



- Expert Verified, Online, **Free**.




CERTIFICATION TEST

- CertificationTest.net - Cheap & Quality Resources With Best Support

Consider the storage of anomaly baseline data that is calculated for different parameters.
Which database is used for storing this data?

- A. Event DB
- B. Profile DB
- C. SVN DB
- D. CMDB

Suggested Answer: *B*

  **Kachiugwu** 5 months, 4 weeks ago

Selected Answer: B

B is the correct answer

upvoted 1 times

  **Geraldinel** 9 months ago



B is correct

upvoted 1 times

Which two FortiSIEM components work together to provide real-time event correlation?

- A. Supervisor and worker
- B. Collector and Windows agent
- C. Worker and collector
- D. Supervisor and collector

Suggested Answer: A

  **linnieOuO** 8 months, 1 week ago

A

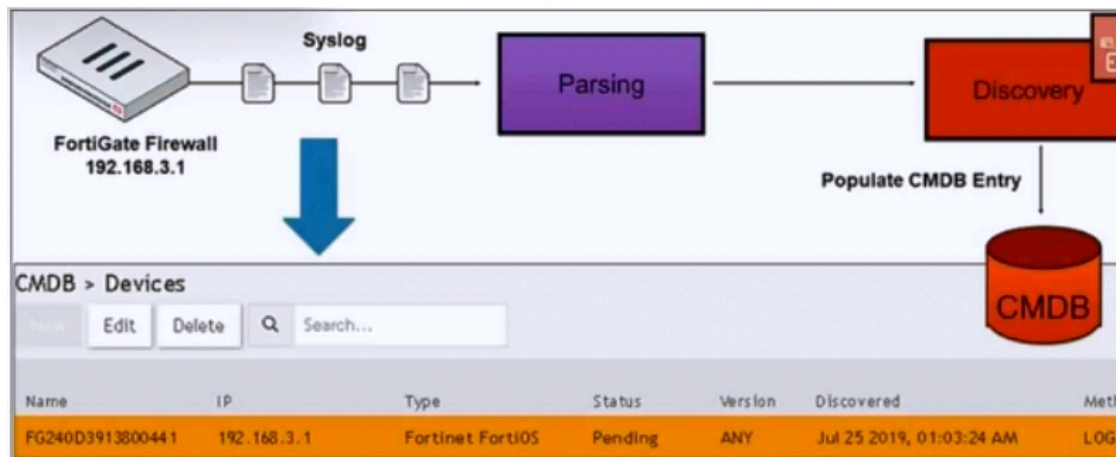
upvoted 1 times

  **Geraldinel** 9 months ago

A is correct

upvoted 1 times

Refer to the exhibit.



How was the FortiGate device discovered by FortiSIEM?

- A. GUI log discovery
- B. Syslog discovery
- C. Pull events discovery
- D. Auto log discovery

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

When configuring collectors located in geographically separated sites, what ports must be open on a front end firewall?

- A. HTTPS, from the collector to the worker upload settings address only
- B. HTTPS, from the collector to the supervisor and worker upload settings addresses
- C. HTTPS, from the Internet to the collector
- D. HTTPS, from the Internet to the collector and from the collector to the FortiSIEM cluster

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

An administrator is configuring FortiSIEM to discover network devices and receive syslog from network devices. Which statement is correct?

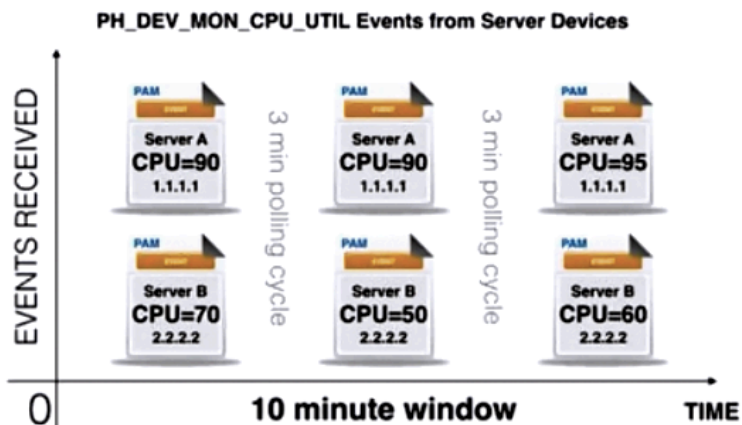
- A. FortiSIEM uses privileged credentials to log in to devices and make network configuration changes.
- B. FortiSIEM automatically configures network devices to send syslog using the auto log discovery process.
- C. FortiSIEM automatically configures network devices to send syslog using the GUI discovery process.
- D. Syslog configuration must be done manually on devices by the network administrator.

Correct Answer: D

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibits.

Performance Events



Server A Properties

CMDB > Devices > **Server A** > Edit > Properties

Edit Device

Summary Contact Interfaces **Properties** Parser

Server CPU Util Critical Threshold:

Server CPU Util Warning Threshold:

Server B Properties

CMDB > Devices > **Server B** > Edit > Properties

Edit Device

Summary Contact Interfaces **Properties** Parser

Server CPU Util Critical Threshold:

Server CPU Util Warning Threshold:

Rule Sub Pattern

DeviceToCMDBAttr(Host IP : Server CPU Util Critical Threshold)

Aggregate:	Paren	Attribute	Operator	Value	Paren	Next	Row
	<input type="radio"/>	AVG(CPU Util)	>	DeviceToCMDBAttr(Host IP : Server	<input type="radio"/>	AND	<input type="radio"/>
	<input type="radio"/>	COUNT(Matched Events)	>=	2	<input type="radio"/>	AND	<input type="radio"/>
Group By:							
	Attribute		Row	Move			
	Host IP		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
	Host Name		<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Three events are collected over a 10-minute time period from two servers: Server A and Server B.

Based on the settings for the rule subpattern, how many incidents will the servers generate?

- A. Server A will generate one incident and Server B will generate one incident.
- B. Server A will generate one incident and Server B will not generate any incidents.

C. Server B will generate one incident and Server A will not generate any incidents.

D. Server A will not generate any incidents and Server B will not generate any incidents.

Correct Answer: *B*

Currently there are no comments in this discussion, be the first to comment!

An administrator is using SNMP and WMI credentials to discover a Windows device.
How will the WMI method handle this?

- A. WMI method will collect only traffic and IIS logs.
- B. WMI method will collect only DNS logs.
- C. WMI method will collect only DHCP logs.
- D. WMI method will collect security, application, and system events logs.

Correct Answer: *D*

Currently there are no comments in this discussion, be the first to comment!

An administrator is in the process of renewing a FortiSIEM license.
Which two commands will provide the system ID? (Choose two.)

- A. phgetHWID
- B. ./phLicenseTool -support
- C. phgetUUID
- D. ./phLicenseTool -show

Correct Answer: AC

🗉 👤 **Geraldinel** 4 months, 1 week ago

Selected Answer: CD

Correct Answer is C and D

upvoted 1 times

🗉 👤 **ffdfa63** 6 months ago

Selected Answer: CD

I checked on the FSM CLI, and the correct answers are C and D.

upvoted 2 times

If a performance rule is triggered repeatedly due to high CPU use, what occurs in the incident table?

- A. A new incident is created each time the rule is triggered, and the First Seen and Last Seen times are updated.
- B. A new incident is created based on the Rule Frequency value, and the First Seen and Last Seen times are updated.
- C. The Incident Count value increases, and the First Seen and Last Seen times update.
- D. The incident status changes to Repeated, and the First Seen and Last Seen times are updated.

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

The screenshot shows the FortiSIEM search interface. At the top, a search bar contains the query: `Reporting IP = 192.168.1.1 AND Reporting IP = 172.16.10.3`. Below the search bar, there are radio buttons for **Keyword** and **Attribute**, with **Attribute** selected. A table below shows the search criteria:

Paren	Attribute	Operator	Value	Paren
(Reporting IP	=	192.168.1.1)
(Reporting IP	=	172.16.10.3)

Below the table, there are radio buttons for **Time** selection: **Real Time**, **Relative**, and **Absolute**, with **Absolute** selected. The **From** date is `01/13/2020 13:19:41` and the **To** date is `01/20/2020 13:29:41`. There is also a checkbox for **Always prior**.

The FortiSIEM administrator is examining events for two devices to investigate an issue. However, the administrator is not getting any results from their search,

Based on the selected filters shown in the exhibit, why is the search returning no results?

- A. Parenthesis are missing.
- B. The wrong boolean operator is selected in the Next column.
- C. The wrong option is selected in the Operator column.
- D. An invalid IP subnet is typed in the Value column.

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

The screenshot shows the 'Edit SubPattern' window for a pattern named 'DomainAcctLockout'. It contains three main sections: Filters, Aggregate, and Group By.

Filters:

Filter	Attribute	Operator	Value
1	Event Type	IN	EventTypes: Domain Account Lockout
2	Reporting IP	IN	Applications: Domain Controller

Aggregate:

Attribute	Operator	Value
COUNT(Matched Events)	>=	1

Group By:

Attribute	Row	Move
Reporting Device	1	1
Reporting IP	2	2
User	3	3

Which section contains the settings that determine how many incidents are created?

- A. Actions
- B. Group By
- C. Aggregate
- D. Filters

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by User, Source IP, and Application Category attributes in FortiSIEM, how many results will be displayed?

- A. Three results will be displayed.
- B. Five results will be displayed.
- C. No results will be displayed.
- D. Seven results will be displayed.

Correct Answer: B

Currently there are no comments in this discussion, be the first to comment!

Refer to the exhibit.

Event Receive Time	Reporting IP	Event Type	User	Source IP	Application Category
09:12:11	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:12:56	10.10.10.11	Failed Logon	John	5.5.5.5	DB
09:15:56	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App
09:20:01	10.10.10.10	Failed Logon	Paul	3.3.2.1	Web App
10:10:43	10.10.10.11	Failed Logon	Ryan	1.1.1.15	DB
10:45:08	10.10.10.11	Failed Logon	Wendy	1.1.1.6	DB
11:23:33	10.10.10.10	Failed Logon	Ryan	1.1.1.15	DB
12:05:52	10.10.10.10	Failed Logon	Ryan	1.1.1.1	Web App

If events are grouped by Event Type and User attributes in FortiSIEM, how many results will be displayed?

- A. Four results will be displayed.
- B. Eight results will be displayed.
- C. Two results will be displayed.
- D. No results will be displayed.


Suggested Answer: B

 **Beatledrew** 2 months ago

Selected Answer: A

A is correct.

upvoted 1 times

 **PRASAD180** 3 months, 1 week ago

A is correct


upvoted 1 times

 **Goudy** 3 months, 1 week ago

Selected Answer: A

There is just one Event Type, and 4 different names, it should be (A), why is (B) selected?

upvoted 1 times

 **burcrt21** 9 months, 1 week ago

the answer should be 4 (A) because we are grouping according to user.

upvoted 3 times

Which process converts raw log data to structured data?

- A. Data classification
- B. Data validation
- C. Data parsing
- D. Data enrichment

Correct Answer: C

Currently there are no comments in this discussion, be the first to comment!