Secure Introduction with Vault Webinar Follow-up Q&A

1. Is identity based access available in GCP as well?
    a. Yes. https://developer.hashicorp.com/vault/docs/auth/gcp

2. Is the secret-0 referring to VAULT_ROOT_TOKEN ?
    a. The "secret zero" problem is referring to the first "secret" required for apps/machines to authenticate to Vault. Check out more about this here: https://www.hashicorp.com/blog/how-and-why-to-use-approle-correctly-in-hashicorp-vault

3. Do you need to be authenticated to unwrap a token?
    a. No. If you have a valid wrapping token, a Vault client token (retrieved upon authenticating to Vault) is not required. Check this learn guide for an example: https://developer.hashicorp.com/vault/tutorials/secrets-management/cubbyhole-response-wrapping

4. Is this Vault agent managed by application teams?
    a. The teams in charge of managing Vault Agents vary widely from customer to customer. For example, Vault Agents may be managed by the platform team that manages machine images. Application teams may also manage Vault Agents in their deployments, especially if they're deploying Vault Agents as sidecars.

5. What kind of communication does the agent need? Outbound 443?
    a. The Vault Agent needs a network path back to the Vault Cluster. Typically this is on port 8200.

6. Is wrapping available just for cubby holes or all secret engines?
    a. Wrapping is available on other secret engines, such as PKI and Transit. All of these wrapped responses end up in a cubbyhole, from which you then unwrap to get the secret.

7. Is this feature available just for appRole? Can other auth methods also use it?

    a. Wrapping is auth method agnostic. You can create wrapped secrets after authenticating through any means (as long as policies and such allow it).

8. Why is the secret ID different before and after unwrap?
    a. Is it possible the SecretID and wrapped token are being confused? SecretIDs may be long lived, and infrequently changed: https://developer.hashicorp.com/vault/docs/auth/approle#secretid

9. Is response wrapping a feature exclusive to Vault Enterprise, or is this also available for self-hosted Vault installations?
    a. Response wrapping is a basic feature in Vault OSS, but when paired with additional features in Vault Enterprise, such as Namespaces and Sentinel, you can gain a lot of security and value.