Up-to-date Questions and Answers from authentic resources to improve knowledge and pass the exam at very first attempt. ----- Guaranteed.

KILL EXAMS

C1000-127 MCQs
C1000-127 TestPrep
C1000-127 Study Guide
C1000-127 Practice Test
C1000-127 Exam Questions

PASS

killexams.com

IBM

C1000-127

IBM Security Guardium v11.x Administrator

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/C1000-127

Question: 553

In IBM Security Guardium, how do different policy actions affect the response to detected violations, particularly in scenarios where immediate remediation is necessary?

A. They are only applicable to user authentication failures
B. They are solely used for reporting purposes
C. They do not influence the system's response
D. They can either log, alert, or block access based on severity

Answer: D

Explanation: Different policy actions provide varied responses based on the severity of detected violations, allowing for logging, alerting, or blocking access as necessary for immediate remediation.

Question: 554

In order to harden an SQL Server instance, which of the following configurations should be prioritized in the security settings?

A. Enable SQL Server Authentication for all user accounts
B. Configure firewall rules to allow all incoming traffic
C. Use weak passwords to ensure compatibility
D. Disable unnecessary services and features within SQL Server

Answer: D

Explanation: Disabling unnecessary services and features reduces the attack surface of the SQL Server instance, making it a crucial step in hardening its security settings.

Question: 555

You are generating an entitlement report to audit access to a PostgreSQL database's "orders" table. The report must list all users with UPDATE privileges, including those granted through roles, and highlight any users with excessive permissions (e.g., both UPDATE and DELETE). Which report configuration would you use?

A. Use "User Access" report, filter by table=orders, access=UPDATE, enable "Include Groups", and disable "Permission Overlap"
B. Use "Entitlement Snapshot" report, filter by object=orders, permission=UPDATE, disable "Role Expansion", and enable "Excessive Access Check"
C. Use "Database Permissions" report, filter by table=orders, privilege=UPDATE, enable

"Include Roles", and enable "Highlight Excessive Permissions"
D. Use "Privilege Analysis" report, filter by object=orders, privilege=UPDATE, enable "Direct Permissions Only", and enable "Flag Overlaps"

Answer: C

Explanation: The "Database Permissions" report, filtered by table=orders, privilege=UPDATE, with "Include Roles" and "Highlight Excessive Permissions" enabled, meets the requirements.

Question: 556

Your organization uses IBM Security Guardium v11.x to manage access to a PostgreSQL database. You are configuring access groups to allow only users in the "HR_Admins" role to execute INSERT queries on the "EMPLOYEE" table. The access group is:

Access Group: HR_Access
Users: HR_Admins
Objects: EMPLOYEE
Permissions: Insert
Which policy rule enforces this restriction?

A. Rule: Allow_HR, Action: Allow, Condition: User IN GROUP HR_Admins AND SQL Command = INSERT AND Object = EMPLOYEE
B. Rule: Restrict_Non_HR, Action: Block, Condition: User NOT IN GROUP HR_Admins AND SQL Command = INSERT AND Object = EMPLOYEE
C. Rule: Block_All, Action: Block, Condition: SQL Command = INSERT AND Object = EMPLOYEE
D. Rule: Log_Non_HR, Action: Log Only, Condition: User NOT IN GROUP HR_Admins AND Object = EMPLOYEE

Answer: B

Explanation: To restrict INSERT queries to the HR_Admins role, a policy rule must block unauthorized users. The rule with Action: Block and Condition: User NOT IN GROUP HR_Admins AND SQL Command = INSERT AND Object = EMPLOYEE ensures only authorized users can insert. An Allow rule does not block unauthorized access, blocking all users is too restrictive, and logging only does not enforce control.

Question: 557

When deploying IBM Guardium appliances in a clustered environment, what is the recommended configuration to ensure high availability and load balancing across multiple appliances?

A. Configuring only one appliance as the primary and others as backup.
B. Using a load balancer in front of the appliances to distribute requests evenly.
C. Setting up each appliance with identical configurations but without clustering.
D. Storing configuration files on a shared network drive accessible by all appliances.

Answer: B

Explanation: Using a load balancer in front of the appliances helps distribute requests evenly across the cluster, ensuring high availability and optimal performance.

Question: 558

You are using GRD to deploy a Guardium v11.x Aggregator to a VMware ESXi 7.0 VM. The deployment fails with "GRD template validation failed." You verify the VM meets hardware requirements (16 GB RAM, 4 vCPUs, 200 GB disk). What is the most likely cause, and how should you resolve it?

A. The VM’s network adapter is incorrect. Change it to VMXNET3 in the VMware settings.
B. The OVA template is corrupted. Re-download the Guardium OVA file from IBM.
C. The GRD server’s template cache is outdated. Clear the cache using grd template clear.
D. The ESXi host lacks sufficient resources. Allocate more resources to the host.

Answer: A

Explanation: The "GRD template validation failed" error can occur if the VM’s network adapter is incompatible (e.g., E1000). Changing to VMXNET3, which is supported by Guardium, resolves this.

Question: 559

Your Guardium deployment manages a group of MySQL 8.0 databases tagged “Marketing.” You need to exclude databases with the “Dev” tag from compliance policies. Which configuration ensures dynamic exclusion?

A. Create a static group without “Dev” databases

B. Update the dynamic group query to exclude “Dev” tagged databases
C. Configure a CAS task to remove the “Dev” tag from Marketing databases
D. Use a Security Policy to block “Dev” database data

Answer: B

Explanation: Dynamic groups use queries to exclude tags like “Dev,” ensuring automatic updates. Static groups require manual changes. CAS doesn’t manage group tags. Policies control access, not membership.

Question: 560

A Guardium administrator needs to troubleshoot a policy violation alert that is not triggering as expected on a v11.5 Collector. The administrator runs the CLI command show policy and confirms the policy is installed correctly. To investigate further, the administrator wants to enable detailed debugging for the policy engine. Which CLI command should the administrator use to enable debug logging and capture relevant policy execution details in /var/log/guardium/policy.log?

A. store log_level policy debug
B. support enable_debug policy
C. store debug_policy on
D. support debug_policy enable

Answer: A

Explanation: To enable debug logging for the policy engine, the administrator should use the store log_level policy debug command, which sets the logging level for the policy engine to debug, capturing detailed execution details in /var/log/guardium/policy.log. The other commands are either invalid (support debug_policy enable, support enable_debug policy) or do not specifically target policy logging (store debug_policy on is not a recognized command).

Question: 561

In configuring the Guardium Collector, which of the following settings must be adjusted to handle SSL-encrypted database traffic effectively?

A. Enable data compression settings in the Collector
B. Limit the maximum number of concurrent connections
C. Disable all encryption settings to ensure compatibility
D. Configure the Collector to utilize an SSL certificate for decryption

Answer: D

Explanation: Configuring the Collector to utilize an SSL certificate for decryption is essential for effectively handling SSL-encrypted database traffic.

Question: 562

You are configuring a Guardium Aggregator to consolidate data from three Collectors in a Distributed deployment. The Aggregator is a virtual appliance with 16 vCPUs and 64 GB RAM. During the setup, you execute store aggregator add_collector for each Collector. However, the Aggregator fails to process data from one Collector, and the logs show a “data format error.” The Collector is running Guardium 11.5.0.2, and the Aggregator is running 11.5.0.1. What is the most likely cause, and how should you resolve it?

A. The Collector’s IP address is incorrect in the Aggregator’s configuration, and you must update it using store aggregator update_collector .
B. The Collector’s data is corrupted, and you must rebuild its database using db rebuild.
C. The Aggregator’s schema is misconfigured, and you must synchronize it using sync_schemas.
D. The Aggregator’s software version is outdated, and you must upgrade it to 11.5.0.2 using system upgrade.

Answer: D

Explanation: A “data format error” often results from a version mismatch between the Aggregator and Collector, as newer versions may introduce changes to data formats. Upgrading the Aggregator to match the Collector’s version (11.5.0.2) using system upgrade will resolve the issue. Rebuilding the Collector’s database, synchronizing schemas, or updating the IP address does not address version-related format errors.

Question: 563

During the installation of a Guardium v11.x S-TAP agent on a Linux server hosting a PostgreSQL database, the installation fails with “Invalid Collector IP.” Exhibit: The installation command is sudo ./guardium-stap-installer.sh --collector 10.0.0.30, and the Collector is at 10.0.0.30. What is the likely cause and resolution?

A. Network issue; verify connectivity to 10.0.0.30:16016
B. Typo in IP; verify and re-run with correct IP
C. Missing Collector certificate; add --collector-cert cert.pem

D. Incorrect port; update the firewall to allow port 8443

Answer: A

Explanation: The “Invalid Collector IP” error may indicate a network issue preventing the S-TAP from reaching the Collector at 10.0.0.30:16016, despite the correct IP. Verifying connectivity, including firewall rules for port 16016, resolves the issue. Port 8443 is for Central Manager communication, a certificate is not required unless TLS is enforced, and the IP is correct per the exhibit.

Question: 564

When integrating Guardium with existing security information and event management (SIEM) systems, which of the following protocols is commonly used for data transmission?

A. FTP
B. SNMP
C. Syslog
D. HTTP

Answer: C

Explanation: Syslog is commonly used for data transmission when integrating Guardium with existing SIEM systems, allowing for efficient log management and analysis.

Question: 565

In a multi-appliance Guardium deployment, what is the primary advantage of utilizing an Aggregator appliance?

A. It centralizes log data from multiple Collectors for easier reporting.
B. It directly connects to all data sources without needing Collectors.
C. It serves as a backup for all other appliances.
D. It eliminates the need for a Management Console.

Answer: A

Explanation: The Aggregator appliance centralizes log data from multiple Collectors, simplifying reporting and analysis across the deployment.

Question: 566

A Guardium administrator is troubleshooting an issue where an S-TAP on a Solaris server is not capturing traffic from an Oracle database. The guard_diag output shows "Inspection engine offline," and the Collector's show stap_status confirms the S-TAP is connected. The administrator verifies that port 9500 is open and the guard_tap.ini file is correct. What should the administrator do to resolve this issue?

A. Reinstall the S-TAP using the latest Solaris bundle
B. Restart the inspection engine on the Collector with restart inspection-core
C. Update the Oracle database configuration to enable Guardium auditing
D. Increase the S-TAP buffer size with store stap_buffer 512

Answer: B

Explanation: The "Inspection engine offline" error indicates that the inspection engine on the Collector, responsible for processing S-TAP data, is not running. Restarting it with restart inspection-core should bring it back online, allowing traffic capture. Reinstalling the S-TAP or updating the Oracle configuration is unnecessary since the S-TAP is connected. Increasing the buffer size does not address an offline inspection engine.

Question: 567

When configuring the network settings for Guardium Appliances, which of the following best describes a critical requirement?

A. All appliances must be on a single subnet
B. Each appliance must have a unique IP address
C. Network traffic can be unencrypted for performance
D. Limit bandwidth to avoid congestion

Answer: B

Explanation: Each Guardium appliance must have a unique IP address to ensure proper communication and functionality within the deployment.

Question: 568

In a Guardium v11.x environment, you are using the Policy Builder to create a policy that blocks unauthorized TRUNCATE TABLE commands on a MySQL database's "LOG" table. The rule is:

Rule: Block_Truncate
Action: Block
Condition: SQL Command = TRUNCATE TABLE AND Object = LOG
Alert: Notify_Security
Some TRUNCATE commands are logged but not blocked. Which configuration should you investigate?

A. Check for an exception list overriding the Block action
B. Verify the S-TAP parameter BLOCK_ENABLED=true
C. Ensure the policy group is assigned to the correct database instance
D. Update the audit process to include blocking actions

Answer: A

Explanation: If TRUNCATE commands are logged but not blocked, an exception list may be overriding the Block action. Exception lists take precedence over policy rules. BLOCK_ENABLED does not exist, policy group assignment affects monitoring, and audit processes do not handle blocking.

Question: 569

When configuring an IBM Guardium appliance, which of the following steps is critical for ensuring secure communication between Guardium and the databases it monitors?

A. Assigning a static IP address to the Guardium appliance
B. Installing the latest firmware updates
C. Configuring SSL certificates for encrypted communication
D. Setting up a VPN connection to the cloud

Answer: C

Explanation: Configuring SSL certificates ensures that the communication between Guardium and databases is encrypted, providing a secure channel for data transmission.

KILLEXAMS.COM

Killexams.com is a leading online platform specializing in high-quality certification exam preparation. Offering a robust suite of tools, including MCQs, practice tests, and advanced test engines, Killexams.com empowers candidates to excel in their certification exams. Discover the key features that make Killexams.com the go-to choice for exam success.

Exam Questions:

Killexams.com provides exam questions that are experienced in test centers. These questions are updated regularly to ensure they are up-to-date and relevant to the latest exam syllabus. By studying these questions, candidates can familiarize themselves with the content and format of the real exam.

Exam MCQs:

Killexams.com offers exam MCQs in PDF format. These questions contain a comprehensive collection of questions and answers that cover the exam topics. By using these MCQs, candidate can enhance their knowledge and improve their chances of success in the certification exam.

Practice Test:

Killexams.com provides practice test through their desktop test engine and online test engine. These practice tests simulate the real exam environment and help candidates assess their readiness for the actual exam. The practice test cover a wide range of questions and enable candidates to identify their strengths and weaknesses.

Guaranteed Success:

Killexams.com offers a success guarantee with the exam MCQs. Killexams claim that by using this materials, candidates will pass their exams on the first attempt or they will get refund for the purchase price. This guarantee provides assurance and confidence to individuals preparing for certification exam.

Updated Contents:

Killexams.com regularly updates its question bank of MCQs to ensure that they are current and reflect the latest changes in the exam syllabus. This helps candidates stay up-to-date with the exam content and increases their chances of success.