Controlling Access in Vault

Ned Bellavance
MICROSOFT AZURE MVP

@ned1313 | nedinthecloud.com

Overview

Using authentication methods

Creating and applying policies

Managing client tokens

Authentication Methods

Internal Authentication

External Authentication

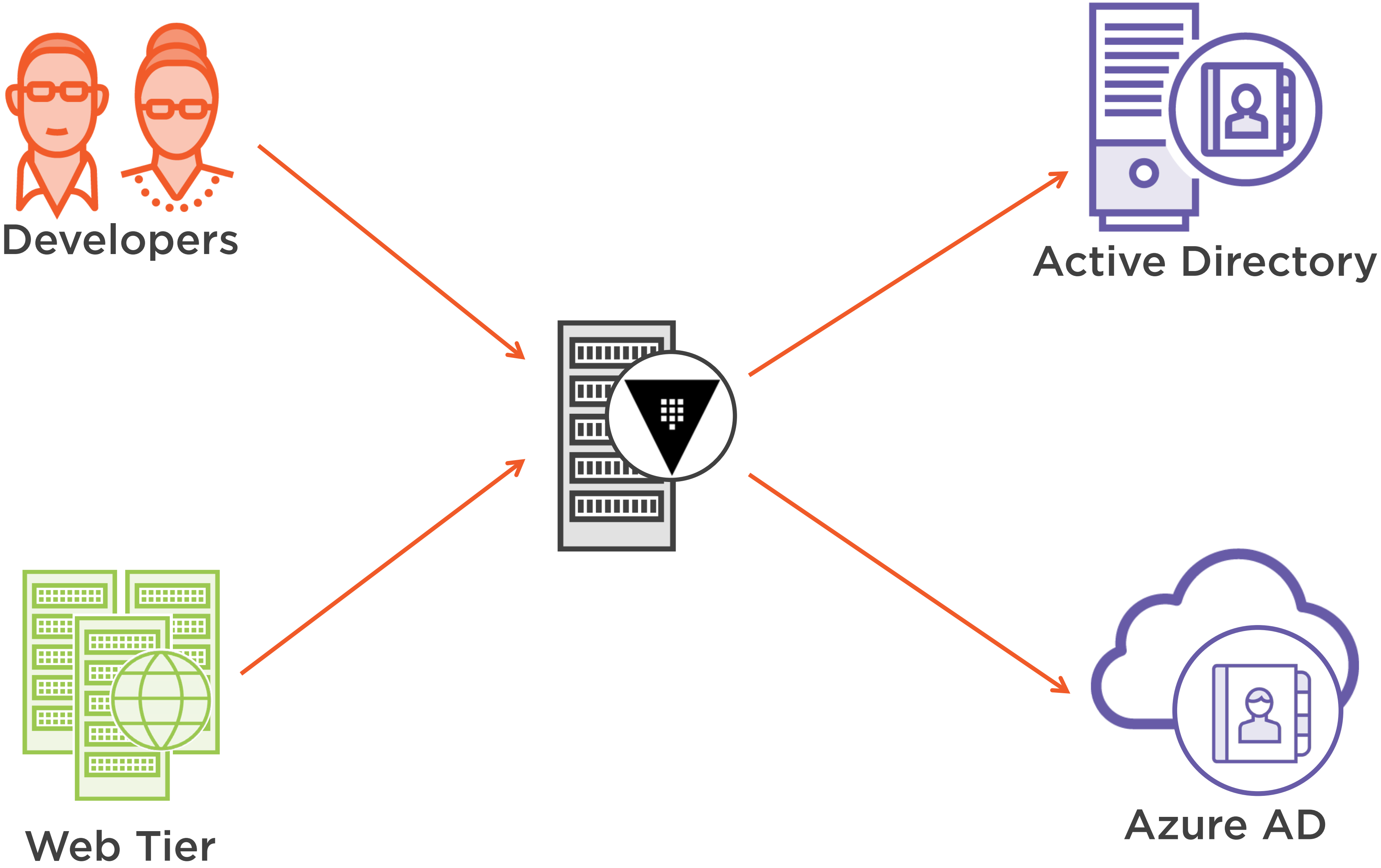
Multiple Methods

Basic Setup

Working with Auth Methods

```
#Enable an auth method

vault auth enable [method]

#Write the config to an auth method

vault write auth/[method]/config

#Add a role to the auth method

vault write auth/[method]/role/[role_name]

#Disable an auth method

vault auth disable [method]
```

Globomantics Scenario



Vault Policies

Who, what, and how

HCL or JSON (mostly HCL)

Variables for identity

Specify parameters

Default and root policies

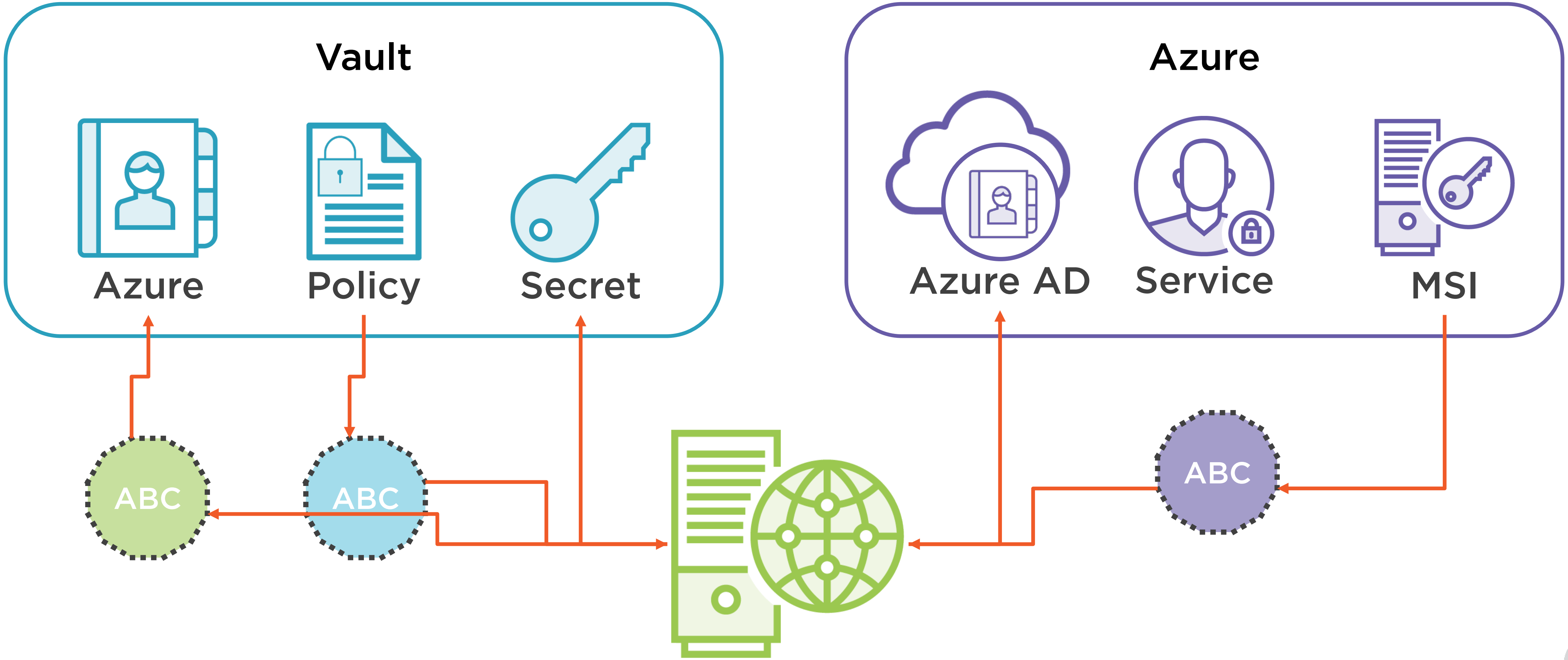
Policy Document

```
path “path_of_secret_data/[*]” {
  capabilities = [“create”,”read”,”update”…]
  required parameters = [“param_name”]
  allowed parameters = {
    param_name = [“list”,”of”,“values”]
  }
  denied_parameters = {
    param_name = [“list”,”of”,“values”]
  }
}
```

Working with Policies

```
#List all policies

vault policy list

#Create a policy

vault policy write [policy] [policy_file.hcl]

#Update a policy

vault write sys/policy/[policy] policy=[policy_file.hcl]

#Delete a policy

vault delete sys/policy/[policy]
```

Azure AD Auth



Client Tokens

ABC

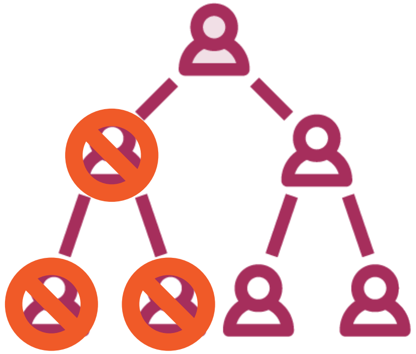
Service

XYZ

Batch

Policies

Metadata

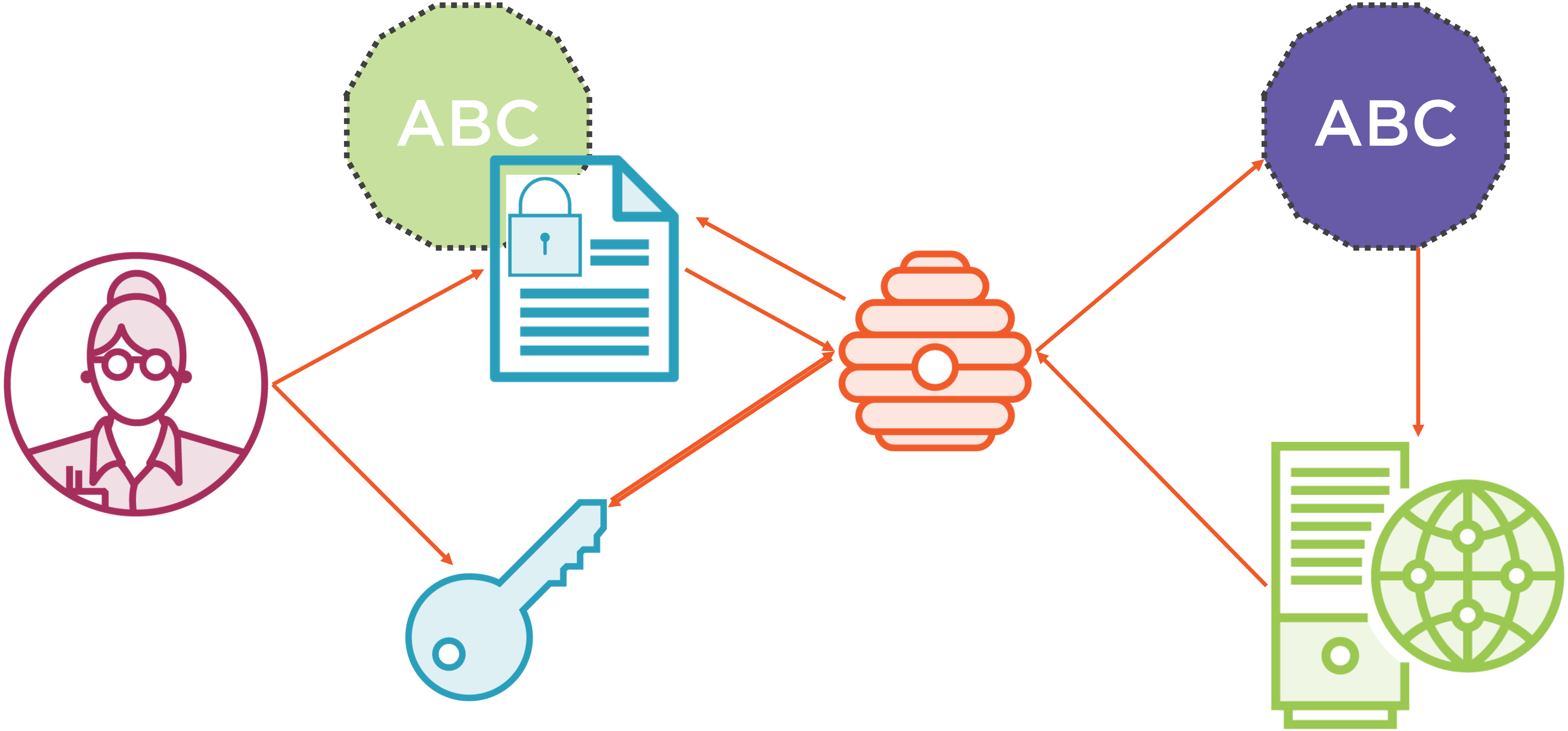


Token hierarchy

ABC

Token accessors

Response Wrapping



Conclusion

Authentication is all about tokens

Policies are added to tokens

Tokens are the foundation of Vault access

Coming up:

- Operating Vault Server