PASS QUESTION

QUESTION & ANSWER

HIGHER QUALITY, BETTER SERVICE

Provide One Year Free Update!

https://www.passquestion.com

Exam : **VMCSE_v13**

Title : Veeam Certified Security Expert v13

Version : DEMO

1.Scenario: A financial institution is deploying a new Ubuntu server to act as a Linux Hardened Repository (LHR) to ensure data immutability. The security policy dictates that the attack surface of the Veeam Backup & Replication (VBR) server must be minimized, specifically preventing credential theft from compromising the backup storage. The architect must configure the server connection in a way that adheres to strict zero-trust principles post-deployment.
A. Utilize persistent root credentials stored within the VBR database with native AES-256 encryption enabled.
B. Implement key-based SSH authentication stored in VBR to ensure continuous secure background monitoring.
C. Employ single-use credentials for deployment and subsequently disable SSH and sudo access on the Linux host.
D. Assign persistent non-root credentials with sudo privileges managed centrally via Windows Active Directory.
Answer: C
Explanation:
The absolute best practice for deploying a Linux Hardened Repository in Veeam is utilizing single-use credentials. VBR only requires SSH and sudo privileges during the initial deployment of the Veeam Data Mover components. Once deployed, the communication transitions entirely to certificate-based authentication over a specific port. By using single-use credentials and subsequently removing sudo rights (or disabling SSH entirely), administrators ensure that even if the VBR server is fully compromised, attackers cannot extract valid credentials to access the underlying immutable Linux file system.
Options A, B, and D all leave highly privileged, persistent authentication vectors active or stored within the VBR environment, fundamentally violating zero-trust architecture and creating a severe vulnerability.

2.Scenario: An enterprise organization has successfully upgraded to Veeam Data Platform v13 and strictly enabled the global "Four-Eyes Authorization" mechanism to mitigate insider threats. A disgruntled backup administrator attempts to sabotage the environment by executing multiple destructive actions through the VBR console.
Which of the following specific actions will be intercepted by the system and require secondary approval?
A. Deleting a critical backup chain directly from the underlying disk repository via the console.
B. Modifying an active backup job to immediately remove all mission-critical virtual machines.
C. Changing the retention policy of an existing backup job to the minimum permissible duration.
D. Revoking the multi-factor authentication token for the lead backup infrastructure architect.
Answer: A
Explanation:
Veeam's Four-Eyes Authorization (multi-person authorization) is explicitly engineered to intercept and block destructive, irreversible data operations. Deleting a backup chain from a disk or object repository, removing a repository entirely, or erasing a tape are all classified as destructive actions that will trigger the approval workflow. Modifying a backup job (Option B) or changing retention policies (Option C) does not immediately destroy existing data; while malicious, these actions halt future backups or alter future retention, but they do not actively purge historical immutable data, hence they bypass the Four-Eyes trigger. Revoking MFA tokens (Option D) is an administrative security function, not a data destruction event.

3.Scenario: The compliance department mandates the immediate enforcement of Multi-Factor Authentication (MFA) for all users accessing the Veeam Backup & Replication console. Concurrently, the IT automation team utilizes a dedicated service account to execute hundreds of daily recovery testing scripts via the Veeam REST API. The infrastructure team must apply the MFA policy without disrupting the automated testing workflows.
A. The automated API scripts automatically inherit the requirement and require hardcoded MFA seed tokens.
B. The REST API access utilizing Bearer Tokens remains entirely unaffected by the console GUI MFA policy.
C. The automated API access is blocked unless the service account is placed in the explicit MFA exclusion list.
D. The API scripts must be completely rewritten to utilize the specialized Veeam API Gateway component.
Answer: B
Explanation:
In the Veeam architecture, MFA is specifically designed to protect interactive, user-facing login sessions through the VBR Console (GUI). Automated programmatic access via the REST API utilizes standard OAuth 2.0 authorization flows, authenticating with valid credentials to generate a Bearer Token. Because API calls are inherently non-interactive, the Veeam engine seamlessly permits API token generation without enforcing an MFA prompt. Therefore, enabling global MFA will secure the console without breaking existing REST API automation.
Options A, C, and D represent fundamental misunderstandings of Veeam's security architecture; there is no need for hardcoded MFA tokens, there is no separate API Gateway component required for this, and an MFA exclusion list is unnecessary for API-only service accounts.

4.Scenario: A centralized Security Operations Center (SOC) requires access to the Veeam infrastructure to conduct forensic investigations during suspected malware outbreaks. The SOC analysts must be able to mount backups and perform Guest OS file-level restores to extract potentially malicious executables. However, strict separation of duties mandates that these analysts must have absolutely no ability to modify infrastructure, edit backup jobs, or alter retention policies.
A. Assign the SOC security team the built-in Veeam Backup Viewer administrative role.
B. Assign the SOC security team the built-in Veeam Backup Operator administrative role.
C. Assign the SOC security team the built-in Veeam Backup Administrator administrative role.
D. Assign the SOC security team the built-in Veeam Restore Operator administrative role.
Answer: D
Explanation:
The Veeam Restore Operator role adheres perfectly to the principle of least privilege for this scenario. It grants the precise permissions required to perform various restore operations (such as Guest OS file restores, application item restores, and full VM restores) but strictly prohibits the user from altering backup infrastructure, modifying job configurations, or starting/stopping backup tasks.
Option A (Backup Viewer) provides read-only access to configurations but prevents any restore operations.
Option B (Backup Operator) allows starting and stopping of backup jobs, violating the separation of

duties.
Option C (Backup Administrator) grants full, unrestricted access to the entire environment, entirely disregarding the security mandate.

5.Scenario: A highly regulated healthcare provider mandates that all backup data must be encrypted at rest utilizing their centralized enterprise Key Management System (KMS) via the KMIP protocol. They strictly forbid the use of standalone passwords managed within the backup software. The Veeam architect must configure the environment to dynamically fetch encryption keys from the external KMS provider for the primary backup jobs.
A. Format the underlying repository with ReFS and configure the KMS integration at the OS volume level.
B. Deploy the Veeam KMS Gateway component directly onto the target backup repository storage server.
C. Register the KMS server within VBR Security Settings and select the managed key in the job settings.
D. Disable the Veeam inline deduplication engine globally to allow external KMS encryption to function.
Answer: C
Explanation:
To integrate Veeam with an external KMS via KMIP, the configuration is a two-step native process. First, the administrator must register the external KMS server within the global "Security Settings" of the VBR console, establishing the certificate trust and authentication. Second, within the specific Backup Job settings (Storage -> Advanced), the administrator enables backup file encryption and selects the centralized key provided by the newly registered KMS.
Option A delegates encryption to the OS hardware level, bypassing Veeam's software encryption entirely.
Option B references a fictitious component; Veeam natively handles KMIP communication without a specialized gateway agent on the repository.
Option D is incorrect because Veeam's encryption architecture is explicitly designed to occur after compression and deduplication, ensuring both features operate optimally together.