

Fortinet

Exam Questions NSE5_FAZ-7.0

Fortinet NSE 5 - FortiAnalyzer 7.0



NEW QUESTION 1

What FortiView tool can you use to automatically build a dataset and chart based on a filtered search result?

- A. Chart Builder
- B. Export to Report Chart
- C. Dataset Library
- D. Custom View

Answer: B

NEW QUESTION 2

FortiAnalyzer uses the Optimized Fabric Transfer Protocol (OFTP) over SSL for what purpose?

- A. To upload logs to an SFTP server
- B. To prevent log modification during backup
- C. To send an identical set of logs to a second logging server
- D. To encrypt log communication between devices

Answer: D

NEW QUESTION 3

When working with FortiAnalyzer reports, what is the purpose of a dataset?

- A. To provide the layout used for reports
- B. To define the chart type to be used
- C. To retrieve data from the database
- D. To set the data included in templates

Answer: C

NEW QUESTION 4

Which statements are true regarding securing communications between FortiAnalyzer and FortiGate with SSL? (Choose two.)

- A. SSL is the default setting.
- B. SSL communications are auto-negotiated between the two devices.
- C. SSL can send logs in real-time only.
- D. SSL encryption levels are globally set on FortiAnalyzer.
- E. FortiAnalyzer encryption level must be equal to, or higher than, FortiGate.

Answer: AD

NEW QUESTION 5

What is the purpose of using prefilters when configuring event handlers?

- A. They limit which logs are checked for matches by the other filters.
- B. They can filter the logs before they are processed by FortiAnalyzer
- C. They download new filters to be used in event handlers.
- D. They are common filters applied simultaneously to all event handlers.

Answer: A

NEW QUESTION 6

What statements are true regarding the "store and upload" log transfer option between FortiAnalyzer and FortiGate? (Choose three.)

- A. All FortiGates can send logs to FortiAnalyzer using the store and upload option.
- B. Only FortiGate models with hard disks can send logs to FortiAnalyzer using the store and upload option.
- C. Both secure communications methods (SSL and IPsec) allow the store and upload option.
- D. Disk logging is enabled on the FortiGate through the CLI only.
- E. Disk logging is enabled by default on the FortiGate.

Answer: BCD

NEW QUESTION 7

FortiAnalyzer centralizes which functions? (Choose three)

- A. Network analysis
- B. Graphical reporting
- C. Content archiving / data mining
- D. Vulnerability assessment
- E. Security log analysis / forensics

Answer: BCE

NEW QUESTION 8

What must you configure on FortiAnalyzer to upload a FortiAnalyzer report to a supported external server? (Choose two.)

- A. SFTP, FTP, or SCP server
- B. Mail server
- C. Output profile
- D. Report scheduling

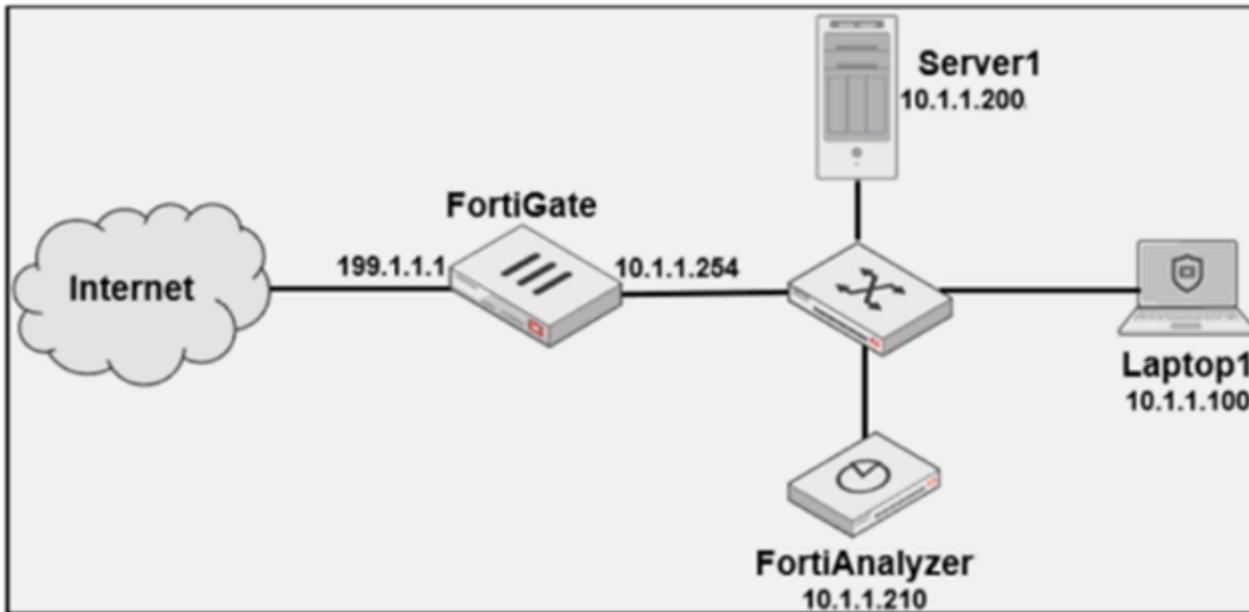
Answer: AC

Explanation:

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

NEW QUESTION 9

Refer to the exhibit.



Laptop1 is used by several administrators to manage FortiAnalyzer. You want to configure a generic text filter that matches all login attempts to the web interface generated by any user other than "admin", and coming from Laptop1. Which filter will achieve the desired result?

- A. operation-login & dstip==10.1.1.210 & user!=admin
- B. operation-login & srcip==10.1.1.100 & dstip==10.1.1.210 & user==admin
- C. operation-login & performed_on=="GUI(10.1.1.210)" & user!=admin
- D. operation-login & performed_on=="GUI(10.1.1.100)" & user!=admin

Answer: D

NEW QUESTION 10

If a hard disk fails on a FortiAnalyzer that supports software RAID, what should you do to bring the FortiAnalyzer back to functioning normally, without losing data?

- A. Hot swap the disk
- B. Replace the disk and rebuild the RAID manually
- C. Take no action if the RAID level supports a failed disk
- D. Shut down FortiAnalyzer and replace the disk

Answer: D

Explanation:

<https://kb.fortinet.com/kb/documentLink.do?externalID=FD46446#:~:text=On%20FortiAnalyzer%2FFortiMana> 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 – known as hot swapping. On FortiAnalyzer units with software RAID, the device must be shutdown prior to exchanging the hard disk.

NEW QUESTION 10

Which statement about sending notifications with incident updates is true?

- A. Notifications can be sent only when an incident is created or deleted.
- B. You must configure an output profile to send notifications by email.
- C. Each incident can send notifications to a single external platform.
- D. Each connector used can have different notification settings.

Answer: D

NEW QUESTION 15

Which clause is considered mandatory in SELECT statements used by the FortiAnalyzer to generate reports?

- A. FROM
- B. LIMIT
- C. WHERE
- D. ORDER BY

Answer: A

NEW QUESTION 19

What are two advantages of setting up fabric ADOM? (Choose two.)

- A. It can be used for fast data processing and log correlation
- B. It can be used to facilitate communication between devices in same Security Fabric
- C. It can include all Fortinet devices that are part of the same Security Fabric
- D. It can include only FortiGate devices that are part of the same Security Fabric

Answer: AC

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/448471/creating-a-security-fabric-a>

NEW QUESTION 23

What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

- A. Hot swap the disk.
- B. There is no need to do anything because the disk will self-recover.
- C. Run execute format disk to format and restart the FortiAnalyzer device.
- D. Shut down FortiAnalyzer and replace the disk

Answer: A

Explanation:

https://help.fortinet.com/fa/faz50hlp/56/5-6-2/FMG-FAZ/0700_RAID/0800_Swapping%20Disks.htm#:~:text=If

NEW QUESTION 25

Which two statements are true regarding ADOM modes? (Choose two.)

- A. You can only change ADOM modes through CLI.
- B. In normal mode, the disk quota of the ADOM is fixed and cannot be modified, but in advance mode, the disk quota of the ADOM is flexible because new devices are added to the ADOM.
- C. In an advanced mode ADO
- D. you can assign FortiGate VDOMs from a single FortiGate device to multiple FortiAnalyzer ADOMs.
- E. Normal mode is the default ADOM mode.

Answer: CD

NEW QUESTION 30

What is Log Insert Lag Time on FortiAnalyzer?

- A. The number of times in the logs where end users experienced slowness while accessing resources.
- B. The amount of lag time that occurs when the administrator is rebuilding the ADOM database.
- C. The amount of time that passes between the time a log was received and when it was indexed on FortiAnalyzer.
- D. The amount of time FortiAnalyzer takes to receive logs from a registered device

Answer: C

NEW QUESTION 32

Which two statement are true regardless initial Logs sync and Log Data Sync for Ha on FortiAnalyzer?

- A. By default, Log Data Sync is disabled on all backup device.
- B. Log Data Sync provides real-time log synchronization to all backup devices.
- C. With initial Logs Sync, when you add a unit to an HA cluster, the primary device synchronizes its logs with the backup device.
- D. When Logs Data Sync is turned on, the backup device will reboot and then rebuilt the log database with the synchronized logs.

Answer: CD

NEW QUESTION 36

Which statement describes a dataset in FortiAnalyzer?

- A. They determine what data is retrieved from the databas
- B. They provide the layout used for reports.
- C. They are used to set the data included in template
- D. They define the chart types to be used in report

Answer: A

NEW QUESTION 39

On FortiAnalyzer, what is a wildcard administrator account?

- A. An account that permits access to members of an LDAP group
- B. An account that allows guest access with read-only privileges

- C. An account that requires two-factor authentication
- D. An account that validates against any user account on a FortiAuthenticator

Answer: A

Explanation:

<https://docs.fortinet.com/document/fortigate/6.2.0/cookbook/747268/configuring-wildcard-admin-accounts>

NEW QUESTION 42

Logs are being deleted from one of your ADOMs earlier than the configured setting for archiving in your data policy. What is the most likely problem?

- A. The total disk space is insufficient and you need to add other disk.
- B. CPU resources are too high.
- C. The ADOM disk quota is set too low based on log rates.
- D. Logs in that ADOM are being forwarded in real-time to another FortiAnalyzer device.

Answer: C

Explanation:

https://help.fortinet.com/fmgr/50hlp/56/5-6-1/FMG_FAZ/1100_Storage/0017_Deleted%20device%20logs.htm
<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/87802/automatic-deletion>

NEW QUESTION 45

How can you attach a report to an incident?

- A. By attaching it to an event handler alert
- B. By editing the settings of the desired report
- C. From the properties of an existing incident
- D. Saving it in JSON format, and then importing it

Answer: C

NEW QUESTION 46

What can you do on FortiAnalyzer to restrict administrative access from specific locations?

- A. Configure trusted hosts for that administrator.
- B. Enable geo-location services on accessible interface.
- C. Configure two-factor authentication with a remote RADIUS server.
- D. Configure an ADOM for respective location.

Answer: A

NEW QUESTION 48

Logs are being deleted from one of the ADOMs earlier than the configured setting for archiving in the data policy. What is the most likely problem?

- A. CPU resources are too high
- B. Logs in that ADOM are being forwarded, in real-time, to another FortiAnalyzer device
- C. The total disk space is insufficient and you need to add other disk
- D. The ADOM disk quota is set too low, based on log rates

Answer: D

NEW QUESTION 50

After you have moved a registered logging device out of one ADOM and into a new ADOM, what is the purpose of running the following CLI command?
execute sql-local rebuild-adom <new-ADOM-name>

- A. To reset the disk quota enforcement to default
- B. To remove the analytics logs of the device from the old database
- C. To migrate the archive logs to the new ADOM
- D. To populate the new ADOM with analytical logs for the moved device, so you can run reports

Answer: D

Explanation:

- Are the device's analytics logs required for reports in the *new* ADOM? If so, rebuild the new ADOM database:

```
# exe sql-local rebuild-adom <new-ADOM-name>
```

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 128: Are the device analytics logs required for reports in the new ADOM? If so, rebuild the new ADOM database

NEW QUESTION 52

What is the purpose of employing RAID with FortiAnalyzer?

- A. To introduce redundancy to your log data
- B. To provide data separation between ADOMs
- C. To separate analytical and archive data

D. To back up your logs

Answer: A

Explanation:

[https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20\(%22Redundant%20Array%20of%20Inexpensive,%2C%](https://en.wikipedia.org/wiki/RAID#:~:text=RAID%20(%22Redundant%20Array%20of%20Inexpensive,%2C%)

NEW QUESTION 55

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 mail server that can be used to send email. What could be the problem?

- A. Fortinet is assigned the Standard_ User administrator profile.
- B. A trusted host is configured.
- C. ADOM mode is configured with Advanced mode.
- D. Fortinet is assigned the Restricted_ User administrator profile.

Answer: A

Explanation:

- 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

NEW QUESTION 56

You are using RAID with a FortiAnalyzer that supports software RAID, and one of the hard disks on FortiAnalyzer has failed. What is the recommended method to replace the disk?

- A. Shut down FortiAnalyzer and then replace the disk
- B. Downgrade your RAID level, replace the disk, and then upgrade your RAID level
- C. Clear all RAID alarms and replace the disk while FortiAnalyzer is still running
- D. Perform a hot swap

Answer: A

Explanation:

supports hot swapping on hardware RAID only, so it is recommended that on FortiAnalyzer devices with software RAID you should shutdown FortiAnalyzer prior to exchanging the hard disk.

<https://community.fortinet.com/t5/FortiAnalyzer/Technical-Note-How-to-swap-Hard-Disk-on-FortiAnalyzer/ta->

NEW QUESTION 59

What is the purpose of a predefined template on the FortiAnalyzer?

- A. It can be edited and modified as required
- B. It specifies the report layout which contains predefined texts, charts, and macros
- C. It specifies report settings which contains time period, device selection, and schedule
- D. It contains predefined data to generate mock reports

Answer: B

NEW QUESTION 61

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?

- A. FortiAnalyzer is ensuring that the parity data of a redundant drive is valid
- B. FortiAnalyzer is writing data to a newly added hard drive to restore it to an optimal state
- C. FortiAnalyzer is writing to all of its hard drives to make the array fault tolerant
- D. FortiAnalyzer is functioning normally

Answer: C

NEW QUESTION 63

Which two settings must you configure on FortiAnalyzer to allow non-local administrators to authenticate to FortiAnalyzer with any user account in a single LDAP group? (Choose two.)

- A. A local wildcard administrator account
- B. A remote LDAP server
- C. A trusted host profile that restricts access to the LDAP group
- D. An administrator group

Answer: AB

NEW QUESTION 64

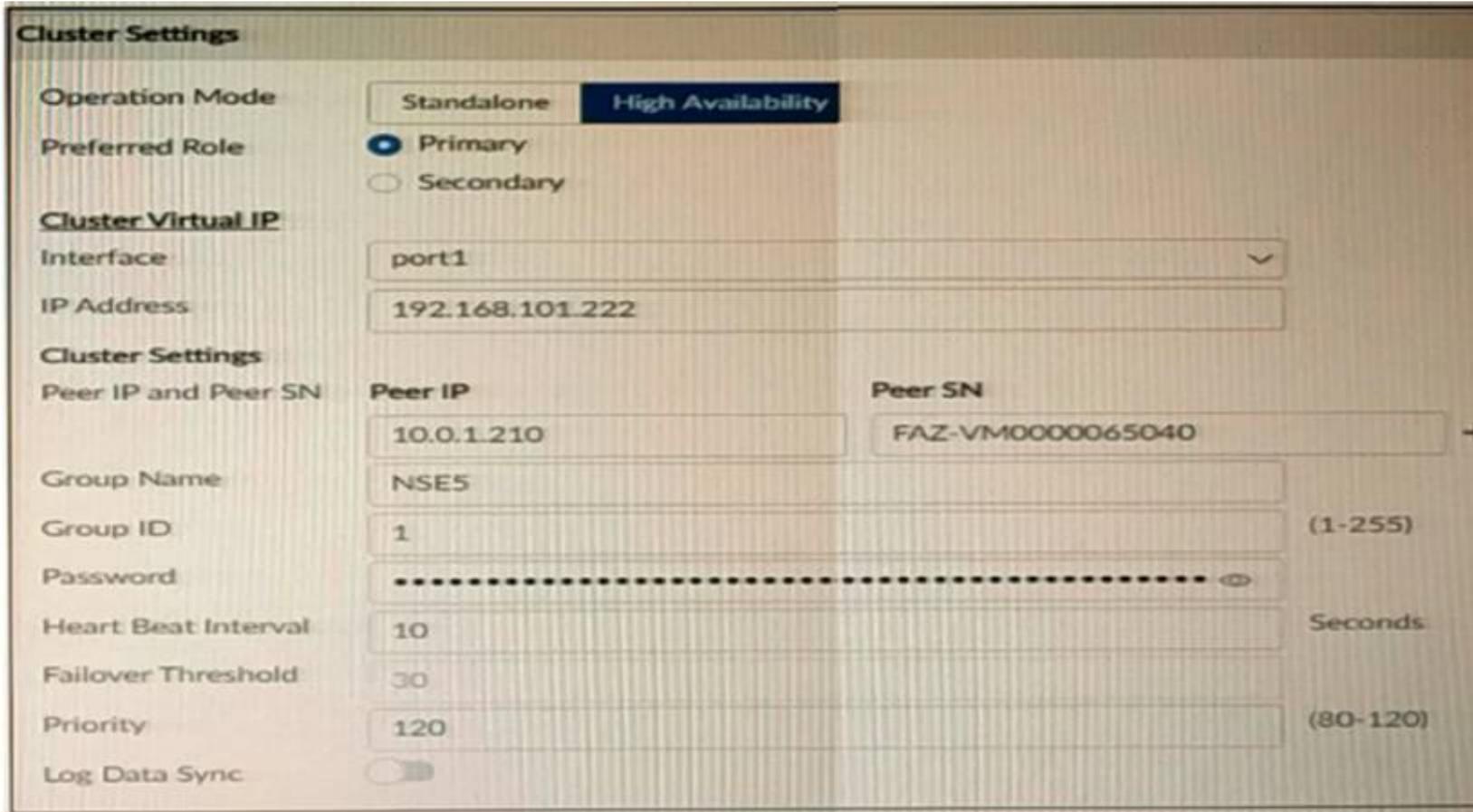
A playbook contains five tasks in total. An administrator runs the playbook and four out of five tasks finish successfully, but one task fails. What will be the status of the playbook after it is run?

- A. Running
- B. Failed
- C. Upstream_failed
- D. Success

Answer: B

NEW QUESTION 67

Refer to the exhibit.



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?

- A. This FortiAnalyzer will join to the existing HA cluster as the primary.
- B. This FortiAnalyzer is configured to receive logs in its port1.
- C. This FortiAnalyzer will trigger a failover after losing communication with its peers for 10 seconds.
- D. After joining to the cluster, this FortiAnalyzer will keep an updated log database.

Answer: B

Explanation:

"If the preferred role is Primary, then this unit becomes the primary unit if it is configured first in a new HA cluster. If there is an existing primary unit, then this unit becomes a secondary unit." (<https://docs.fortinet.com/document/fortianalyzer/7.0.5/administration-guide/275104>)

NEW QUESTION 72

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?

- A. 3.6% of the system storage is already being used.
- B. Some space is reserved for system use, such as storage of compression files, upload files, and temporary report files
- C. The oftpd process has not archived the logs yet
- D. The logfiled process is just estimating the total quota

Answer: B

Explanation:

<https://docs.fortinet.com/document/fortianalyzer/6.2.5/administration-guide/368682/disk-space-allocation>

NEW QUESTION 74

Refer to the exhibit.

| | |
|---|--|
| <pre>FortiAnalyzer1# get system status Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM Version : v7.2.1-build1215 220809 (GA) Serial Number : FAZ-VM0000065040 BIOS version : 04000002 Hostname : FortiAnalyzer1 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 1215 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 43.60GB, Total 58.80GB File System : Ext4 License Status : Valid FortiAnalyzer1# get system global adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer2 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 1 oftp-ssl-protocol : tlsv1.2 ssl-low-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 : 2000 : tlsv1.3 tlsv1.2</pre> | <pre>FortiAnalyzer3# get system status Platform Type : FAZVM64-KVM Platform Full Name : FortiAnalyzer-VM64-KVM Version : v7.2.1-build1215 220809 (GA) Serial Number : FAZ-VM0000065042 BIOS version : 04000002 Hostname : FortiAnalyzer3 Max Number of Admin Domains : 5 Admin Domain Configuration : Enabled FIPS Mode : Disabled HA Mode : Stand Alone Branch Point : 1215 Release Version Information : GA Time Zone : (GMT-8:00) Pacific Time (US & Canada) Disk Usage : Free 12.98GB, Total 79.80GB File System : Ext4 License Status : Valid FortiAnalyzer3# get system global adom-mode : normal adom-select : enable adom-status : enable console-output : standard country-flag : enable enc-algorithm : high ha-member-auto-grouping : enable hostname : FortiAnalyzer3 log-checksum : md5 log-forward-cache-size : 5 log-mode : analyzer longitude : (null) max-aggregation-tasks : 0 max-running-reports : 5 oftp-ssl-protocol : tlsv1.2 ssl-low-encryption : disable ssl-protocol : tlsv1.3 tlsv1.2 : 2000 : tlsv1.3 tlsv1.2 webservice-proto : tlsv1.3 tlsv1.2</pre> |
|---|--|

Based on the partial outputs displayed, which devices can be members of a FortiAnalyzer Fabric?

- A. FortiAnalyzer1 and FortiAnalyzer3
- B. FortiAnalyzer1 and FortiAnalyzer2
- C. All devices listed can be members
- D. FortiAnalyzer2 and FortiAnalyzer3

Answer: C

NEW QUESTION 76

What statements are true regarding FortiAnalyzer 's treatment of high availability (HA) dusters? (Choose two)

- A. FortiAnalyzer distinguishes different devices by their serial number.
- B. FortiAnalyzer receives logs from d devices in a duster.
- C. FortiAnalyzer receives bgs only from the primary device in the cluster.
- D. FortiAnalyzer only needs to know (he serial number of the primary device in the cluster-it automatically discovers the other devices.

Answer: AB

NEW QUESTION 81

Which daemon is responsible for enforcing the log file size?

- A. sqlplugind
- B. logfiled
- C. miglogd
- D. ofrpd

Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 121: The logfiled process enforces the log file size and is also responsible for disk quota enforcement by monitoring the other processes.

NEW QUESTION 84

An administrator has configured the following settings: config system fortiview settings

set resolve-ip enable end

What is the significance of executing this command?

- A. Use this command only if the source IP addresses are not resolved on FortiGate.
- B. It resolves the source and destination IP addresses to a hostname in FortiView on FortiAnalyzer.
- C. You must configure local DNS servers on FortiGate for this command to resolve IP addresses on Forti Analyzer.
- D. It resolves the destination IP address to a hostname in FortiView on FortiAnalyzer.

Answer: D

NEW QUESTION 86

When you perform a system backup, what does the backup configuration contain? (Choose two.)

- A. Generated reports
- B. Device list
- C. Authorized devices logs
- D. System information

Answer: BD

Explanation:

https://help.fortinet.com/fa/cli-ohl/5-6-5/Content/Document/1400_execute/backup.htm

NEW QUESTION 89

What statements are true regarding disk log quota? (Choose two)

- A. The FortiAnalyzer stops logging once the disk log quota is met.
- B. The FortiAnalyzer automatically sets the disk log quota based on the device.
- C. The FortiAnalyzer can overwrite the oldest logs or stop logging once the disk log quota is met.
- D. The FortiAnalyzer disk log quota is configurable, but has a minimum of 100mb a maximum based on the reserved system space.

Answer: CD

NEW QUESTION 93

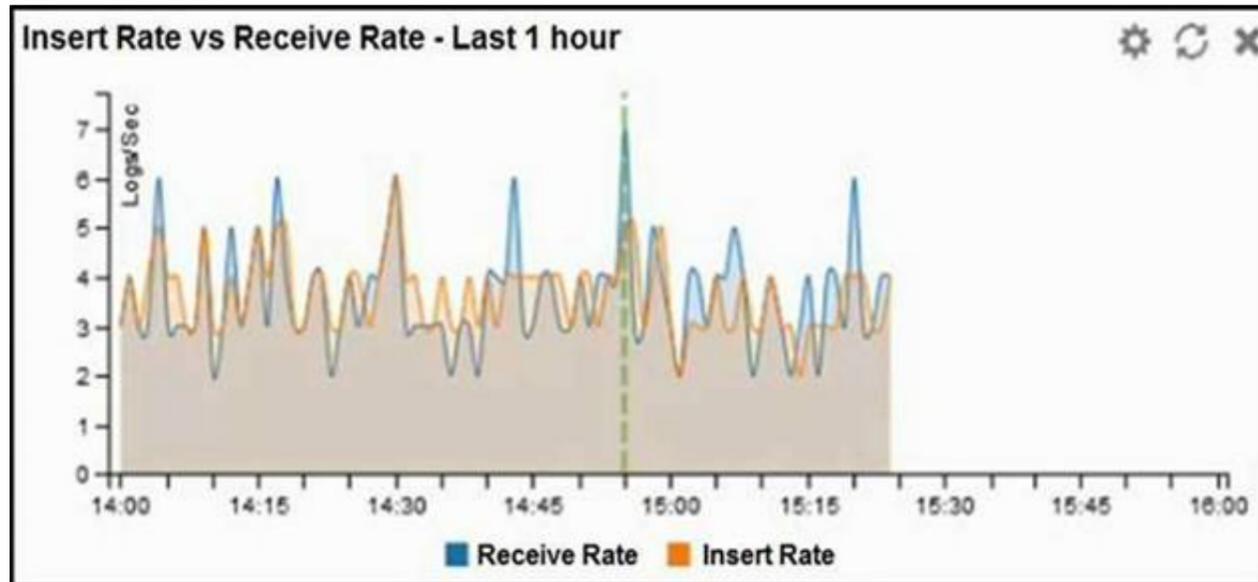
What purposes does the auto-cache setting on reports serve? (Choose two.)

- A. To reduce report generation time
- B. To automatically update the hcache when new logs arrive
- C. To reduce the log insert lag rate
- D. To provide diagnostics on report generation time

Answer: AB

NEW QUESTION 97

Refer to the exhibit.



What does the data point at 14:55 tell you?

- A. The received rate is almost at its maximum for this device
- B. The sqlplugind daemon is behind in log indexing by two logs
- C. Logs are being dropped
- D. Raw logs are reaching FortiAnalyzer faster than they can be indexed

Answer: D

NEW QUESTION 99

Refer to the exhibit.



What does the data point at 12:20 indicate?

- A. The performance of FortiAnalyzer is below the baseline.
- B. FortiAnalyzer is using its cache to avoid dropping logs.
- C. The log insert lag time is increasing.
- D. The sqlplugind service is caught up with new logs.

Answer: C

NEW QUESTION 102

What are analytics logs on FortiAnalyzer?

- A. Log type Traffic logs.
- B. Logs that roll over when the log file reaches a specific size.
- C. Logs that are indexed and stored in the SQL.
- D. Raw logs that are compressed and saved to a log file.

Answer: C

NEW QUESTION 104

What is the purpose of output variables?

- A. To store playbook execution statistics
- B. To use the output of the previous task as the input of the current task
- C. To display details of the connectors used by a playbook
- D. To save all the task settings when a playbook is exported

Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 242: Output variables allow you to use the output from a preceding task as an input to the current task. "Output variables allow you to use the output from a preceding task as an input to the current task." FortiAnalyzer_7.0_Study_Guide-Online page 242

NEW QUESTION 108

In Log View, you can use the Chart Builder feature to build a dataset and chart based on the filtered search results. Similarly, which feature you can use for FortiView?

- A. Export to Report Chart
- B. Export to PDF
- C. Export to Chart Builder
- D. Export to Custom Chart

Answer: A

NEW QUESTION 109

Which two of the following must you configure on FortiAnalyzer to email a FortiAnalyzer report externally? (Choose two.)

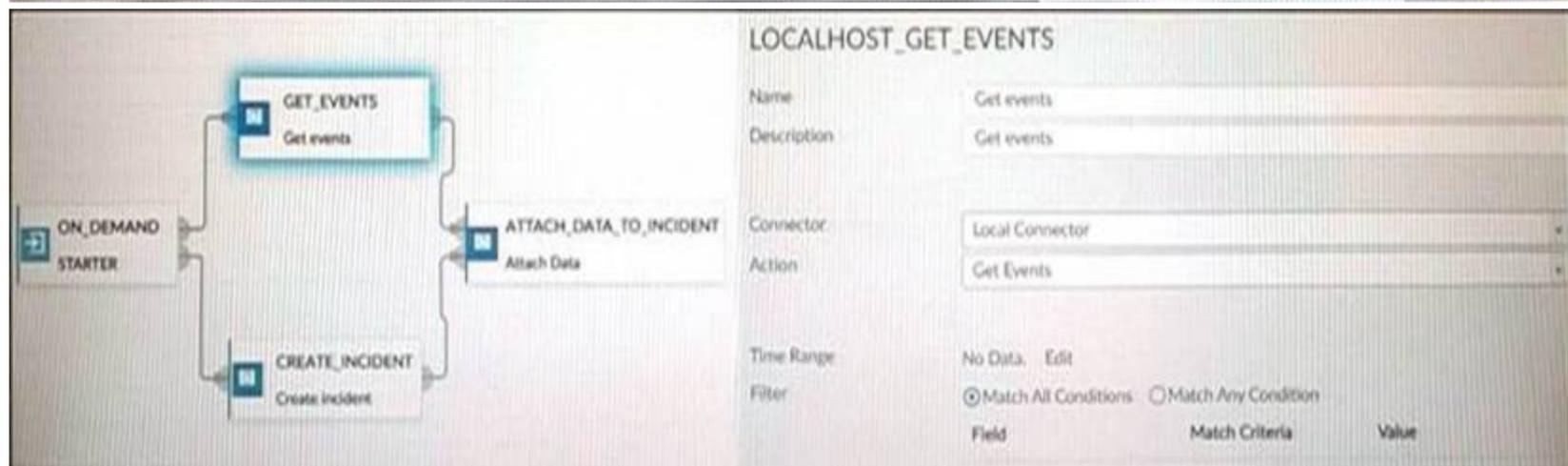
- A. Mail server
- B. Output profile
- C. SFTP server
- D. Report scheduling

Answer: AB

NEW QUESTION 111

Refer to the exhibits.

| Event | Event Status | Event Type | Count | Severity | First Occurrence | Last Update | Handler | Tags |
|---|--------------|------------|-------|----------|---------------------|---------------------|---|---------------------|
| > MS.IIS.bdir.HTR.Information.Disclosure (2) | Mitigated | IPS | 4 | Medium | 2 hours ago | 2 hours ago | Default-Malicious-Code-Detection-By-Threat | |
| > PHPURL.Code.Injection (2) | Mitigated | IPS | 4 | Medium | 2 hours ago | 2 hours ago | Default-Malicious-Code-Detection-By-Threat | |
| > 91.189.92.18 (1) | Mitigated | SSL | 5 | Low | 2 hours ago | 2 hours ago | Default-Risky-Destination-Detection-By-Threat | Risky SSL |
| > HTTP.Request.URI.Directory.Traversal (2) | Mitigated | IPS | 4 | Medium | 2 hours ago | 2 hours ago | Default-Malicious-Code-Detection-By-Threat | |
| > Apache.Expect.Header.XSS (2) | Mitigated | IPS | 4 | Medium | 2 hours ago | 2 hours ago | Default-Malicious-Code-Detection-By-Threat | |
| √ 10.0.1.10 (7) | | | | | | | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion MS.IIS.bdir.HTR.Informati... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:32:33 | 2021-12-01 21:32:41 | Default-Risky-Destination-Detection-By-Endpoint | Risky SSL |
| Internal intrusion PHPURL.Code.Injection bl... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:32:11 | 2021-12-01 21:32:21 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Insecure SSL connection blocked | Mitigated | SSL | 5 | Low | 2021-12-01 21:32:01 | 2021-12-01 21:32:01 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion HTTP.Request.URI Direct... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:31:51 | 2021-12-01 21:32:01 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion Apache.Expect.Header.XS... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:31:31 | 2021-12-01 21:31:41 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| √ 10.200.1.254 (6) | | | | | | | | |
| Internal intrusion MS.IIS.bdir.HTR.Informati... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:32:31 | 2021-12-01 21:32:41 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion PHPURL.Code.Injection bl... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:32:11 | 2021-12-01 21:32:21 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion HTTP.Request.URI Direct... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:31:51 | 2021-12-01 21:32:01 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion Apache.Expect.Header.XS... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:31:31 | 2021-12-01 21:31:41 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion HTTP.Password.Access blocke... | Mitigated | IPS | 2 | Medium | 2021-12-01 21:31:11 | 2021-12-01 21:31:21 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |
| Internal intrusion Nikto.Web-Scanner detect... | Univariate | IPS | 21 | High | 2021-12-01 21:31:11 | 2021-12-01 21:32:36 | Default-Malicious-Code-Detection-By-Endpoint | Intrusion Signature |



How many events will be added to the incident created after running this playbook?

- A. Ten events will be added.
- B. No events will be added.
- C. Five events will be added.
- D. Thirteen events will be added.

Answer: A

NEW QUESTION 113

What is the purpose of the following CLI command?

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

- A. To add a log file checksum
- B. To add the MD's hash value and authentication code
- C. To add a unique tag to each log to prove that it came from this FortiAnalyzer
- D. To encrypt log communications

Answer: A

Explanation:

<https://docs2.fortinet.com/document/fortianalyzer/6.0.3/cli-reference/849211/global>

NEW QUESTION 115

Which FortiAnalyzer feature allows you to use a proactive approach when managing your network security?

- A. Incidents dashboards
- B. Threat hunting
- C. FortiView Monitor
- D. Outbreak alert services

Answer: B

Explanation:

FortiAnalyzer_7.0_Study_Guide-Online.pdf page 217: Threat hunting consists in proactively searching for suspicious or potentially risky network activity in your environment. The proactive approach will help administrator find any threats that might have eluded detection by the current security solutions or configurations.

NEW QUESTION 118

.....

Thank You for Trying Our Product

We offer two products:

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

2nd - Questions and Answers in PDF Format

NSE5_FAZ-7.0 Practice Exam Features:

- * NSE5_FAZ-7.0 Questions and Answers Updated Frequently
- * NSE5_FAZ-7.0 Practice Questions Verified by Expert Senior Certified Staff
- * NSE5_FAZ-7.0 Most Realistic Questions that Guarantee you a Pass on Your FirstTry
- * NSE5_FAZ-7.0 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The NSE5_FAZ-7.0 Practice Test Here](#)