Link to 2024 ACAMP Wiki

Advance CAMP Fri. Dec 13, 2024

Room - I

Session Title: Secrets Mgmt with Hashicorp

CONVENER: Gray

MAIN SCRIBE(S): Warren A

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 10

DISCUSSION:

Following on from non-human identities, where 80% of examples are handled with HashiCorp Vault at Gray's institution, eg. GitLab CI/CD generating JWT. Thousands of non-human authentications per day. Also doing certificate ssh via Vault.

Clay (RIT): Are you doing k8s secrets with Vault? Gray: Not currently, but have containers running vault agent.
Justin (UWash): Using external secrets operator? We are. Experience is interesting but weird. Not using dynamic secrets creation. Gray: using dynamic secrets creation for things like lets encrypt.
Clay (RIT): Justin, how do you manage namespaces? Justin (UWash): Namespacing by app. Vault is read-only. Alot is not automated, and this prevents automation.
Richard (): Are people using enterprise?
Gray: Trying to migrate, but it has been painful because of namespace. They are lifting the community edition namespace and migrating to enterprise.
Gray: What percentage of interaction is human?
??: None is human, all service accounts.
Gray: Have a significant amount of human interactions. But roles are tied to auth methods, so if you have multiple AuthN methods (SAML, OIDC,...) have to replicate roles. Leveraging jsonnet to automatically duplicate roles between AuthN methods.

LIGO primarily has human interaction

Gray: Another problem is ACL policy is difficult for people to understand, especially JIT processing. Has no awareness of whether secret exists, just whether policy exists. Are going to create a long training video for users. Warren: Can you make that available to other communities? Gray: Yes. And vault's own training is good, just not on policy.
Shumin Lee (UNC); Have CLIinterface.
Gray: Only use web ui for things they are not familiar with. Also, no good tooling for "who has access to a secret known to be stored." Violates the basic premise of vault which is to not expose what secrets exists. Gray working on index tooling. Others have also had to do it. In order to do it properly, have to stamp every secret with a GUID. Usefult to think of it as a non-relational database.
Everyone seems to be using CLI interface for everything, e.g. terraform. For GitLab CI/CD Gray generates JWT in the job. Vault trusts tokens from GitLab. Great documentation from GitLab on how this works. Kubernetes works in a similar way. Gray's GitLab integration is an Auth engine.

How are DB accounts managed? Gray - not using it, manually creating credentials and entering into KV store. PostGres, Oracle, MySQL secrets engines available for Vault. How do grants work? Not sure. Ed (Canarie) says it is described in the docs.

Gray: One vault outage in five years, from bug in Terraform. Gatekeep TF repository with merge requests with reviews. New person reviewing forgot to check Terraform plan before merge. Also had not tied Terraform to a specific version. Overwrote key. Because they had enterprise and support, walked them through generating root token on backup, finding keys, and restoring.
Shuman: supports versioning of KV, why not up version? Gray: No versioning on ssh keys, which is what we corrupted.
General discussion about how scary this would be. Ed has been wary of adopting for this sort of reason. G

Proposed maturity model: Level 0 - get all secrets stored in one place. Level 1 - access by multiple applications. Level 2 - automatic rotation of secrets. Level 3 - autogenerate secrets.
Gray's insight - don't duplicate secrets in the KV store? People want to silo, but keeps rotation from breaking things. Can spend an infinite amount of time trying to plan namespaces.
Questions about where the wildcards go. Gray's group will duplicate policy definitions to allow multiple roles to use same policy with different names. Part of offboarding microservices.
Shuman's group has started disallowing sharing of secrets. Gray can't do that for application ssl

certs that are behind a common proxy. This could be done if it was terminated at the proxy. Clay does not use a load balancer but uses BGP routing.

Are host names and port numbers being put in? Gray's group does. Creation of non-secret secrets.