IBM.Premium.C2150-624.by.VCEplus.60q

Number: C2150-624 VCEplus
Passing Score: 800
Time Limit: 120 min
File Version: 1.2

Exam Code: C2150-624
Exam Name: IBM Security QRadar SIEM V7.2.8 Fundamental Administration
Certification Provider: IBM
Corresponding Certification: IBM Certified Associate Administrator - Security QRadar SIEM V7.2.8
Website: www.vceplus.com
Free Exam: https://vceplus.com/exam-c2150-624/
Questions & Answers Exam Engine is rigorously checked before being put up for sale. We make sure there is nothing irrelevant in C2150-624 exam products and you get latest questions. We strive to deliver the best C2150-624 exam product for top grades in your first attempt.

VCE to PDF Converter : https://vceplus.com/vce-to-pdf/
Facebook: https://www.facebook.com/VCE.For.All.VN/
Twitter : https://twitter.com/VCE_Plus
Google+ : https://plus.google.com/+Vcepluscom
LinkedIn : https://www.linkedin.com/company/vceplus

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:
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:
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:
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:
Section: (none)
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 thereport 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:
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:
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?

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:
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
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.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
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.
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 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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The QRadar SIEM Event Processor Virtual 1699 appliance supports the following items:
Up to 10,000 events per second
2 TB or larger dedicated event storage
Reference https://www.ibm.com/support/knowledgecenter/SS42VS_7.2.4/com.ibm.qradar.doc_7.2.4/c_siem_vrt_ap_ov.html

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.

Correct Answer: C
Section: (none)
Explanation

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

QUESTION 11
Which is an officially supported operating system for IBM Security QRadar SIEM V7.2.8 installations on customer supplied hardware?

A. Ubuntu Linux
B. Windows 2012
C. Fedora Linux
D. Red Hat Enterprise Linux

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
The IBM Security QRadar Application Framework SDK can be installed on Windows, Linux, or OSX operating system.
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_appframework_devguide.pdf

QUESTION 12
An Administrator working with IBM Security QRadar SIEM V7.2.8 needs to assign a report to a group named Network Management.
What is the process for this task to be completed?

A. Reports Tab -> Select report -> Actions -> Assign Groups -> Item Groups -> select Network Management -> Assign Groups
B. Admin Tab -> Report Permissions -> select report -> Actions -> Assign Groups -> select Network Management -> Assign
C. Reports Tab -> Select report -> Actions -> Assign Users -> User Groups -> select Network Management -> Assign Users
D. Admin Tab -> Report Permissions -> select report -> Actions -> Assign Users -> select Network Management -> Assign

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
You can use the Assign Groups option to assign a report to another group
1.Click the Reports tab.
2.Select the report that you want to assign to a group.
3.From the Actions list box, select Assign Groups.
4.From the Item Groups list, select the check box of the group you want to assign to this report. 5. Click Assign Groups
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_users_guide.pdf

QUESTION 13
The Administrator of an IBM Security QRadar SIEM V7.2.8 deployment needs to determine which rules are most active in generating offenses.
How would the Administrator accomplish this from the Offenses tab of the QRadar console?

A. Rules -> Group -> “Most Active Offenses”.
B. Rules -> Rules -> Offense Count to reorder the column in descending order.
C. All Offenses -> All Offenses -> Offense Count to reorder the column in descending order.
D. All Offenses -> All Offenses -> Events to reorder the column in descending order. Use the Actions menu to view the rule information for a specific offence.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
1.Click the Offenses tab.
2.On the navigation menu, click Rules. To determine which rules are most active in generating offenses, from the rules page, click Offense Count to reorder thecolumn in descending order.
3.Double-click any rule to display the Rule Wizard. You can configure a response to each rule.
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_qradar_tuning_guide.pdf

QUESTION 14
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:
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 15
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:
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 16
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 17
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:
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 18
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:
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 19
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:
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 20
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:
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 21
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:
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 22
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:
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 23
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:
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 24
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:
Reference ftp://ftp.software.ibm.com/software/security/products/qradar/documents/7.2.8/en/b_QRadar_hardware_guide.pdf

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

QUESTION 25
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:
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 26
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:
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 storageuntil 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 thisbucket 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 27
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 28
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 29
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: