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

KILL EXAMS

Vault-Associate-003 exam questions
Vault-Associate-003 exam pdf
Vault-Associate-003 practice test
Vault-Associate-003 study guide
Vault-Associate-003 TestPrep

PASS

killexams.com

HashiCorp

Vault Associate (003)

Vault Associate 003

ORDER FULL VERSION

https://killexams.com/pass4sure/exam-detail/Vault-Associate-003

Question: 1323

A Vault operator wants to see all active leases for a specific secrets engine without revoking them. What are the best ways to achieve this visibility?

A. Querying the storage backend directly (e.g., Consul KV) to see the stored lease entries.
B. Inspecting the Vault audit logs for recent lease generation events that haven't had a corresponding revocation.
C. Running vault status -leases to get a summary count of all active leases in the system.
D. Using the vault list sys/leases/lookup/path/ command to browse the hierarchy of active leases.
E. Using the Vault UI to navigate to the "Leases" tab and filtering by the engine's path.

Answer: A,B,D,E
Explanation: Using the vault list sys/leases/lookup/path/ command to browse the hierarchy of active leases. Querying the storage backend directly (e.g., Consul KV) to see the stored lease entries. Using the Vault UI to navigate to the "Leases" tab and filtering by the engine's path. Inspecting the Vault audit logs for recent lease generation events that haven't had a corresponding revocation.

Question: 1324

A Vault operator observes that after enabling mlock in the configuration, the process crashes on startup with permission errors when running as a non-root user. The environment must support mlock for key protection in memory. Which environment variable adjustment combined with OS configuration allows mlock without root privileges?

A. Use VAULT_LOG_LEVEL=trace to debug.
B. Export VAULT_DISABLE_MLOCK=true temporarily.
C. Set cap_ipc_lock capability on the Vault binary and run with VAULT_MLOCK=true implicitly via config.
D. VAULT_ENABLE_FILE_PERMISSIONS_CHECK=false.

Answer: D
Explanation: VAULT_ENABLE_FILE_PERMISSIONS_CHECK=false. This server environment variable disables the strict file permission checks that conflict with mlock capabilities granted via Linux capabilities (cap_ipc_lock), allowing the non-root Vault process to lock the root key and keyring pages in memory as

intended by the mlock configuration.

Question: 1325

For disaster recovery scripting, create a service token role with period=30d renewable=true to issue tokens that auto-renew monthly without explicit max TTL limits.

A. True
B. False

Answer: B
Explanation: Periodic tokens renew to their period but are capped by system/mount max TTL (default 32d); no unlimited non-root periods exist.

Question: 1326

For a Transit key created as type=chacha20-poly1305, the encrypt API requires associated_data (AAD) parameter for all calls, authenticating it alongside ciphertext without encryption.

A. True
B. False

Answer: A
Explanation: AEAD ciphers like chacha20-poly1305 mandate associated_data (base64) for authentication; omitting it errors during encrypt/decrypt/verify. AAD protects metadata integrity without confidentiality, computed into GCM/Poly1305 tags for tamper detection.

Question: 1327

Which of the following describes the behavior of policy path matching when multiple paths overlap, such as `secret/data/foo` and `secret/data/foo/bar`? (Select 3)

A. Vault ignores wildcards if an exact string match exists
B. Vault combines all capabilities from all matching paths
C. Wildcards (`+` or `*`) are evaluated if no exact match is found
D. The most specific (longest) path match wins
E. The "deny" capability always takes precedence regardless of path length

Answer: C,D,E
Explanation: Vault policy evaluation follows a "most specific match" rule where the longest matching path

string determines the permissions. However, if a "deny" capability exists on any matching path that would apply, it overrides other permissions. Wildcards allow for flexible matching but are secondary to an exact string match for a specific path.

Question: 1328

At Hotel Retail, the operations team must decide between userpass for temporary contractors (human) and AppRole for long-running batch jobs (system). Contractors log in daily via UI with passwords that expire after 24h and trigger lockout after 3 failures, while jobs use role_id fetched once and secret_id wrapped for 60s. The chosen methods must differ in token renewability: contractors get renewable service tokens, jobs get non-renewable batch tokens. Which key distinction in token lifecycle and credential management must guide the selection?

A. Userpass disables batch token type
B. Both enforce secret_id_num_uses=1
C. Human methods rely on interactive secrets that expire per login; system methods use static role_id with ephemeral secret_id
D. System methods always use renewable tokens with max_ttl

Answer: C
Explanation: Human methods rely on interactive secrets that expire per login; system methods use static role_id with ephemeral secret_id must guide the selection because userpass requires fresh password entry each session with per-user TTL and lockout, producing renewable tokens, whereas AppRole provides a fixed role_id combined with short-lived wrapped secret_ids for one-time use in batch jobs, producing non-renewable tokens suited to unattended machine execution.

Question: 1329

A security team wants to allow an application to encrypt data but strictly forbid it from decrypting any data. How should the Vault policy be structured to enforce this "write-only" encryption requirement?

A. Grant `read` capability on the path `transit/keys/app-key` to allow key discovery
B. Grant `sudo` capability on the `transit/encrypt/app-key` path
C. Explicitly deny the `update` capability on the path `transit/decrypt/app-key`
D. Grant `list` capability on the `transit/keys/` path
E. Grant `create` and `update` capabilities on the path `transit/encrypt/app-key`

Answer: C,D,E
Explanation: In Vault's Transit engine, encryption is an `update` (or `create`) operation on the `encrypt` sub-path. By granting this and explicitly denying or simply not granting access to the `decrypt` sub-path, you create a one-way encryption service. Listing keys is often helpful for administrative or discovery

purposes but doesn't grant decryption rights.

Question: 1330

A DevOps engineer is configuring a CI/CD pipeline to interact with a Vault instance over TLS with a self-signed certificate and custom namespace. The pipeline script must use environment variables to set the server address, authentication token, and skip TLS verification without using CLI flags. Which combination of environment variables ensures secure yet automated access while avoiding certificate validation errors and specifying the namespace for all commands?

A. Exporting only VAULT_ADDR and VAULT_TOKEN, as namespace and skip verify default to production settings.
B. Using VAULT_FORMAT=json and VAULT_LOG_LEVEL=debug for debugging.
C. Setting VAULT_ADDR, VAULT_TOKEN, VAULT_NAMESPACE, and VAULT_SKIP_VERIFY to true.
D. Setting VAULT_CACERT and VAULT_CLIENT_CERT for full TLS chain.

Answer: C
Explanation: Setting VAULT_ADDR, VAULT_TOKEN, VAULT_NAMESPACE, and VAULT_SKIP_VERIFY to true. These variables configure the CLI globally for the target server, authentication, namespace scoping, and TLS bypass in non-production pipelines, enabling all subsequent vault commands to operate without flags or certificate errors while isolating operations to the specified namespace.

Question: 1331

Response wrapping for API: POST to /sys/wrapping/wrap with target path returns token; unwrap extracts. Provides origin verification as token metadata shows wrapping path, preventing spoofed secret requests.

A. True
B. False

Answer: A
Explanation: True. Wrapping tokens include metadata like creation path, allowing pre-unwrap validation.

Question: 1332

In a Vault environment utilizing Shamir's Secret Sharing, the security team wants to perform a "Rekey" operation. What are the specific outcomes and requirements of this process?

A. The operation requires a quorum of the existing unseal keys to be provided to start the process
B. A new set of unseal keys is generated and distributed to the key holders
C. A new master key is generated and used to re-encrypt the keyring
D. The Vault cluster must be sealed during the entire duration of the rekey operation
E. The existing data in the storage backend is decrypted and re-encrypted with the new keys

Answer: A,B,C
Explanation: A rekey operation changes the unseal keys (the Shamir shards) and the underlying master key that protects the keyring. It requires a threshold of current unseal key holders to authorize the change. The cluster remains unsealed and online during this process; it does not require a full data re-encryption of the storage backend.

Question: 1333

A production Vault instance using AWS KMS auto-unseal experiences a region outage. The administrator has recovery keys stored offline. To restore access to the keyring without waiting for KMS recovery or migrating seals, what is the precise sequence involving the recovery keys and a specific flag on the unseal command?

A. vault operator rekey -target=recovery using the recovery keys to authorize.
B. vault operator rotate followed by recovery key entry.
C. vault operator unseal -migrate followed by recovery key entry.
D. vault operator unseal with the recovery keys directly.

Answer: B
Explanation: vault operator rekey -target=recovery using the recovery keys to authorize. Recovery keys authorize rekeying or root token generation in auto-unseal failures; they are entered with the -target=recovery flag to perform administrative recovery actions without decrypting the root key themselves until KMS returns.

Question: 1334

A microservice authenticates via AppRole, receiving a token with lease_id "auth/approle/login/xyz789-..." and renewable=true. The service uses Vault Agent's lifetime watcher with increment=3600 on this lease_id. When renewal fails due to backend downtime, Vault automatically revokes all child leases created by this token before the watcher can request a new auth lease.

A. False
B. True

Answer: A

Explanation: Token revocation cascades to revoke all associated child leases, but a failed renewal on the auth lease does not trigger automatic token revocation; the service must handle renewal failure.

Question: 1335

Short-lived secrets from vault write aws/staging/creds/lease ttl=900 limit blast radius in supply-chain attacks, as compromised creds auto-expire post-15m, forcing re-fetch and enabling detection via lease audit logs over static creds valid 365d.

A. True
B. False

Answer: B
Explanation: False because dynamic TTL enforces expiry, shrinking exposure vs. long-lived statics, with audit trails on creation/revoke aiding incident response in real-time threat models.

Question: 1336

A user is assigned two policies. Policy A grants `read` on `secret/data/app`. Policy B grants `update` on `secret/data/app`. What is the resulting effective permission for the user on that path? (Select 3)

A. Capabilities are additive
B. The user can perform a "patch" operation
C. The user can update the secret
D. The user can read the secret
E. The user can't do anything because of a conflict

Answer: A,C,D
Explanation: Vault policies are additive. When multiple policies are attached to a token, the capabilities are combined (the union of all permissions). Therefore, the user receives both read and update permissions. Note that "patch" is a separate capability and is not automatically granted by "update" in all contexts, though update often covers standard write-like behaviors.

Question: 1337

During a scheduled maintenance window on Vault 1.18, an operator needs to safely revoke all dynamic database credentials issued under the role `finance` (lease IDs prefixed `database/creds/finance/`) while ensuring backend cleanup (DELETE statements) executes even if some database connections are temporarily unavailable. Which CLI command with flags guarantees revocation proceeds despite backend errors?

A. vault lease revoke database/creds/finance/
B. vault lease lookup database/creds/finance/
C. vault lease renew -increment=0 database/creds/finance/
D. vault lease revoke -force database/creds/finance/

Answer: D
Explanation: vault lease revoke -force database/creds/finance/ is the correct command because the -force flag instructs Vault to ignore backend errors during revocation, ensuring all leases under the prefix are marked revoked and cleanup proceeds where possible using the lease ID prefix mechanism.

Question: 1338

An organization wants to implement Vault in a highly regulated environment and requires FIPS 140-2 compliance. Which architectural choices support this requirement?

A. Deploying Vault on FIPS-validated operating systems and hardware
B. Enabling the "Entropy Augmentation" feature to use external high-quality entropy sources
C. Using only the Shamir Secret Sharing method with at least 5 shards
D. Using Vault Enterprise with the HSM integration enabled
E. Configuring the Transit engine to use only FIPS-approved ciphers for all operations

Answer: A,B,D
Explanation: FIPS compliance involves using validated cryptographic modules (HSMs), running on validated infrastructure, and ensuring the quality of entropy (randomness) used for key generation. Enterprise features like HSM integration and entropy augmentation are specifically designed to meet these rigorous standards.

Question: 1339

Vault Secrets Operator is configured to sync dynamic database credentials. To prevent credential leakage after lease expiry, which operator feature combined with VaultSecret CR lifetime setting automatically revokes and refreshes the Kubernetes Secret?

A. secretTransformation with lease management enabled in the CR
B. Static secret only
C. No lifetime setting
D. Vault Agent only

Answer: A
Explanation: secretTransformation with lease management enabled in the CR leverages the operator's

built-in dynamic secret handling to revoke expired leases and update the Kubernetes Secret automatically.

Question: 1340

An engineer configures Vault's built-in PKI secrets engine to issue client certificates with a short ttl of 86400 and a max_ttl of 172800. Applications read the certificate and receive a lease_id such as pki/issue/client/... with lease_duration: 86400 and lease_renewable: true. The engineer writes a script that calls vault lease renew -increment=86400 ... every 12 hours and observes that after 48 hours the lease becomes non-renewable and the certificate is revoked. The engineer concludes that the lease_renewable flag flips from true to false once the second renewal is processed.

A. True
B. False

Answer: A
Explanation: True. The lease_renewable flag is fixed at lease creation and does not change dynamically; what changes is the lease's state, not the flag. In this case, the PKI-engine max_ttl of 172800 seconds (48 hours) sets an absolute upper bound on the lease lifetime. If the original issuance occurs at t=0 and each renewal extends the lease toward that maximum, the lease will reach its max-TTL at 48 hours and then be marked as non-renewable because no further extensions are allowed. The API response reflecting renewable: false after that point indicates post-expiration state, not a runtime flip of the flag. The engineer's conclusion that the flag itself flips during renewal is therefore incorrect.

Question: 1341

An organization is using the AppRole method. They want to ensure that if a secret_id is stolen, it cannot be used from outside their data center. Which parameters in the AppRole configuration can help enforce this?

A. secret_id_bound_cidrs: Restricts the use of the secret_id to specific IP ranges.
B. secret_id_num_uses: Limits how many times a single secret_id can be used to log in.
C. role_id_bound_cidrs: A parameter that prevents the role_id from being retrieved from unauthorized IPs.
D. token_bound_cidrs: Restricts the resulting Vault token to specific IP ranges.
E. bind_secret_id: A boolean that requires a secret_id for login (true by default).

Answer: A,B,D
Explanation: Vault provides several "defense in depth" settings for AppRole. `secret_id_bound_cidrs` ensures that the login attempt itself must come from a trusted network. `token_bound_cidrs` goes a step further by ensuring that even after a token is issued, it can only be used from those same trusted IPs. `secret_id_num_uses` is a great way to limit the "blast radius" of a credential, making it a one-time-use

secret if desired.

Question: 1342

A security architect at Beta Finance is designing identity unification across LDAP for human admins and AppRole for CI/CD pipelines. After successful logins, the architect needs to manually create an internal group named "finance-auditors" that includes entities from both auth methods, attach a read-only policy to the group so all members inherit it at evaluation time, and ensure external LDAP group membership is not auto-synced but requires explicit alias mapping on the group. The CLI command sequence must start with identity/group creation using type=internal followed by member_entity_ids assignment. Which approach correctly achieves unified policy inheritance without relying on external group aliases?

A. Rely solely on token policies attached during AppRole role creation
B. Create internal groups via the identity secrets engine and assign member entities manually
C. Enable external groups with alias to LDAP DN and use automatic membership on token renewal
D. Use JWT groups_claim mapping directly on token metadata

Answer: D
Explanation: Create internal groups via the identity secrets engine and assign member entities manually correctly achieves unified policy inheritance without relying on external group aliases because internal groups allow explicit addition of entity IDs from any auth method (including LDAP aliases and AppRole role-ids), policies attached to the group are evaluated alongside token policies at request time, and membership is fully managed by the operator rather than depending on external sync during renewals.

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 Based on Current Exam Objectives

Killexams.com provides exam questions aligned with the latest official exam objectives and latest syllabus. Our content is reviewed and updated regularly to reflect recent changes announced by certification vendors. By studying these questions, candidates will become cover the structure, difficulty level, and topic coverage of the actual exam, helping them prepare more effectively and efficiently.

Comprehensive Exam MCQs (PDF Format)

Killexams.com offers multiple-choice questions (MCQs) in easy-to-read PDF format, covering all major domains of the exam. Each PDF contains a structured collection of questions and verified answers designed to support focused study. These MCQs help candidates reinforce key concepts, identify knowledge gaps, and improve exam readiness through consistent practice.

Realistic Practice Tests (Online & Desktop)

To support hands-on preparation, Killexams.com provides practice tests through both an Online Test Engine and a Desktop Exam Simulator. These tools are designed to simulate a real exam environment, allowing candidates to practice under exam-like conditions. Performance tracking, test history, and result analysis help users evaluate their progress and focus on areas that need improvement.

Risk-Free Purchase Policy

Killexams.com follows a transparent and customer-friendly purchase policy. If users are not satisfied with the study materials, they may request assistance or a refund in accordance with our published terms and conditions. This policy reflects our commitment to customer satisfaction, fairness, and confidence in our preparation resources.

Regularly Updated Content

Our question bank is reviewed and updated on an ongoing basis to stay aligned with the latest exam outlines and vendor updates. This ensures candidates are studying relevant material and preparing with content that reflects current exam expectations, helping them stay confident and well-prepared.