HashiCorp
Vault **Vault LDAP Auth Using Active Dirctory**

1 | enable the vault LDAP Auth method

Infra

Kubernetes	LDAP	Okta	RADIUS
○	◉	○	○

2 | type the windows active directory domain name

Configure LDAP

Configuration   Method Options

URL ⓘ

ldap://vault.dom

3 | Under LDAP Options Configure

User Attribute ⓘ

samaccountname

HashiCorp
Vault Vault LDAP Auth Method Using Active Directory

2 | **Under User Search**

Name of Object to bind (binddn) ⓘ

cn=vault,ou=VaultDemo,dc=vault,dc=dom

User DN ⓘ

ou=VaultDemo,dc=vault,dc=dom

Bindpass ⓘ

Enter vault Password

User Search Filter ⓘ

({{.UserAttr}}={{.Username}})

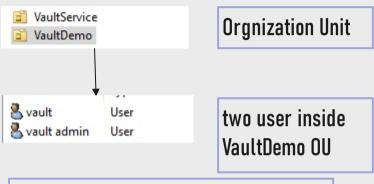**3** | **Under Group Membership**

Group Filter ⓘ

(&(objectClass=person)(uid={{.Username}}))

Group Attribute ⓘ

memberOf

Group DN ⓘ

ou=VaultDemo,dc=vault,dc=dom

☐ Use token groups ⓘ

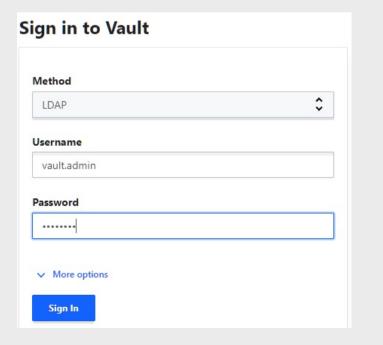**Configuration from command line**

```
vault write auth/ldap/config \
    url="ldap://vault.dom" \
    userattr=sAMAccountName \
    userdn="ou=VaultDemo,dc=vault,dc=dom" \
    groupdn="ou=VaultDemo,dc=vault,dc=dom" \
    groupfilter="(&(objectClass=person)(uid={{.Username}}))" \
    groupattr="memberOf" \
    binddn="cn=vault,ou=VaultDemo,dc=vault,dc=dom" \
    bindpass="Lock@123"
```
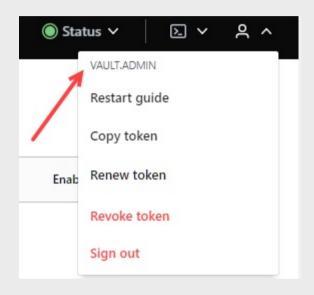
HashiCorp
Vault   Vault LDAP Auth Method using Active Directory

4   Active Directory Configuration

VaultService
VaultDemo

Orgnization Unit

vault   User
vault admin User

two user inside
VaultDemo OU

5   Login from Vault Ui

Sign in to Vault

Method

LDAP

Username

vault.admin

Password

••••••••

⌄ More options

Sign In

6   vault admin Logged in

◉ Status ⌄   ⊠ ⌄   ⌂ ∧

VAULT.ADMIN

Restart guide

Copy token

Renew token

Revoke token

Sign out

Enab

Note Vault Assign Default Policy

HashiCorp Vault   Active Directory Secret Engine

7 | Admin Policy using url

https://learn.hashicorp.com/tutorials/vault/policies

8 | Apply to AD User

Create user vault.admin in vault Auth
Method and Apply admin Policy

Edit user vault.admin

Groups ⓘ

Policies ⓘ

admin

Now Active directory User will get rights
according to vault Policy