Migrating Secrets From OldProd Vault to Substrate Vault

Document Level Classification

200

Introduction

When migrating your service from OldProd to Substrate, usage of secrets in the service and/or application has to be taken into account. Secrets used by your service will need to be migrated from the OldProd Vault to Substrate Vault. This document will serve as an overview of how to evaluate your current secrets in your tag roles and applications, and how

to migrate them from OldProd to Substrate.

Starting from August 2024, it is mandatory that all new Kubernetes clusters use External Secrets Operator (ESO). We strongly recommend using ESO, but the Vault Injector sidecar will still remain available with limited support, bug fixes will be provided if needed to maintain core functionality.

Reference Using External Secrets Operator (ESO) in epic-app to inject secrets for documentation on using ESO.

Evaluating Secrets Usage

In evaluating secrets usage in your service and applications in OldProd, there are two main keywords to look for in your code. Those keywords are `vault` and `secret.` For example, if you are setting an environment variable in your container to the value of a secret in the vault, you would expect so see an assignment to that variable by means of a vault lookup. In the example below you can se we are calling a lookup on the vault for a secret. That secret is the MongoDB password that is then set as the environment variable for NODE_MONGO_PASSWORD. This would later be used by the application to connect to the database.

```
# Example usage of secrets in a tag role
pod:
    containers:
      epic-application:
            image_name: hub.ol.epicgames.net/epicgames/epic-example-app
            image_tag: 2.2.2.master.01010101010101010101010101010
            command:
                start
            environment:
```

```
                EPIC_ENV: "{{ env_context }}"
                EPIC_IMAGE_TAG: "{{ image_tag }}"
                NODE_MEMORY_RESTART_THRESHOLD: 900
                NODE_MAX_MEM: 900
                NODE_MONGO_DATABASE: "application_prod"
                NODE_MONGO_USERNAME: "application_prod"
                NODE_MONGO_PASSWORD: "{{ lookup('vault', 'secret/ansibl
```

While this is just a one line example of using secrets in a tag role, typically your tag role will contain multiple vault lookups to retrieve secrets. All of those secret locations should be documented.

Looking up secrets in OldProd Vault

After you have documented a list of secrets and their location in the vault. You would then log into the OldProd vault here https://vault.ol.epicgames.net/ui/ to look up the secret. Secrets in the OldProd vault follow a naming convention. This should assist in looking up the secret.

Naming Convention:

`<storage>/<tool>/<area_of_usage>/<team_name/<application_type/<environment_name>/<container_name>/<resource_secret_name>`

Example:

`secret/ansible/tag_role/ogs/service/fortnite/ci/fortnite-service/friends_clientsecret`

Creating Secrets in Substrate Vault

Now that you know where your old secrets reside in the OldProd Vault, you can move those secrets over to the Substrate Vault in your Substrate environment. The overview of the process would look like this:

1. Create a secret in Substrate Vault
    1. Sign-in to Vault (using Okta credentials)
    2. Navigate to the secrets location for your environment. For example `/account-name/<cluster-name>/<namespace-name>` . (More on Vault Paths)
    3. Click **Create secret +.**
    4. Enter a name for the secret in the **Key** field and the secret data in the value field next to it.
    5. Click the **Save** button to save the secrete.

Moving Secrets from OldProd Vault to Substrate Vault

If you are looking for a quick way to move secrets without having to manually recreate secrets, you can use the Vault CLI to accomplish this task using the following instructions:

1. Download vault cli from https://releases.hashicorp.com/vault/ and place the executable somewhere in your $PATH.
2. Open a terminal tab

3. Login to OldProd Vault
    - **Mosaic** macros cannot be exported to this format.
4. Copy secrets from OldProd
    - ```
      vault kv get -format=json /source/path | jq .data.data > vault.
      ```
5. Open a new Terminal tab
6. Login to Substrate Vault
    - **Mosaic** macros cannot be exported to this format.
7. Copy secrets to Substrate
    - ```
      vault kv put /destination/path @vault.json
      ```

Using Secrets in Your Substrate Application

Now that your secrets have been created and have been shared with your application. You can use them in your epic-app based Helm chart. These will be in in the form of externalSecrets. Below is a before and after of how secrets are used in OldProd Tag Roles and how they would be converted over for use in Substrate Helm Charts as `externalSecrets`.

Mosaic macros cannot be exported to this format.

Additional Substrate Vault Resources

- For How-To documentation with more in depth use cases and screenshots, refer to Using External Secrets Operator (ESO) in epic-app to inject secrets.