Fortinet

Exam Questions FCP_FAZ_AD-7.4

FCP - FortiAnalyzer 7.4 Administrator

NEW QUESTION 1
An administrator has moved a FortiGate device from the root ADOM to ADOM1. Which two statements are true regarding logs? (Choose two.)

A. Analytics logs will be moved to ADOM1 from the root ADOM automatically.
B. Archived logs will be moved to ADOM1 from the root ADOM automatically.
C. Logs will be present in both ADOMs immediately after the move.
D. Analytics logs will be moved to ADOM1 from the root ADOM after you rebuild the database.

Answer: AD

Explanation:
When a device is moved from one ADOM to another, analytics logs can be moved automatically, but you may need to rebuild the database for the logs to be fully transferred and usable in the new ADOM. Archived logs, however, do not move automatically between ADOMs.

NEW QUESTION 2
What is the best approach to handle a hard disk failure on a FortiAnalyzer that supports hardware RAID?

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

Answer: C

Explanation:
In a hardware RAID setup, FortiAnalyzer supports hot swapping, which allows you to replace a failed disk without shutting down the device. The RAID controller will automatically rebuild the array using the new disk, minimizing downtime and maintaining data integrity.

NEW QUESTION 3
Which process is responsible for enforcing the log file size?

A. oftpd
B. miglogd
C. sqlplugind
D. logfiled

Answer: D

Explanation:
The logfiled process is responsible for enforcing log file size and managing log rotation on FortiAnalyzer. It ensures that log files do not exceed the configured size limits and handles the creation and rotation of new log files when necessary.

NEW QUESTION 4
Which two parameters impact the amount of reserved disk space required by FortiAnalyzer? (Choose two.)

A. Total quota
B. License type
C. RAID level
D. Disk size

Answer: C

Explanation:
RAID level affects how much disk space is reserved for redundancy and fault tolerance. For example, RAID 1 mirrors data, meaning you need more space for redundancy, while RAID 5 or RAID 6 reserves space for parity.
Disk size directly influences the total available and reserved space since the larger the disk, the more space may need to be reserved for system functions, logs, and other operations.
The total quota and license type do not directly impact the reserved disk space, though they do influence other aspects of capacity and functionality.

NEW QUESTION 5
Which two statements about FortiAnalyzer operating modes are true? (Choose two.)

A. When in collector mode, FortiAnalyzer offloads the log receiving task to the analyzer.
B. When in analyzer mode, FortiAnalyzer supports event management and reporting features.
C. For the collector, you should allocate most of the disk space to analytics logs.
D. Analyzer mode is the default operating mode.

Answer: B

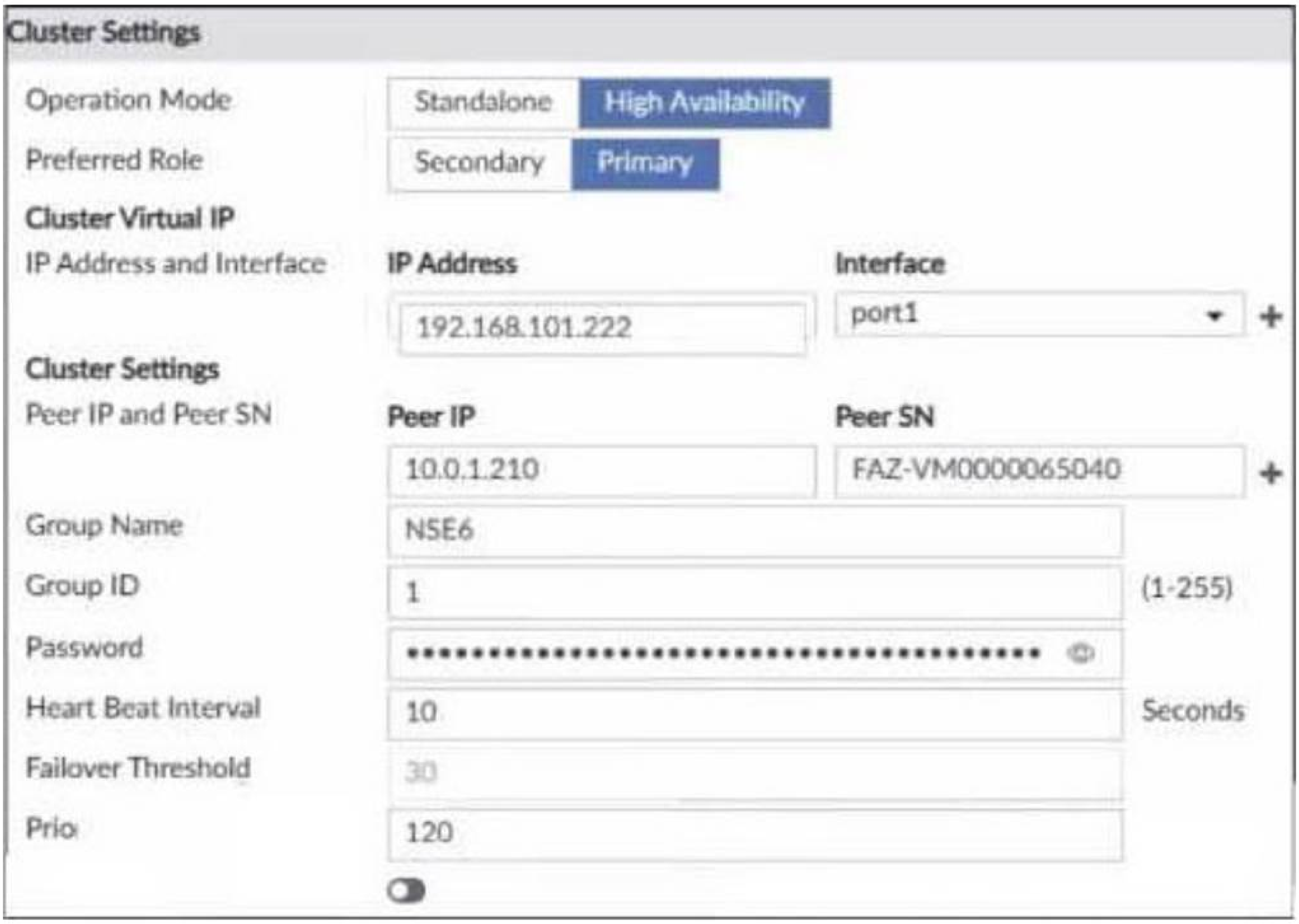
Explanation:
When in analyzer mode, FortiAnalyzer supports event management and reporting features.
In analyzer mode, FortiAnalyzer provides full support for log analysis, event management, and reporting capabilities.
Analyzer mode is the default operating mode.
By default, FortiAnalyzer operates in analyzer mode, which allows for log analysis and reporting. The other options are incorrect because:
In collector mode, the FortiAnalyzer primarily stores logs and forwards them to another FortiAnalyzer in analyzer mode, not the other way around.
In collector mode, most disk space is usually allocated to storage rather than analytics, as the logs are primarily stored for forwarding.

NEW QUESTION 6
Which two statements regarding ADOM modes are true? (Choose two.)

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

Answer: CD

NEW QUESTION 7
Refer to the exhibit.



Cluster Settings

Operation Mode	Standalone / **High Availability**	
Preferred Role	Secondary / **Primary**	
Cluster Virtual IP		
IP Address and Interface	**IP Address**	**Interface**
	192.168.101.222	port1
Cluster Settings		
Peer IP and Peer SN	**Peer IP**	**Peer SN**
	10.0.1.210	FAZ-VM0000065040
Group Name	NSE6	
Group ID	1	(1-255)
Password	●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●●	
Heart Beat Interval	10	Seconds
Failover Threshold	30	
Prio	120	

The image displays "he configuration of a FortiAnalyzer the administrator wants to join to an existing HA cluster.
What can you conclude from the configuration displayed?

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

Answer: A

Explanation:
Operation Mode: The mode is set to "High Availability" which indicates that this FortiAnalyzer is intended to be part of an HA cluster.
Preferred Role: The "Primary" role is selected, meaning this device is configured to act as the primary unit in the HA cluster. This is a crucial setting as it determines the device's behavior and responsibilities within the cluster.
Cluster Virtual IP: A specific IP address (192.168.101.222) is assigned to be used by devices in the network to communicate with the cluster. This Virtual IP will be shared between the units in the cluster.
Cluster Settings: These include configurations for heartbeat interval, failover threshold, and priority which are crucial for maintaining cluster health and managing failover scenarios.
Given these points, the correct conclusion from the options provided is:
* C. This FortiAnalyzer will join the existing HA cluster as the primary.

NEW QUESTION 8
Which statement is true when you are upgrading the firmware on an HA cluster made up of throe

FortiAnalyzer devices?

A. All FortiAnalyzer devices will be upgraded at the same time.
B. Enabling uninterruptible-upgrade prevents normal operations from being interrupted during theupgrade.
C. You can perform the firmware upgrade using only a console connection.
D. First, upgrade the secondary devices, and then upgrade the primary device.

Answer: D

Explanation:
In an HA cluster, the firmware upgrade process involves upgrading the secondary devices first. This approach ensures that the primary device can continue to handle traffic and maintain the operational stability of the network while the secondary devices are being upgraded. Once the secondary devices have successfully upgraded their firmware and are operational, the primary device can then be upgraded. This method minimizes downtime and maintains network integrity during the upgrade process.
When upgrading firmware in a High Availability (HA) cluster of FortiAnalyzer units, the recommended practice is to first upgrade the secondary devices before upgrading the primary device. This approach ensures that the primary device, which coordinates the cluster's operations, remains functional for as long as possible, minimizing the impact on log collection and analysis. Once the secondary devices are successfully upgraded and operational, the primary device can be upgraded, ensuring a smooth transition and maintaining continuous operation of the cluster.
Reference: FortiAnalyzer 7.2 Administrator Guide - "System Administration" and "High Availability" sections.

NEW QUESTION 9
Which two statements regarding FortiAnalyzer log forwarding modes are true? (Choose two.)

A. Both modes, forwarding and aggregation, support encryption of logs between devices.
B. In aggregation mode, you can forward logs to syslog and CEF servers.
C. Forwarding mode forwards logs in real time only to other FortiAnalyzer devices.
D. Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.

Answer: AD

Explanation:
Both modes, forwarding and aggregation, support encryption of logs between devices.
Both forwarding and aggregation modes can use encryption to securely transfer logs between FortiAnalyzer devices.
Aggregation mode stores logs and content files and uploads them to another FortiAnalyzer device at a scheduled time.
In aggregation mode, logs are stored and then transferred to another FortiAnalyzer at a scheduled time, rather than in real-time. This mode is typically used when consolidating logs from multiple devices into a central FortiAnalyzer.
The other options are incorrect because:
Forwarding mode sends logs in real-time but not exclusively to other FortiAnalyzer devices; it can also send logs to external systems like syslog servers.
Aggregation mode is primarily for consolidating logs to another FortiAnalyzer and doesn't focus on forwarding logs to syslog or CEF servers.

NEW QUESTION 10
What does the disk status Degraded mean for RAID management?

A. The hard drive is no longer being used by the RAID controller.
B. One or more drives are missing from the FortiAnalyzer unit.
C. The device is writing data to the disk to restore the volume to an optimal state.
D. FortiAnalyzer determined that the parity data in the disk is not valid.

Answer: B

Explanation:
When the RAID status is Degraded, it typically indicates that one or more drives in the RAID array have failed or are missing, causing the RAID array to operate with reduced redundancy. In this state, the array is still functioning, but it's at risk because the fault tolerance provided by RAID is compromised.

NEW QUESTION 10
In a Fortinet Security Fabric, what can make an upstream FortiGate create traffic logs associated with sessions initiated on downstream FortiGate devices?

A. The traffic destination is another FortiGate in the fabric.
B. The upstream FortiGate is configured to do NAT
C. Log redundancy is configured in the fabric.
D. The downstream device cannot connect to FortiAnalyzer.

Answer: B

Explanation:
When the upstream FortiGate is performing Network Address Translation (NAT), it creates new session entries for traffic passing through it. As a result, it generates its own traffic logs for those sessions, even if the sessions were initiated on a downstream FortiGate.
This is because the upstream FortiGate is altering the source IP address, making it responsible for tracking the session details.

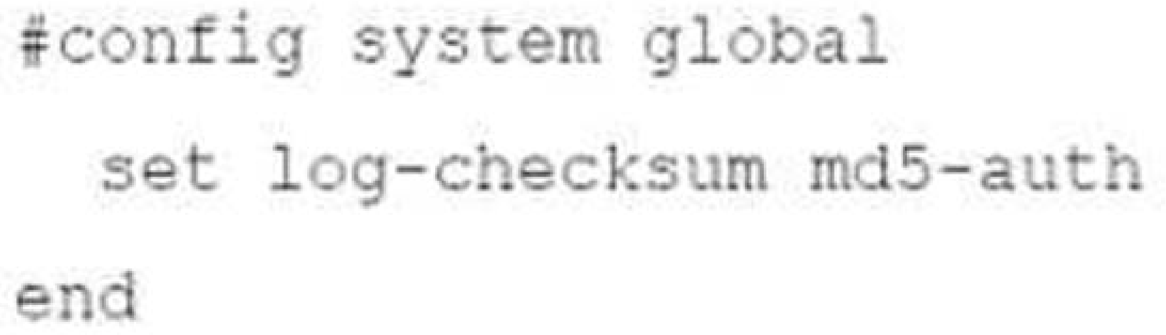
NEW QUESTION 11
Which statement about the communication between FortiGate high availability (HA) clusters and FortiAnalyzer is true?

A. If devices were registered to FortiAnalyzer before forming a cluster, you can manually add them togethe
B. FortiAnalyzer distinguishes each cluster member by the IP addresses in log message header
C. If the HA primary device becomes unavailable, you must remove it from the HA cluster list on FortiAnalyze
D. The FortiGate HA cluster must be in active-passive mode in order to avoid conflict.

Answer: B

Explanation:
This allows FortiAnalyzer to correctly identify and process logs from different members of the HA cluster.

NEW QUESTION 12
An administrator has configured the following settings:



```
#config system global
   set log-checksum md5-auth
end
```

What is the purpose of executing these commands?

A. To record the hash value and authentication code of log file
B. To encrypt log transfer between FortiAnalyzer and other device
C. To create the secure channel used by the OFTP proces
D. To verify the integrity of the log files received.

Answer: A

Explanation:
:
The command set log-checksum md5-auth configures FortiAnalyzer to generate an MD5 hash for each log file, along with an authentication code. This ensures that the integrity of the logs can be verified, confirming that the logs have not been tampered with.

NEW QUESTION 13
You finished registering a FortiGate device. After traffic starts to flow through FortiGate, you notice that only some of the logs expected are being received on FortiAnalyzer.
What could be the reason for the logs not arriving on FortiAnalyzer?

A. This FortiGate is part of an HA cluster but it is the secondary device.
B. This FortiGate model is not fully supported.
C. FortiGate does not have logging configured correctly.
D. FortiGate was added to the wrong ADOM type.

Answer: C

Explanation:
When only some of the expected logs from a FortiGate device are being received on FortiAnalyzer, it often indicates a configuration issue on the FortiGate side. Proper logging configuration on FortiGate involves specifying what types of logs to generate (e.g., traffic, event, security logs) and ensuring that these logs are directed to the FortiAnalyzer unit for storage and analysis. If the logging settings on FortiGate are not correctly configured, it could result in incomplete log data being sent to FortiAnalyzer. This might include missing logs for certain types of traffic or events that are not enabled for logging on the FortiGate device.
Ensuring comprehensive logging is enabled and correctly directed to FortiAnalyzer is crucial for full visibility into network activities and for the effective analysis and reporting of security incidents and network performance.

NEW QUESTION 18
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:
RAID (Redundant Array of Independent Disks) is used in FortiAnalyzer primarily to provide data redundancy and ensure data integrity. Here,s how it relates to each option:
To Introduce Redundancy to Your Log Data (Option A):
The main purpose of employing RAID in FortiAnalyzer is to add redundancy to the storage system. By using RAID configurations (such as RAID 1, RAID 5, or RAID 6), data is replicated across multiple disks, which helps in protecting against disk failures and ensures that log data is not lost if a disk fails. This redundancy enhances the reliability and availability of the log data.

NEW QUESTION 19
Which statements are true of Administrative Domains (ADOMs) in FortiAnalyzer? (Choose two.)

A. ADOMs are enabled by default.
B. ADOMs constrain other administrator??s access privileges to a subset of devices in the device list.
C. Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM.
D. All administrators can create ADOMs--not just the admin administrator.

Answer: BC

Explanation:
ADOMs constrain other administrators' access privileges to a subset of devices in the device list: ADOMs allow you to partition the FortiAnalyzer's management capabilities by restricting access to certain devices and logs based on the administrator's role. This segmentation helps in managing large deployments with different administrative needs.
Once enabled, the Device Manager, FortiView, Event Management, and Reports tab display per ADOM: When ADOMs are enabled, the FortiAnalyzer interface segments the Device Manager, FortiView, Event Management, and Reports tabs based on the selected ADOM. This allows administrators to work within their specific ADOM context.
ADOMs are enabled by default: This is incorrect because ADOMs are not enabled by default. They must be manually configured and enabled according to the organization's needs.
All administrators can create ADOMs--not just the admin administrator: This is not correct. Typically, creating and managing ADOMs requires administrative privileges, often restricted to the main admin or specific roles with sufficient permissions.

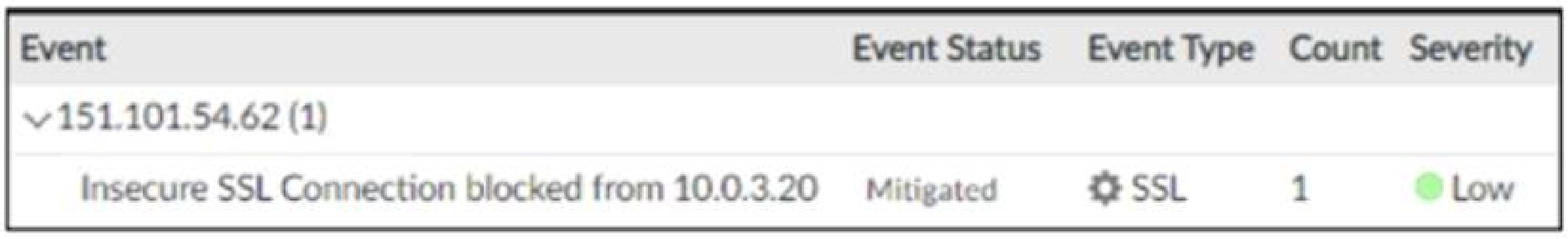
NEW QUESTION 22
Which SQL query is in the correct order to query the database in the FortiAnalyzer?

A. SELECT devid FROM Slog GROOP BY devid WHERE * user' =* USERl'
B. SELECT devid WHERE 'u3er'='USERl' FROM $ log GROUP BY devid
C. SELECT devid FROM Slog- WHERE *user' =' USERl' GROUP BY devid
D. FROM Slog WHERE 'user* =' USERl' SELECT devid GROUP BY devid

Answer: C

Explanation:
C is correct because it follows the proper SQL query structure:
SELECT: Specifies the column(s) to retrieve.
FROM: Indicates the table to query (Slog in this case).
WHERE: Adds a condition to filter the results (user = 'USERl').
GROUP BY: Groups the results by the specified column (devid).
A, B, and D are incorrect because they do not follow the correct SQL query order:
A is incorrect because the GROUP BY clause is incorrectly placed before the WHERE clause.
B is incorrect because the WHERE clause is incorrectly placed before the FROM clause.
D is incorrect because the SELECT clause is incorrectly placed after the FROM and WHERE clauses.

NEW QUESTION 24
Refer to the exhibit.



Event	Event Status	Event Type	Count	Severity
⌄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?

A. An incident was created from this event.
B. The security risk was blocked or dropped.
C. The security event risk is considered open.
D. The risk source is isolated.

Answer: B

Explanation:
The event status is "Mitigated", which indicates that the insecure SSL connection was successfully blocked or prevented.
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.

NEW QUESTION 28
......