
Exam : **FCSS_ADA_AR-6.7**

Title : FCSS—Advanced Analytics
6.7 Architect

Version : DEMO

1.Refer to the exhibit.

0	0	1	1	0	0	0
Routers	Firewalls	Windows	Unix	ESX	AWS	Azure
CMDB > Devices						
New	Edit	Delete	FortiBank	Discovered by All	Q	Actions
Name	IP	Device Type	Status	Discovered	Method	Agent Policy
FortiBank_Collector	10.10.2.64	Generic Unix	Pending	Oct 28, 2021, 12:52:54 PM	LOG	
fortibank_dc.fortibank.net	10.10.2.63	Windows	Unmanaged	Oct 28, 2021, 02:48:42 PM	AGENT	Registered

Is the Windows agent delivering event logs correctly?

- A. The agent is registered and it is sending logs correctly.
- B. The logs are buffered by the agent and will be sent once the status changes to managed.
- C. Because the agent is unmanaged. the logs are dropped silently by the supervisor.
- D. The agent is not sending logs because it did not receive a monitoring template.

Answer: D

2.Refer to the exhibit.

Event Receive Time	Event Type	Source IP	Destination IP	Reporting IP	User	Raw Event Log
08:49:01 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02...
08:49:24 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.4 6	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02...
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02...
08:50:45 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.4 6	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02...
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02...
08:55:09 02/02/2018	FortiGate-ssl-vpn-logon-failure	198.51.100.4 6	192.0.5.30	10.0.2.10	Tom	<189>date=2018-02-02...
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.5	192.0.2.10	10.0.1.99	Admin	<189>date=2018-02-02...
08:52:59 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.4	192.0.2.10	10.0.1.99	Sarah	<189>date=2018-02-02...
08:50:31 02/02/2018	FortiGate-ssl-vpn-logon-failure	203.0.113.50	192.0.2.10	10.2.2.55	Jan	<189>date=2018-02-02...

An administrator runs an analytic search for all FortiGate SSL VPN logon failures. The results are grouped by source IP, reporting IP, and user. The administrator wants to restrict the results to only those rows where the COUNT >=3.

Which user would meet that condition?

- A. Jan
- B. Sarah
- C. Admin
- D. Tom

Answer: D

3.Refer to the exhibit.

PROCESS	UPTIME
phParser	DOWN
phAgentManager	DOWN
phCheckpoint	DOWN
phDiscover	DOWN
phEventPackager	DOWN
phPerfMonitor	DOWN
phEventForwarder	DOWN
phMonitor	13:04
phMonitorAgent	DOWN
Rsyslogd	DOWN

An administrator deploys a new collector for the first time, and notices that all the processes except the phMonitor are down.

How can the administrator bring the processes up?

- A. The collector was not deployed properly and must be redeployed.
- B. The administrator needs to run the command phtools - start all on the collector.
- C. Rebooting the collector will bring up the processes.
- D. The processes will come up after the collector is registered to the supervisor.

Answer: D

4.What happens to UEBA events when a user is off-net?

- A. The agent will cache events locally if it cannot upload them to a FortiSIEM collector
- B. The agent will drop the events if it cannot upload them to a FortiSIEM collector
- C. The agent will upload the events to the Worker if it cannot upload them to a FortiSIEM collector
- D. The agent will upload the events the events to the Supervisor if it cannot upload them to a FortiSIEM collector

Answer: A

5.Refer to the exhibit.

Edit SubPattern

Name:
DomainAcctLockout

Filters:

Paren	Attribute	Operator	Value	Paren	Next	Row
☐	Event Type	IN	EventTypes: Domain Account Locked	☐	AND	☐
☐	Reporting IP	IN	Applications: Domain Controller	☐	AND	☐

Aggregate:

Paren	Attribute	Operator	Value	Paren	Next	Row
☐	COUNT(Matched Events)	>=	1	☐	AND	☐

Group By:

Attribute	Row	Move
Reporting Device	☐	☐
Reporting IP	☐	☐
User	☐	☐

Consider the five account locked events received by FortiSIEM from domain controllers within the last 10 minutes (ten minutes is the evaluation window for the subpattern DomainAcctLockout):

Reporting IP: 1.1.1.1, Reporting Device: Server101, User: John, Domain: USA, Event Type: Account Locked

Reporting IP: 1.1.1.1, Reporting Device: Server101, User: Craig, Domain: USA, Event Type: Account Locked

Reporting IP: 1.1.1.2, Reporting Device: Server109, User: Mary, Domain: UK, Event Type: Account Locked

Reporting IP: 1.1.1.1, Reporting Device: Server101, User: Craig, Domain: USA, Event Type: Account Locked

Reporting IP: 1.1.1.1, Reporting Device: Server101, User: John, Domain: USA, Event Type: Account Locked

If you look for one or more matching events and groupings by the same reporting IP address, reporting device, and user, how many incidents are created?

- A. 3
- B. 4

C. 2

D. 1

Answer: C