Managing Administrator Access Using Roles

Ned Bellavance
MICROSOFT AZURE MVP

@ned1313 | nedinthecloud.com

Overview

Operator actions

Globomantics scenario

Policies and association

Vault Paths Refresher

Everything is a path

API first and always

Common paths:

- Identity
- Secret
- Auth
- Sys

Operator and Privileged Actions

Auditing

/sys/audit

Authentication

/auth

Seal

/sys/seal

Policies

/sys/policy

Secret Engines

/sys/mounts

Globomantics Scenario

Full Administrator

- Can do almost everything

Engine Administrator

- Works with secret engines

Audit Administrator

- Configures audit settings

Helpdesk Administrator

- Works with auth and secrets issues

Vault Policies

Who, where, and what

HCL or JSON (mostly HCL)

Token and identity policies

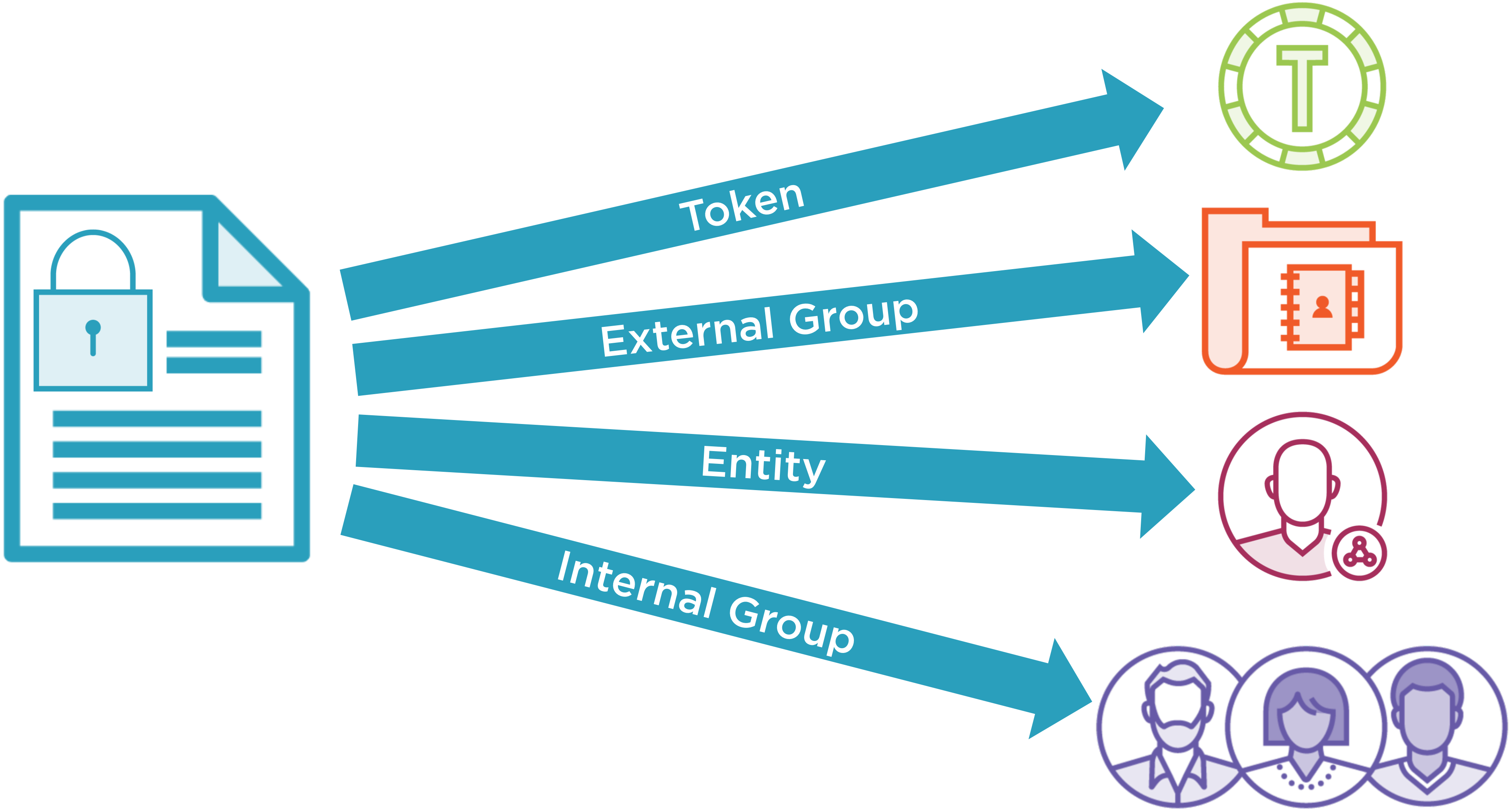
Default and root policies

Special actions

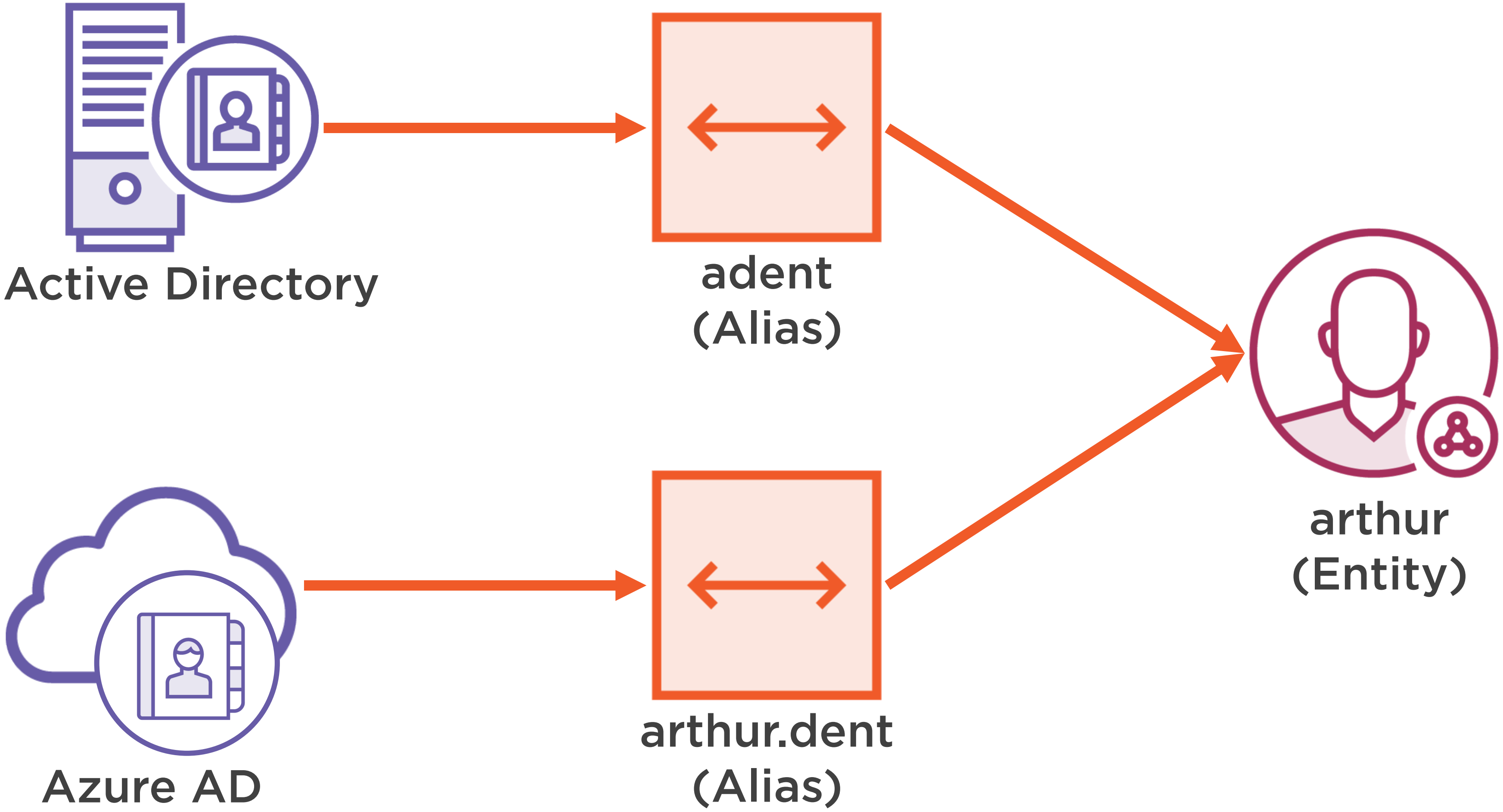
Policy Examples

```
path "sys/policy"
{
  capabilities = ["read"]
}


path "sys/policy/*"
{
  capabilities = ["create", "read", "update", "delete",

    "list", "sudo"]
}
```

Policy Association



Aliases and Entities



Summary

No formal role construct

Token and identity policies

Policies are finicky, test them

Coming up:

- Monitoring Vault Server