Tag Based Protection using gCloud for Vaulted Backups

Ashika Ganesh | Last Updated: Nov 26, 2024

Overview

This document provides a way to manage backups for your Google Compute Engine Virtual Machines (VMs) using tags. By leveraging the provided script and Google Cloud Shell, you can automate the association and removal of backup plans based on VM tags, simplifying backup management and ensuring consistent protection for your dynamic cloud environments. Note that this script only works for project level tags that are assigned to VMs including inherited tags.

This guide will enable you to:

- **Automate backup association:** Easily include or exclude VMs from backup plans based on their assigned tags. This eliminates the need to manually configure individual VMs, saving time and reducing the risk of errors.
- **Simplify backup management:** Control backup policies for large numbers of VMs efficiently by grouping them with tags representing application names, environments (production, development, testing), or criticality levels.
- **Enhance protection:** Ensure that your critical VMs are always protected by dynamically associating them with backup plans based on their tags.

Set up and Permissions

You will need to obtain the following Role on the Project where your VMs exist with tags:

- Tag Viewer
- Backup and DR Backup User

Please ensure that:

1. The backup vault service agent for the vault you intend to use to backup your VMs has the `roles/backupdr.computeEngineOperator` role in the VM project. If you do not

have the correct Role for the backup vault provided in your VM Project, the script will succeed but you will encounter a failure error.
2. Both projects have the necessary APIs enabled
3. The user running the script has the required permissions in both projects

Getting Started

Follow the below steps to apply your protection:

1. Locate and download the **backup_script.sh.**

2. **Open Google Cloud Shell**:

    1. Navigate to Google Cloud Console.
    2. Open the Cloud Shell by clicking the terminal icon in the top-right corner.

3. **Open the Cloud Shell File Upload Dialog**:

    1. In the Cloud Shell terminal, click the **three vertical dots** in the top-right corner of the Cloud Shell window.
    2. Select **Upload**.

2. **Select Your File**:

    1. Choose `backup_script.sh` from your local machine.
    2. The file will upload to the home directory (`~/`) in the Cloud Shell.

2. Run `chmod +x backup_script.sh` in your cloudshell to make it executable.

3. Run your file by providing the following required **parameters**:

    1. `--unprotect:`(Optional) Use this flag and skip (b) - (d) if you intent to only remove active backup plans associated with VMs with certain tags.
    2. `--backup-project-id`: The project ID where the backup plan is located.
    3. `--location`: The region where the backup plan is located (e.g., `us-central1`).
    4. `--backup-plan`: The name of your backup plan.
    5. `--tag-key`: The tag key used to identify VMs (e.g., `environment`). See here on how to create and manage tag keys.
    6. `--tag-value`: The tag value used to identify VMs (e.g., `production`). See here on how to create and manage tag values.

    Note: You must provide at least 1 project OR 1 folder.

7. `--projects`: (Optional) A comma-separated list of project IDs to include.
8. `--folders`: (Optional) A comma-separated list of folder IDs whose projects you want to include (e.g., --folders 345678901234).
    1. NOTE: Please ensure that you have all required permissions for accessing all projects within the specific folders
    2. NOTE: Please ensure the Backup Vault Service Agent is provided the required roles on the specified folders.
9. `--exclude-projects`: (Optional) A comma-separated list of project IDs to exclude from processing (e.g., –exclude-projects projectC,projectD).

2. Leverage the below examples

```
Unset
bash ./"backup_script.sh" \
--backup-project-id my-backup-project \
--location us-central1 \
--backup-plan bp-bronze \
--tag-key environment \
--tag-value test \
--projects project1,project2,project3 \
--folders 345678901234
```

This command will automatically associate backup plan `bp-bronze` to VMs in `project1`, `project2,project3` as well as all projects under folder `345678901234`, for VMs tagged with `environment:test`.

```
Unset
bash ./"backup_script.sh" \
-- unprotect
--tag-key environment \
--tag-value test \
--projects project1
```

This command will automatically remove any backup plan association from VMs within `project1` that are tagged with `environment:test`.

After setting up the above, view the following files to learn how to further enhance your protection:

- **Automation.md**: Read how to set up a Cloud Run Job in Google Cloud Platform to set up your script to run on an hourly, daily, weekly or monthly basis.
- **Backup_Protect_Report_UserGuide.md**: Read how to export a .txt file that shows you the overall protection summary for your Project or Folder.