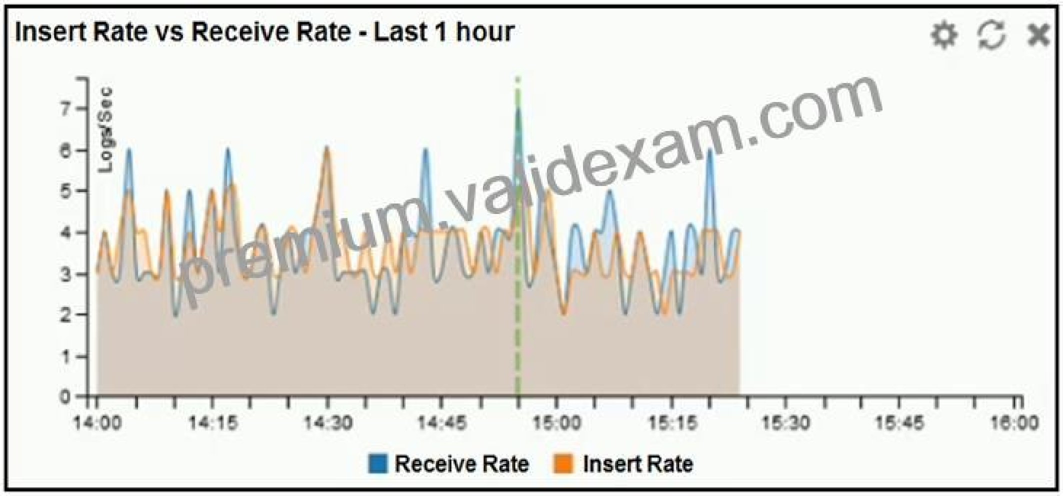
NO.28 Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally?

(Choose two.)
* Mail server
* Output profile
* SFTP server
* Report scheduling

NO.29 What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?
* Chart Builder
* Export to Report Chart
* Dataset Library
* Custom View

NO.30 How do you restrict an administrator&#8217;s access to a subset of your organization&#8217;s ADOMs?
* Set the ADOM mode to Advanced
* Assign the ADOMs to the administrator&#8217;s account
* Configure trusted hosts
* Assign the default Super_User administrator profile
https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/717578/assigning-administrators-to-an-adom

NO.31 Refer to the exhibit.



What does the data point at 14:55 tell you?
* The received rate is almost at its maximum for this device
* The sqlplugind daemon is behind in log indexing by two logs
* Logs are being dropped
* Raw logs are reaching FortiAnalyzer faster than they can be indexed

NO.32 Which statement correctly describes the management extensions available on FortiAnalyzer?
* Management extensions do not require additional licenses.
* Management extensions allow FortiAnalyzer to act as a ForbSIEM supervisor.
* Management extensions require a dedicated VM for best performance.
* Management extensions may require a minimum number of CPU cores to run.

Events in FortiAnalyzer will be in one of four statuses. The current status will determine if more actions need to be taken by the security team or not.

The possible statuses are:

Unhandled: The security event risk is not mitigated or contained, so it is considered open.

Contained: The risk source is isolated.

Mitigated: The security risk is mitigated by being blocked or dropped.

(Blank): Other scenarios.

FortiAnalyzer_7.0_Study_Guide-Online pag. 189.

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 189: Review the hardware requirements before you enable a management extension application. Some of them require a minimum amount of memory or a minimum number of CPU cores.

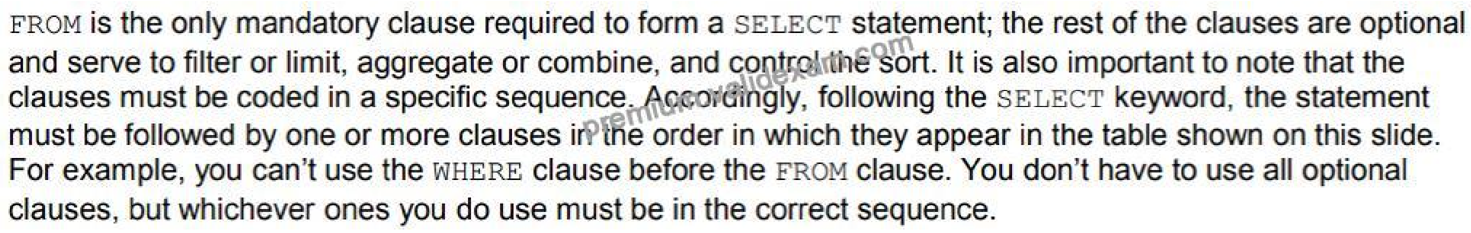
NO.33 For which two purposes would you use the command set log checksum? (Choose two.)
* To help protect against man-in-the-middle attacks during log upload from FortiAnalyzer to an SFTP server
* To prevent log modification or tampering
* To encrypt log communications
* To send an identical set of logs to a second logging server

To prevent logs from being tampered with while in storage, you can add a log checksum using the config system global command. You can configure FortiAnalyzer to record a log file hash value, timestamp, and authentication code when the log is rolled and archived and when the log is uploaded (if that feature is enabled). This can also help against man-in-the-middle only for the transmission from FortiAnalyzer to an SSH File Transfer Protocol (SFTP) server during log upload.

FortiAnalyzer_7.0_Study_Guide-Online page 149

NO.34 Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?
* FROM
* LIMIT
* WHERE
* ORDER BY

Reference:



`FROM` is the only mandatory clause required to form a `SELECT` statement; the rest of the clauses are optional and serve to filter or limit, aggregate or combine, and control the sort. It is also important to note that the clauses must be coded in a specific sequence. Accordingly, following the `SELECT` keyword, the statement must be followed by one or more clauses in the order in which they appear in the table shown on this slide. For example, you can't use the `WHERE` clause before the `FROM` clause. You don't have to use all optional clauses, but whichever ones you do use must be in the correct sequence.

NO.35 Which two statements are correct regarding the export and import of playbooks? (Choose two.)

* You can export only one playbook at a time.
* You can import a playbook even if there is another one with the same name in the destination.
* Playbooks can be exported and imported only within the same FortiAnaryzer.
* A playbook that was disabled when it was exported, will be disabled when it is imported.

Latest NSE5_FAZ-7.0 Exam Dumps Fortinet Exam from Training:
https://www.validexam.com/NSE5_FAZ-7.0-latest-dumps.html]