HashiCorp Vault – Certificate Discovery Integration Guide

Overview

This guide describes the dedicated HashiCorp Vault discovery scan in CertSecure Manager, which enumerates certificates stored/managed within a Vault PKI mount and ingests them into the inventory. It covers configuring Vault discovery targets via the `/vault_config` endpoints, FQDN resolution for host fields, and scheduling scans.

Note: Discovery is read-only. The Vault credential used here needs list/read on the mount's certificates only — it does not require issue or revoke.

Prerequisites

- CertSecure Manager is operational and the Discovery module is enabled/licensed on your tenant.
- Your account has permission to create and run discovery scans.
- A reachable Vault cluster with the PKI mount(s) to be scanned.
- A Vault token/AppRole with read-only PKI access (`list <mount>/certs`, `read <mount>/cert/*`, `read config/urls`).
- Network access from the CertSecure backend to the Vault API (TCP 8200) and working DNS resolution for host-field mapping.

Read-Only Vault Policy for Discovery

```
# certsecure-discovery.hcl
path "<mount>/certs" { capabilities = ["list"] }
path "<mount>/cert/*" { capabilities = ["read"] }
path "<mount>/config/urls" { capabilities = ["read"] }
```

Configuration Steps

Step 1: Register the Vault Discovery Target (/vault_config)

- The Vault discovery configuration is managed through the `/vault_config` CRUD endpoints. In the UI: Discovery > Vault Configurations.
- Create a config: Vault Address, PKI Mount(s), Namespace (Enterprise), Auth Method + credential, and a friendly name.

API reference (if exposed for automation):

```
POST   /vault_config       # create
GET    /vault_config       # list
GET    /vault_config/{id}  # read
PUT    /vault_config/{id}  # update
DELETE /vault_config/{id}  # delete
```

Step 2: FQDN Resolution for Host Fields

- During discovery, host-oriented fields are populated by resolving certificate/host data to an FQDN, so discovered assets map to real endpoints in the inventory.
- Resolution order: SAN dNSName → reverse DNS → Vault metadata. Ensure DNS resolution is available from the CertSecure backend.

Step 3: Create and Schedule the Vault Discovery Scan

- Go to Discovery > Scans > New Scan; set Scan Type: HashiCorp Vault; select the Vault config from Step 1.
- Set the schedule (one-time or recurring) and run.

Step 4: Review Discovered Certificates

- Discovered certificates land in the inventory tagged with source = Vault Discovery.
- Assign ownership/department and enable lifecycle monitoring so expiry alerts route correctly.

Troubleshooting

Symptom	Likely Cause	Fix
No certs discovered	Mount has no stored certs, or policy missing `list` on `<mount>/certs`	Verify the mount; grant the `list` capability.
Hosts show IPs, not FQDNs	Reverse DNS unavailable, or SAN dNSName absent	Configure DNS/resolver; check SANs on the certs.
403 during scan	Read-only policy missing `read` on `<mount>/cert/*`	Grant `read` on `cert/*`.
Scan config rejected	Wrong Vault address/namespace or auth	Re-check `/vault_config` values and credential.