

VAULT

Release Notes | Version 2.4 | July 2025

Version 2.4.0 — July 15, 2025

Release type: Minor | Previous version: 2.3.2 | Upgrade path: Rolling upgrade supported

i Version 2.4.0 requires Vault Agent version 2.3.0 or later. Review the upgrade checklist at vault.io/docs/upgrading/upgrade-to-2.4 before upgrading production clusters.

New Features

Dynamic Secrets — Redis Database Plugin

Vault now supports Redis as a dynamic secrets backend. The Redis database plugin generates short-lived credentials for Redis instances, including Redis Cluster and Redis Sentinel configurations.

- Supports Redis 6.x and 7.x
- Compatible with Redis Cluster (multi-shard) and Sentinel (HA) deployments
- Configurable ACL categories for fine-grained permission control
- Default TTL: 1 hour; Maximum TTL: 24 hours

Enable the Redis plugin:

```
vault write database/config/my-redis \   plugin_name=redis-database-plugin \
\   host=redis.internal.example.com \   port=6379 \   allowed_roles=readonly,readwrite
```

Documentation: vault.io/docs/secrets/databases/redis

KV v2 — JSON Merge Patch (PATCH Method)

KV v2 now supports the HTTP PATCH method for partial secret updates. Previously, updating a single field required re-writing the entire secret. The new PATCH capability updates only specified fields.

Update a single field without overwriting others:

```
vault kv patch secret/myapp/config password="new-password"
```

Or via the API:

```
curl -s -X PATCH \   -H "X-Vault-Token: $VAULT_TOKEN" \   -H "Content-Type: application/merge-patch+json" \   -d '{"data": {"password": "new-password"}}' \   $VAULT_ADDR/v1/secret/data/myapp/config
```

⚠ The PATCH method requires the patch capability in your policy in addition to update. Update existing policies before upgrading if clients will use PATCH.

Transit Engine — AEAD Encryption

The Transit secrets engine now supports Authenticated Encryption with Associated Data (AEAD) using the AES-256-GCM96 algorithm. AEAD binds ciphertext to a context value, ensuring that decryption fails if the ciphertext is used with a different context.

```
vault write transit/encrypt/mykey \   plaintext=$(base64 <<< "my secret") \   associated_data=$(base64 <<< "myapp-context-v1")
```

Web UI — Secret Diffing

The Vault web UI now displays a visual diff when viewing KV v2 secret version history. Users can select any two versions and view added, modified, and deleted fields side-by-side.

Navigate to: KV Engine → Secret Path → Metadata → Select two versions → Compare

Improvements

Component	Improvement	Impact
KV v2	List operation now returns metadata (created_time, version) alongside key names.	Reduced API round-trips for list-then-read workflows.
Auth — AppRole	SecretID can now be bound to specific CIDR ranges at creation time.	Improved security for AppRole deployments.
CLI	vault kv get now supports -mount flag to specify engine mount without embedding in path.	Cleaner CLI scripting.
Audit	Audit log entries now include the auth method display name alongside the accessor.	Improved log readability.
API	All KV v2 list endpoints now support pagination via after and limit query parameters.	Better performance for large secret stores.
Performance	Raft snapshot compression improved — 40% reduction in snapshot size.	Faster disaster recovery and lower storage costs.

Bug Fixes

Issue ID	Component	Description
VLT-4821	KV v2	Fixed: vault kv rollback failed silently when rolling back to a destroyed version. Now returns a clear error message.
VLT-4798	Transit	Fixed: Transit engine returned incorrect key version when rotating keys rapidly under high concurrency.
VLT-4776	Auth — Kubernetes	Fixed: Kubernetes auth method failed to validate service account tokens in clusters with custom API server FQDN.
VLT-4754	Web UI	Fixed: Policy editor in web UI stripped comments from HCL policies on save.
VLT-4731	CLI	Fixed: vault login -method=ldap ignored the -tls-skip-verify flag.
VLT-4709	Audit	Fixed: Audit log entries for failed requests did not include the request path when path parsing failed.

Deprecations

⚠ The following features are deprecated in 2.4.0 and will be removed in 3.0.0.

- KV v1 secrets engine — Migrate to KV v2 using the migration guide at vault.io/docs/secrets/kv/migration.

- `vault ssh -mode=otp` — Use the SSH certificate method instead.
- The `/v1/sys/mounts/:path/tune` endpoint — Use `/v1/sys/mounts/:path/tune-v2` instead.

Upgrade Notes

Policy Changes Required

If your policies use the patch capability, no changes are needed. If clients will begin using the PATCH method for KV v2 updates, ensure their policies include the patch capability:

```
path "secret/data/myapp/*" { capabilities = ["create", "read", "update", "patch", "delete", "list"] }
```

Upgrade Procedure

1. Back up your Vault data and configuration.
2. Review the full upgrade checklist at vault.io/docs/upgrading.
3. Upgrade standby nodes first, then the active node.
4. Verify cluster health after each node upgrade with `vault status`.
5. Test PATCH capability in a staging environment before production rollout.

Version 2.3.2 — June 2, 2025

Release type: Patch | Previous version: 2.3.1

Bug Fixes

Issue ID	Component	Description
VLT-4695	Database engine	Fixed: PostgreSQL plugin failed to clean up expired credentials when the database connection pool was exhausted.
VLT-4681	Raft storage	Fixed: Raft leader election took longer than expected under network partition conditions.
VLT-4662	PKI engine	Fixed: Certificate issuance failed when the Common Name contained Unicode characters.

Version 2.3.1 — May 12, 2025

Release type: Patch | Previous version: 2.3.0

Security Advisory

⚠ CVE-2025-1234 (Medium): A path traversal vulnerability in the KV v1 engine allowed authenticated users with list permissions to enumerate paths outside their policy scope. Users of KV v1 should upgrade immediately. KV v2 is not affected.

Bug Fixes

Issue ID	Component	Description
VLT-4641	KV v1	Security fix: Resolved CVE-2025-1234 path traversal vulnerability.
VLT-4628	Web UI	Fixed: Web UI login page did not correctly handle OIDC providers that return non-standard error codes.