AWX 201: Advanced Automation Techniques with the Ansible AWX Platform

Tim Glen
Security Solutions Engineer

DEVNET-2517

Cisco Webex App

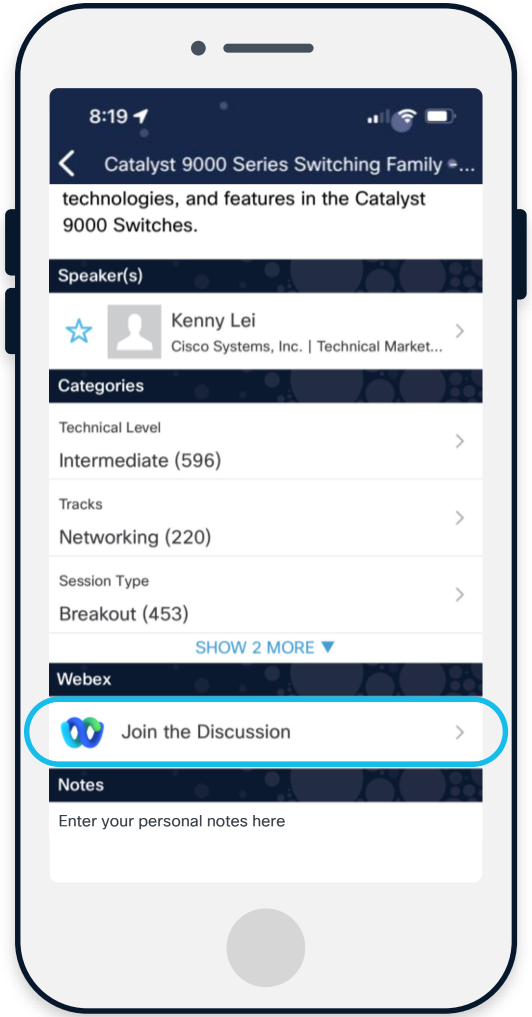
Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until June 13, 2025.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Tim (Personal)

- Human
- Husband
- Father
- Dog Dad
- Outside
- Biking
- Driving
- Travel

Tim (Professional)

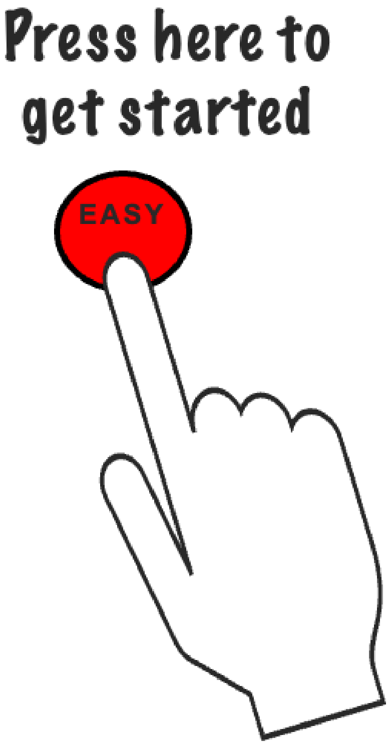
- Started in IT in 1995, Telephone Tech Support
- Worked 23 years at Web Hosting Provider
  - Managed all routers, switches, firewalls, wireless, security
- Worked at Cisco 6 years
  - Security Systems Engineer

github.com/timmayg

linkedin.com/in/timglen

cs.co/TimGlen

Agenda



1 Introduction

2 Execution Environments

3 Custom Credentials with HashiCorp Vault

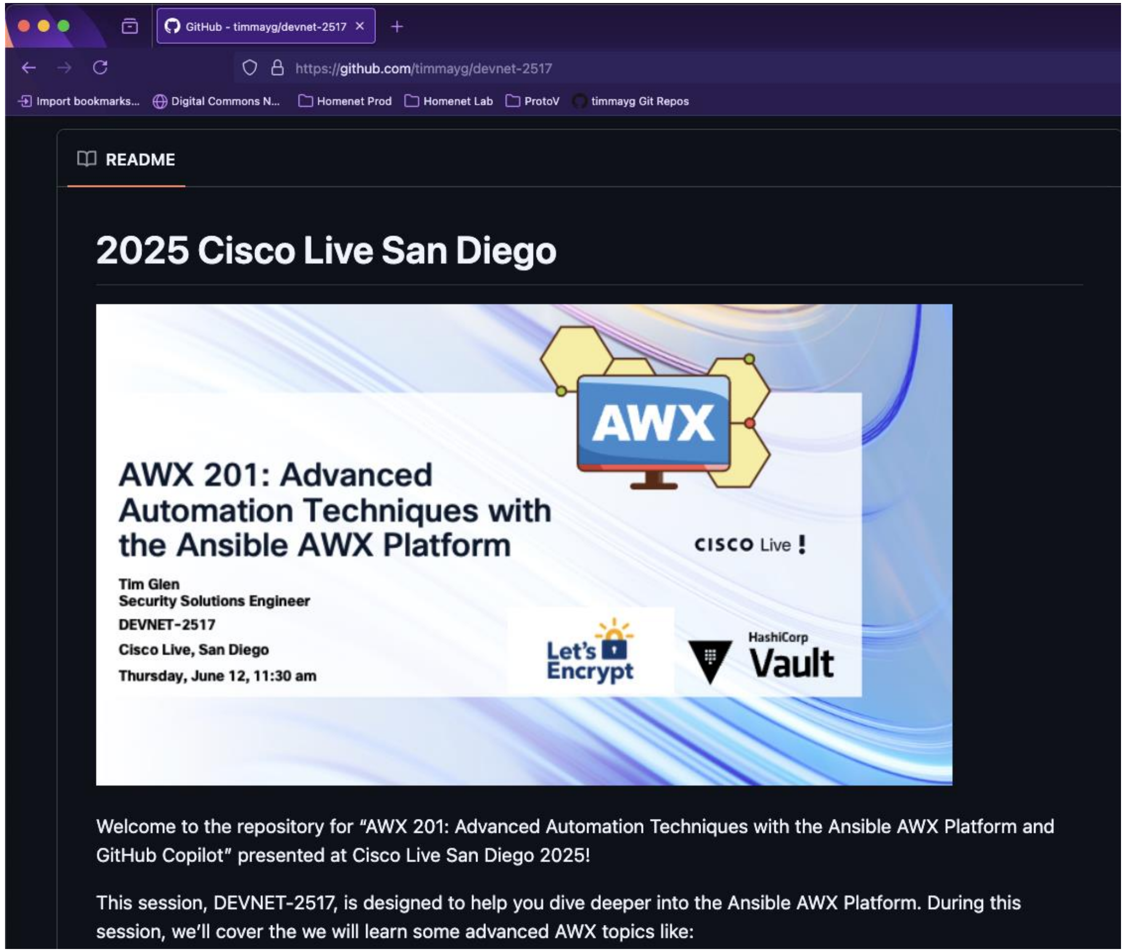
4 Certificate Automation

5 Conclusion

Check Here for Updates

GitHub

https://github.com/timmayg/devnet-2517



2025 Cisco Live San Diego

AWX 201: Advanced Automation Techniques with the Ansible AWX Platform

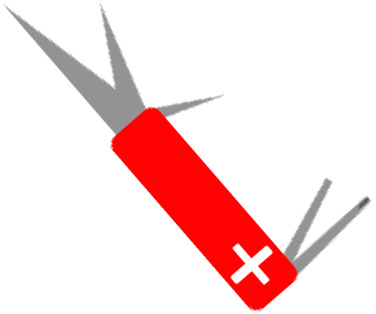
Tim Glen
Security Solutions Engineer
DEVNET-2517
Cisco Live, San Diego
Thursday, June 12, 11:30 am

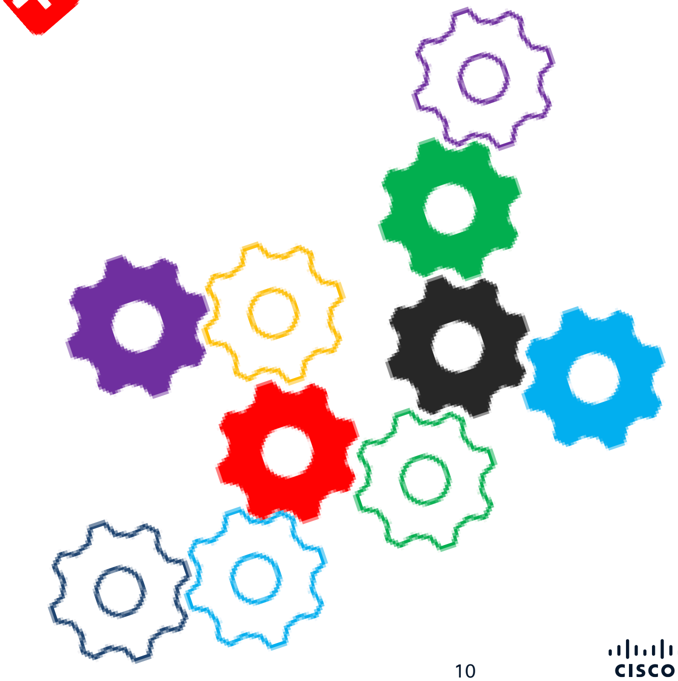
Welcome to the repository for "AWX 201: Advanced Automation Techniques with the Ansible AWX Platform and GitHub Copilot" presented at Cisco Live San Diego 2025!

This session, DEVNET-2517, is designed to help you dive deeper into the Ansible AWX Platform. During this session, we'll cover the we will learn some advanced AWX topics like:

Why Ansible, Why AWX

- Ansible is tool of choice
- Flexibility – Manages Everything
- Easy to write playbooks
- AWX is the next step
- Powerful task engine!
- AWX Web UI & REST API
- Scheduler, Logging





AWX – High Level

- Ansible Automation Platform
- Orgs, Teams & Users
- Templates & Projects
- Hosts & Inventories
- Credentials & Credential Types
- Instances, scaling
- Execution Environments

AWX Integrations & Compatibility

cisco

ISE

aws

Let's Encrypt

HashiCorp Vault

slack

ACME

ANSIBLE

GitHub

Azure

webex by cisco

Terraform

servicenow

netbox

PagerDuty

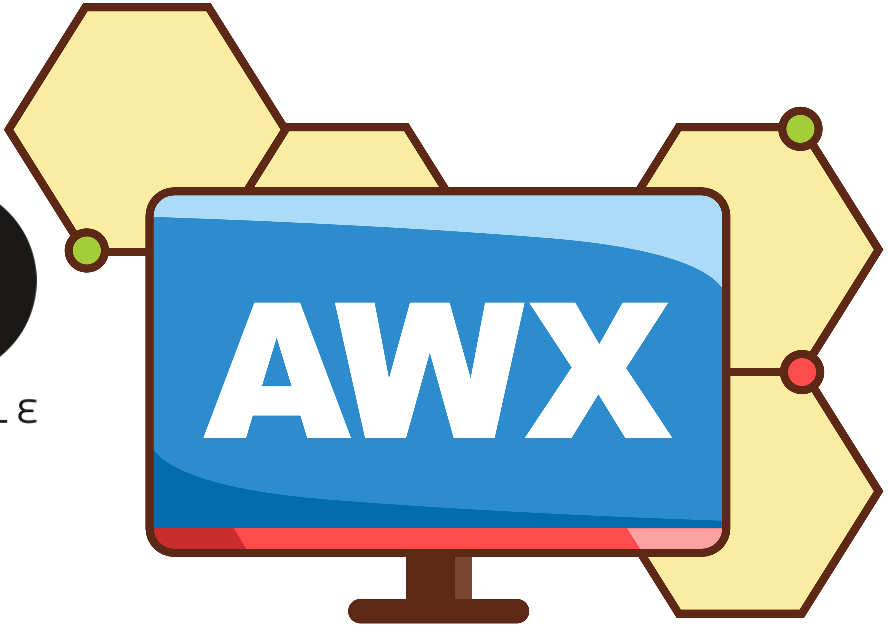
AWX Integrations & Compatibility

HashiCorp Vault

cisco

ACME

ANSIBLE



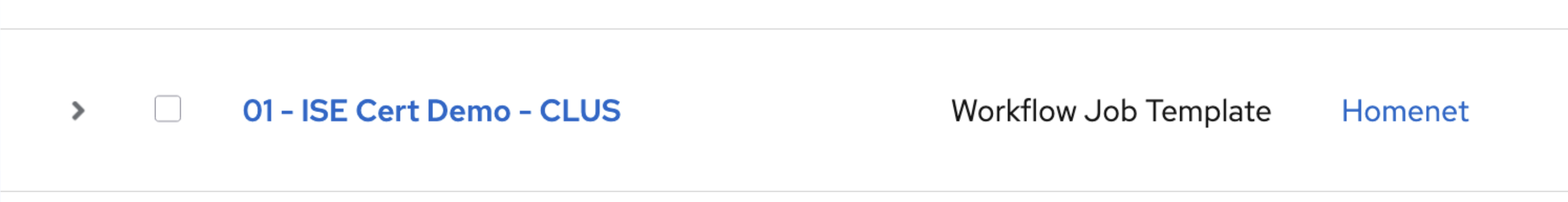
ISE

Let's Encrypt

webex by cisco

Run ISE Cert Job RIGHT NOW

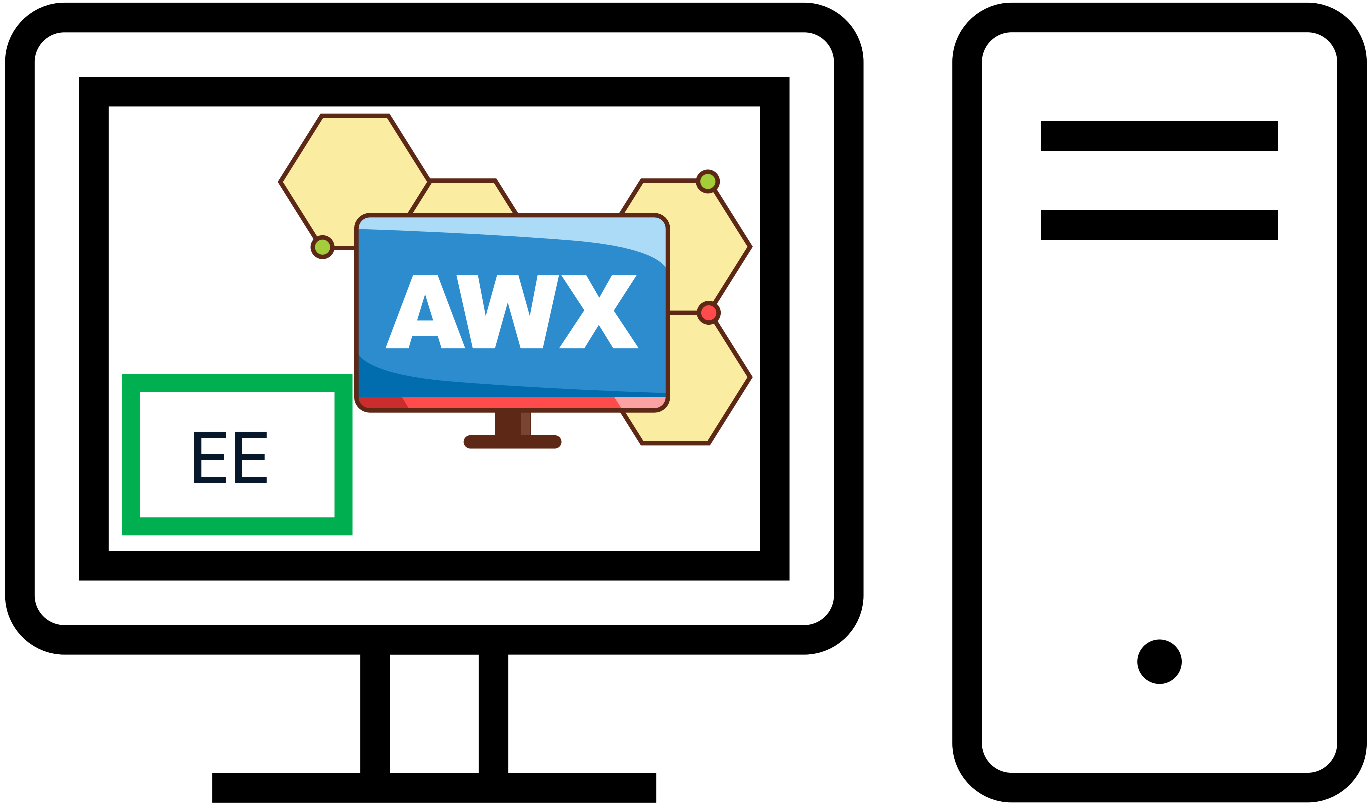
Label: demo



› ☐ 01 - ISE Cert Demo - CLUS | Workflow Job Template | Homenet

Execution Environments

Execution Environment



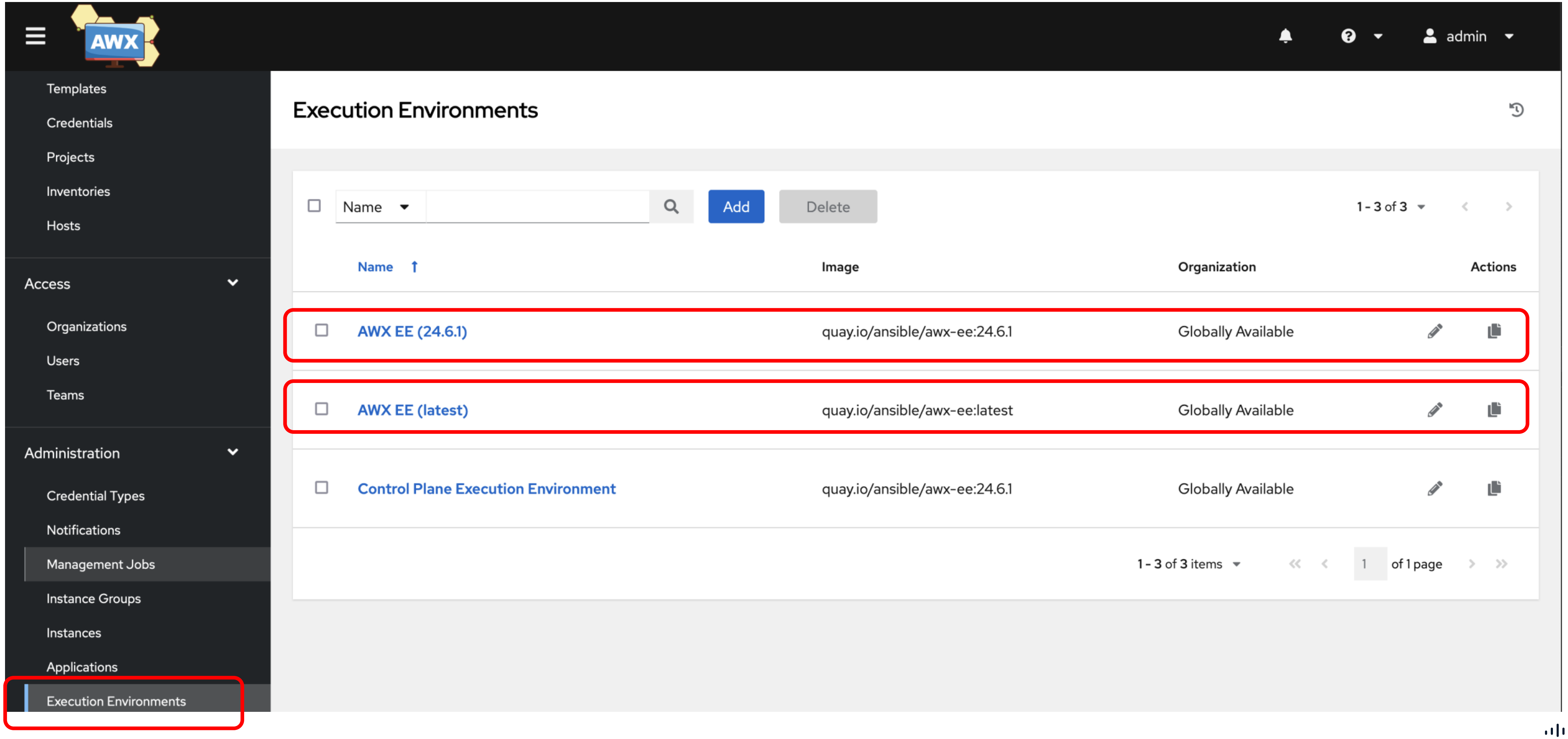
- Playbooks \ templates do not run on AWX host OS
- Playbooks run inside of specialized EE container
- AWX server stays clean
- EE gets python libraries, modules etc.

Execution Environment

- Linux container, spun up by AWX at playbook runtime
- Functional Execution Environment is built into AWX – awx-ee
- Build your own!
- Includes ansible-core, ansible-runner, python, python library & package, ansible collections, system dependencies
- Container provides consistency, and scalability, assuring playbooks run
- Stored Container Registries, Docker Hub, Quay IO, private repos

https://docs.ansible.com/ansible/latest/getting_started_ee/index.html

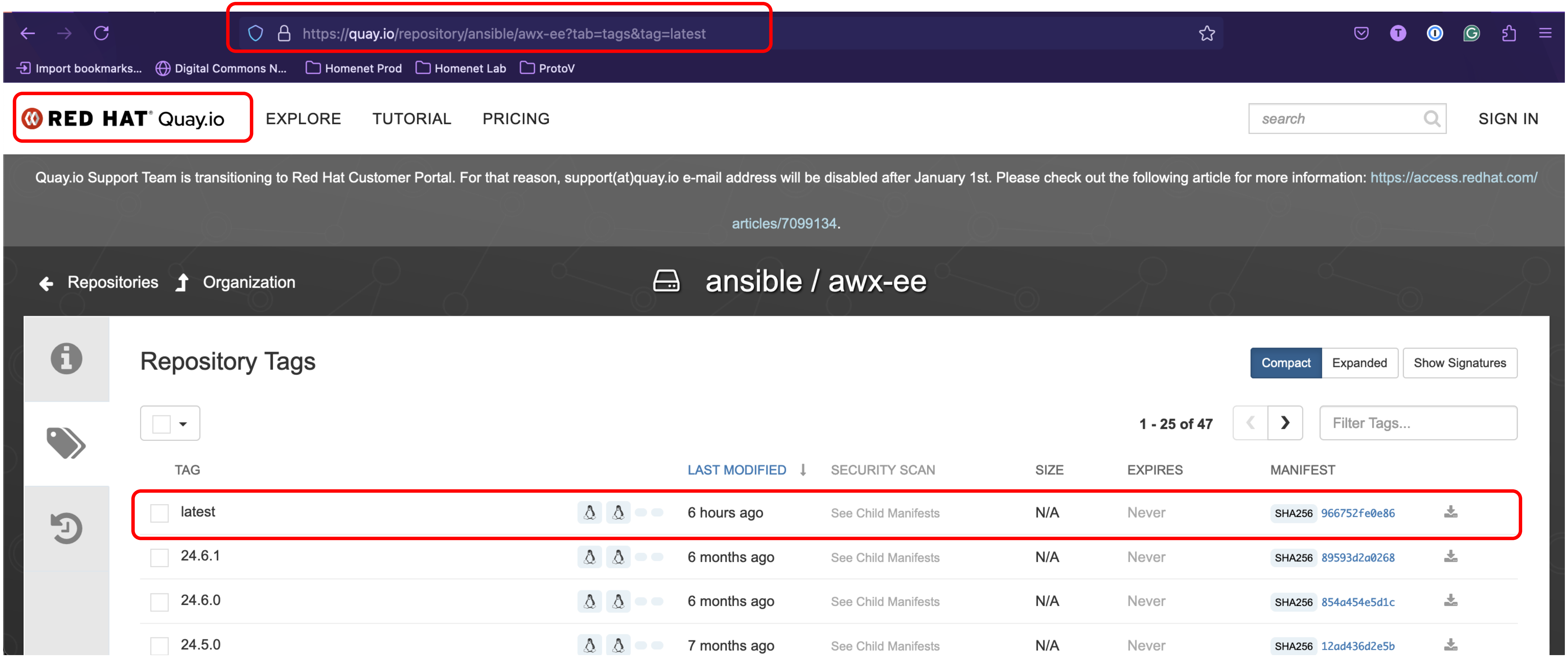
Execution Environment



Execution Environments

	Name	Image	Organization	Actions
□	AWX EE (24.6.1)	quay.io/ansible/awx-ee:24.6.1	Globally Available	
□	AWX EE (latest)	quay.io/ansible/awx-ee:latest	Globally Available	
□	Control Plane Execution Environment	quay.io/ansible/awx-ee:24.6.1	Globally Available	

AWX-EE



https://quay.io/repository/ansible/awx-ee?tab=tags&tag=latest

Quay.io Support Team is transitioning to Red Hat Customer Portal. For that reason, support(at)quay.io e-mail address will be disabled after January 1st. Please check out the following article for more information: https://access.redhat.com/articles/7099134.

ansible / awx-ee

Repository Tags

1 - 25 of 47

TAG	LAST MODIFIED	SECURITY SCAN	SIZE	EXPIRES	MANIFEST
latest	6 hours ago	See Child Manifests	N/A	Never	SHA256 966752fe0e86
24.6.1	6 months ago	See Child Manifests	N/A	Never	SHA256 89593d2a0268
24.6.0	6 months ago	See Child Manifests	N/A	Never	SHA256 854a454e5d1c
24.5.0	7 months ago	See Child Manifests	N/A	Never	SHA256 12ad436d2e5b

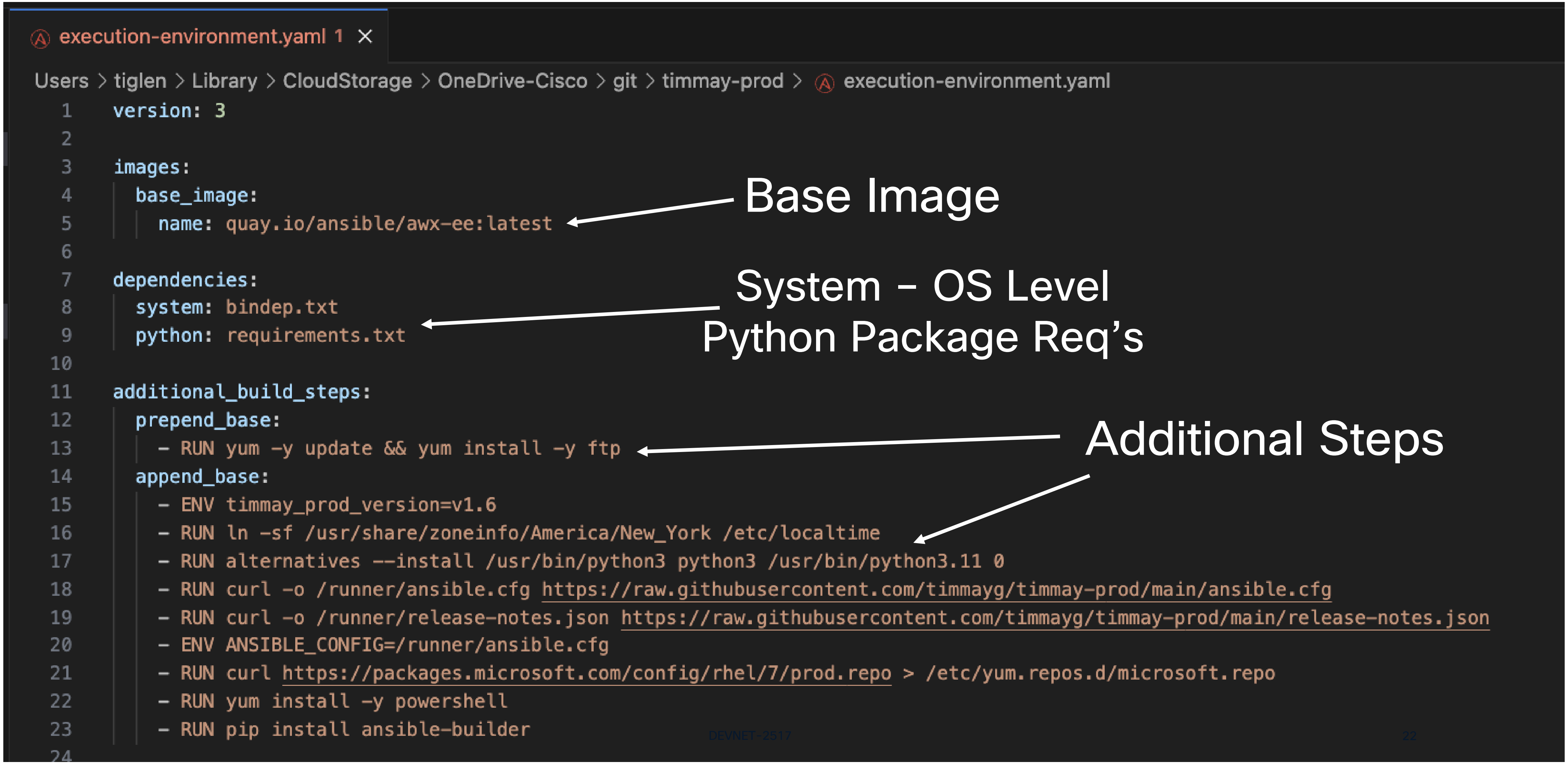
Updating the Execution Environment

- Update one or more of the following files
  - execution-environment.yaml ← 1 Required –base OS, build template
  - bindep.txt ← 2 Optional – system-level dependencies
  - requirements.txt ← 3 Optional – python packages
  - requirements.yaml ← 4 Optional – Ansible Galaxy
- Use ansible-builder to build a new Image
- Verify Image contents using podman
- Upload Image to Container Registry
- AWX downloads the latest image next playbook run

https://developers.redhat.com/articles/2023/05/08/how-create-execution-environments-using-ansible-builder

execution-environment.yaml

- Execution Environment Schema Definition



execution-environment.yaml 1 ×

Users > tiglen > Library > CloudStorage > OneDrive-Cisco > git > timmay-prod > execution-environment.yaml

```yaml
version: 3

images:
  base_image:
    name: quay.io/ansible/awx-ee:latest

dependencies:
  system: bindep.txt
  python: requirements.txt

additional_build_steps:
  prepend_base:
    - RUN yum -y update && yum install -y ftp
  append_base:
    - ENV timmay_prod_version=v1.6
    - RUN ln -sf /usr/share/zoneinfo/America/New_York /etc/localtime
    - RUN alternatives --install /usr/bin/python3 python3 /usr/bin/python3.11 0
    - RUN curl -o /runner/ansible.cfg https://raw.githubusercontent.com/timmayg/timmay-prod/main/ansible.cfg
    - RUN curl -o /runner/release-notes.json https://raw.githubusercontent.com/timmayg/timmay-prod/main/release-notes.json
    - ENV ANSIBLE_CONFIG=/runner/ansible.cfg
    - RUN curl https://packages.microsoft.com/config/rhel/7/prod.repo > /etc/yum.repos.d/microsoft.repo
    - RUN yum install -y powershell
    - RUN pip install ansible-builder

```

Base Image

System – OS Level

Python Package Req’s

Additional Steps

Execution Environment Base Image Options

awx-ee - the default

quay.io/ansible/awx-ee

ee-minimal-rhel8

registry.redhat.io/ansible-automation-platform/ee-minimal-rhel8

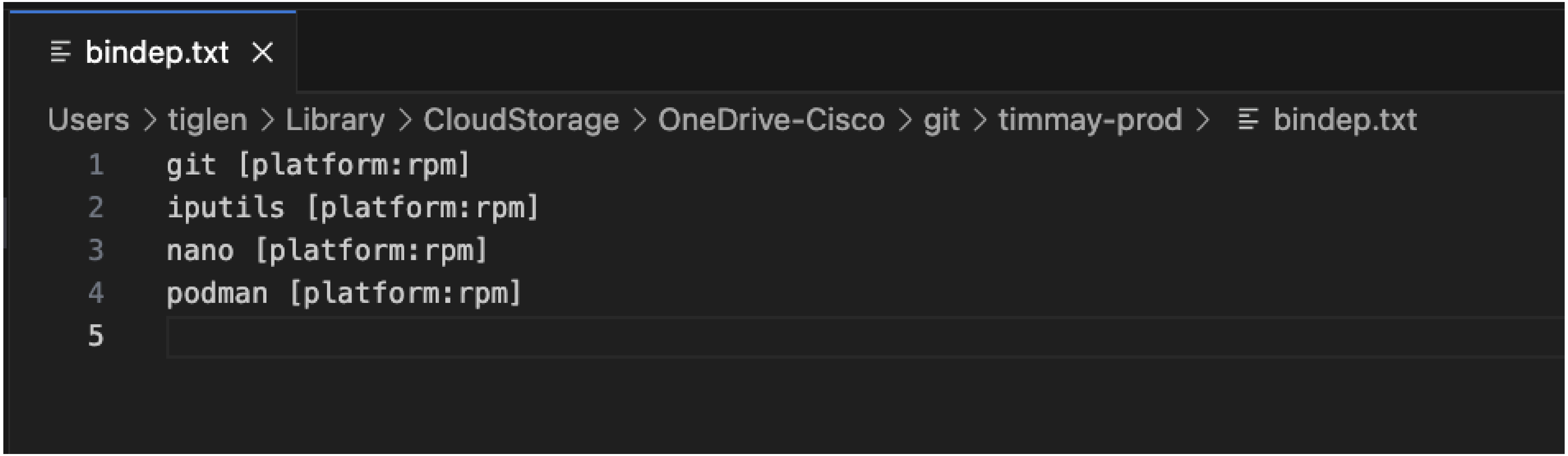
CentOS stream

quay.io/centos/centos:stream9

- Others too!
- Why ???
- Rebuilding using awx-ee takes > 20 minutes
- Rebuilding & Launching can be faster with lighter

bindep.txt

- OS Level Requirements

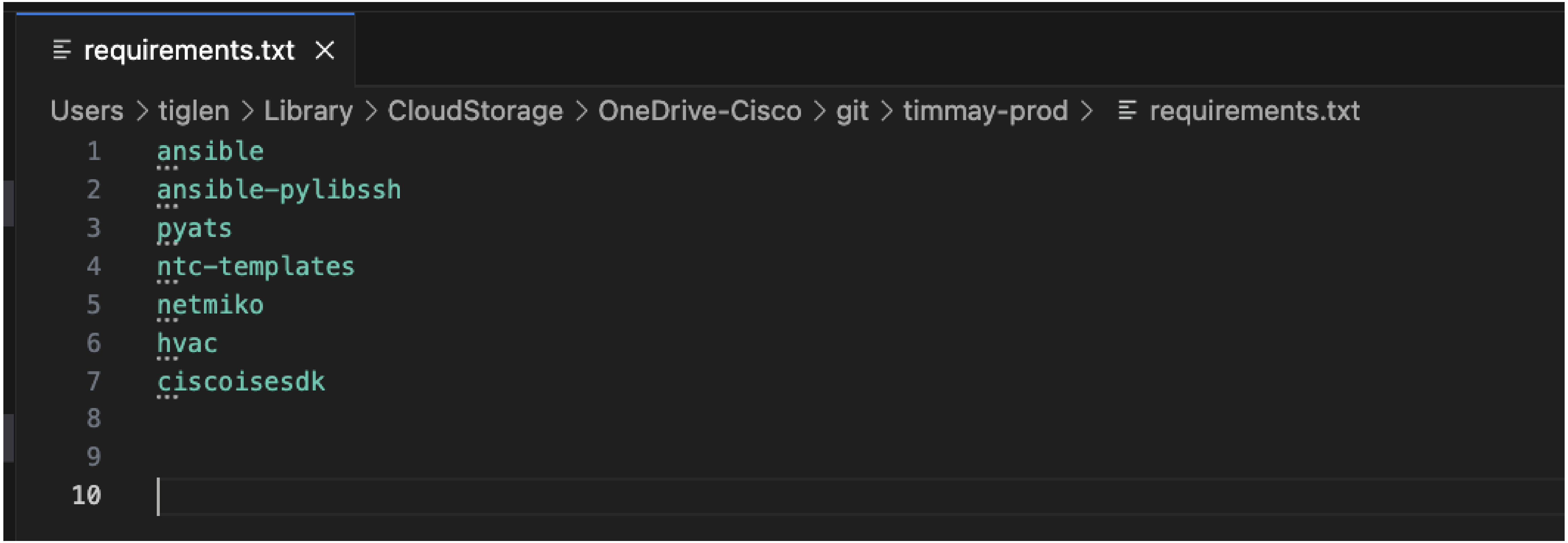


bindep.txt ×
Users > tiglen > Library > CloudStorage > OneDrive-Cisco > git > timmay-prod > bindep.txt

```
git [platform:rpm]
iputils [platform:rpm]
nano [platform:rpm]
podman [platform:rpm]

```

requirements.txt

- Python Package requirements

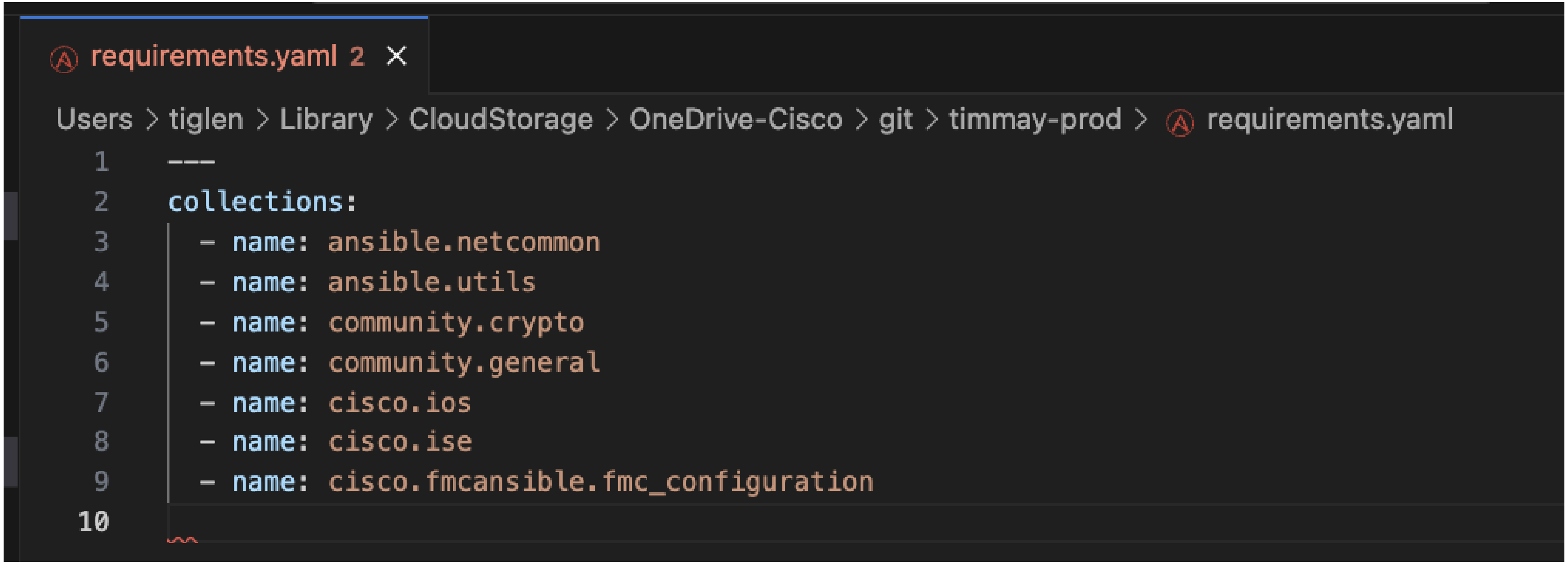


requirements.txt
Users > tiglen > Library > CloudStorage > OneDrive-Cisco > git > timmay-prod > requirements.txt

```
ansible
ansible-pylibssh
pyats
ntc-templates
netmiko
hvac
ciscoisesdk


```

requirements.yaml

- Ansible Galaxy Collections


requirements.yaml 2 ×
Users > tiglen > Library > CloudStorage > OneDrive-Cisco > git > timmay-prod > requirements.yaml

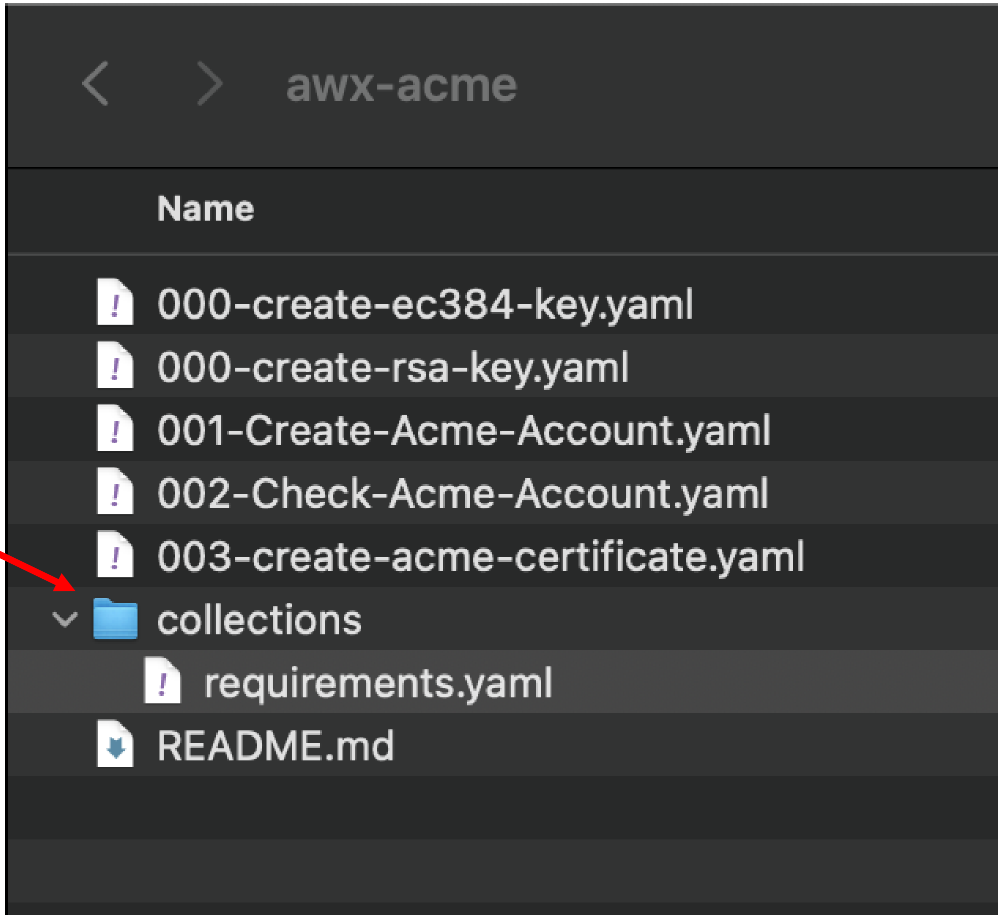
```yaml
---
collections:
  - name: ansible.netcommon
  - name: ansible.utils
  - name: community.crypto
  - name: community.general
  - name: cisco.ios
  - name: cisco.ise
  - name: cisco.fmcansible.fmc_configuration

```

Collections in EE vs Collections in Projects

- Collections in EE are present for any \ all playbooks that are run
- This is speedy

or

- Collections are specified in collections/requirements.yaml
  - This is specified in the Project
  - Every time you Sync an AWX Project the Galaxy Collections need to be downloaded
  - This slows syncing down

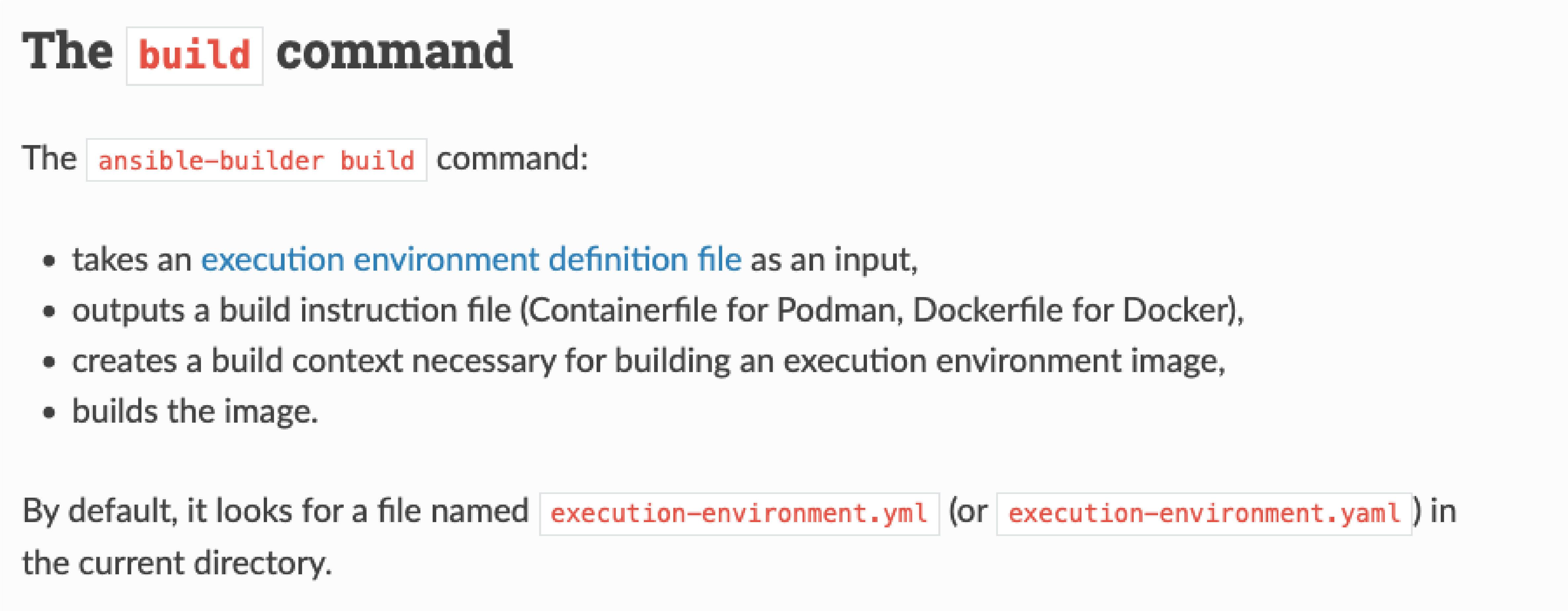


awx-acme

Name

- 000-create-ec384-key.yaml
- 000-create-rsa-key.yaml
- 001-Create-Acme-Account.yaml
- 002-Check-Acme-Account.yaml
- 003-create-acme-certificate.yaml
- collections
  - requirements.yaml
- README.md

Ansible Builder



The `build` command

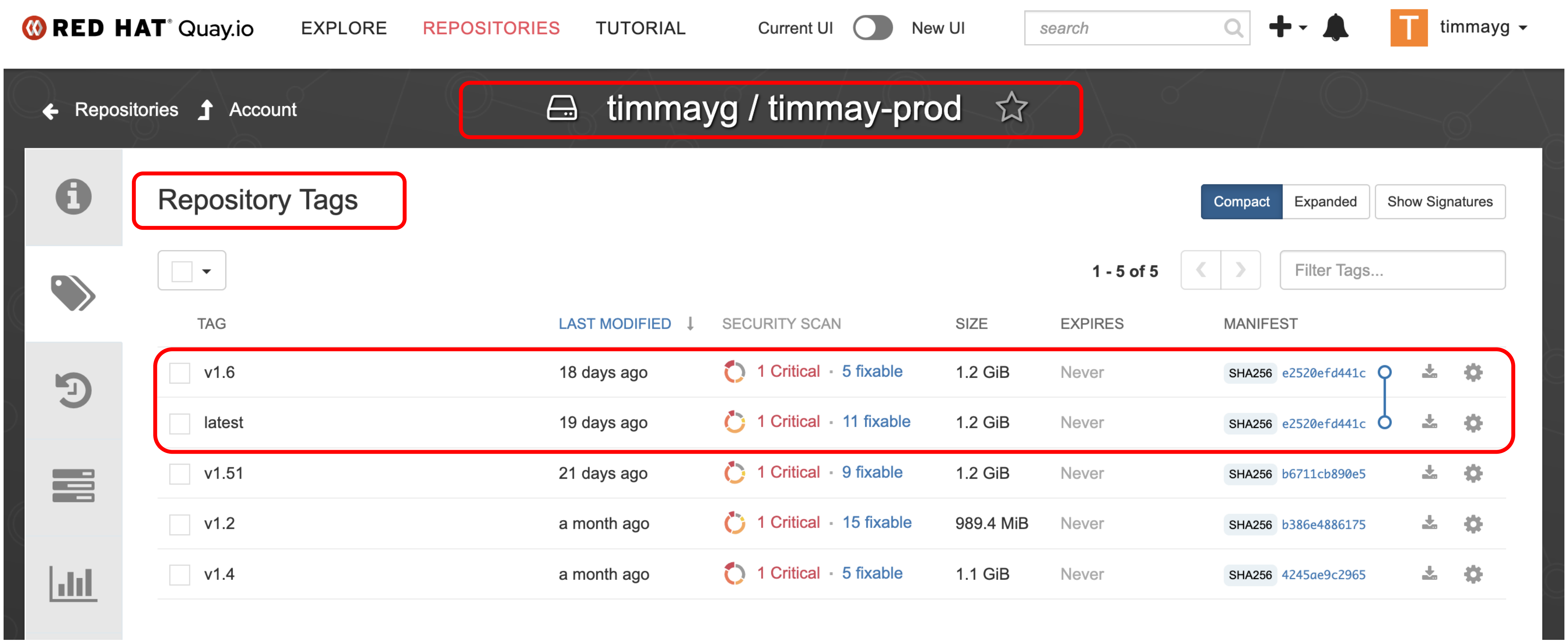
The `ansible-builder build` command:

- takes an execution environment definition file as an input,
- outputs a build instruction file (Containerfile for Podman, Dockerfile for Docker),
- creates a build context necessary for building an execution environment image,
- builds the image.

By default, it looks for a file named `execution-environment.yml` (or `execution-environment.yaml`) in the current directory.

https://ansible.readthedocs.io/projects/builder/en/latest/

Upload your EE to a Container Registry



timmayg / timmay-prod

Repository Tags

TAG	LAST MODIFIED	SECURITY SCAN	SIZE	EXPIRES	MANIFEST
v1.6	18 days ago	1 Critical · 5 fixable	1.2 GiB	Never	SHA256 e2520efd441c
latest	19 days ago	1 Critical · 11 fixable	1.2 GiB	Never	SHA256 e2520efd441c
v1.51	21 days ago	1 Critical · 9 fixable	1.2 GiB	Never	SHA256 b6711cb890e5
v1.2	a month ago	1 Critical · 15 fixable	989.4 MiB	Never	SHA256 b386e4886175
v1.4	a month ago	1 Critical · 5 fixable	1.1 GiB	Never	SHA256 4245ae9c2965

AWX Custom Credentials
&
External Secret Management
&
Hashi Corp Vault

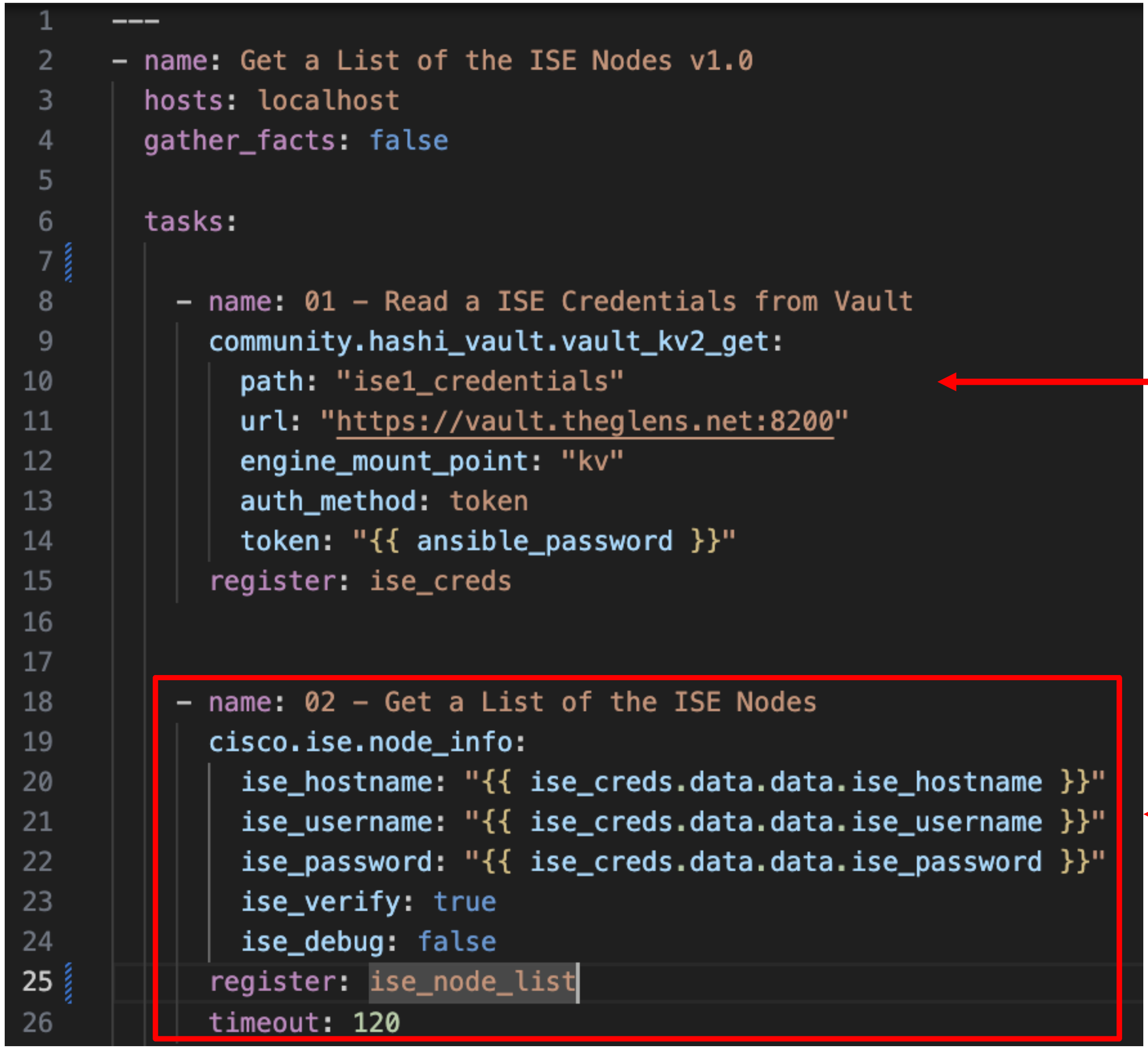
Secrets Managers

- AWX = Excellent Task Engine
- HashiCorp Vault = Excellent Secrets Management
- AWS Secrets Manager = Excellent Secrets Management
- Azure Key Vault = Excellent Secrets Management

Challenges with AWX built-in Credentials

- Machine Cred Challenges
- Familiarity but limited options

Lessons Learned
Limitation of Built-in Credentials



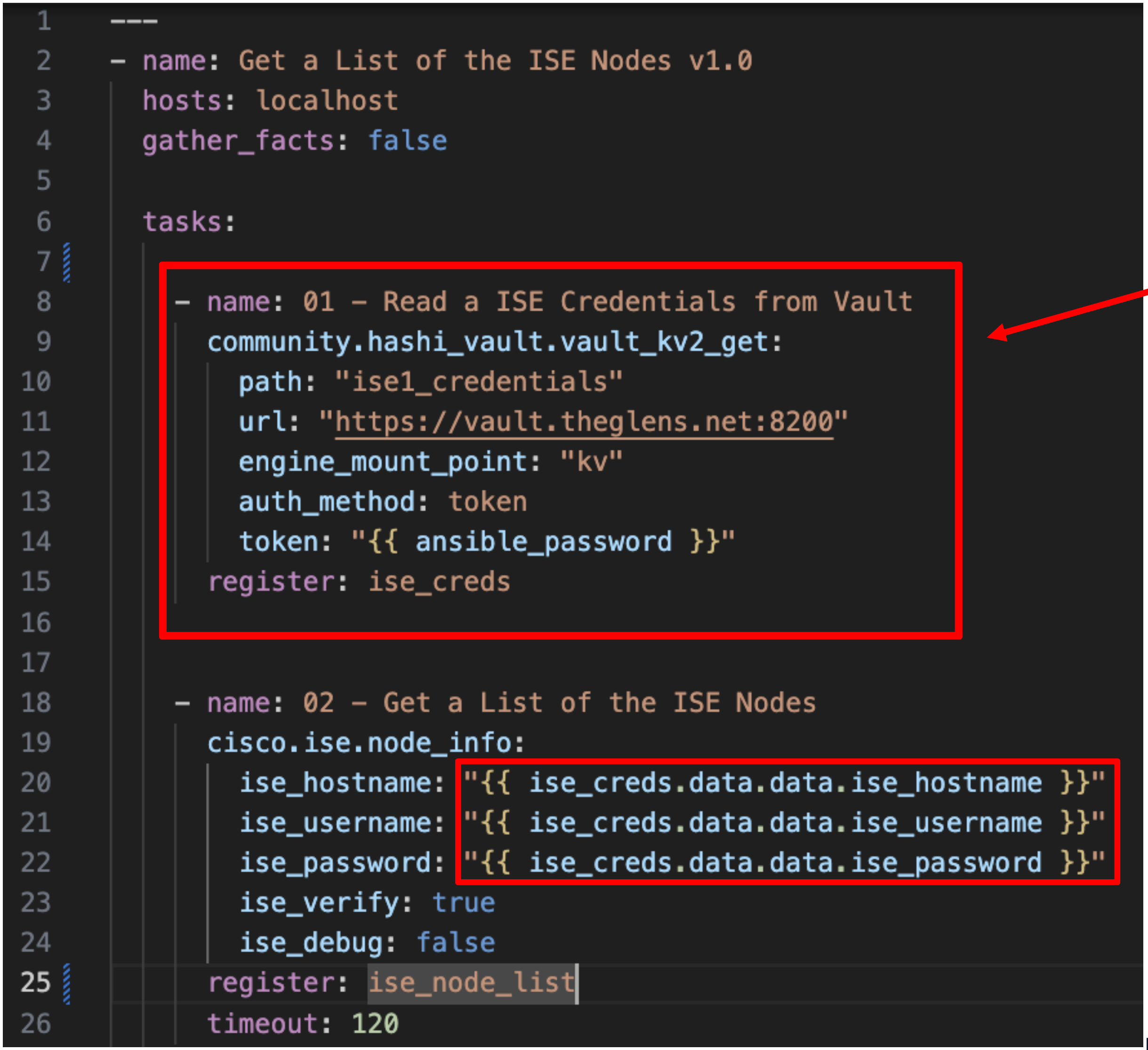
```yaml
---
- name: Get a List of the ISE Nodes v1.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Read a ISE Credentials from Vault
      community.hashi_vault.vault_kv2_get:
        path: "ise1_credentials"
        url: "https://vault.theglens.net:8200"
        engine_mount_point: "kv"
        auth_method: token
        token: "{{ ansible_password }}"
      register: ise_creds


    - name: 02 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_creds.data.data.ise_hostname }}"
        ise_username: "{{ ise_creds.data.data.ise_username }}"
        ise_password: "{{ ise_creds.data.data.ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 120
```

We need to run ansible playbooks to perform ISE Tasks.

Retrieve ISE User, Pass & hostname from Vault

Each ISE task requires authentication

Lessons Learned
Limitation of Built-in Credentials



```yaml
---
- name: Get a List of the ISE Nodes v1.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Read a ISE Credentials from Vault
      community.hashi_vault.vault_kv2_get:
        path: "ise1_credentials"
        url: "https://vault.theglens.net:8200"
        engine_mount_point: "kv"
        auth_method: token
        token: "{{ ansible_password }}"
      register: ise_creds


    - name: 02 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_creds.data.data.ise_hostname }}"
        ise_username: "{{ ise_creds.data.data.ise_username }}"
        ise_password: "{{ ise_creds.data.data.ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 120
```

This task only runs to query \ obtain a cred from Vault.

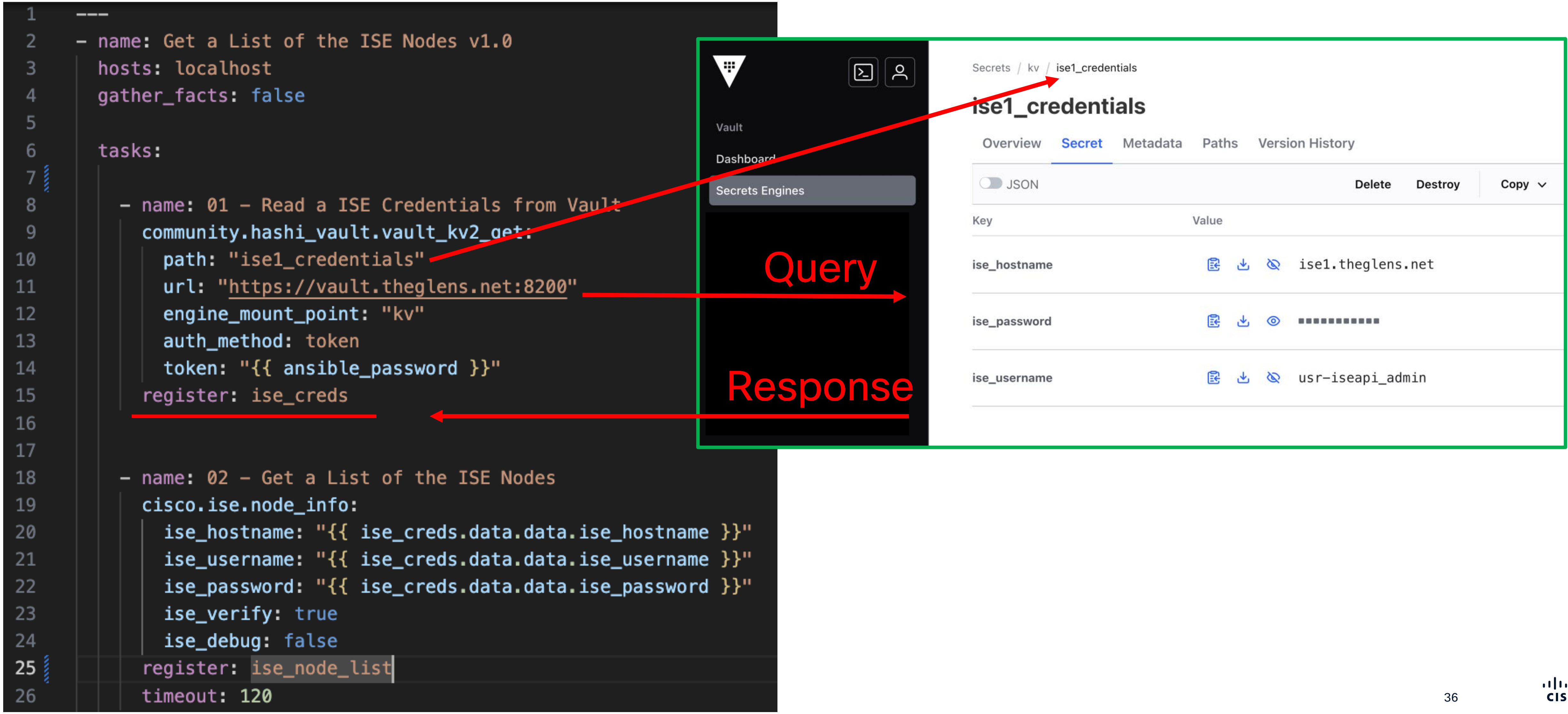
Not very efficient.

What if we need multiple creds?

Copy \ paste this code into **how many** playbooks ?

How readable is this for the next person?

Lessons Learned
Limitation of Built-in Credentials

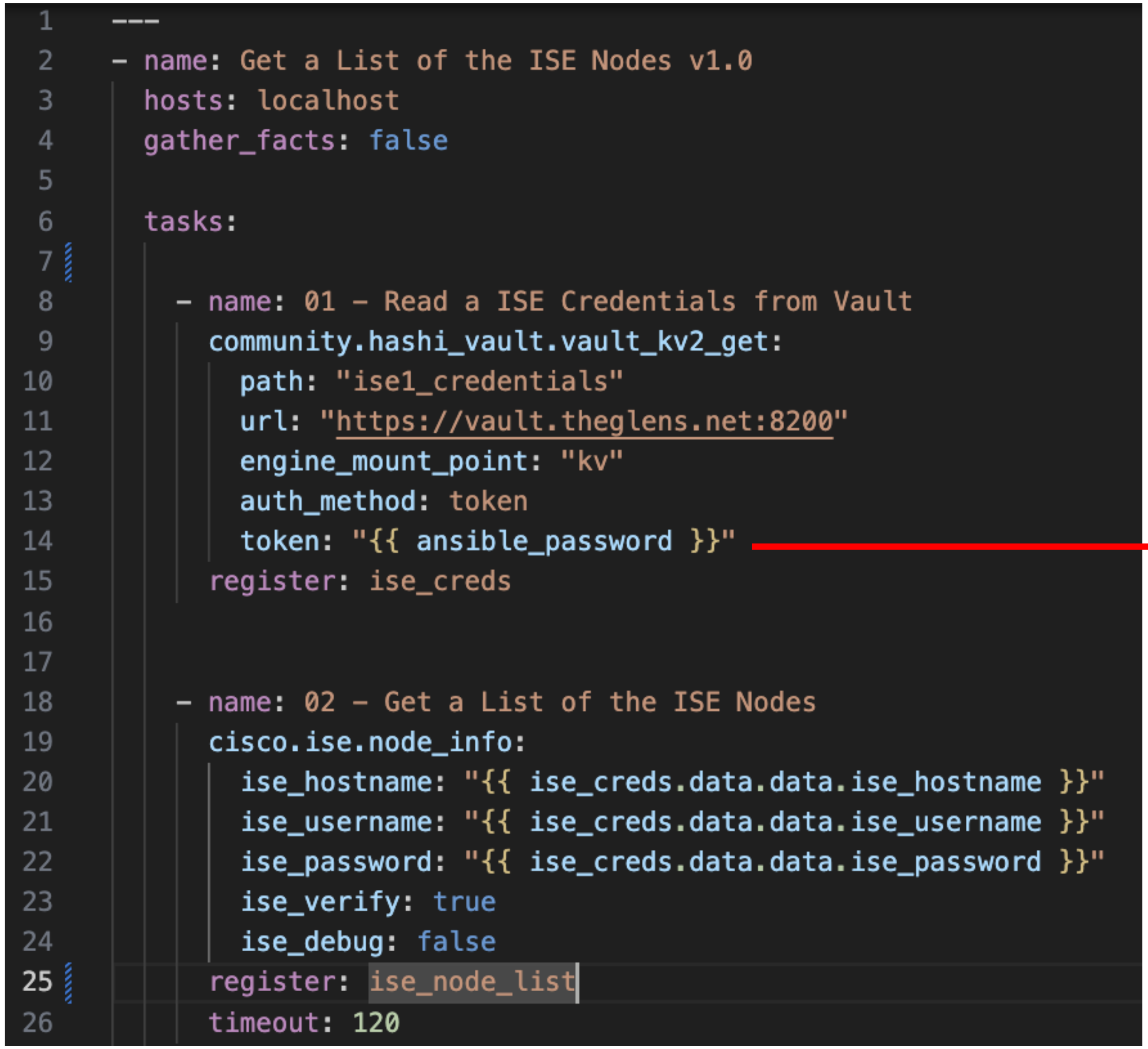


```
---
- name: Get a List of the ISE Nodes v1.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Read a ISE Credentials from Vault
      community.hashi_vault.vault_kv2_get:
        path: "ise1_credentials"
        url: "https://vault.theglens.net:8200"
        engine_mount_point: "kv"
        auth_method: token
        token: "{{ ansible_password }}"
      register: ise_creds


    - name: 02 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_creds.data.data.ise_hostname }}"
        ise_username: "{{ ise_creds.data.data.ise_username }}"
        ise_password: "{{ ise_creds.data.data.ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 120
```

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	•••••••••••
ise_username	usr-iseapi_admin

Lessons Learned
Limitation of Built-in Credentials



```yaml
---
- name: Get a List of the ISE Nodes v1.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Read a ISE Credentials from Vault
      community.hashi_vault.vault_kv2_get:
        path: "ise1_credentials"
        url: "https://vault.theglens.net:8200"
        engine_mount_point: "kv"
        auth_method: token
        token: "{{ ansible_password }}"
      register: ise_creds


    - name: 02 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_creds.data.data.ise_hostname }}"
        ise_username: "{{ ise_creds.data.data.ise_username }}"
        ise_password: "{{ ise_creds.data.data.ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 120
```

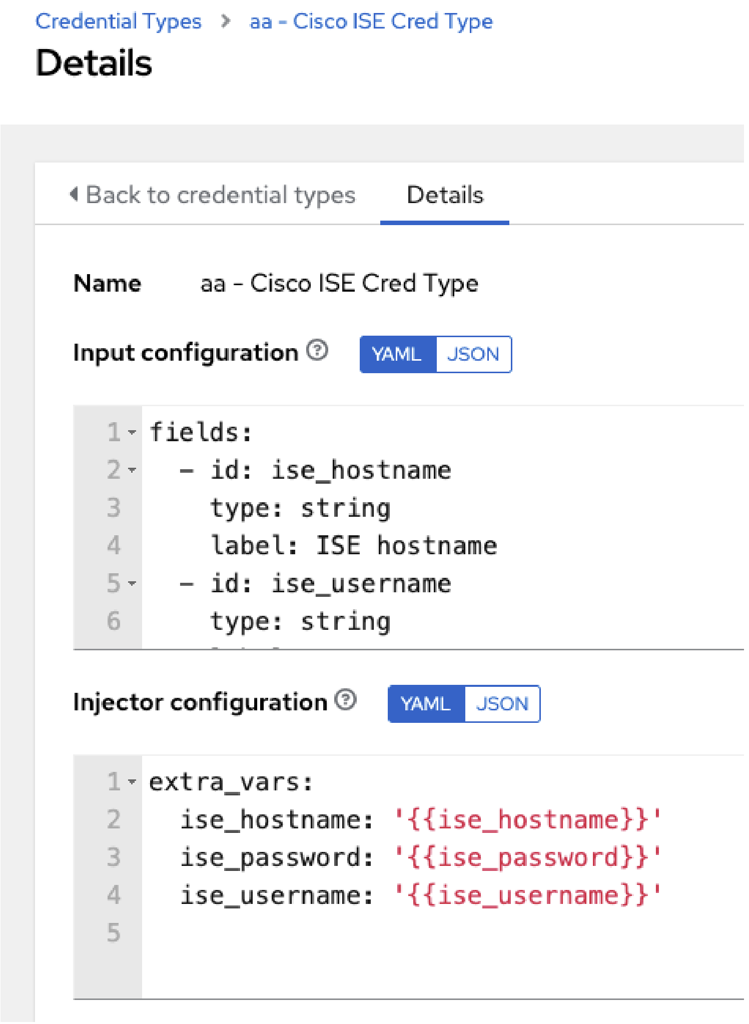
Limitation
AWX Machine Credential
ansible_password

- Reserved variable name
- Limited usage
- Not designed to be used this way
- Doesn’t feel good, it’s a hack

Why did I do it this way?

- Familiar with ‘machine credential’ / SSH cred in Ansible
  - ansible_username / ansible_passord
- Knew that AWX would encrypt ansible_password
- Comfortable storing api_key, tokens, in ansible_password
- Knew it was a hack but it worked, till it didn’t

Welcome, Custom Credential Type



Credential Types > aa - Cisco ISE Cred Type

Details

◂ Back to credential types | Details

Name aa - Cisco ISE Cred Type

Input configuration ⓘ YAML JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration ⓘ YAML JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

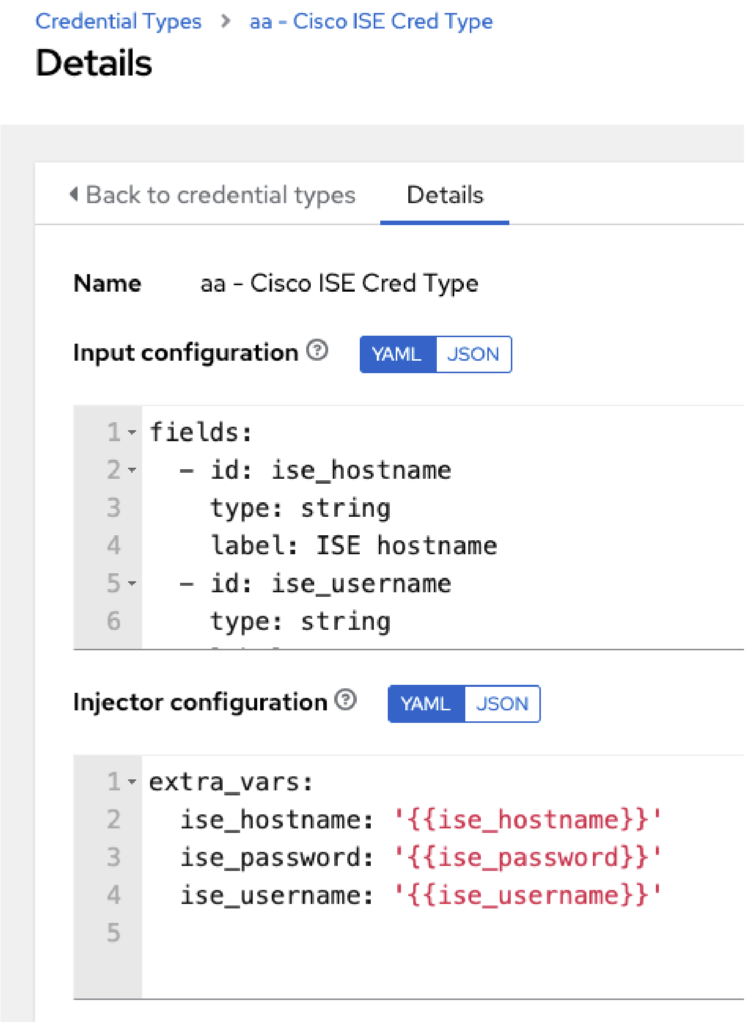
Injector configuration

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Welcome, Custom Credential Type

AWX ♥ HashiCorp Vault



Credential Types › aa - Cisco ISE Cred Type

Details

◂ Back to credential types | Details

Name: aa - Cisco ISE Cred Type

Input configuration: YAML | JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration: YAML | JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

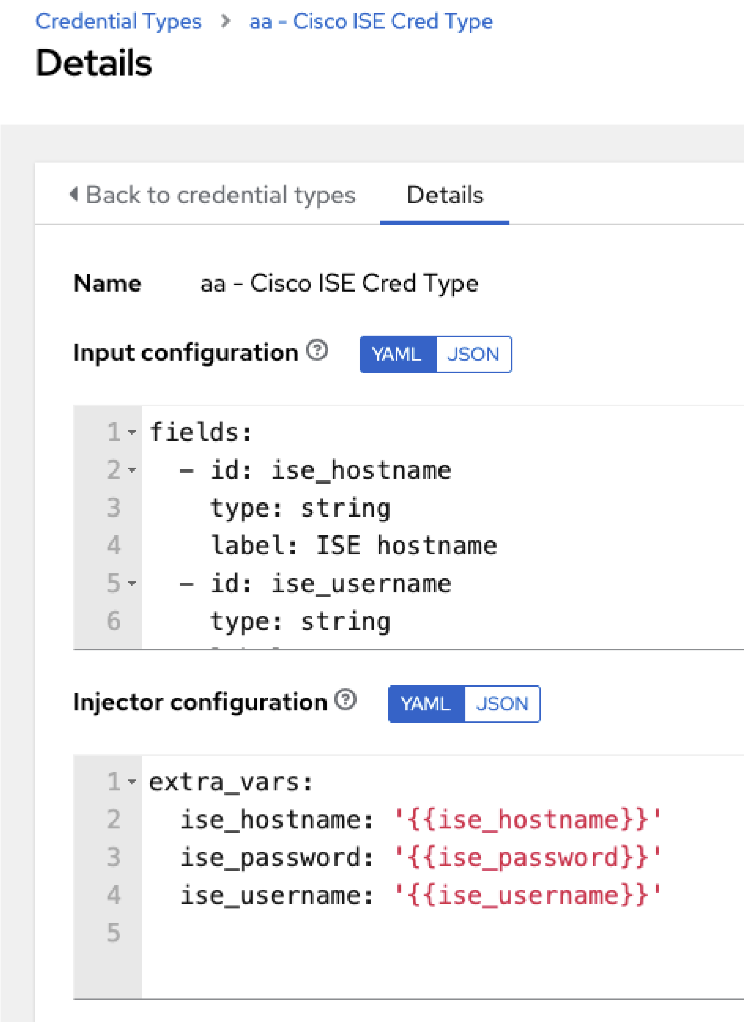
Injector configuration

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Welcome, Custom Credential Type

AWX ♥ HashiCorp Vault



Credential Types › aa - Cisco ISE Cred Type

Details

Back to credential types | Details

Name: aa - Cisco ISE Cred Type

Input configuration: YAML | JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration: YAML | JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

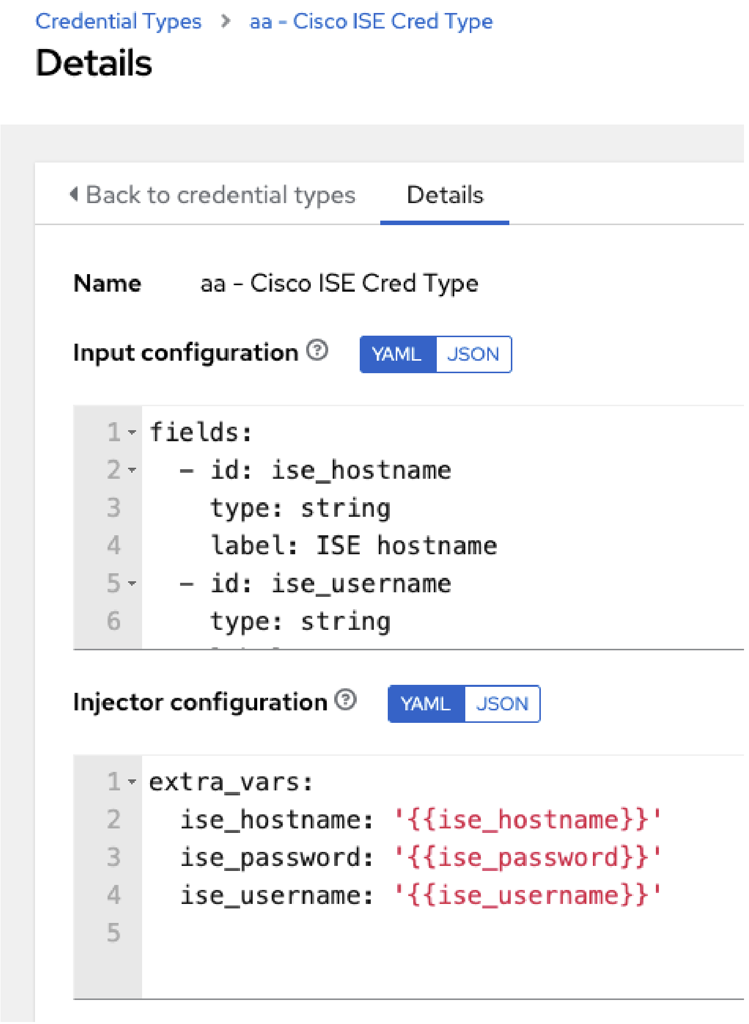
```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

Injector configuration

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Welcome, Custom Credential Type



Credential Types › aa - Cisco ISE Cred Type

Details

◂ Back to credential types | Details

Name aa - Cisco ISE Cred Type

Input configuration ⓘ YAML JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration ⓘ YAML JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

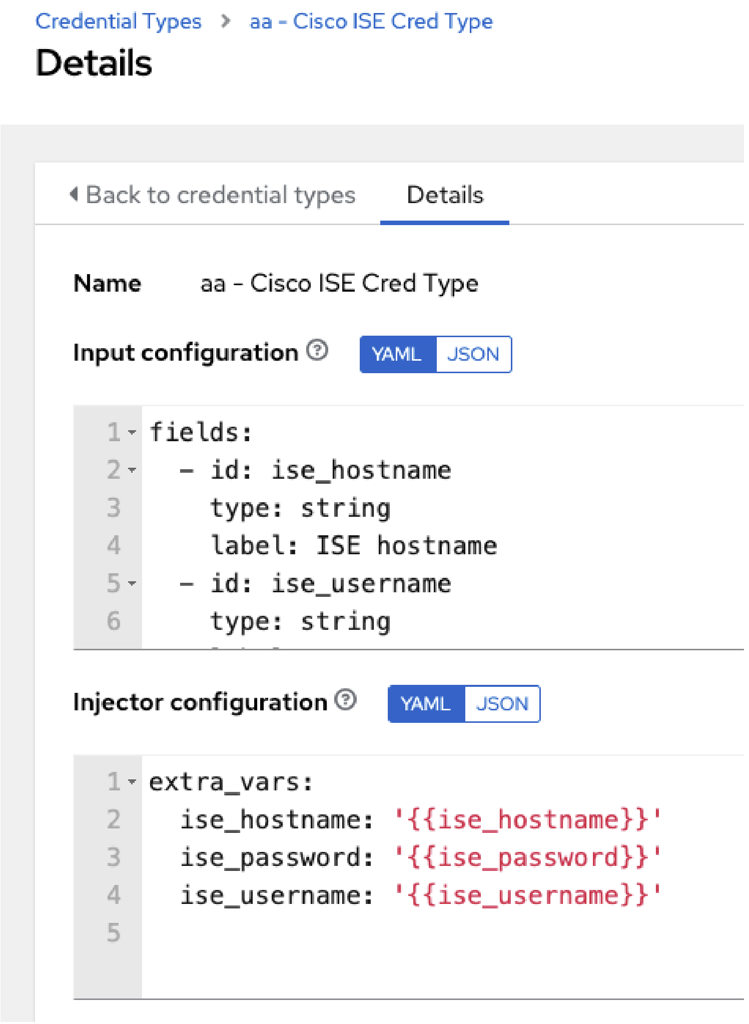
```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

Injector configuration

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Welcome, Custom Credential Type



Credential Types › aa - Cisco ISE Cred Type

Details

Name aa - Cisco ISE Cred Type

Input configuration ⓘ YAML JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration ⓘ YAML JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

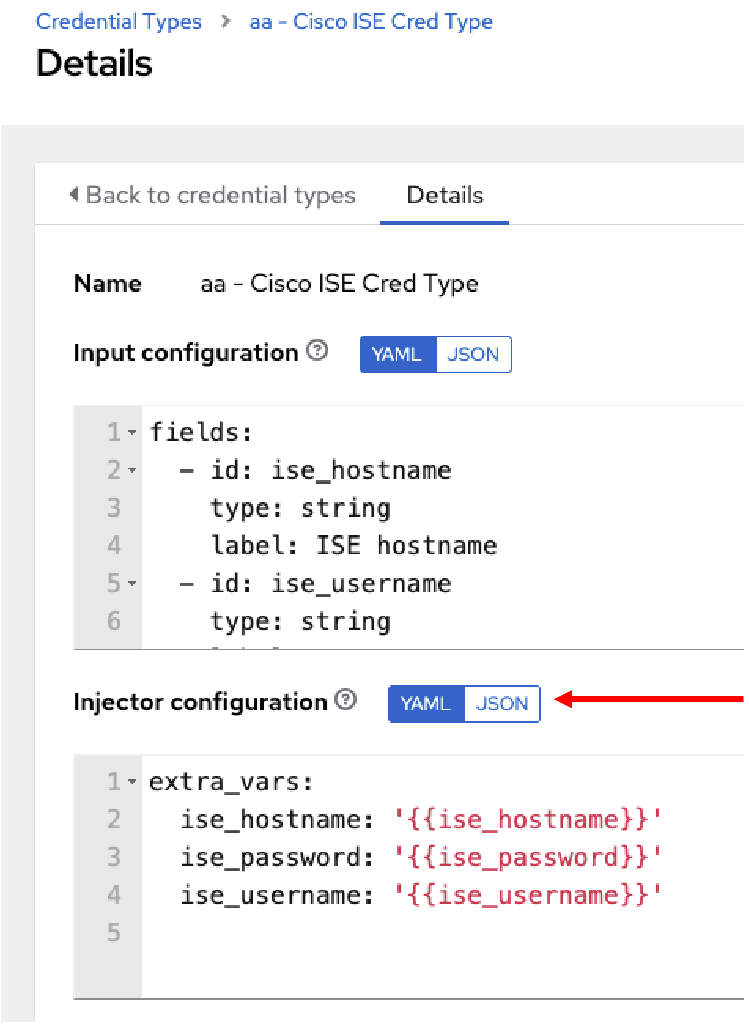
```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

Injector configuration

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Welcome, Custom Credential Type



Credential Types > aa - Cisco ISE Cred Type

Details

Name aa - Cisco ISE Cred Type

Input configuration ⓘ YAML JSON

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
```

Injector configuration ⓘ YAML JSON

```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

Input configuration

```
fields:
  - id: ise_hostname
    type: string
    label: ISE hostname
  - id: ise_username
    type: string
    label: Username
  - id: ise_password
    type: string
    label: Password
    secret: true
required:
  - ise_hostname
  - ise_username
  - ise_password
```

Injector configuration

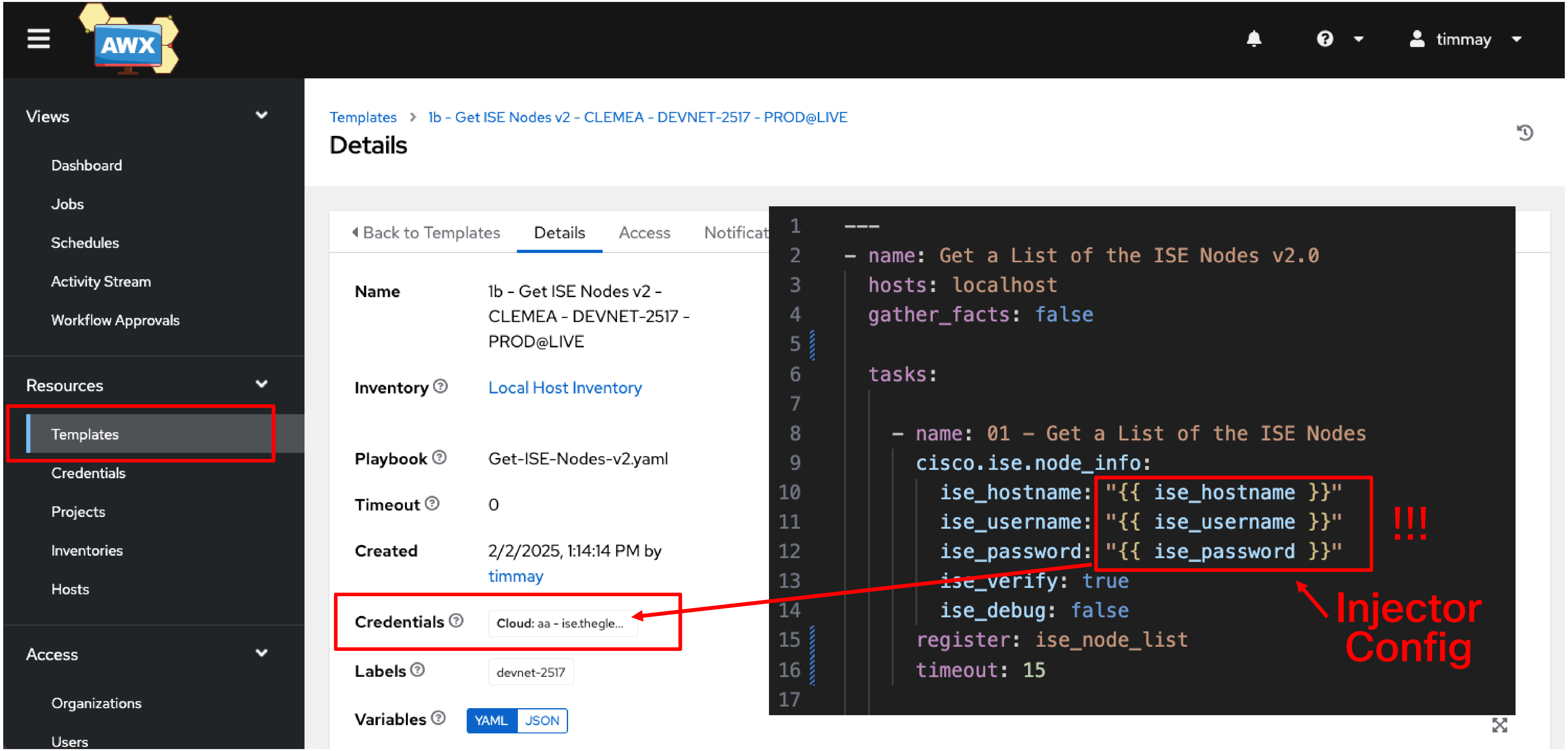
```
extra_vars:
  ise_hostname: '{{ise_hostname}}'
  ise_password: '{{ise_password}}'
  ise_username: '{{ise_username}}'
```

id

vars in playbook

https://docs.ansible.com/automation-controller/4.4/html/userguide/credential_types.html

Template to Playbook Cred Mapping



Templates > 1b - Get ISE Nodes v2 - CLEMEA - DEVNET-2517 - PROD@LIVE

Details

Name	1b - Get ISE Nodes v2 - CLEMEA - DEVNET-2517 - PROD@LIVE
Inventory	Local Host Inventory
Playbook	Get-ISE-Nodes-v2.yaml
Timeout	0
Created	2/2/2025, 1:14:14 PM by timmay
Credentials	Cloud: aa - ise.thegle...
Labels	devnet-2517
Variables	YAML JSON

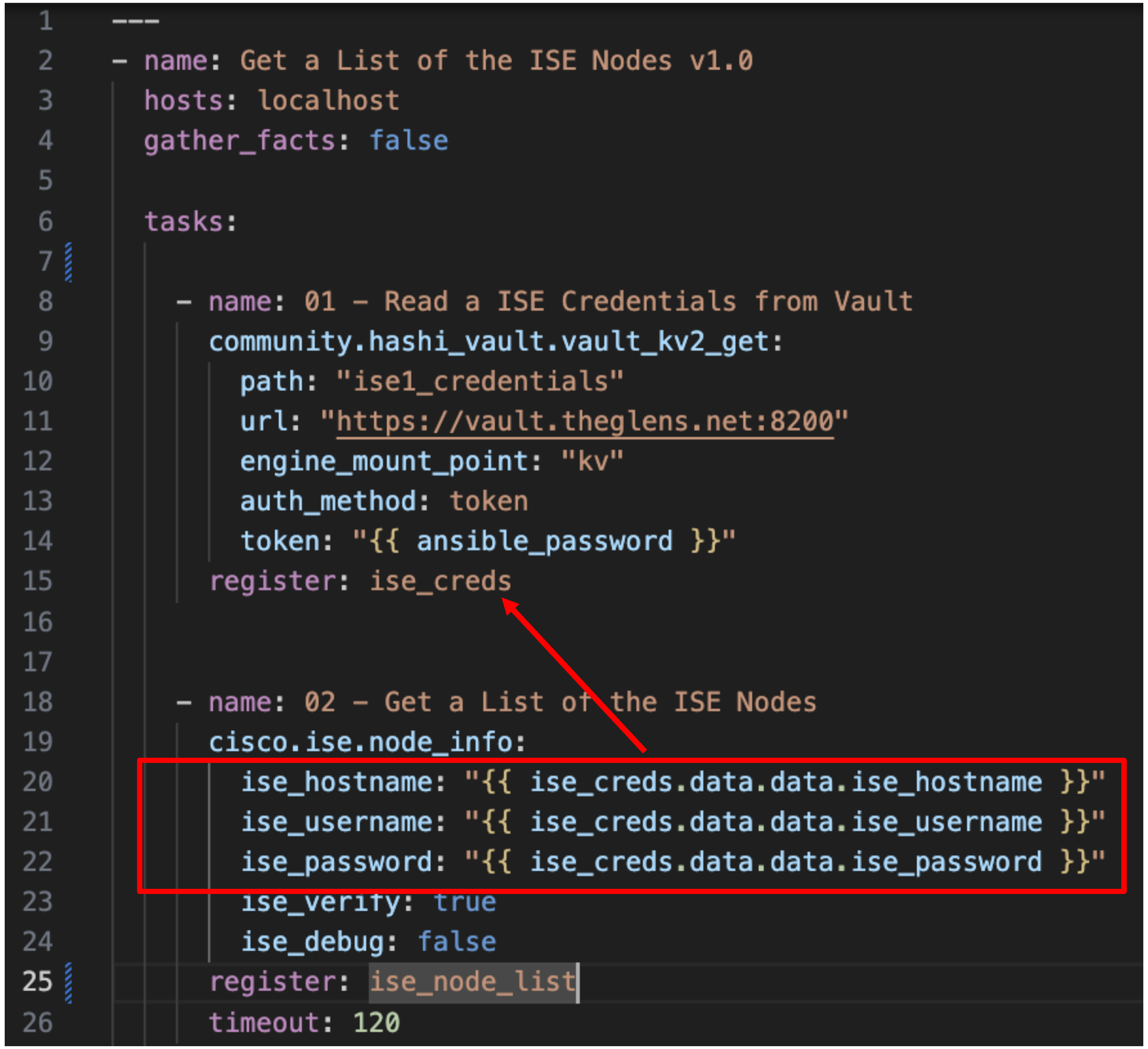
```yaml
---
- name: Get a List of the ISE Nodes v2.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_hostname }}"
        ise_username: "{{ ise_username }}"
        ise_password: "{{ ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 15

```

!!!

Injector Config

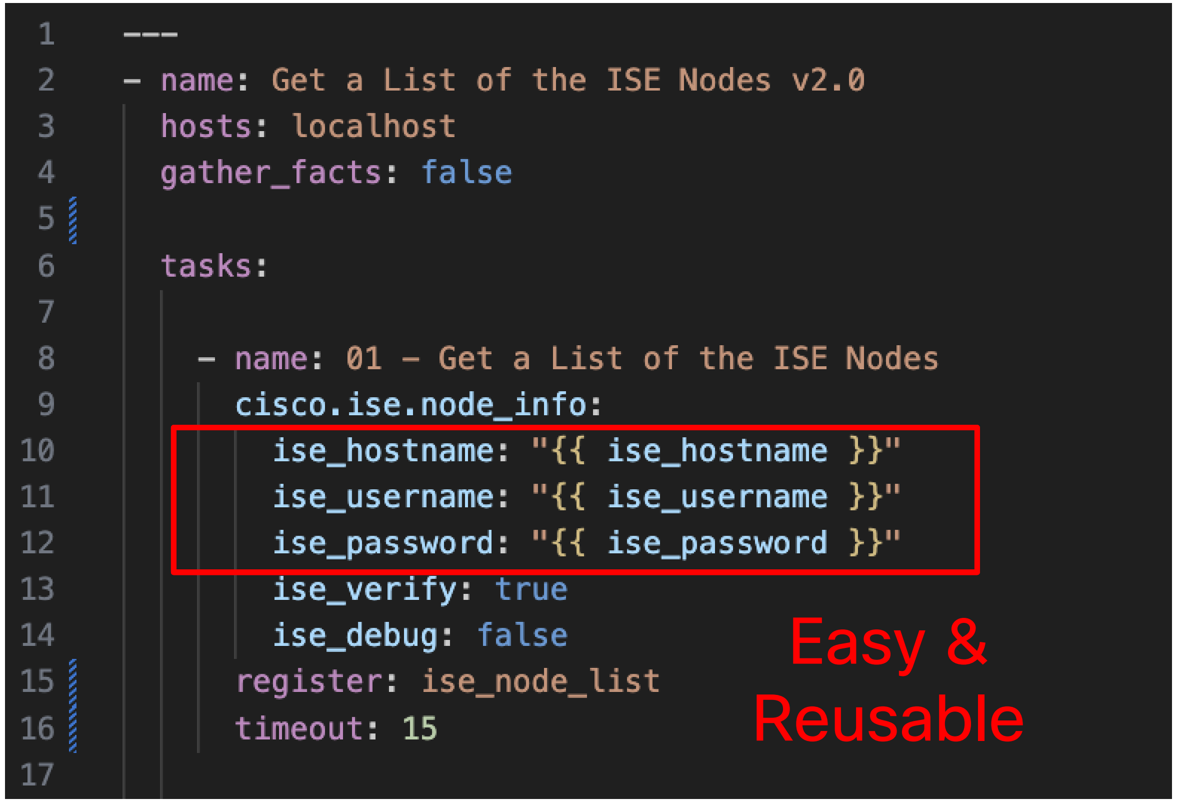
Old vs New Playbook

AWX ♥ HashiCorp Vault



```yaml
---
- name: Get a List of the ISE Nodes v1.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Read a ISE Credentials from Vault
      community.hashi_vault.vault_kv2_get:
        path: "ise1_credentials"
        url: "https://vault.theglens.net:8200"
        engine_mount_point: "kv"
        auth_method: token
        token: "{{ ansible_password }}"
      register: ise_creds


    - name: 02 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_creds.data.data.ise_hostname }}"
        ise_username: "{{ ise_creds.data.data.ise_username }}"
        ise_password: "{{ ise_creds.data.data.ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 120
```

Which credential should we use?



```yaml
---
- name: Get a List of the ISE Nodes v2.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_hostname }}"
        ise_username: "{{ ise_username }}"
        ise_password: "{{ ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 15

```

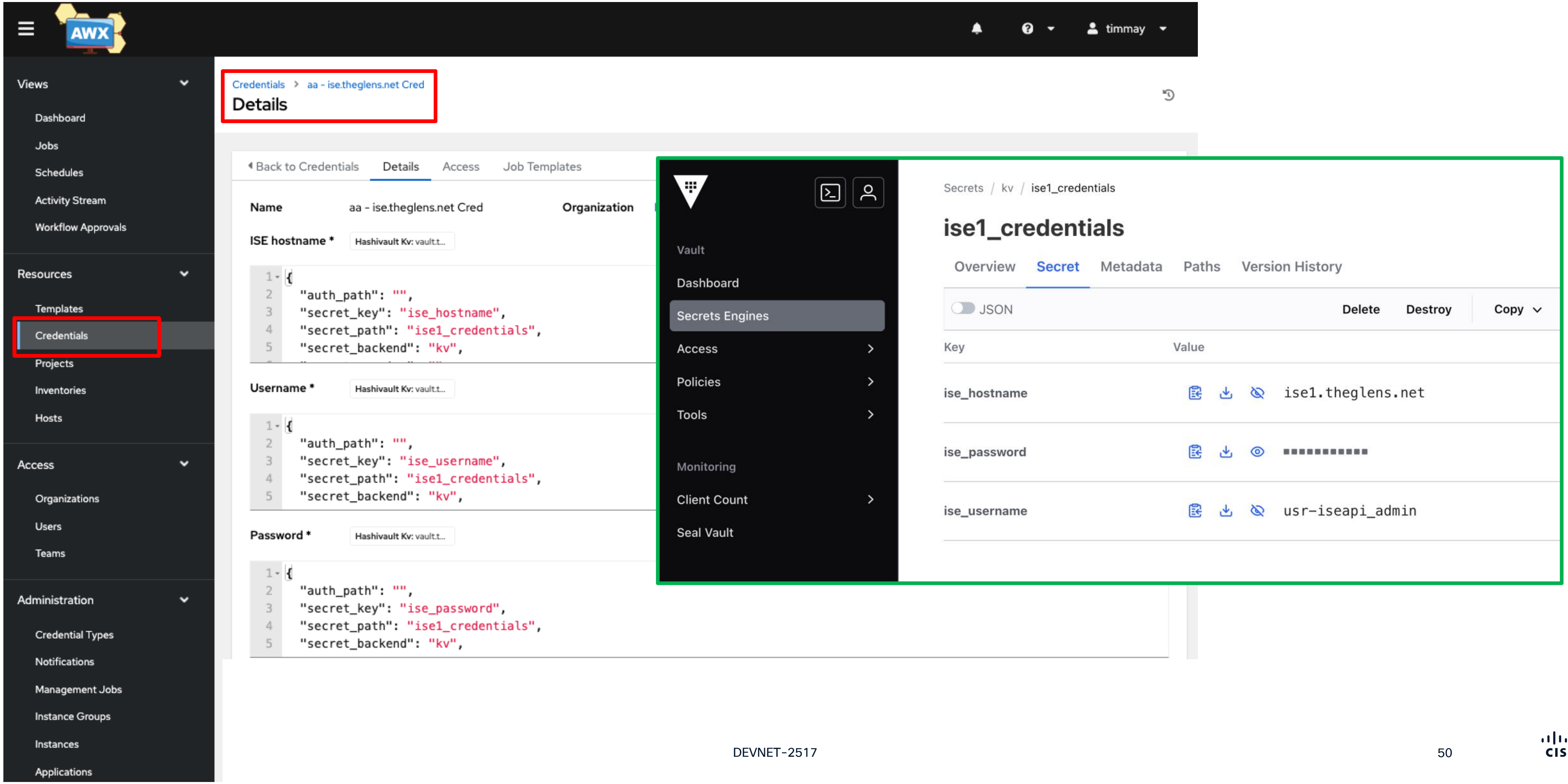
Easy & Reusable

DEMO – Build a Simple ISE Cred

- Show Existing Custom Credential Type – aa – Cisco ISE Cred Type

- Create new Credential
- Type aa– ISE
- Name

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

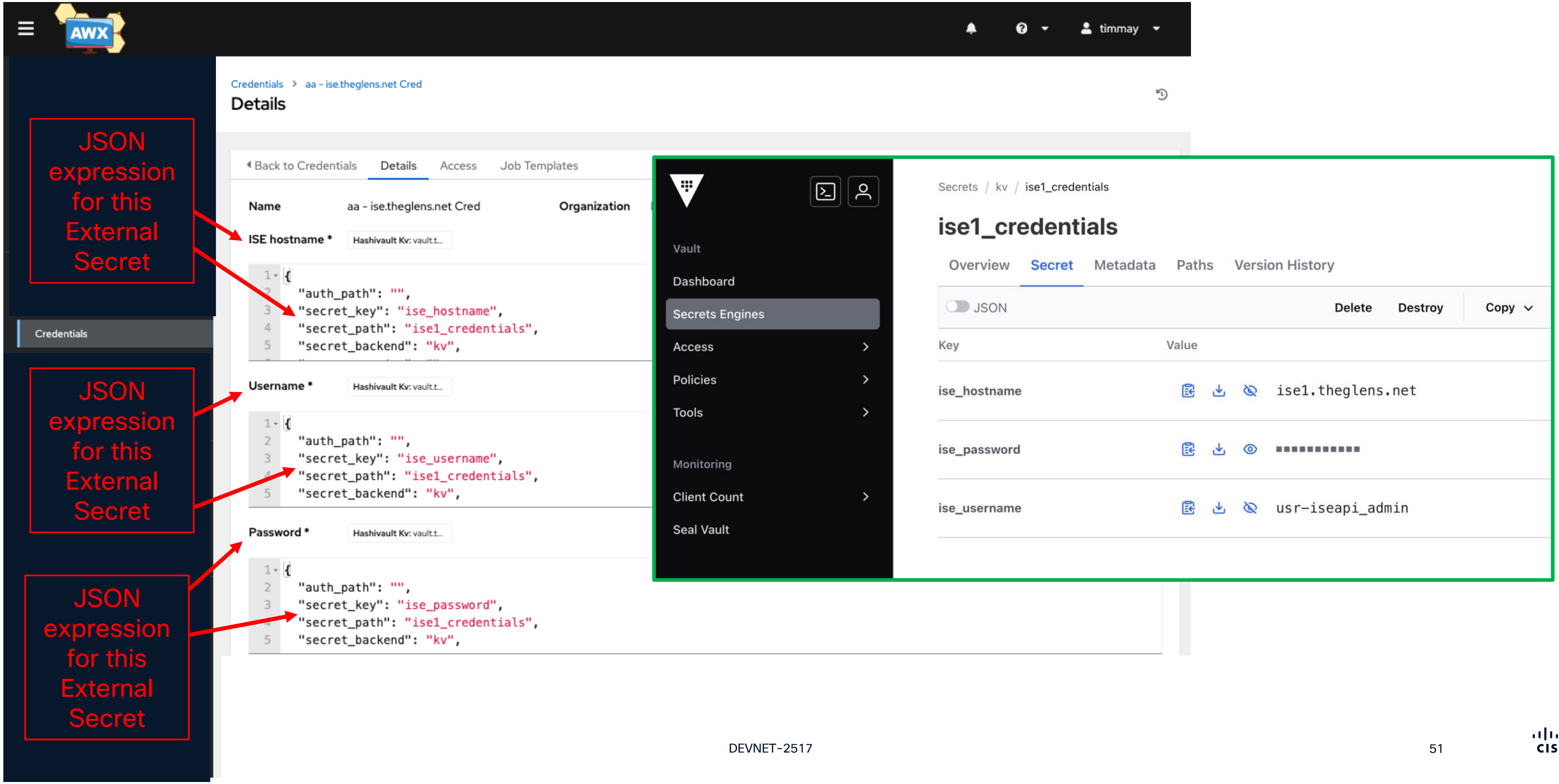
```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



JSON expression for this External Secret

JSON expression for this External Secret

JSON expression for this External Secret

Credentials > aa - ise.theglens.net Cred

Details

Back to Credentials | Details | Access | Job Templates

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

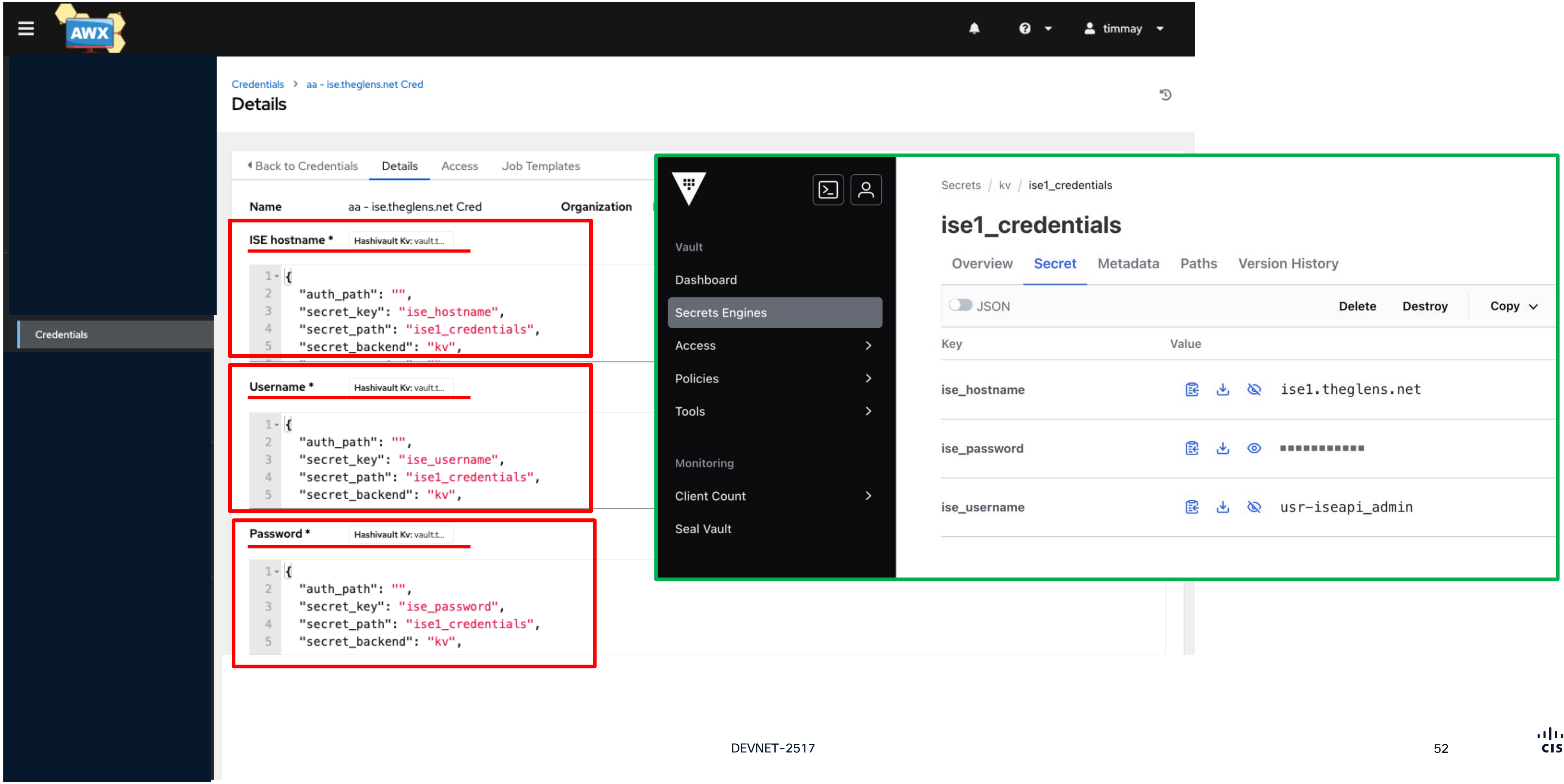
ise1_credentials

Overview | Secret | Metadata | Paths | Version History

JSON | Delete | Destroy | Copy

Key	Value
ise_hostname	ise1.theglens.net
ise_password	▪▪▪▪▪▪▪▪▪▪▪▪
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Name aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

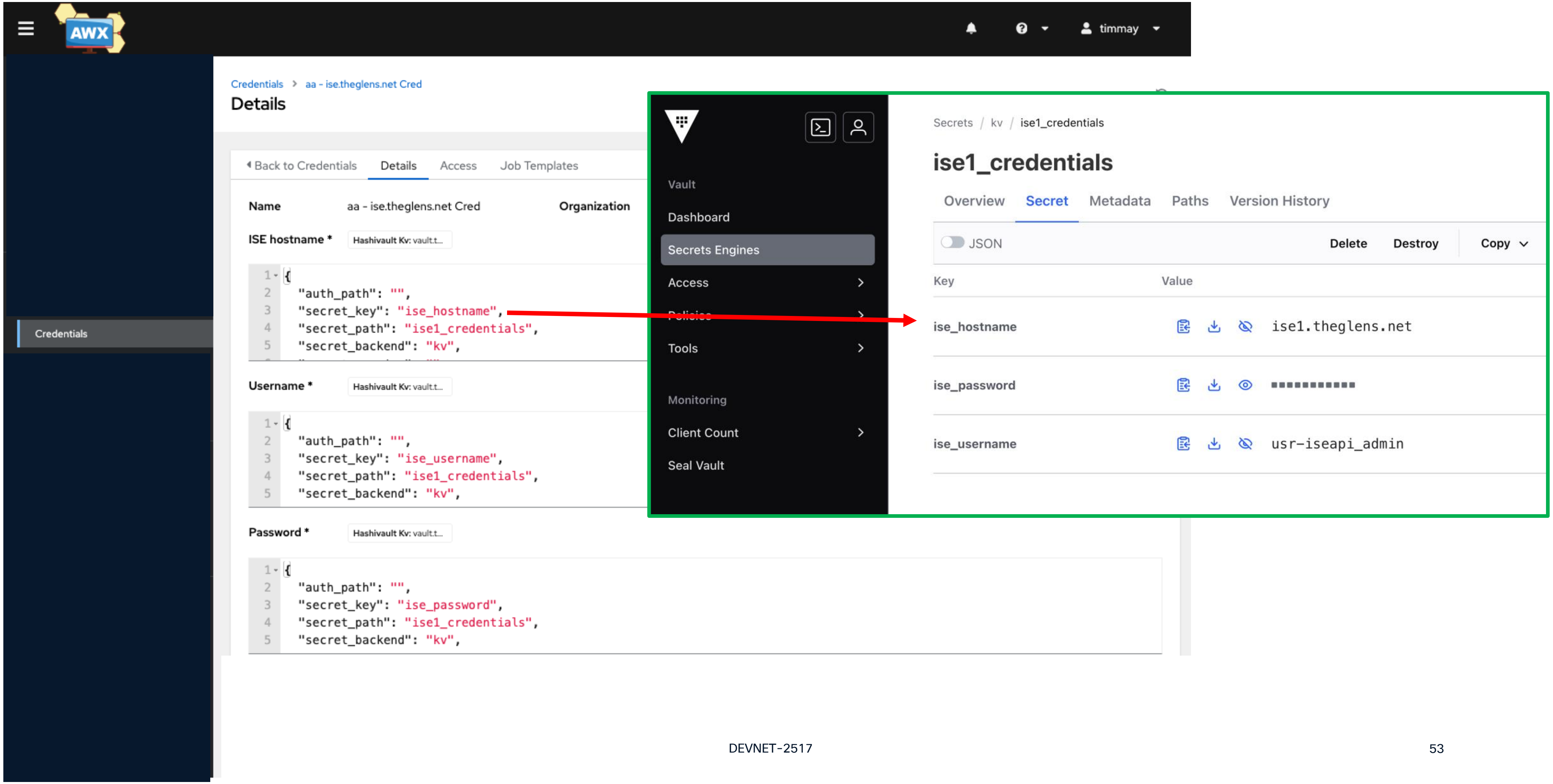
```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	●●●●●●●●●●●●
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Details

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

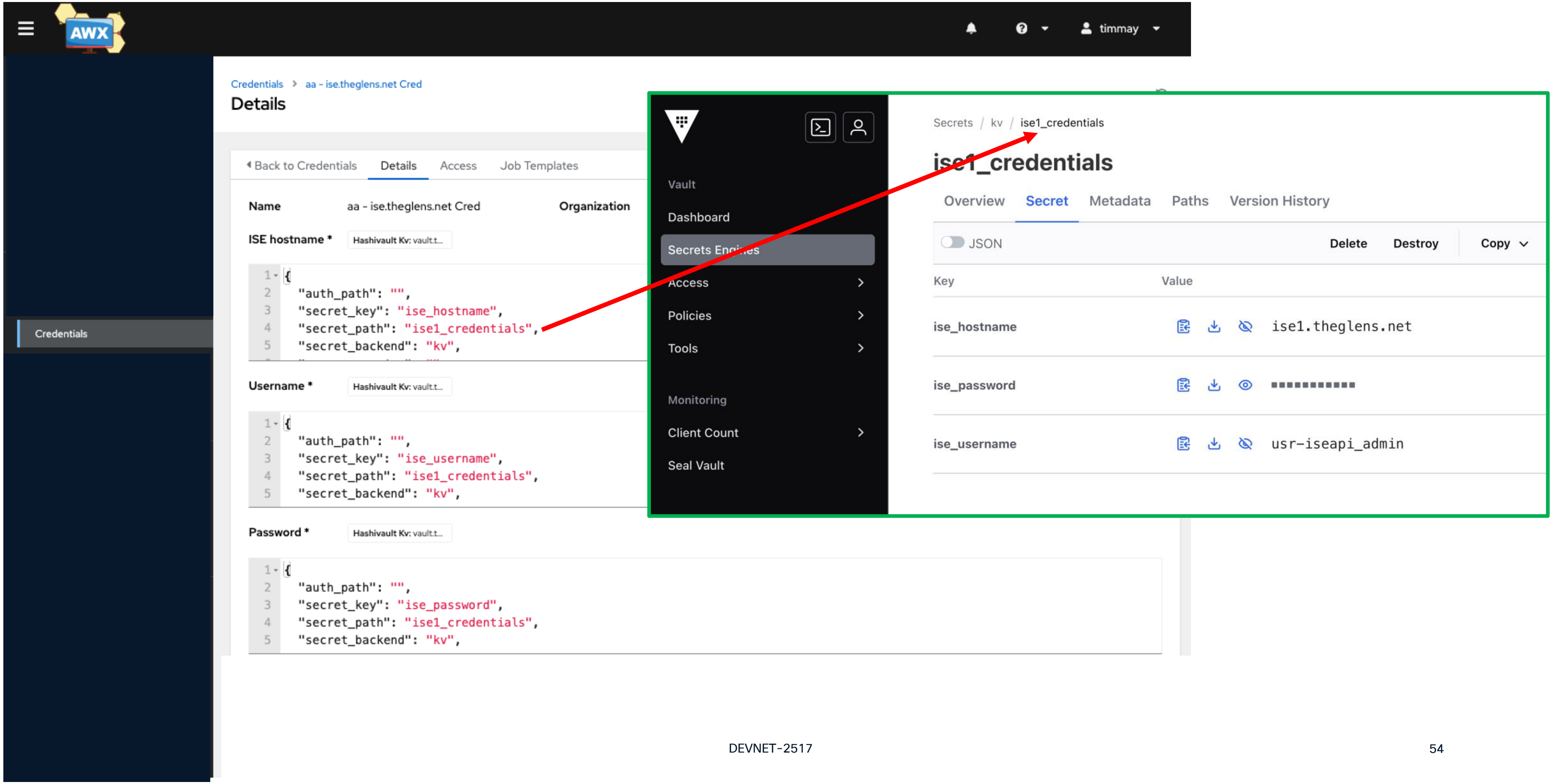
Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Name: aa - ise.theglens.net Cred

Organization

ISE hostname *: Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username *: Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password *: Hashivault Kv: vault.t...

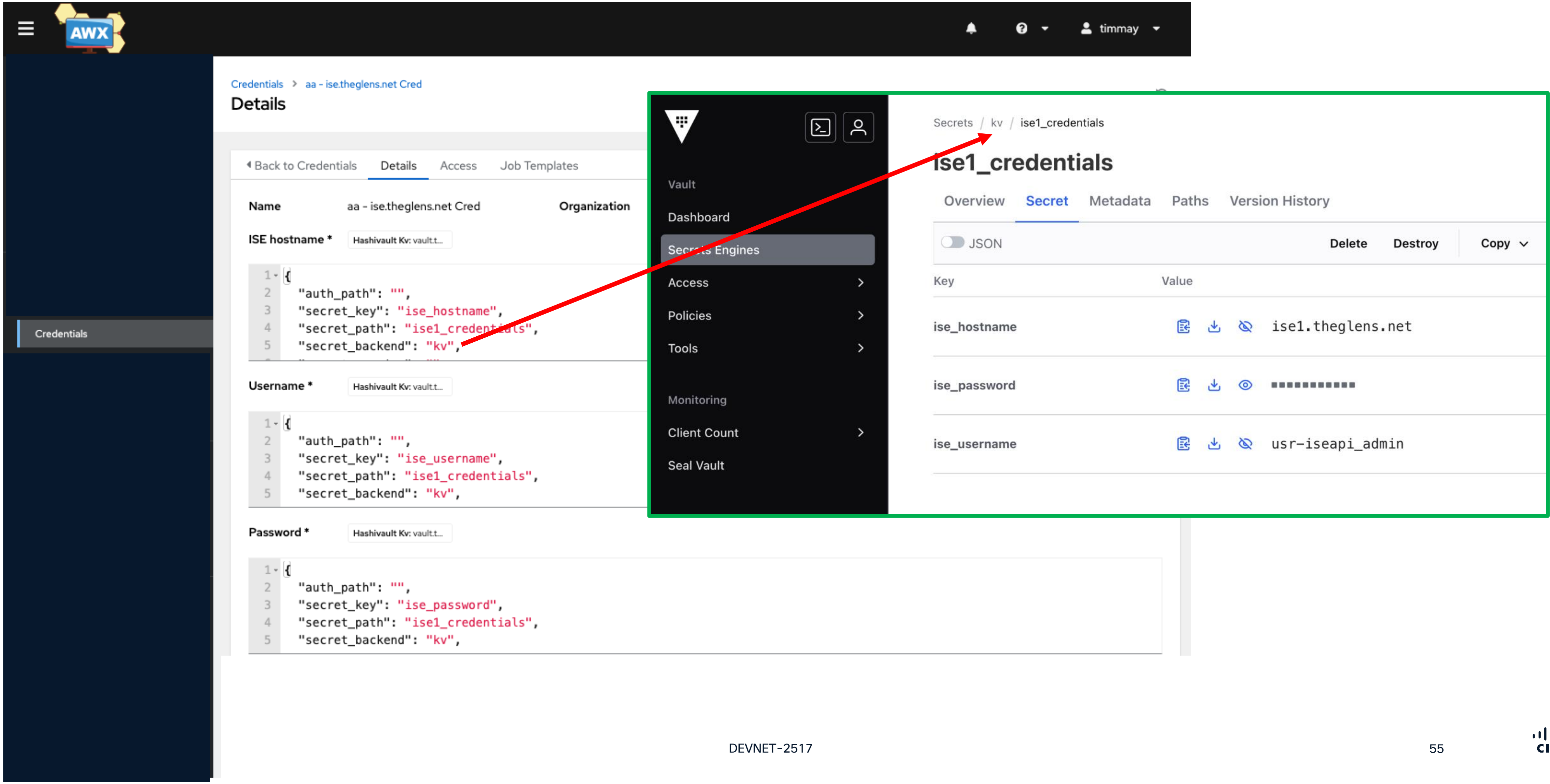
```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Name: aa - ise.theglens.net Cred

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

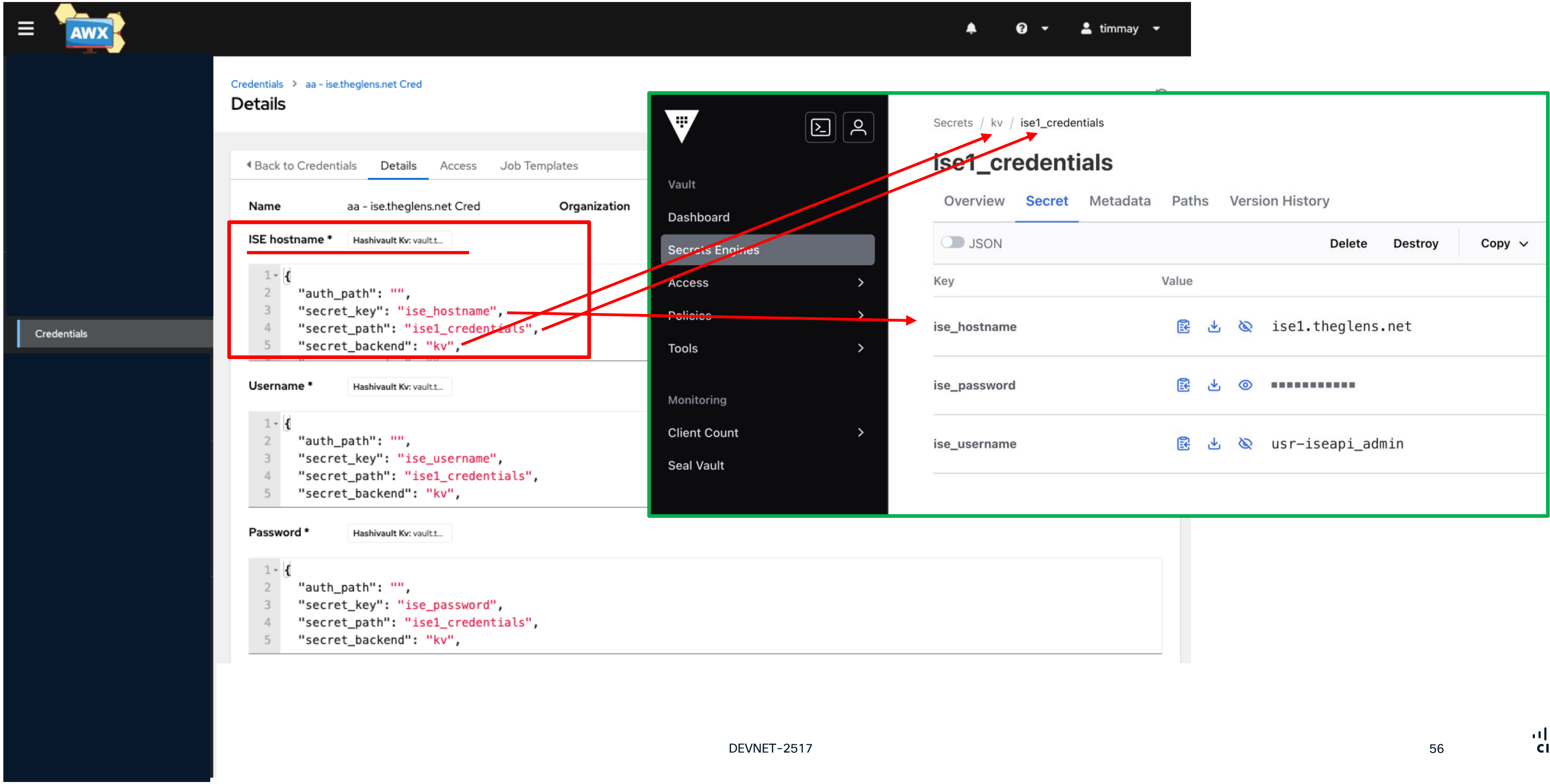
```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	▪▪▪▪▪▪▪▪▪▪▪
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

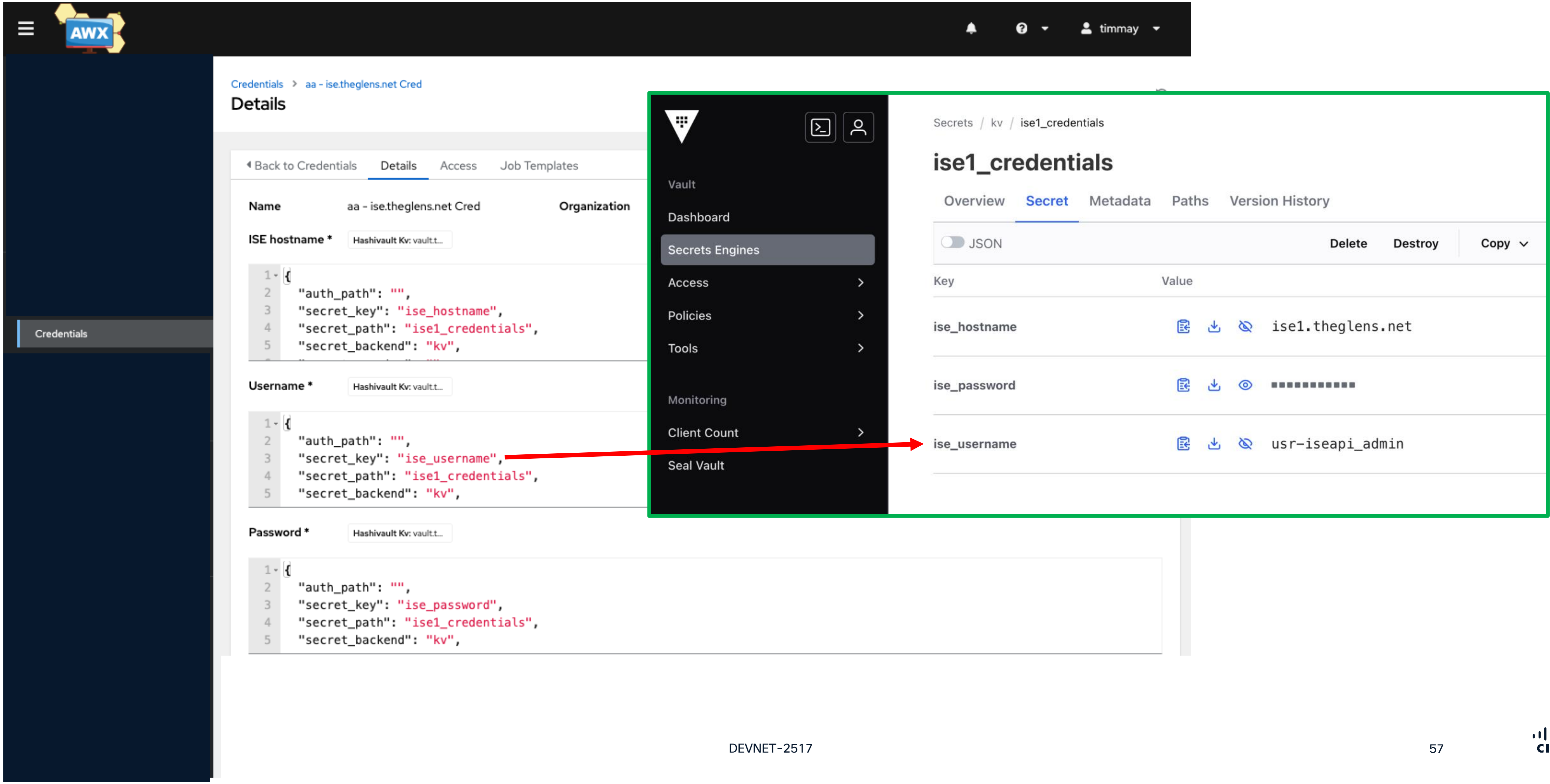
```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

‹ Back to Credentials | Details | Access | Job Templates

Name: aa - ise.theglens.net Cred

Organization

ISE hostname *: Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username *: Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password *: Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

ise1_credentials

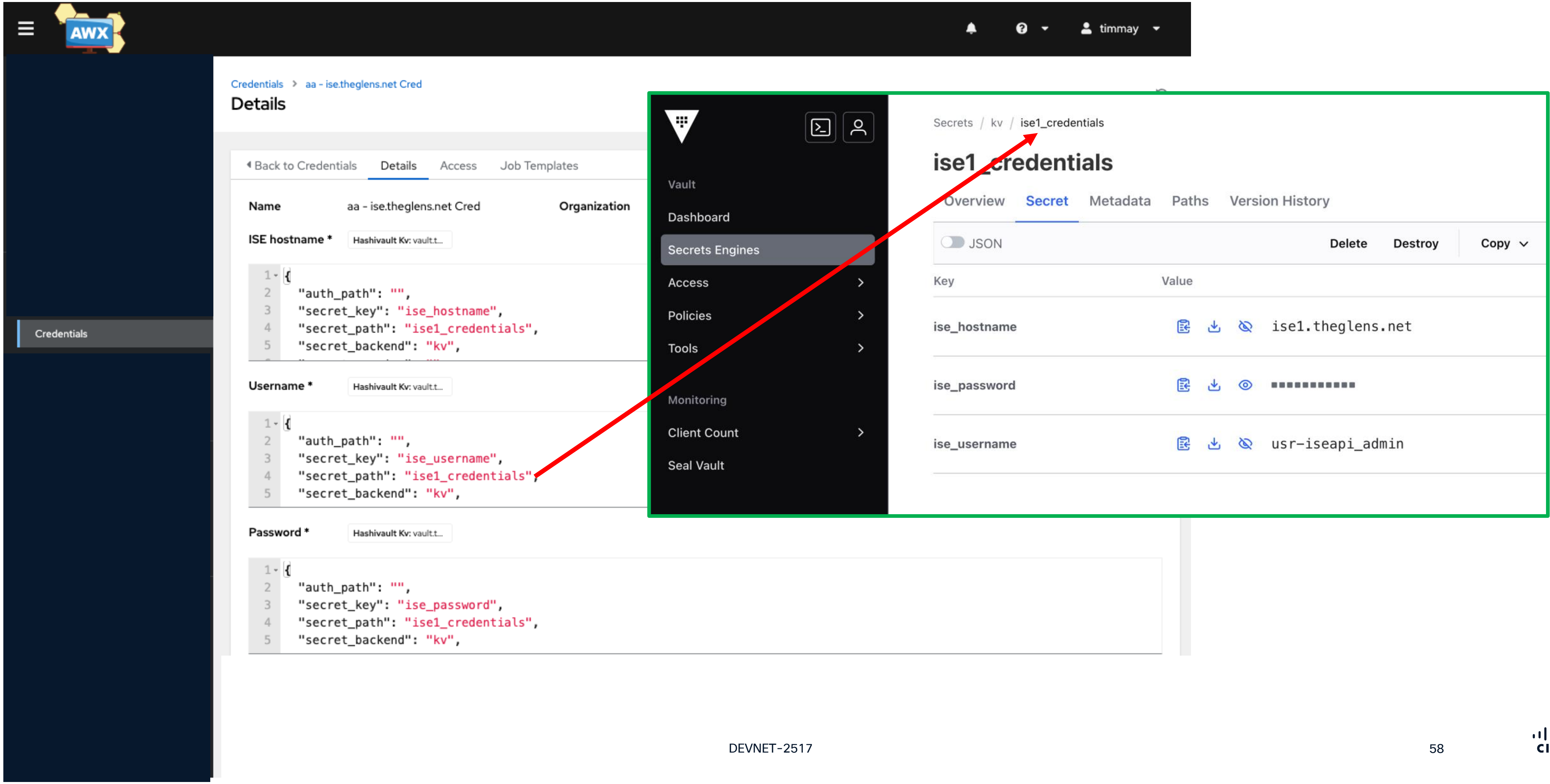
Overview | Secret | Metadata | Paths | Version History

JSON | Delete | Destroy | Copy

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping

AWX ♥ HashiCorp Vault



Credentials > aa - ise.theglens.net Cred

Details

< Back to Credentials | Details | Access | Job Templates

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

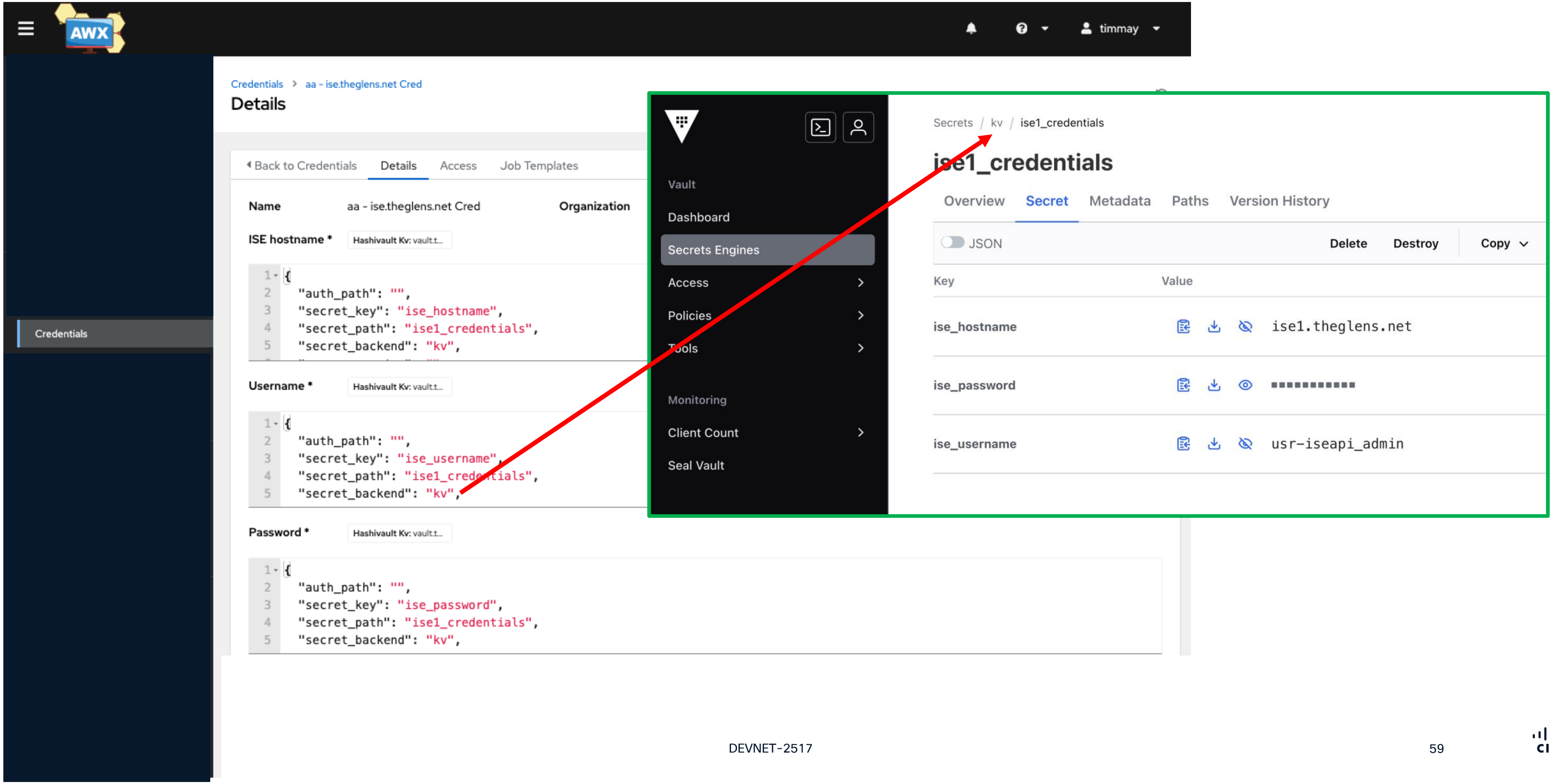
ise1_credentials

Overview | Secret | Metadata | Paths | Version History

JSON | Delete | Destroy | Copy

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Credentials > aa - ise.theglens.net Cred

Details

Back to Credentials | Details | Access | Job Templates

Name: aa - ise.theglens.net Cred

Organization

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Secrets / kv / ise1_credentials

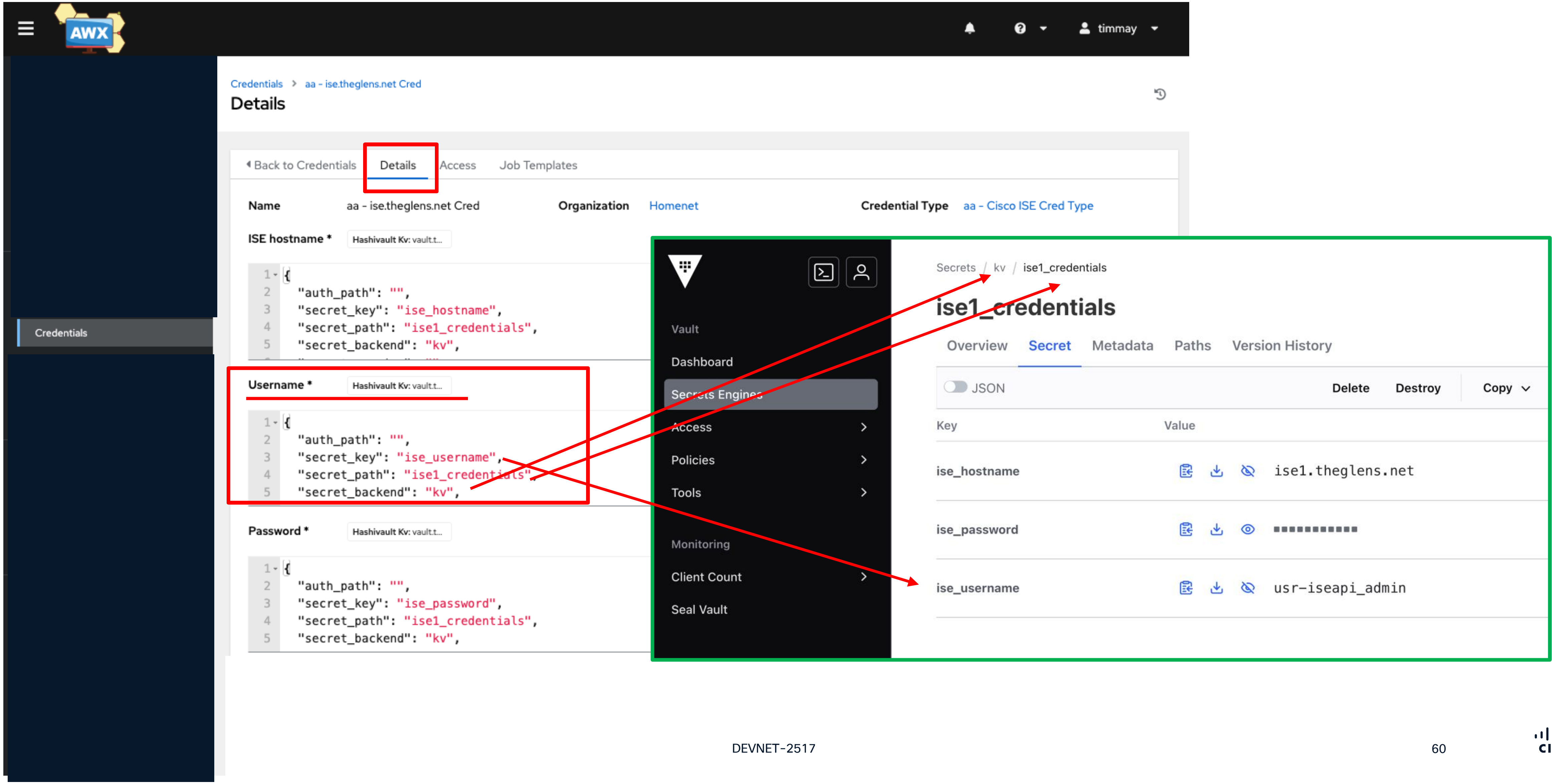
ise1_credentials

Overview | Secret | Metadata | Paths | Version History

JSON | Delete | Destroy | Copy

Key	Value
ise_hostname	ise1.theglens.net
ise_password	▪▪▪▪▪▪▪▪▪▪▪▪
ise_username	usr-iseapi_admin

Custom Cred to Vault Mapping



Details

Name: aa - ise.theglens.net Cred
Organization: Homenet
Credential Type: aa - Cisco ISE Cred Type

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

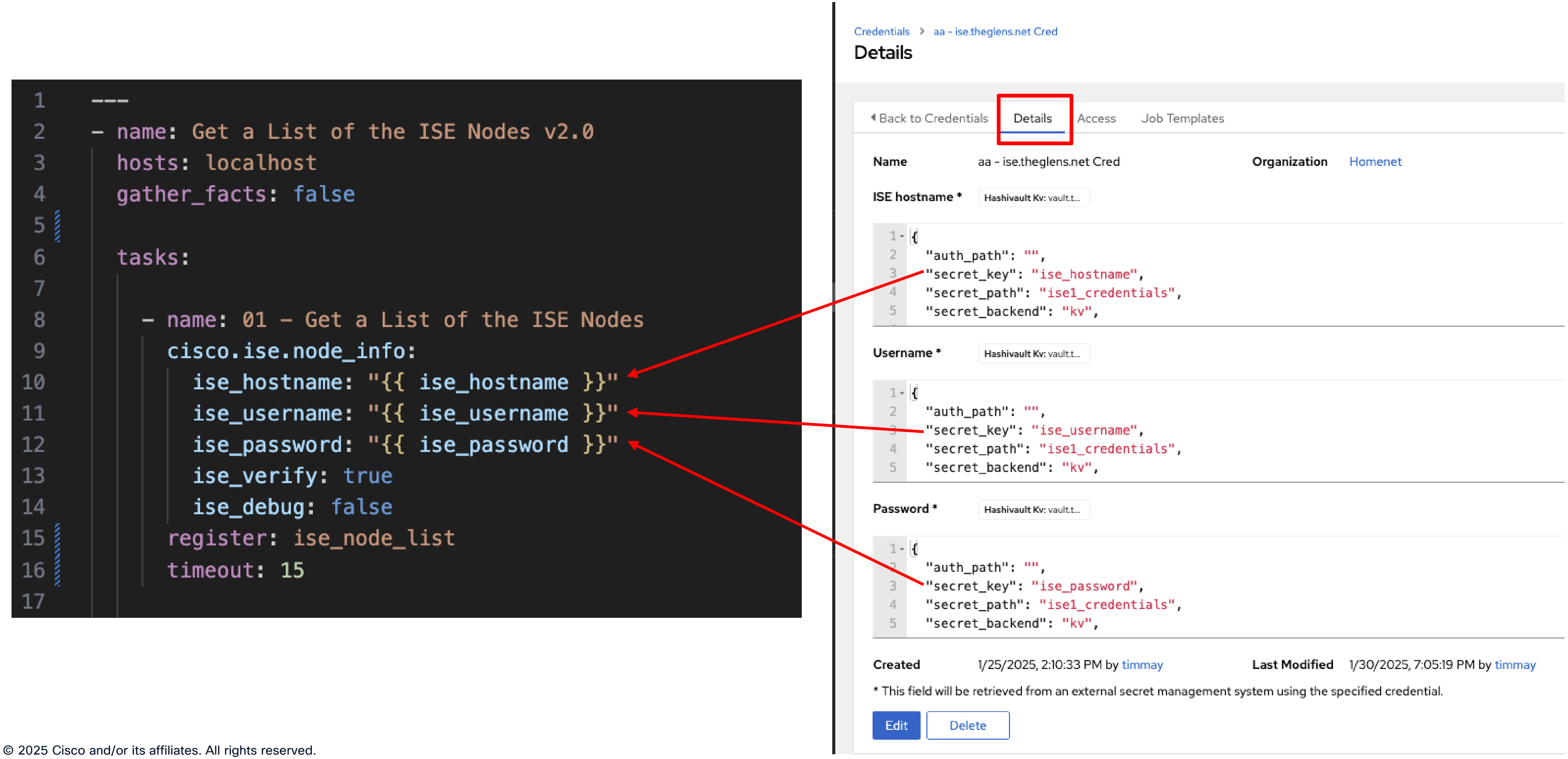
Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

ise1_credentials

Key	Value
ise_hostname	ise1.theglens.net
ise_password	■■■■■■■■■■■■
ise_username	usr-iseapi_admin

Playbook to Custom Cred Mapping



```yaml
---
- name: Get a List of the ISE Nodes v2.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_hostname }}"
        ise_username: "{{ ise_username }}"
        ise_password: "{{ ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 15

```

Details

Name aa - ise.theglens.net Cred

Organization Homenet

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Created 1/25/2025, 2:10:33 PM by timmay

Last Modified 1/30/2025, 7:05:19 PM by timmay

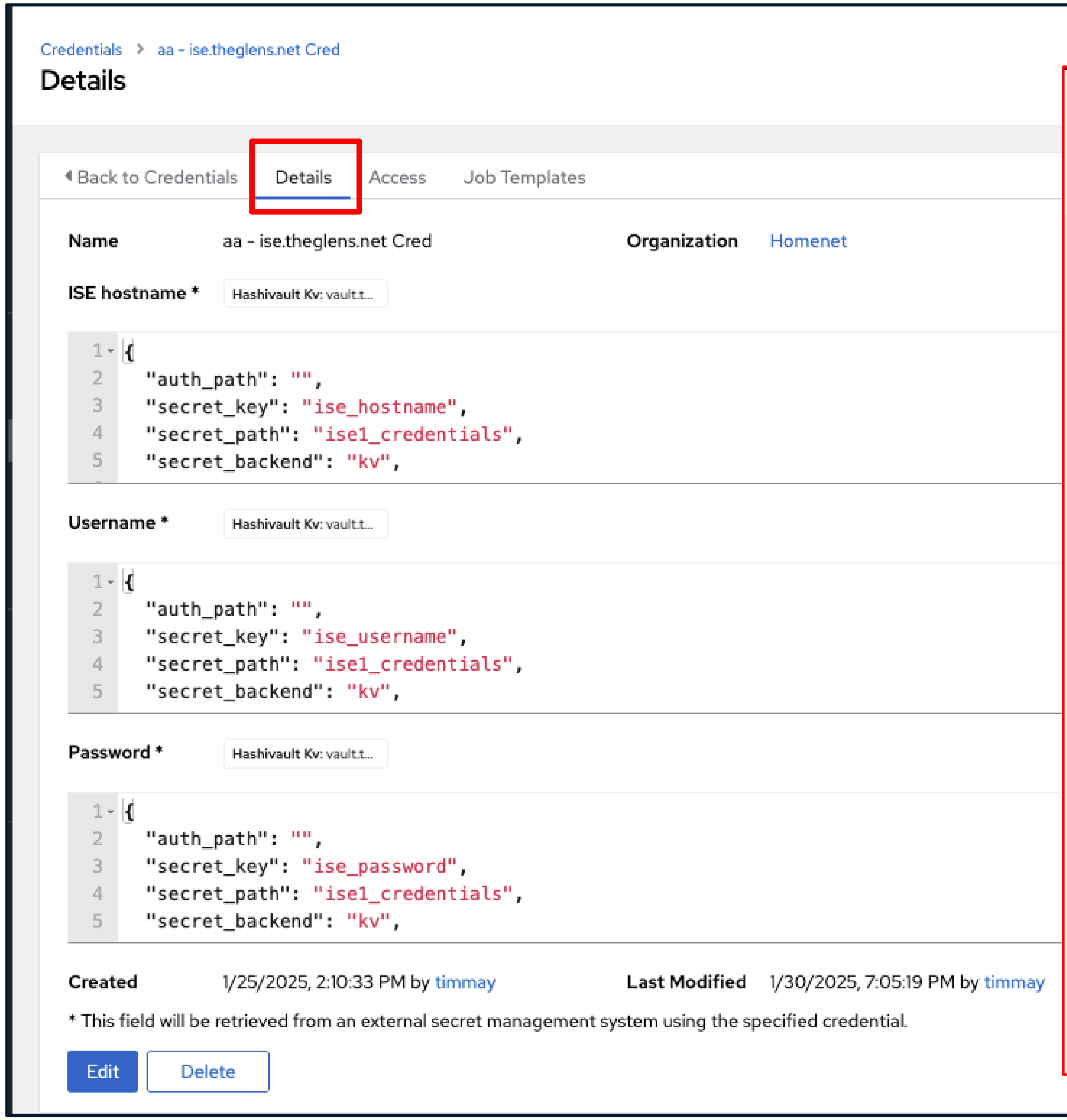
* This field will be retrieved from an external secret management system using the specified credential.

Sorry for making you focus on all those arrows.

There will be a Cisco certification test after this session, and you will have to drag and drop from one side to the other.

I hope you were paying attention!!!

Custom Cred Reuse



Credentials > aa - ise.theglens.net Cred

Details

Name aa - ise.theglens.net Cred **Organization** Homenet

ISE hostname * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_hostname",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Username * Hashivault Kv: vault.t...

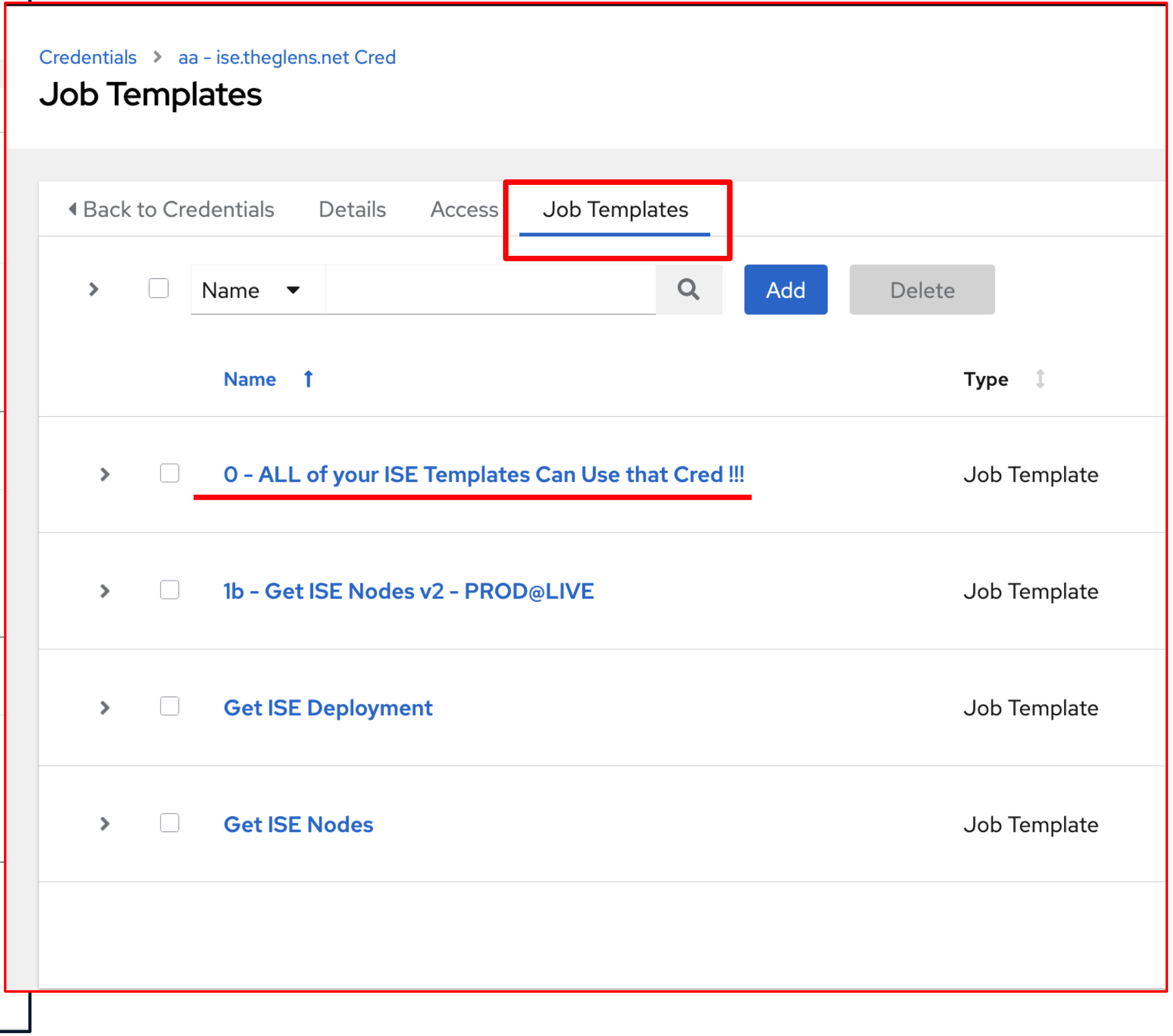
```
{
  "auth_path": "",
  "secret_key": "ise_username",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Password * Hashivault Kv: vault.t...

```
{
  "auth_path": "",
  "secret_key": "ise_password",
  "secret_path": "ise1_credentials",
  "secret_backend": "kv",
```

Created 1/25/2025, 2:10:33 PM by timmay **Last Modified** 1/30/2025, 7:05:19 PM by timmay

* This field will be retrieved from an external secret management system using the specified credential.

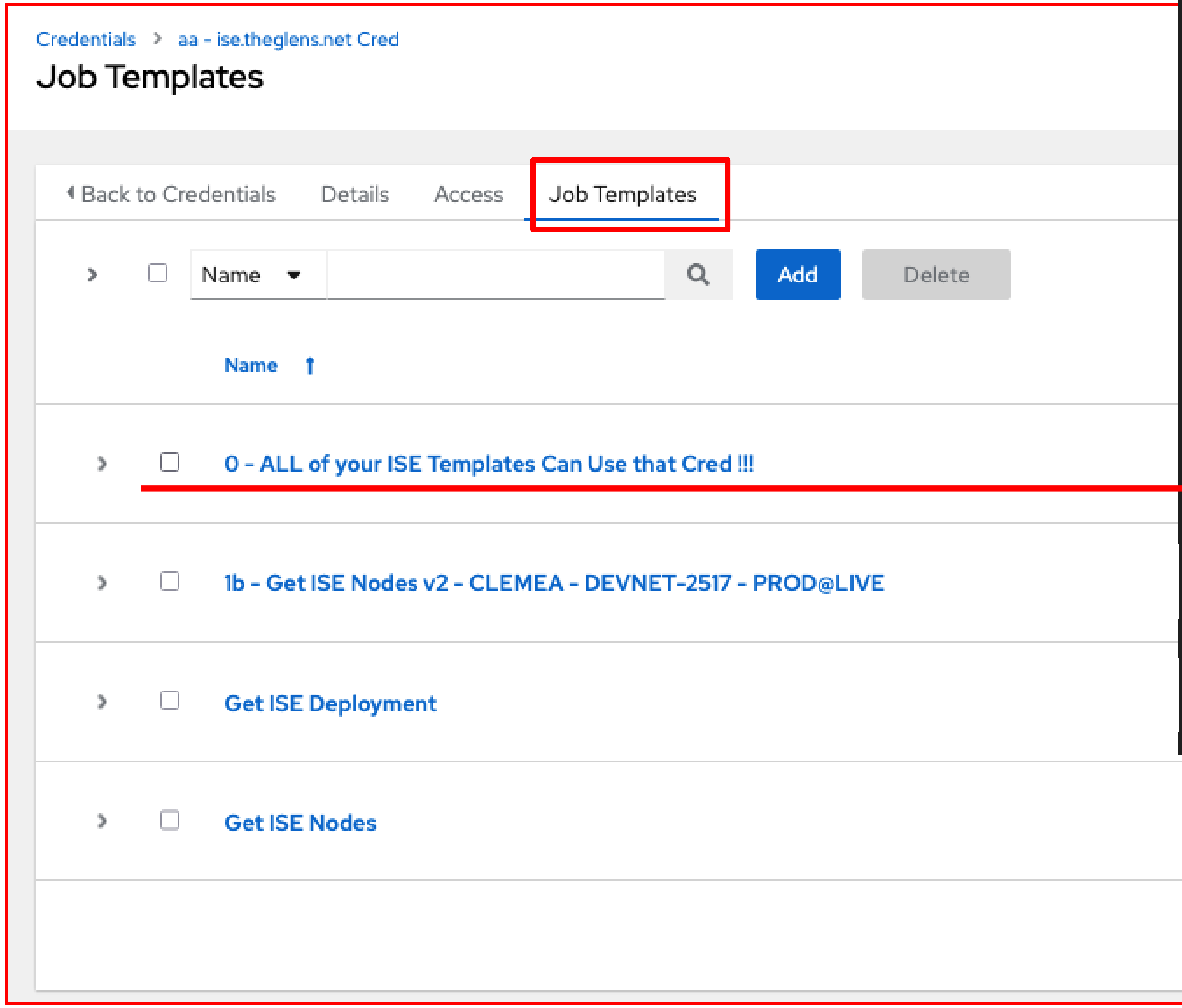


Credentials > aa - ise.theglens.net Cred

Job Templates

Name ↑	Type
0 - ALL of your ISE Templates Can Use that Cred !!!	Job Template
1b - Get ISE Nodes v2 - PROD@LIVE	Job Template
Get ISE Deployment	Job Template
Get ISE Nodes	Job Template

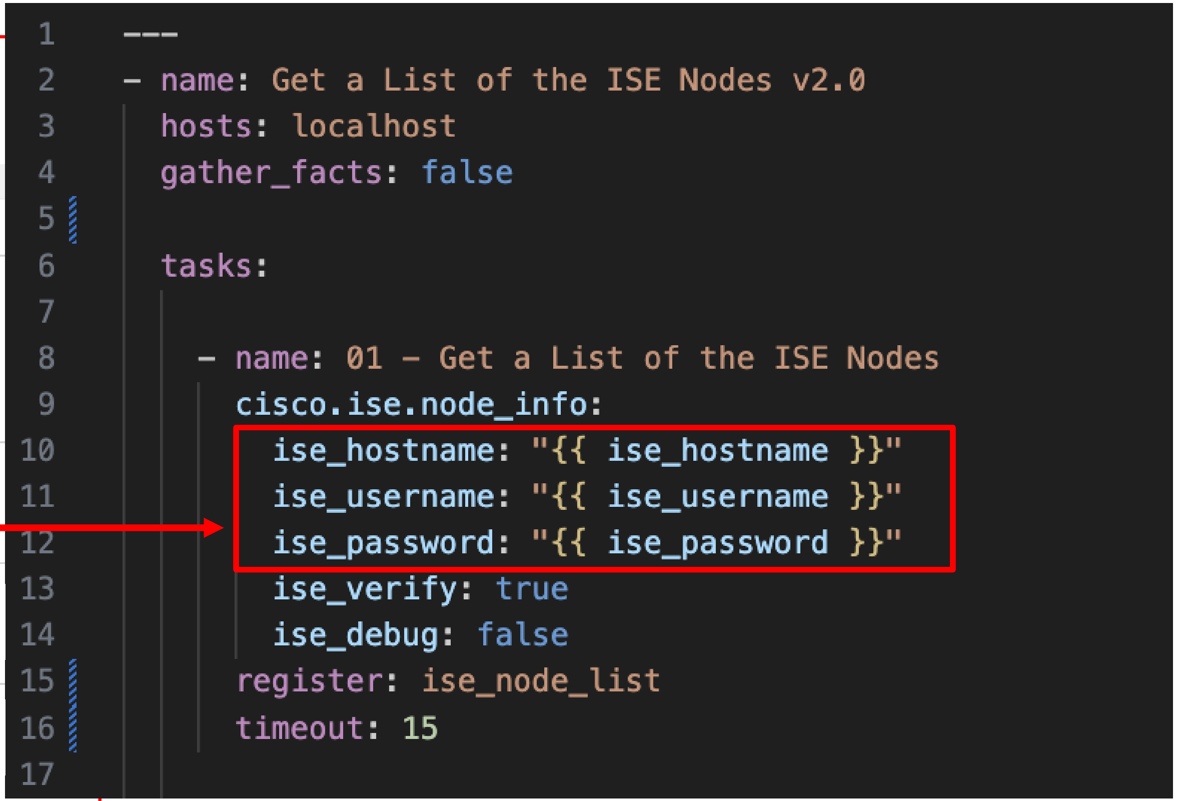
Custom Cred Reuse



Credentials > aa - ise.theglens.net Cred

Job Templates

- □ 0 - ALL of your ISE Templates Can Use that Cred !!!
- □ 1b - Get ISE Nodes v2 - CLEMEA - DEVNET-2517 - PROD@LIVE
- □ Get ISE Deployment
- □ Get ISE Nodes

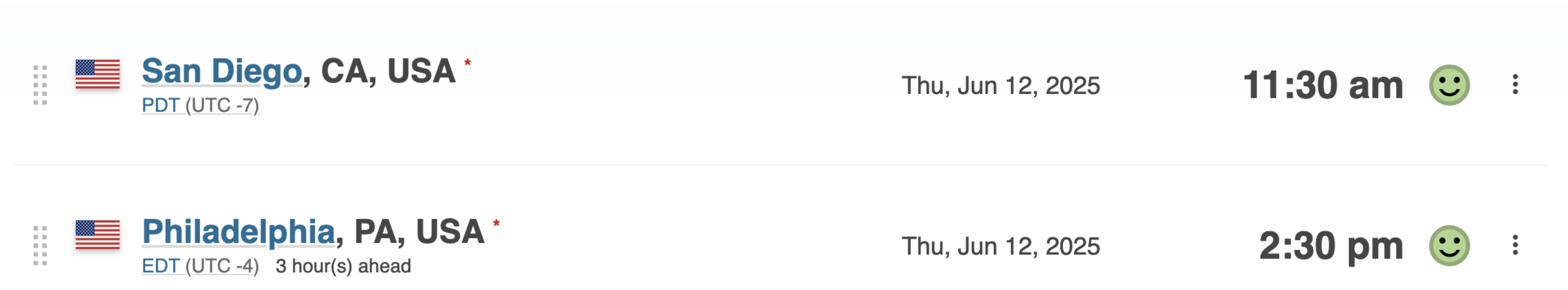


```yaml
---
- name: Get a List of the ISE Nodes v2.0
  hosts: localhost
  gather_facts: false

  tasks:

    - name: 01 - Get a List of the ISE Nodes
      cisco.ise.node_info:
        ise_hostname: "{{ ise_hostname }}"
        ise_username: "{{ ise_username }}"
        ise_password: "{{ ise_password }}"
        ise_verify: true
        ise_debug: false
      register: ise_node_list
      timeout: 15

```

Easy Button

Demo – External Secret Management

- Replace the Certificate on ISE during the Business Day

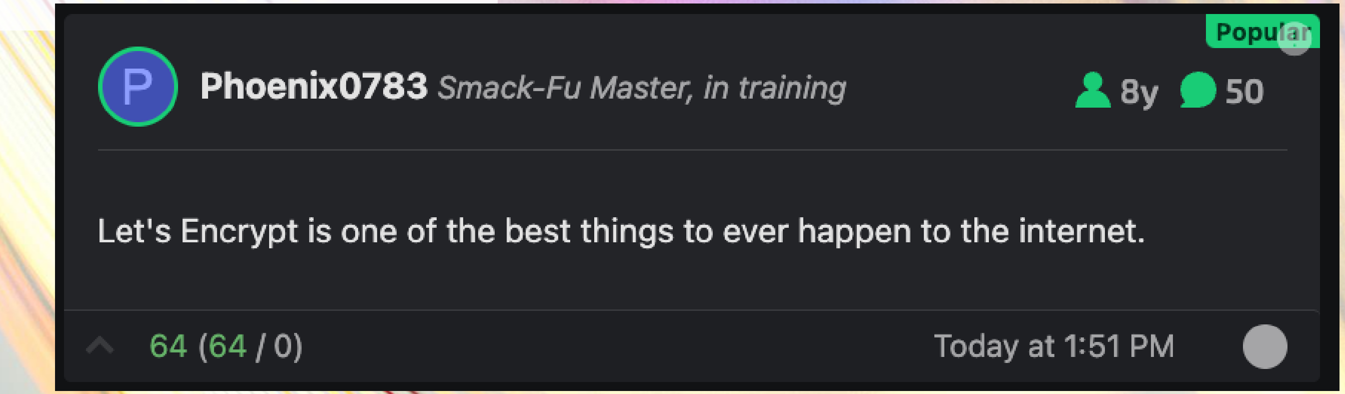


San Diego, CA, USA * PDT (UTC -7)	Thu, Jun 12, 2025	11:30 am
Philadelphia, PA, USA * EDT (UTC -4) 3 hour(s) ahead	Thu, Jun 12, 2025	2:30 pm

- Show Playbooks
- ISE Should be finished restarting soon

Demo

Certificate Automation



Popular

Phoenix0783 *Smack-Fu Master, in training*

8y 50

Let's Encrypt is one of the best things to ever happen to the internet.

64 (64 / 0)

Today at 1:51 PM

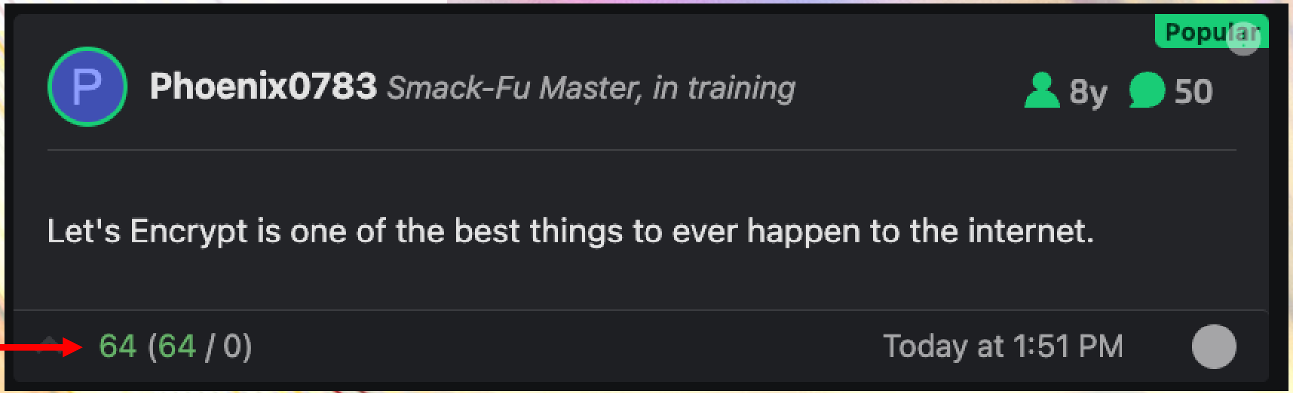
AWX

Let's Encrypt

Demo

Certificate Automation

No Downvotes



Popular

Phoenix0783 *Smack-Fu Master, in training*

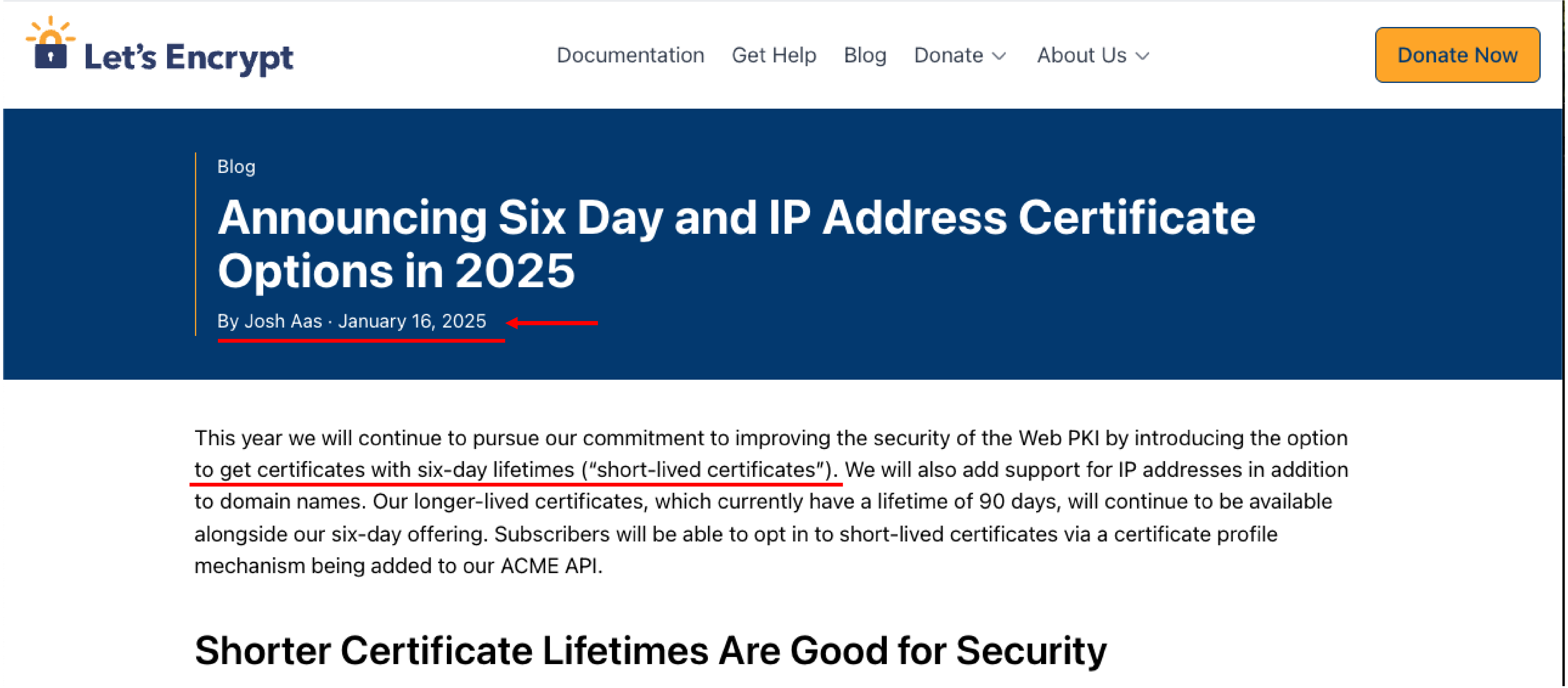
8y 50

Let's Encrypt is one of the best things to ever happen to the internet.

64 (64 / 0)

Today at 1:51 PM

Shorter Certificate Lifetimes are Coming...



Blog

Announcing Six Day and IP Address Certificate Options in 2025

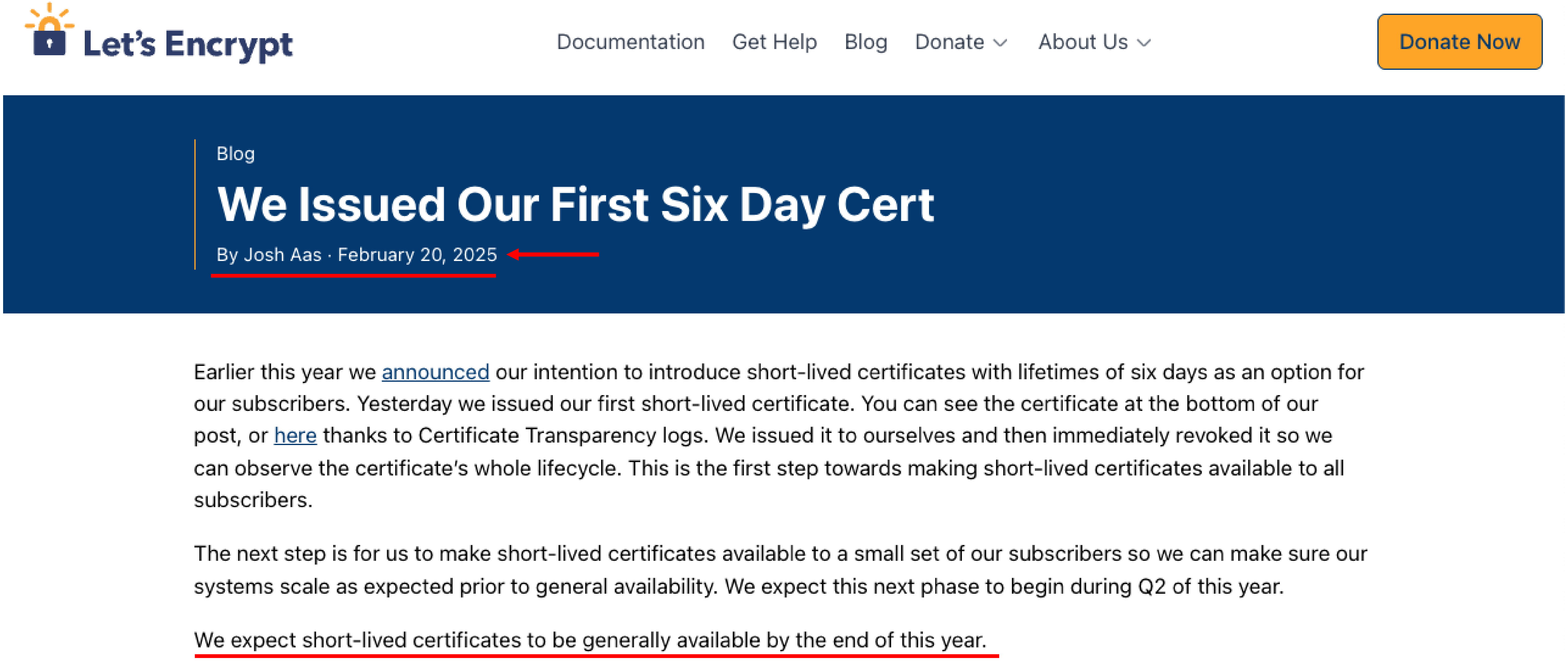
By Josh Aas · January 16, 2025

This year we will continue to pursue our commitment to improving the security of the Web PKI by introducing the option to get certificates with six-day lifetimes ("short-lived certificates"). We will also add support for IP addresses in addition to domain names. Our longer-lived certificates, which currently have a lifetime of 90 days, will continue to be available alongside our six-day offering. Subscribers will be able to opt in to short-lived certificates via a certificate profile mechanism being added to our ACME API.

Shorter Certificate Lifetimes Are Good for Security

https://letsencrypt.org/2025/01/16/6-day-and-ip-certs/

Shorter Certificate Lifetimes are Coming...



Blog

We Issued Our First Six Day Cert

By Josh Aas · February 20, 2025

Earlier this year we announced our intention to introduce short-lived certificates with lifetimes of six days as an option for our subscribers. Yesterday we issued our first short-lived certificate. You can see the certificate at the bottom of our post, or here thanks to Certificate Transparency logs. We issued it to ourselves and then immediately revoked it so we can observe the certificate's whole lifecycle. This is the first step towards making short-lived certificates available to all subscribers.

The next step is for us to make short-lived certificates available to a small set of our subscribers so we can make sure our systems scale as expected prior to general availability. We expect this next phase to begin during Q2 of this year.

We expect short-lived certificates to be generally available by the end of this year.

https://letsencrypt.org/2025/02/20/first-short-lived-cert-issued/

Demo – Let’s Encrypt for Newbies

- Create a new Let’s Encrypt Account
- Generate a new Let’s Encrypt Certificate

Wrap this party up!!!

Recap

- Build your own Execution Environment
- Build Custom Credentials for your AuthC needs
- Certificates are great Automation Use Case

- ☑ Use AWX for your basic and for your advanced ansible playbooks
- ☑ Store your automation credentials securely in a External Vault
- ☑ Create Custom Credential Types when more than a ‘password’ is required
- ☑ Configure a credential (if req’d)
  Create a Job Tempate
- ☑ Run the Job
  Monitor the output
  Schedule the job to run again!

ACTION ITEMS
★★★
ACTION ITEMS
★★★
ACTION ITEMS

Complete your session evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2026.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn exclusive prizes!

Complete your surveys in the Cisco Live mobile app.

Continue your education

Visit the Cisco Showcase for related demos

Book your one-on-one Meet the Engineer meeting

Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs

Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand

Contact me at: Webex

Thank you