Vault Wrapping Tokens

When creating access tokens for HashiCorp Vault, you always want to prevent them from falling into the wrong hands, or showing up as clear-text in command line history, logs and audit trains.

To reduce the chance of tokens being passed in the clear, you can create a new user token in a response-wrapped state.
This allows the token to be given to a user, over chat, or text, without much concern.

The response-wrapped token has a very short lifetime, and can only be redeemed once.

Here's how to create a response-wrapped token:

```
vault token create -role=admin -orphan -wrap-ttl=5m -format=json
```

The command response will include the wrapping token, like this:


```
{
  "request_id": "",
  "lease_id": "",
  "lease_duration": 0,
  "renewable": false,
  "data": null,
  "warnings": null,
  "wrap_info": {
    "token": "hvs.tH5Wn8bD3eJxvMq1iP7F",
    "accessor": "PNowpcQP0jJ9Jpz06o2oueYW",
    "ttl": 300,
    "creation_time": "2025-09-04T02:26:49.859843035Z",
    "creation_path": "auth/token/create/admin",
    "wrapped_accessor": "5KlfcQwbo05Ej37YOqBJnfHM"
  }
}
```


The wrap_info/token property is what you give to the user.

The user can then, redeem their access token by submitting the wrapping token, like this:

```
vault unwrap hvs.tH5Wn8bD3eJxvMq1iP7F
```

Vault will respond with the real token, and revoke further usage of the wrapping token.

> NOTE: The wrapping token has an expiry. If exceeded, the user will need to request another.

Wrapped Token Benefits

Using wrapped tokens, prevents exposure in shell history or logs.

Delivery is safer, as you can drop the short-lived wrapper into a config management pipeline or paste in a chat.

The Vault audit log records that the wrapping token was created and who unwrapped it.

Revision #1
Created 4 September 2025 02:32:09 by glwhite
Updated 4 September 2025 03:13:03 by glwhite