Upgrading Vault Guide

HashiCorp | Enterprise Architecture

2020-05-27

Upgrading Vault - Standard Operating Procedures

Introduction

The objective of this document is to provide a set of standard operating procedures (SOP) for upgrading up a Vault cluster.

In this document we are going to focus on upgrade procedures for Vault Enterprise. This assumes that all Vault clusters are running a minimum of three (3) nodes as recommended in our Vault Reference Architecture guide.

As of Vault 1.4, it is possible to run Vault using integrated Raft storage, rather than an external storage backend such as Consul. The upgrade procedures differ depending on which storage backend is used (Raft Integrated Storage or Consul Storage Backend). The difference in the steps to be followed are highlighted in these procedures.

Personas

These SOPs are primarily aimed at Ops personnel.

Prerequisites

The following prerequisite steps and knowledge are required in order to upgrade a Vault cluster. All of the following are required to be understood or carried out **before** a scenario where you may need to attempt an upgrade of Vault.

1. Working Knowledge of Vault

Some working knowledge of Vault is required in order to follow these SOPs

2. Vault and Consul Infrastructure Configured as per Vault Reference Architecture

A cluster configuration as defined in our Vault Reference Architecture guide is required.

3. Vault has been initialised

This SOP assumes you have already initialised Vault, keyholders are available with access to the unseal keys for each, that you have access to tokens with sufficient privileges for both clusters and encrypted data is stored in the storage backend.

4. Upgrading Vault Guide

These SOPs assume that you have already reviewed Upgrading Vault Guides along with the Vault version-specific upgrade notes in that area of the documentation.

General Guidance

When upgrading Vault, you should bear in mind this general advice:

- Follow the Rolling Update Procedures (defined below) when updating Vault for a minor version update or less.
- If an upgrade involves more than a minor version update, then follow the DR Upgrade Approach (also defined below).
- As well as following the above advice, always check the release notes and changelog (Upgrading Vault - Guides) to see if there are any breaking changes or special steps required for an upgrade of Vault.
- You should never fail over from a newer version of Vault to an older version. Our procedures are designed to prevent this.
- Vault does not support true zero-downtime upgrades, but with proper upgrade procedure the downtime should be very short (a few hundred milliseconds to a second depending on how the speed of access to the storage backend).
- **IMPORTANT NOTE:** Always back up your data before upgrading! Vault does not make backward-compatibility guarantees for its data store. Simply replacing the newly-installed Vault binary with the previous version will not cleanly downgrade Vault, as upgrades may perform changes to the underlying data structure that make the data incompatible with a downgrade. If you need to roll back to a previous version of Vault, you should roll back your data store as well. The procedures defined below include steps to backup Vault's storage as step in the upgrade procedure.

Understanding your Vault installation

Typical Vault Enterprise installations may have multiple Disaster Recovery Replicas and Performance Replica clusters, usually located in different region or datacenters. Additionally, Vault HA setups can differ on whether a load balancer is in use, what addresses clients are being given to connect to Vault (standby + leader, leader-only, or discovered via service discovery), etc.

Before beginning the upgrade procedure, you should make a note of each of these details and carefully produce an upgrade schedule, taking into account the advice given in these operating procedures.

Procedures

Procedures are given below for 3 different scenarios:

- Performing a rolling upgrade of a HA Vault cluster
- Performing an upgrade of multiple Vault replication clusters and a primary cluster.
- Performing an upgrade of a Vault Cluster greater than a minor version.

Rolling Upgrade Procedure (for upgrading a single HA cluster)

NOTE: If your Vault Enterprise deployment consists of Disaster Recovery or Performance Replica clusters, then please read the next section on Per Replication Cluster upgrades in conjunction with this section.

Perform the following steps in order to perform a rolling upgrade of a Vault HA cluster:

1. Take a backup of your Vault cluster, the steps to which will depend on whether you're using Consul Storage Backend or Raft Integrated Storage.
    1. Consul Storage Backend:
        1. Take a Consul snapshot using the following command: `consul operator raft snapshot`
        2. Save the created snapshot file in a safe location in case the need arises to restore from the snapshot.
    2. Raft Integrated Storage:
        1. Take a snapshot of the raft storage layer of Vault using this command. `vault operator raft snapshot save demo.snapshot`
        2. Save the created snapshot file in a safe location in case the need arises to restore from the snapshot.
2. Determine the leader and followers nodes in your Vault cluster.
    1. When using Raft Integrated Storage: `vault operator raft list-peers`
    2. When using any other storage backend (e.g. Consul): `curl http://127.0.0.1:8200/v1/sys/leader`
3. Bring down a follower node using the following command: `systemctl stop vault`
4. Replace the old Vault binary with the new Vault binary
5. Test the new binary is in place `vault --version` to confirm the new version is correctly installed.
6. Restart Vault on the updated node `systemctl start vault`
7. Check the logs on the restarted node for any errors. Address these and roll-back if necessary.
8. Otherwise, perform steps 2-7 on the other follower nodes.
9. Next, bring down the active node `systemctl stop vault`.
10. This should trigger a change in the active Vault node, as well as a leadership change in the underlying raft storage layer (in case of raft integrated storage)- follow step 2 again to verify this. Additionally, examine the logs streaming from the remaining Vault HA nodes to confirm the active node.
11. If leadership and logs look ok, update the old vault binary on the old active/leader node by replacing it with the new Vault binary. Restart vault with `systemctl start vault`

It should be added back into the cluster automatically. Perform step 2 again to confirm this.

12. If a problem is experienced during the upgrade process, then remove all updated nodes and restore the backup from step 1 and bring up the old leader (not upgraded) and check logs for errors. Then restore the old version to all followers and add them back into the cluster making sure the Leader does not change.
13. Otherwise, if the cluster upgrade is complete, don’t forget to unseal it if using the Shamir Shards unseal method.

Replication Clusters Upgrade Procedure

Vault Enterprise installations can consist of multiple Disaster Recovery and Performance Replica clusters. With this in mind, it's very important to *upgrade secondary clusters first*. These procedures should be followed

- If you're not already aware of the status of a given cluster, use the following command to identify whether it is a primary or secondary cluster `vault read -format=json sys/replication/status`. If it is a primary, then in either the `dr` or `performance` sections of the response, you will see something similar to, stating that it has known secondaries. These secondary clusters should therefore be upgraded first:

```
...
    "dr": {
      "cluster_id": "12ace5c2-3876-8f99-db57-ee60f4cc6c80",
      "known_secondaries": [
        "secondary"
      ],
      "last_reindex_epoch": "0",
      "last_wal": 37,
      "merkle_root": "c519ae23573c4108c634c48d272a48d86d39bd65",
      "mode": "primary",
      "primary_cluster_addr": "",
      "state": "running"
    },
...
```

If the cluster you're currently working with is indeed a secondary, the above command will return something similar to the below:

```
...
    "dr": {
      "cluster_id": "12ace5c2-3876-8f99-db57-ee60f4cc6c80",
      "known_primary_cluster_addrs": [
        "https://10.0.0.10:8201"
      ],
      "last_reindex_epoch": "1586437497",
      "last_remote_wal": 0,
      "merkle_root": "c519ae23573c4108c634c48d272a48d86d39bd65",
      "mode": "secondary",
      "primary_cluster_addr": "https://10.0.0.10:8201",
      "secondary_id": "secondary",
      "state": "stream-wals"
    },
...
```

- Once you have confirmed the current cluster is a secondary, you should then follow the Rolling Upgrade Procedure (for upgrading a single HA cluster) to upgrade the nodes within that secondary cluster. Within those steps it is still very important to take backups of your cluster prior to upgrading.
- Once the secondary cluster has been upgraded, it is important re-verify the replication

status of your cluster

```
# Via API
$ curl -s $VAULT_ADDR/v1/sys/replication/status | jq
# CLI
$ vault read -format=json sys/replication/status
```

- Repeat steps 2-3 for each secondary until you need to upgrade your primary cluster.
- Once satisfied with the functionality of the upgraded secondary instances, upgrade the primary instance.

Performing an upgrade of a Vault cluster greater than a minor version

This procedure (also known as the DR Update Method), involves creating a new cluster running the target version of Vault, configuring Disaster Recovery Replication onto it, before failing over from the primary to the new DR cluster.

1. Take a snapshot of the underlying storage for the existing primary cluster. Depending on whether your cluster is using Consul storage backend of Vault Raft Integrated storage:

2. Consul Storage Backend: 1. Take a Consul snapshot using the following command: `consul operator raft snapshot` 1. Save the created snapshot file in a safe location in case the need arises to restore from the snapshot.

3. Raft Integrated Storage: 1. Take a snapshot of the raft storage layer of Vault using this command. `vault operator raft snapshot save demo.snapshot` 1. Save the created snapshot file in a safe location in case the need arises to restore from the snapshot.

4. Build the infrastructure necessary to support the new DR replica. The resources allocated to this replica should be identical to your existing primary, but have your target version of Vault installed.

5. Follow the Vault Documentation to configure Disaster Recovery replication from the primary onto this new DR secondary cluster.

6. Confirm that DR has been successfully configured by running the following command `vault read -format=json sys/replication/status`. You should see something similar to the below when running on the primary:

```
...
"dr": {
  "cluster_id": "12ace5c2-3876-8f99-db57-ee60f4cc6c80",
  "known_secondaries": [
    "secondary"
  ],
  "last_reindex_epoch": "0",
  "last_wal": 37,
  "merkle_root": "c519ae23573c4108c634c48d272a48d86d39bd65",
  "mode": "primary",
  "primary_cluster_addr": "",
  "state": "running"
},
...
```

and something similar to the below when running on the secondary:

```
...
    "dr": {
      "cluster_id": "12ace5c2-3876-8f99-db57-ee60f4cc6c80",
      "known_primary_cluster_addrs": [
        "https://10.0.0.10:8201"
      ],
      "last_reindex_epoch": "1586437497",
      "last_remote_wal": 0,
      "merkle_root": "c519ae23573c4108c634c48d272a48d86d39bd65",
      "mode": "secondary",
      "primary_cluster_addr": "https://10.0.0.10:8201",
      "secondary_id": "secondary",
      "state": "stream-wals"
    },
...
```

7. Follow the DR failover Standard Operating Procedure (documented separately) to fail over from the Primary to the new DR Secondary cluster.

8. Don’t forget to take any necessary steps to ensure clients can communicate with the new primary, such as updating DNS records to point to the new cluster once failover has completed.