Vault Token Administration

Here are notes on access token administration.

Be sure that you've already setup an administrative policy in your vault cluster.

See this page for how: Vault Administrative Setup

Creating Admin Tokens

Once the admin policy exists, you can create administrative access tokens.

To do so, log into the leader note, with this:

```
# Use the root token...
vault login <root_token>
```

You can create a simple admin token that lasts 24 hours:

```
# Create an admin token that lasts 24 hours...
vault token create -policy=admin -ttl=24h
```

The above will issue short-lived admin tokens, so that the vault is more protected.
These can be minted by an automated script, that issues token as needed.

Traditional Admin

A more traditional administrative token needs to be longer-lived than a 24 hour token.

So, we will create a token role for admins.

This will create a periodic, orphan role so that admin tokens can be renewed forever (until revoked), and aren't tied to a parent token:

> NOTE: You will need to be logged into the vault leader (vault login <token>).

```
vault write auth/token/roles/admin \
  allowed_policies="admin,default" \
```

```
orphan=true \
renewable=true \
period=720h
```

The above token role, can create tokens that last 30 days, and can be renewed, without changing the token.

With the above admin role, you can create admin tokens of a more traditional lifetime, with this:

```
vault token create -role=admin -orphan -format=json
```

The above command will create admin tokens that can be given to your ops group, for longer-lived administrative access.

> NOTE: Be sure to save the client_token field in a secure place, such as a private password manager.

Token Renewal

Before a token expires, you can renew it with this command:

```
VAULT_TOKEN=<admin_token> vault token renew
```

> NOTE: The above can be automated, if the admin token is used by scripts or services. (Automate with a small systemd timer/cron on a secure host or in your gateway.)

Creating Other Admins

You can use an admin token to create other admins, like this:

```
# Another admin token (same role)
vault login <admin_token>
vault token create -role=admin -orphan -format=json
```

Creating Tokens for other Groups

Once you have other roles established as policies, you can create tokens for users, in those roles/policies, like this:

```
vault token create -policy=kv-readers -ttl=8h
```

Response-Wrapped Tokens

See this page for Response Wrapped Tokens: Vault Wrapping Token

---

Revision #2
Created 4 September 2025 02:35:10 by glwhite
Updated 4 September 2025 03:12:50 by glwhite