Novell

Exam 050-728

Identity and Security PartnerNet Specialization: Sentinel 6.1

Version: 7.0

[Total Questions: 56]

Question No : 1

To achieve better system performance and scalability in regards to Event collection and processing, which Sentinel components can you install multiple instances of? (Choose 2)

A. Reporting server
B. Solution Designer
C. Collection Manager
D. Correlation engine
E. Sentinel Control centre

Answer: C,D

Explanation: At most one Communication Server and DAS component can be installed across all
Sentinel Servers in a distributed Sentinel installation. On the other hand, multiple instances of
Correlation Engine and Collector Managers are allowed.

Question No : 2

Which actions does the Right click option on events within an Active View allow an Administrator to perform? (Choose 3)

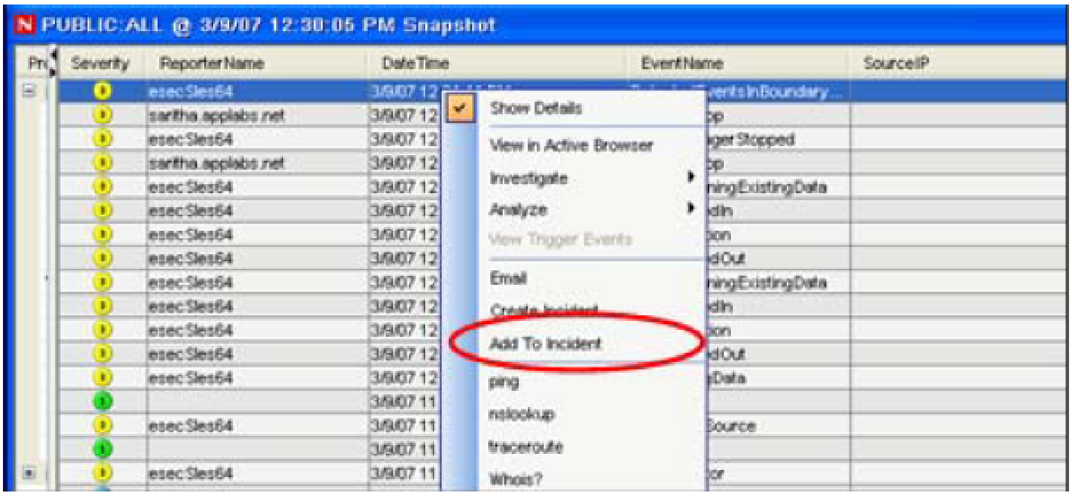
A. Email
B. Create Incident
C. Add to Incident
D. Connect to advisor
E. Display DAS statistics
F. Create iTRAC template

Answer: A,B,C

Explanation: A: To send an event message by e-mail:
In a Real Time Event Table, select an event or a group of events, right-click and select Email.

B: To create an incident:
In a Real Time Event Table of the Navigator or a Snapshot Real Time Event Table, select an

event or a group of events and right-click and select Create Incident.



PUBLIC:ALL @ 3/9/07 12:30:05 PM Snapshot

Pri	Severity	ReporterName	DateTime	EventName	SourceIP
	●	esecSles64	3/9/07 12	entsInBoundary ...	
	●	sartha.applabs.net	3/9/07 12	op	
	●	esecSles64	3/9/07 12	ger Stopped	
	●	sartha.applabs.net	3/9/07 12	op	
	●	esecSles64	3/9/07 12	ningExistingData	
	●	esecSles64	3/9/07 12	dIn	
	●	esecSles64	3/9/07 12	ion	
	●	esecSles64	3/9/07 12	dOut	
	●	esecSles64	3/9/07 12	ningExistingData	
	●	esecSles64	3/9/07 12	dIn	
	●	esecSles64	3/9/07 12	ion	
	●	esecSles64	3/9/07 12	dOut	
	●	esecSles64	3/9/07 12	Data	
	●		3/9/07 11		
	●	esecSles64	3/9/07 11	Source	
	●		3/9/07 11		
	●	esecSles64	3/9/07 11	or	

C: **To add events to an incident:**

In a Real Time Event Table or a Snapshot, select an event or a group of events and right-click.

Click Add To Incident.

Question No : 3

What compliance and regulatory Solution Pack is the first one offered for sale by Novell?

A. Sarbanes-Oxley
B. GLBA (Gramrn-Leach-Bliley Act)
C. PCI-DSS(Payment Card Industry)
D. HIPAA(Health insurance portability and accountability)

Answer: D

Question No : 4

Which RuleLG operation compares the current event to a set of past events that are stored in temporary memory?

A. Flow

B. Filter()
C. Trigger()
D. Window

Answer: D

Question No : 5

You want to configure a menu action to execute a script against an event on an Active View. Where do you need to store the script?

A. The exec directory of the Sentinel Communication Server
B. The config directory of Sentinel Communication Server
C. The exec directory of every Sentinel control centre machine
D. The script directory of every Sentinel control centre machine

Answer: C

Question No : 6

Which component is used to communicate with the Sentinel database?

A. iScale
B. DAS RT
C. DAS PROXY
D. DAS binary

Answer: C

Question No : 7

Which attributes influence when an element is removed from a Dynamic list? (Choose 3.)

A. Database capacity
B. Element life span
C. Maximum number of elements
D. Persistent/transient setting

E. Sentinel data manager scheduling
F. Amount of memory on iScale message Bus
G. Number of correlation rules that are deployed

Answer: B,C,D

Explanation: There are several ways an element can be removed from a Dynamic List.

/ A user can remove it manually

/ (The element can be removed by a correlation rule action

/ (BD) The Transient elements life span can expire

/ (C) If the maximum number of elements for a Dynamic List is reached, elements are removed from

the list to keep the list at or below the maximum list size. The transient elements are removed

(from oldest to newest) before any persistent elements are removed.

Question No : 8

Which functions are performed using the Sentinel Data Manager? (Choose 2)

A. User creation
B. Manual achieving
C. Database creation
D. Raw Event Storage
E. Re-import partitions
F. Correlation rule Management

Answer: B,E

Explanation: Sentinel Data Manager (SDM) allows you to manage the Sentinel Database.

You can perform the following operations in the SDM:

* Monitor Database Space Utilization

* (E) View and Manage Database Partitions

* (B) Manage Database Archives

* Import Data into the Database

Question No : 9

Which Sentinel objects can contain one or more events? (Choose 2)