IBM

C2150-624 Exam

IBM Security QRadar SIEM V7.2.8 Fundamental Administration Exam

Thank you for Downloading C2150-624 exam PDF Demo

You can Buy Latest C2150-624 Full Version Download

https://www.certkillers.net/Exam/C2150-624

Version: 9.0

Question: 1

Administrators on versions of IBM Security QRadar SIEM older than V7.2.4 must use a specific upgrade path to transition to newer software versions. These requirements are outlined in what technical document?

A. Fix Level Recommendation Tool
B. IBM latest firmware release notes
C. QRadar Software upgrade progress technical note
D. IBM System Security Interoperation Center (SSIC)

Answer: C

Most of the upgrades of IBM products are available in technical notes. IBM security Qradar SIEM upgrade process and information can be obtained through technical notes that IBM publishes on the web.

Question: 2

What is a precaution an Administrator should take before beginning an upgrade of IBM Security QRadar SIEM V7.2.8?

A. Close all open offenses.
B. Purge old data and events.
C. Check and close all open messages.
D. Confirm that a backup of the data is complete.

Answer: D

The first precaution listed in the IBM document states that the administrator should backup data before preparing for software upgrade. Backup of the current settings is important because if anything bad happens during the upgrade, you can always revert back to the original settings.

Question: 3

After downloading the <QRadar_patchupdate>.sfs file from Fix Central, what is the next step to upgrade IBM Security QRadar SIEM V7.2.8?

A. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Clean SIM Model.
B. Log in to the console as the Admin user-> Admin tab -> Advanced Menu -> Upgrade option.
C. Use SSH to log in to the system as the root user -> Run the patch installer with the following command: /media/updates/upgrade_qradar.
D. Use SSH to log in to the system as the root user -> Copy the patch file to the /tmp directory or to

another location that has sufficient disk space.

Answer: D

Question: 4

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to enable the PCI report template.
What is the procedure to accomplish this task?

A. Admin Tab -> Reports -> Templates -> Compliance -> PCI -> Select “Enable”
B. Report Tab -> Enable “Show all templates” -> Group List -> Compliance -> PCI
C. Reports Tab -> Clear “Hide Inactive Reports” box -> Group List -> Compliance -> PCI
D. Admin Tab -> Reports -> Templates -> Compliance -> PCI -> uncheck “Hide Template”

Answer: C

1. Click the Reports tab.
2. Clear the Hide Inactive Reports check box.
3. In the Group list, select Compliance > PCI. 4. Select all report templates on the list:
a. Click the first report on the list.
b. Select all report templates by holding down the Shift key, while you click the last report on the list.
5. In the Actions list, select Toggle Scheduling. 6. Access generated reports:
a. From the list in the Generated Reports column, select the time stamp of the report that you want to view.
b. In the Format column, click the icon for report format that you want to view.

Question: 5

An IBM Security QRadar SIEM V7.2.8 Administrator assigned to a company that is looking to add QRadar into their current network. The company has requirements for 250,000 FPM, 15,000 EPS and FIPS.
Which QRadar appliance solution will support this requirement?

A. QRadar 3128-C with Basic License
B. QRadar 2100-C with Basic License
C. QRadar 3128-C with Upgraded License
D. QRadar 2100-C with Upgraded License

Answer: C

The upgraded license of Qradar 3128-C has 300k FPM and 15000 EPS and FIPs. Therefore the Qradar 3128-C with upgraded license is the best choice for the company.

Question: 6

An Administrators will add a secondary host to an IBM Security QRadar SIEM V7.2.8 Console in a High Availability (HA) deployment scenario.
After checking the compatibility between primary and secondary HA pairs, what other prerequisite should the Administrator check within Managed Interfaces?

A. The shared external storage.
B. The server certificate that is issued by the local CA.
C. The existence of an additional distributed file system.
D. The communication for Distributed Replicated Block Device.

Answer: D

CP port 7789 must be open and allow communication between the primary and secondary for Distributed Replicated Block Device (DRBD) traffic.
DRBD traffic is responsible for disk replication and is bidirectional between the primary and secondary host.

Question: 7

An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to delete a single value named User1 from a reference set with the name “Allowed Users” from the command line interface.
Which command will accomplish this?

A. ./UtilReferenceSet.sh purge “Allowed Users” User1
B. ./ReferenceSetUtil.sh purge “Allowed Users” User1
C. ./ReferenceSetUtil.sh delete “Allowed\ Users” User1
D. ./UtilReferenceSet.sh delete “Allowed\ Users” User1

Answer: B

The Referencesetutil.sh purge is the correct syntax of the command. It deletes the specific user when you mention it within the reference set.

Question: 8

When it comes to licensing, what is the difference between Events and Flows and how they are licensed?

A. Flows are licensed based on overall count over a minute, where Events are licensed based on overall count per second.
B. Flows are licensed based on overall count per second, where Events are licensed based on overall count over a minute.
C. Flows and Events are both licensed by overall count per minute under an Upgraded License and per second on a Basic License.
D. Flows and Events are both licensed by overall count per second under an Upgraded License and per second on a Basic License.

Answer: A

A significant difference between event and flow data is that an event, which typically is a log of a specific action such as a user login, or a VPN connection, occurs at a specific time and the event is logged at that time. A flow is a record of network activity that can last for seconds, minutes, hours, or days, depending on the activity within the session. For example, a web request might download multiple files such as images, ads, video, and last for 5 to 10 seconds, or a user who watches a Netflix movie might be in a network session that lasts up to a few hours. The flow is a record of network activity between two hosts.

Question: 9

When an IBM Security QRadar SIEM V7.2.8 distributed deployment requires scaling horizontally to achieve Event per Second (EPS) requirements, what QRadar Component needs to be added to meet the EPS demands?

A. Event Manager
B. Event Indexing
C. Event Collector
D. Event Processor

Answer: D

The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:

Question: 10

The event data collected by IBM Security QRadar SIEM V7.2.8 is being deleted after one month. The legal department required the data be kept for two months.
What can the administrator do to accommodate this requirement?

A. Change the nightly backup Priority to “High”.
B. Change the nightly backup to a monthly backup.
C. Change the Default Event Retention Policy property field “Do not delete data in this bucket” to two months.
D. Change the Default Event Retention Policy property field “Keep data placed in this bucket for” to two months.

Answer: D

When storage space is required - Select this option if you want events or flows that match the Keep data placed in this bucket for parameter to remain in storage until the disk monitoring system detects that storage is required. If used disk space reaches 85% for records and 83% for payloads, data will be deleted. Deletion continues until the used disk space reaches 82% for records and 81% for payloads.
When storage is required, only events or flows that match the Keep data placed in this bucket for parameter are deleted.

Thank You for trying C2150-624 PDF Demo

To Buy Latest C2150-624 Full Version Download visit link below

https://www.certkillers.net/Exam/C2150-624

Start Your C2150-624 Preparation

[Limited Time Offer] Use Coupon "CKNET" for Further discount on your purchase. Test your C2150-624 preparation with actual exam questions.