C2150-624

Number: C2150-624
Passing Score: 800
Time Limit: 120 min
File Version: 1.0

C2150-624

IBM Security QRadar SIEM V7.2.8 Fundamental Administration

Version 1.0

Exam A

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)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

Reference http://www-01.ibm.com/support/docview.wss?uid=swg27038118

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.

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:
Explanation:

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. Reference http://www-01.ibm.com/support/docview.wss?uid=swg27048793

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
- Download the fix pack to install QRadar 7.2.8 Patch 1 from the IBM Fix Central website: http://www.ibm.com/support/fixcentral/swg/quickorder?parent=IBM%2BSecurity&product=ibm/Other+software/IBM+Security+QRadar+SIEM&release=7.2.0&platform=Linux&function=fixId&fixids=7.2.8-QRADAR-QRSIEM20161118202122&includeRequisites=1&includeSupersedes=0&downloadMethod=http&source=fc
- Using SSH, log in to your system as the root user.
- Copy the fix pack to the /tmp directory on the QRadar Console. Note: If space in the /tmp directory is limited, copy the fix pack to another location that has sufficient space.
- To create the /media/updates directory, type the following command: mkdir -p /media/updates Reference

http://www-01.ibm.com/support/docview.wss?uid=swg27049111

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”

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_gs_guide.pdf

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.8/com.ibm.qradar.doc/c_hwg_3128_allone.html

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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
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.

Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_appliance_require.html

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?

https://vceplus.com

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
Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

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

Reference https://www.ibm.com/developerworks/community/forums/html/topic?id=77777777-0000-0000-0000-000014967953

QUESTION 8
An IBM Security QRadar SIEM V7.2.8 Administrator needs to download a nightly configuration backup file from a past day through the Web Console.

Which steps must be followed to achieve this?

A. Admin Tab -> System Configuration -> Backup and Recovery -> Generate new backup -> Save
B. Admin Tab -> System Configuration -> Backup and Recovery -> Choose the name of an Existing backup
C. Admin Tab -> System Configuration -> Backup and Recovery -> Import New Backup -> Select file extension -> Save
D. Admin Tab -> System Configuration -> System Settings -> Database Settings -> Choose the name of an Existing backup

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The backups are listed in Backup and recovery section of the system configuration in the admin tab. You can click on the existing backup and it will show you the options to download it.

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf

QUESTION 9
Which permission can be assigned to a user from User Roles in the IBM Security QRadar SIEM V7.2.8 Console?

A. Admin
B. DSM Updates
C. Flow Activity
D. Configuration Management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Grants administrative access to the user interface. You can grant specific Admin permissions. Users with System Administrator permission can access all areas of the user interface. Users who have this access cannot edit other administrator accounts.

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf

QUESTION 10
An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to copy data and configuration backup files from the previous day to an off-site location.

What is the default location where these files can be found?

A. /store/backup
B. /store/exports
C. /store/postgres
D. /store/backupHost

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation
The default location is /store/backup. This path must exist before the backup process is initiated. If this path does not exist, the backup process aborts. If you modify this path, make sure the new path is valid on every system in your deployment.

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf

QUESTION 11

How many dashboards come by default in IBM Security QRadar SIEM V7.2.8?

A. 1
B. 5
C. 7
D. 10

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
There are five default dashboards:

1 – application overview
2 – compliance overview
3 – network overview
4 – system monitoring
5 – threat and security monitoring

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_users_guide.pdf

QUESTION 12
An IBM Security QRadar SIEM V7.2.8 Administrator is receiving an I/O error on the console.

Which command can the Administrator run to begin diagnosing this issue?

A. /etc/init.d/tomcat status
B. /etc/init.d/ariel_query_server status
C. /opt/qradar/init/apply_tunning status
D. /opt/qradar/init/ariel_query_server status

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

Explanation:
If the Ariel Query Server is not running, a full configuration deployment may resolve this issue by restarting all services on the managed host after deploying the most recent configuration on it. If the Ariel Query Server is still not running after a full deployment, contact support for further assistance. Reference http://www-01.ibm.com/support/docview.wss?uid=swg21991038

QUESTION 13
An Administrator working with IBM Security QRadar SIEM V7.2.8 has updated the date/time on the QRadar console system and wants to update these date/time settings to all his hosts in the distributed environment.

What command should be run?

A. /opt/qradar/bin/datesync_all_servers.sh
B. /opt/qradar/support/all_servers.sh /opt/qradar/bin/time_sync.sh
C. /opt/qradar/support/fullDeployment.sh /opt/qradar/bin/time_sync.sh
D. /opt/qradar/support/all_servers.sh /opt/qradar/bin/check_date_change.sh

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To run time synchronization on all hosts and see if any fail to synchronize with the Console, from the root directory (/) type the following command: ./opt/qradar/support/all_servers.sh "/opt/qradar/bin/time_sync.sh"

Reference http://www-01.ibm.com/support/docview.wss?uid=swg21700463

QUESTION 14
An IBM Security QRadar SIEM V7.2.8 Administrator wants to create a security profile within the system but receives an error upon saving.

What is a possible reason for this error?

A. The Administrator has used non alpha numeric value(s) in the name which is not allowed.
B. The Administrator has used less than 3 characters or more than 30 characters as name of the security profile.
C. The Administrator has mixed non alpha numeric value(s) and alpha numeric value(s) in the name which is not allowed.
D. The Administrator must bring the IBM Security QRadar SIEM V7.2.8 system first in edit mode before changes are allowed.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Explanation:
In the Security Profile Name field, type a unique name for the security profile. The security profile name must meet the following requirements: minimum of 3 characters and maximum of 30 characters.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.1/QRadar/EN/b_qradar_admin_guide.pdf

QUESTION 15
An Administrator working with a customer looking to add IBM Security QRadar SIEM V7.2.8 into their network, has some requirements. The customer is looking to have 40Tb of raw storage space for events and console data.

What appliances allow for this requirement to be met?

A. QRadar 3128 Console + QRadar 1410 Data Node
B. QRadar 3128 Console + QRadar 1400 Data Node
C. QRadar 3118 Console + QRadar 1410 Data Node
D. QRadar 3128 Console + QRadar Flow Processor 1728

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The IBM Security QRadar 1400 Data Node (MTM 4380-Q1E) appliance provides scalable data storage solution for QRadar deployments. The QRadar 1400 Data Node enhances data retention capabilities of a deployment as well as augment overall query performance

Reference http://documentation.extremenetworks.com/PDFs/SIEM-IPS/IBM_QRadar_Hardware_Guide_7.7.2.6.pdf

QUESTION 16
What data is purged by the SIM reset process “Hard Clean” in IBM Security QRadar SIEM V7.2.8?

A. All current and historical SIM data.
B. All historical SIM data, current SIM data is retained.
C. All SIEM data, a complete reconfiguration is required.

D. All source and destination IP addresses are purged, all offenses in the database are closed.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Hard clean Purges all current and historical SIM data, which includes offenses, source IP addresses, and destination IP addresses.
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_admin_guide.pdf

QUESTION 17
Where are the logs for QFlow stored on IBM Security QRadar SIEM V7.2.8?

A. /var/log/qflow.debug
B. /opt/var/log/qflow.debug
C. /opt/log/qradar/qflow.debug
D. /opt/qradar/log/qflow.debug

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

To help you troubleshoot errors or exceptions, review the following log files.
/var/log/qradar.log
/var/log/qradar.error

If you require more information, review the following log files:
/var/log/qradar-sql.log
/opt/tomcat6/logs/catalina.out
/var/log/qflow.debug

Review all logs by selecting Admin > System & License Mgmt > Actions > Collect Log Files.

Reference https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.6/com.ibm.qradar.doc/c_qradar_siem_inst_logs.html

QUESTION 18
What is the Events Per Second (EPS) basic license limit in an IBM Security QRadar V7.2.8 2100 hardware appliance?

A. 200
B. 1000
C. 2500
D. 10000

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Table 5. QRadar Event Collector 1501

Description	Value
Events per second	2500 EPS
Log Sources	750
Interfaces	Six 10/100/1000 Base-T network monitoring interfaces One 10/100/1000 Base-T management interface
Memory	24 GB
Storage	1.3 TB dedicated storage
Power supply	Dual Redundant 675W AC Power Supply
Dimensions	28" D x 17.3" W x 1.69" H
Included components	QRadar Event Collector 1501

Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_QRadar_hardware_guide.pdf

QUESTION 19
What is the maximum number of dashboards a user can create with IBM Security QRadar SIEM V7.2.8?

A. 10
B. 25
C. 100
D. 255

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Create custom dashboards that are relevant to your responsibilities. 255 dashboards per user is the maximum; however, performance issues might occur if you create more than 10 dashboards.

Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.3/com.ibm.qradar.doc_7.2.3/c_qradar_custom_dboard.html

QUESTION 20

A retention policy allows an IBM Security QRadar SIEM V7.2.8 Administrator to define how long the system is required to keep certain types of data and what to do when data reaches a certain age. If a 3-month retention policy is defined for all events, then the system will not delete event data until it's on disk timestamp is 3 months in the past.

Which two choices are available in the 'delete data in this bucket'? (Choose two.)

A. When the index is full
B. Upon reboot of the system
C. When storage space is required
D. When performance is heavily affected
E. Immediately after retention period has expired

Correct Answer: CE
Section: (none)
Explanation

Explanation/Reference:
Explanation:
From the list box, select a deletion policy. Options include:

- 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.

- Immediately after the retention period has expired – Select this option if you want events to be deleted immediately on matching the Keep data placed in this bucket for parameter.

The events or flows are deleted at the next scheduled disk maintenance process, regardless of free disk space or compression requirements.

Reference https://www.ibm.com/developerworks/community/forums/atom/download/Event_Flow_Retention_QRadar_72_AdminGuide.pdf?nodeId=593f2b31-a8584210-b380-4674894a6ad9

QUESTION 21
An Administrator using IBM Security QRadar SIEM V7.2.8 needs to force an instant backup to run.

Which option should be selected?

A. Backup Now

B. On Demand Backup
C. Launch On Demand Backup
D. Configure On Demand Backup

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
Where are the IBM Security QRadar SIEM V7.2.8 log files located?

A. /var/qradar.log
B. /var/log/qradar.log
C. /opt/qradar/log/qradar.log
D. /opt/qradar/support/qradar.log

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation
You can review the log files for the current session individually or you can collect them to review later.

Follow these steps to review the QRadar log files.

To help you troubleshoot errors or exceptions, review the following log files.
/var/log/qradar.log
/var/log/qradar.error
If you require more information, review the following log files:
/var/log/qradar-sql.log
/opt/tomcat6/logs/catalina.out
/var/log/qflow.debug

Review all logs by selecting Admin > System & License Mgmt > Actions > Collect Log Files.

Reference https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.6/com.ibm.qradar.doc/c_qradar_siem_inst_logs.html

QUESTION 23
An IBM Security QRadar SIEM V7.2.8 Administrator needs to check if the “hostcontext” process is running.

How can the Administrator do this?

A. hostcontext status
B. status hostcontext service
C. service hostcontext status
D. /etc/qradar/hostcontext status

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference http://qradar360.blogspot.com/p/guides-material.html

QUESTION 24
An IBM Security QRadar SIEM V7.2.8 Administrator will install a High Availability (HA) pair of appliances. The primary and secondary hosts are formatted with the same file system.

To ensure compatibility between hosts, which statement is considered a prerequisite?

A. The size of the /home partition on the secondary must be larger than the /home partition of the primary.
B. The size of the /var/opt/ha on the secondary must be larger than the /var/opt/ha partition of the primary.
C. The size of the /store partition on the secondary must be lesser than the /store partition of the primary.
D. The size of the /store partition on the secondary must be equal to or larger than the /store partition of the primary.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:

Store partition requirements

- The file system of the /store partition must match between your primary and secondary host.
- The size of the /store partition on the secondary must be equal to or larger than the /store partition of the primary.

For example, do not pair a primary host that uses a 3 TB /store partition to a secondary host that has a 2 TB /store partition.

Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.7/com.ibm.qradar.doc/c_qradar_appliance_require.html

QUESTION 25
An Administrator using IBM Security QRadar SIEM V7.2.8 is using the following RegEx:

([-+]?\d*$)

What type of information is it designed to extract?

A. Integer
B. IP address
C. Port number
D. Domain name

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sample regular expressions:
• email: (.+@[^\.].*\.[a-z]{2,}$)
• URL: (http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\ S*)?$)
• Domain Name: (http[s]?://(.+?)["/?:])
• Floating Point Number: ([-+]?\d*\.?\d*$)
• Integer: ([-+]?\d*$)
• IP Address: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

For example: To match a log that resembles: SEVERITY=43 Construct the following Regular Expression: SEVERITY=([-+]?\d*$)

Reference http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 26
Offense data has become corrupted, what option should an IBM Security QRadar SIEM V7.2.8 Administrator consider to recover the offenses?

A. Use Clean SIM option.
B. Log out and Log back in.
C. Use Revert Offenses option.
D. Restore the most recent backup archive.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can back up and recover QRadar® configuration information and data.
You can use the backup and recovery feature to back up your event and flow data; however, you must restore event and flow data manually.
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_qradar_adm_man_back_recovery.html

QUESTION 27
An Administrator is tasked with installing additional log resources into an IBM Security QRadar SIEM V7.2.8 deployment, bringing the total number of log source to 900. The deployment is using the default license and the Administrator is getting an error attempting to add these additional log sources.

Why is this error happening?

A. The default license only allows 250 log sources.
B. The default license only allows 500 log sources.
C. The default license only allows 750 log sources.
D. The default license only allows 800 log sources.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/shc_act_lic_keys.html

QUESTION 28
An Administrator working with IBM Security QRadar SIEM V7.2.8 appliances needs to update firmware.

How are the files acquired?

A. Firmware updates can be retrieved from IBM developerWorks.
B. Refer to support documents to download the firmware approved for QRadar appliances.
C. All firmware is automatically downloaded and no Administrator intervention is required.
D. All firmware updates are applied as part of the QRadar software patching process, and should not be applied independently.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Administrators looking for the latest firmware downloads can review this page to locate firmware updates for QRadar appliances. The installation instructions include a direct download link to the firmware from IBM Fix Central.

Reference http://www-01.ibm.com/support/docview.wss?uid=swg27047121

QUESTION 29
Where are system notifications located in IBM Security QRadar SIEM V7.2.8?

A. Only in the Admin Tab -> System Messages.
B. Only on the banner above the QRadar navigation tabs.
C. On the banner above the QRadar navigation tabs or on the System Monitoring dashboard.
D. On the banner above the QRadar navigation tabs or in the Admin Tab -> System Messages.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
After collecting system log files, the system notification message that appears in the Messages box on the QRadar Console is available in English only.

Reference http://www-01.ibm.com/support/docview.wss?uid=swg21882761

QUESTION 30

An Administrator working within IBM Security QRadar SIEM V7.2.8 has a network hierarchy that cannot support anymore network objects. To remedy this, they want to implement a supernet. Some of the customer CIDRs are:
- 209.60.128.0/24
- 209.60.129.0/24
- 209.60.130.0/24
- 209.60.131.0/24

Which supernet should be used to shrink the amount of network objects for the supplied group of CIDRs?

A. 209.60.128.0/22
B. 209.60.129.0/23
C.
209.60.128.0/23
D. 209.60.127.0/27

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Supernetting, also called Classless Inter-Domain Routing (CIDR), is a way to aggregate multiple Internet addresses of the same class. Using supernetting, the network address 209.60.128.0/24 and an adjacent address 209.60.129.0/24 can be merged into 209.60.128.0/23. The "23" at the end of the address says that the first 23 bits are the network part of the address, leaving the remaining nine bits for specific host addresses

QUESTION 31
An Administrator working within IBM Security QRadar SIEM V7.2.8 has created a network hierarchy that includes the following groups and subgroups:

Office #1 Group
- Miscellaneous 10.10.0.0/24

- Sales 10.10.8.0/24
- Marketing 10.10.1.0/24

Office #2 Group
- Miscellaneous 10.20.0.0/16
- Sales 10.20.8.0/24
- Marketing 10.20.1.0/24

A new subgroup is added to Office #1 having a CIDR of 10.10.50.0/24. Offenses are being triggered and during the investigation, it is noticed the rule should not fire if traffic is L2L. The offense is being triggered on traffic from 10.10.4.17 to 10.20.1.8.

Is this rule using the network hierarchy correctly?

A. This rule is parsing the network hierarchy correctly, as the 10.10.4.17 address is not contained in a group, and therefore is remote.
B. This rule is parsing the network hierarchy correctly, as the offices are both remotely geo-located, and connecting over the Internet, it is remote traffic.
C. This rule isn't parsing the network hierarchy correctly, as the network hierarchy contains the CIDR for 10.10.4.17 and 10.20.1.0/24, therefore being L2L traffic.
D. This rule isn't parsing the network hierarchy correctly, as the network hierarchy contains both subnets, but is viewing traffic between groups to be remote instead of local.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
An Administrator working with IBM Security QRadar SIEM V7.2.8 is constantly receiving the following message:

"SAR Sentinal: Threshold crossed."

Where will the Administrator tune the settings for these messages?

A. Admin tab -> General Settings -> Global System Notifications
B. Admin tab -> System Configuration -> Global System Notifications
C. Admin tab -> System Notifications -> System Activity Reporter Notifications
D. Admin tab -> System Configuration -> General Settings -> System Notifications

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
The SAR Sentinel utility monitors QRadar for a broad number of functions, such as running processes, CPU usage, and hardware functions. The function of the SAR Sentinel is to monitor the system and provide notifications when the system load exceeds a set threshold.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.1/QRadar/EN/QRadar_721_Troubleshooting_System_Notifications.pdf

QUESTION 33
An Administrator needs to see Events per Second (EPS) and Flows per Minute (FPM) coming to IBM Security QRadar SIEM V7.2.8 through a dashboard. How could this be accomplished?

A. Download the dashboard from IBM Security App Exchange.
B. Go to CLI and run the script /opt/qradar/bin/createdashboard.sh
C. Select any dashboard and customize it. Add a system summary item.
D. Create a new dashboard and then go to admin tab. Add item into the dashboard created.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
Explanation:
To determine the average EPS rate, users can click the Dashboard tab, then select the System Monitoring dashboard item. This dashboard contains and event per second and flows per minute dashboard item. To see EPS details, click the View in Log Activity link. This will give an estimate of the data size for events per day.
Reference http://www-01.ibm.com/support/docview.wss?uid=swg21685322

QUESTION 34
Which AQL query, when run from IBM Security QRadar SIEM V7.2.8, will show EPS broken down by domains?

A. select DOMAINNAME (domainid) as LogSource, sum(eventcount) / ((max(endTime) – min(startTime)) / 1000) as EPS from events group by domainid order by EPS desc last 24 hours
B. select DOMAINNAME (domainqid) as LogSource, sum(eventcount) / ((max(endTime) – min(startTime)) / 1000) as EPS from events group by domainqid order by FPM desc last 24 hours

C. select DOMAINNAME (domainid) as LogSource, sum(events) / ((max(endTime) – min(startTime)) / 1000) as EPS from events group by domainid order by FPM desc last 24 hours
D. select DOMAINNAME (domainid) as LogSource, sum(events) / ((max(endTime) – min(startTime)) / 1000) as EPS from events group by domainid order by EPS desc last 24 hours

Correct Answer: A
Section: (none)
Explanation
Explanation/Reference:
Explanation:
You would use single-quotes to define this search string. I believe I had an example in the presentation yesterday I need to fix where I accidently used doubleqoutes, which is incorrect.

The AQL search below uses quotes correctly:
select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min(startTime)) / 1000) as EPS from events WHERE logsourcename(logsourceid) = 'Windows Auth @ 10.10.10.10' group by logsourceid order by EPS desc last 5 MINUTES

Or to snag multiple log sources, for example Windows events, you could use the following:
select logsourcename(logsourceid) as LogSource, sum(eventcount) / ((max(endTime) - min(startTime)) / 1000) as EPS from events WHERE logsourcename(logsourceid) is ILIKE '%Windows%' group by logsourceid order by EPS desc last 5 MINUTES

Reference https://www.ibm.com/developerworks/community/forums/html/topic?id=dea8ff96-1372-4242-be14-473b6e4be798

QUESTION 35
An IBM Security QRadar SIEM V7.2.8 Administrator notices a specific MAC address added to the Asset Reconciliation Domain MAC was blacklisted.

What scenario is causing this to occur?

A. When a MAC address is associated to three or more different IP addresses in 2 hours or less.
B. When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less.
C. When a MAC address is associated to three or more different IP addresses in 10 minutes or less.
D. When an IPv4 address is associated to three or more different MAC addresses in 10 minutes or less.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

Explanation:

Table 18. Rule tests and responses

Scenario	Rule response
When a MAC address is associated to three or more different IP addresses in 2 hours or less	Add the MAC address to the Asset Reconciliation Domain MAC blacklist
When a DNS host name is associated to three or more different IP addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When a NetBIOS host name is associated to three or more different IP addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When an IPv4 address is associated to three or more different MAC addresses in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different MAC addresses in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist
When a DNS host name is associated to three or more different MAC addresses in 2 hours or less	Add the DNS host name to the Asset Reconciliation Domain DNS blacklist
When an IPv4 address is associated to three or more different DNS host names in 2 hours or less	Add the IP address to the Asset Reconciliation Domain IPv4 blacklist
When a NetBIOS host name is associated to three or more different DNS host names in 2 hours or less	Add the NetBIOS host name to the Asset Reconciliation Domain NetBIOS blacklist

Reference: ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.5/EN/b_qlm_users_guide.pdf

QUESTION 36

The event pipeline for processing event data before viewing and using event data on the IBM Security QRadar SIEM V7.2.8 console consists of many components, what is one component?

https://vceplus.com

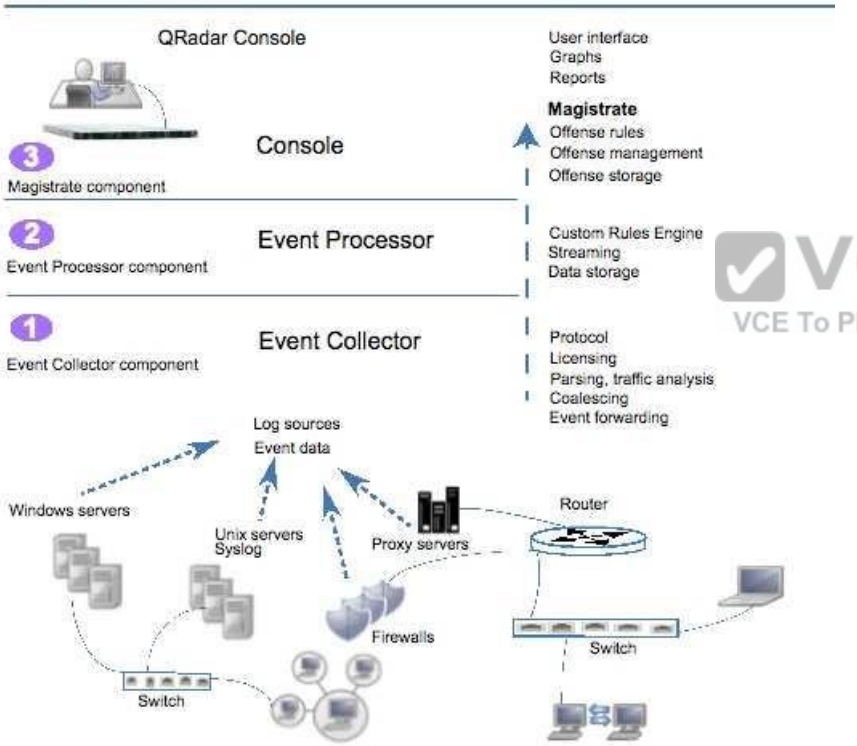
A. Indexing Component

B. Flow Data Component
C. Magistrate Component
D. Event Data Component

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation

Figure 1. Event pipeline



Reference https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_qradar_deploy_event_and_flow_pipeline.html

QUESTION 37

An Administrator has configured a customized log source extension to provide asset updates to IBM Security QRadar SIEM V7.2.8. Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.
In this situation what will QRadar report?

A. This will cause stale asset data.
B. This will cause asset growth deviations.
C. This will cause excessive authentication failure events.
D. This will cause excessive flow data to be processed by the Magistrate.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Instead of QRadar receiving an update that has the host name of the asset that the user logged in to, the log source generates many asset updates that all have the same host name.

In this situation, the asset growth deviation is caused by one asset profile that contains many IP addresses and user names.

Reference https://www.ibm.com/support/knowledgecenter/SSKMKU/com.ibm.qradar.doc/c_qradar_ug_usecase_customized_lsx.html

QUESTION 38
Which appliance of the IBM Security QRadar SIEM V7.2.8 family is a specifically used to gather events from local and remote log sources?

A. QRadar Event Console
B. QRadar QFlow Collector
C. QRadar Event Collector
D. QRadar Event Processor

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation

Gathers events from local and remote log sources. Normalizes raw log source events. During this process, the Magistrate component examines the event from the log source and maps the event to a QRadar Identifier (QID). Then, the Event Collector bundles identical events to conserve system usage and sends the information to the Event Processor.

Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.1/com.ibm.qradar.doc_7.2.1/shc_qradar_comps.html

QUESTION 39
During the IBM Security QRadar SIEM V7.2.8 installation, which two default user roles are defined? (Choose two.)

A. All
B. Any
C. Admin
D. SuperUser
E. SuperAdmin

Correct Answer: AC
Section: (none)
Explanation

Explanation/Reference:
Explanation
Two default user roles are listed in the left pane of the window: Admin and All. You can select a role in the left pane to view the associated role permissions in the right pane.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/CoreDocs/QRadar_71MR1_AdminGuide.pdf

QUESTION 40
An Administrator working with IBM Security QRadar SIEM V7.2.8 was tasked with adding a new Microsoft Azure log source.

What protocol is supported for this?

A. FTP
B. JDBC
C. Syslog
D. WinCollect

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.4/com.ibm.dsm.doc/c_dsm_guide_microsoft_azure_overview.html

QUESTION 41
An Administrator working with IBM Security QRadar SIEM V7.2.8 only needs to remove a single host (10.1.95.142) from the reference set with the name “Asset Reconciliation IPv4 Whitelist” from the command line interface.
Which command would accomplish this task?

A. ./RefereceSetUtil.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
B. ./RefereceSetUtil.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
C. ./RefereceSetData.sh purge Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142
D. ./RefereceSetData.sh delete Asset\ Reconciliation\ IPv4\ Whitelist 10.1.95.142

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:

The syntax for the command is:

ReferenceSetUtil.sh add "Asset Reconciliation IPv4 Whitelist" IP

Reference http://www.juniper.net/techpubs/en_US/jsa2014.8/information-products/topic-collections/jsa-administration-guide.pdf

QUESTION 42
When replacing a Console appliance in an IBM Security QRadar SIEM V7.2.8 deployment using a new IP address or host name, what must be the same on the two Console appliances?

A. The amount of storage must be the same.
B. The Basic and Upgrade license must be the same.
C. The software versions of both appliances must match.
D. The Network Configuration and Protocol must be the same.

Correct Answer: C

Section: (none)
Explanation

Explanation/Reference:
Explanation
The software version of the new Console appliance must match the software version of the old Console appliance. QRadar does not allow appliances at different software versions in the deployment. Administrators might be required to reinstall an ISO for the appliance to downgrade or use a Fix Pack (SFS) to upgrade on the new appliance. The paperwork that came with your appliance lists the installed software version.
Reference http://www-01.ibm.com/support/docview.wss?uid=swg21984320

QUESTION 43
An Administrator needs to create a new user role in the IBM Security QRadar SIEM V7.2.8 system.

What steps need to be followed?

A. System Configuration tab -> Users and Roles -> Add New Role -> Add
B. Admin tab -> System Configuration -> User Management -> User Roles -> New
C. Admin tab -> System and Settings -> Users and Roles -> Role Management -> New
D. System Management tab -> System Configuration -> User Management -> User Roles -> New

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation
By default, your system provides a default administrative user role, which provides access to all areas of QRadar SIEM. Users who are assigned an administrative user role cannot edit their own account. This restriction applies to the default Admin user role. Another administrative user must make any account changes.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/7.2.1/QRadar/EN/b_qradar_admin_guide.pdf

QUESTION 44
An Administrator using IBM Security QRadar SIEM V7.2.8 is using the RegEx syntax below:

(\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

What type of information is it designed to extract?

A. An IP Address
B. GPS Coordinates
C. A Telephone Number
D. A simple integer no longer than 4 digits
Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
Sample regular expressions:
• email: (.+@[^\.].*\.[a-z]{2,}$)
• URL: (http\://[a-zA-Z0-9\-\.]+\.[a-zA-Z]{2,3}(/\ S*)?$)
• Domain Name: (http[s]?://(.+?)["/?:])
• Floating Point Number: ([-+]?\d*\.?\d*$)
• Integer: ([-+]?\d*$)
• IP Address: (\b\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\b)

For example: To match a log that resembles: SEVERITY=43 Construct the following Regular

Expression: SEVERITY=([-+]?\d*$)

Reference http://www.siem.su/docs/ibm/Administration_and_introduction/User_Guide.pdf

QUESTION 45
An IBM Security QRadar SIEM V7.2.8 Administrator needs to retain authentication failure data to a specific domain, for a longer period than the rest of the event data being collected.

How is this task completed?

A. The administrator will need to create a custom rule with the appropriate filters and retention period.
B. The administrator will need to create a new Event Retention Bucket with the appropriate filters and retention period.
C. The administrator will need to create a custom filter in the log activity tab with the appropriate parameters and retention period.
D. The administrator will need to create a custom report with the appropriate parameters and use the report format TAR (Tape archive).

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation

In current versions of QRadar you can set custom retention buckets for Events and Flows. The 10 non-default retention buckets are processed sequentially from top to bottom. Any events that do not match the retention buckets are automatically placed in the default retention bucket, located at the bottom of the list. Custom retention buckets allow the ability to add a time period and filters. If you enable a retention bucket with a defined criteria it will start deleting data from the time is was created. Any data that matches the custom retention bucket before it was created is subject to the criteria of the default retention bucket setting. If you need to delete data from before the Custom retention bucket was created you can shorten the default retention bucket so data is deleted immediately. Reference http://www-01.ibm.com/support/docview.wss?uid=swg21622758

QUESTION 46
An Administrator of an IBM Security QRadar SIEM V7.2.8 deployment needs to exclude the mail servers from a custom rule.

How would the Administrator complete this task?

A. Create a building block that includes the IP addresses of all mail servers, use that building block in the custom rule, to exclude those hosts.
B. Create several rules excluding each mail server. Place these rules with the custom rule in a master rule, making sure the custom rule is last in the sequence.
C. Create a custom rule. In the “Rule Response” section of the Rule Wizard, select the Trigger Scan option. Add the mail server IP Addresses to the table and select exclude.
D. Create the custom rule. Create a Custom Action from the Admin Tab, to exclude the mail servers IP Addresses. In the “Rule Response” section of the Rule Wizard, select the Execute Custom Action option, selecting the appropriate Custom Action.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
explanation
Building blocks use the same tests as rules, but have no actions associated with them. Building blocks group together commonly used tests, to build complex logic, so they can be used in rules. Building blocks are often configured to test groups of IP addresses, privileged usernames, or collections of event names. For

example, you might create a building block that includes the IP addresses of all mail servers in your network, then use that building block in another rule, to exclude those hosts. The building block defaults are provided as guidelines, which should be reviewed and edited based on the needs of your network.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/CoreDocs/QRadar_71MR1_TuningGuide.pdf

QUESTION 47
How can an IBM Security QRadar SIEM V7.2.8 Administrator capture specific data to a reference set when QRadar receives the data from events or flow data?

A. Create or modify a report so the required data is exported to a Reference Set.
B. On the Admin tab. create or modify the reference set to capture the required data.
C. On the Admin tab define a Custom Action to add the required data to a Reference Set.
D. Create or modify a rule so the Rule Response will add the required data to a Reference Set.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You can click on the admin tab and select system configuration. The Reference set management will be seen. Click New and configure the parameters.

Reference ftp://public.dhe.ibm.com/software/security/products/qradar/documents/71MR1/SIEM/CoreDocs/QRadar_71MR1_AdminGuide.pdf

QUESTION 48
What are three protocols that collect flow data from network devices, such as routers, and send this data to IBM Security QRadar SIEM V7.2.8?

A. NetFlow, J-Flow and sFlow
B. NetFlow, IPFIX and syslog
C. NetFlow, rsyslog and sFlow
D. NetFlow, Packeteer and syslog

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation
NetFlow, J-Flow, and sFlow are protocols that collect flow data from network devices, such as routers, and send this data to QRadar.

Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_tuning_guide_deploy_cfgflowsource.html

QUESTION 49
An Administrator is adding a log source in IBM Security QRadar SIEM V7.2.8.

What required software application that supports the log source should be used for this procedure?

A. QRadar QFlow Collector
B. QRadar Event Collector
C. Device Support Module (DSM)
D. IBM X-Force Exchange plug-in for QRadar

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:
Explanation
Download and install a device support module (DSM) that supports the log source. A DSM is software application that contains the event patterns that are required to identify and parse events from the original format of the event log to the format that QRadar can use.

Reference http://documentation.extremenetworks.com/PDFs/SIEM-IPS/IBM_QRadar_Log_Sources_User_Guide_7.7.2.6.pdf

QUESTION 50
What is the difference between Flows and Event data collected by IBM Security QRadar SIEM V7.2.8?

A. Events are streamed each minute to the Event Processor. Flows are streamed immediately to the Flow Processor.
B. Flow data is collected from different log sources. Event data is collected from internal or external network sources.
C. An Event occurs at a specific time and is logged at that time. A Flow is a record of network activity that can last for seconds, minutes, hours, or days.
D. An Event can span time lasting seconds, minutes, hours depending on the duration of a network session. A Flow happens at a single point in time and then is complete.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference https://www.ibm.com/support/knowledgecenter/en/SS42VS_7.2.8/com.ibm.qradar.doc/c_qradar_deploy_event_and_flow_pipeline.html

QUESTION 51
What is needed to send the same events and flows to separate data centers or geographically separate sites and enable data redundancy in IBM Security QRadar SIEM V7.2.8?

A. A Flashcopy or GlobalMirror License.
B. A dark fibre network and proper configuration of the backup and recovery feature.
C. A load balancer or other method to deliver the same data to mirrored appliances.
D. Use the Backup and Recovery automation feature in QRadar and a dedicated fiber channel connection.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Explanation
Distribute the same event and flow data to two live sites by using a load balancer or other method to deliver the same data to mirrored appliances. Each site has a record of the log data that is sent.
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.6/com.ibm.qradar.doc/c_qradar_ha_data_redundancy_overview.html