Guide to backups and VM recovery

So far in this course, you've explored recovery processes, like restoring systems to normal operations using recovery plans and tools. In this reading, you'll learn about how you can use Google Cloud Backup and Disaster Recovery (DR) to create a backup plan to restore a virtual machine (VM).

Backup and DR

Google Cloud Backup and DR is a backup and disaster recovery solution that enables organizations to quickly recover data, so they can return to running critical business operations.

As a cloud data professional, you can use Cloud Backup and DR is your managed backup and disaster recovery service for a centralized way to protect your data and workloads running on Google Cloud and on-premises. You can use Cloud Backup and DR to create and manage backups of your Compute Engine disks, Cloud SQL databases, and Cloud Storage buckets. You can also use it to restore your backups to Google Cloud, or to an on-premises environment.

Management console and appliances

In the forthcoming lab, you'll access Google Cloud Backup and DR by logging into the management console using the login information provided in the **Lab Details** panel. The **Management console** is where you can configure and manage your backup and restore activities and access backup / recovery appliances. A backup / recovery appliance is a data mover that captures, moves, and manages the lifecycle of your backup data. Appliances perform the actual work of coordinating backup data. Before you start backing up VMs, you'll need to create a backup plan template and apply a backup plan template.

Backup plan template

Backup plans are the rules that the management console uses to define how data is backed up, how often it is backed up, how long it is retained, and where and how to replicate the application's data backups. In the corresponding lab, you'll create a backup template and configure a set of policies in the template that defines the management console rules.

There are different backup policy types but you'll focus on creating a *production to snapshot* backup policy in the lab for this course. Production to snapshot policies define how to capture application production data as a snapshot. As a reminder, a snapshot captures the state of a VM at a specific moment in time.

Note: In the lab, you'll back up a Compute Engine instance that can only contain production to snapshot policies.

Create a backup template

To create a backup template, complete the following steps:

1. In the **Backup and DR management** console, click **Backup Plans > Templates**.
2. Click **+ Create Template**.
3. In the **Template** and **Description** fields, provide a name and description for the template.
4. In the **Policies** box, next to **Snapshot**, click **+ Add** to add a production to snapshot backup policy.
5. In the **Policy Name** field, provide a name for the policy.
6. For the **Scheduling** option, select **Continuous,** and specify **2 hour(s)**. A continuous snapshot backup schedule sets scheduling for the backup at the specified time interval.
7. Click **Create Policy**.
8. Click **Save Template**.

Backup a VM

After you've created a backup policy, you'll need to select the cloud resource that you'll apply the backup template to—which is **lab-vm**, a VM that's been pre-configured for the lab. To apply a backup plan to the VM, you need to search for and apply a backup plan template to it.

Complete the following steps to apply a backup plan template to a VM:

1. In the **Backup and DR management** console, click **Back Up & Recover > Back Up**.
2. Select **Compute Engine**.
3. Select the service account that should back up the VM, and click **Next**.
4. Select a filter search for the **lab-vm** Compute Engine instance for backup, and click **Next**.
5. Select **lab-vm** and from the **Action** drop-down, select **Apply a backup template**.
6. From the **Backup** template drop-down, select **vm-backup** and click **OK**.
7. Click **Finish**.

The status will update to confirm whether the policy template successfully attached to the VM.

Recover a VM

After you've applied a backup plan template to the VM you want to recover, you can now recover the VM.

Complete the following steps to apply a backup plan template to a VM:

1. In the **Backup and DR management** console, click **Back Up & Recover > Recover**.
2. Select the VM you want to recover, and click **Next**.
3. Click **Table** and select the image you want, and click **Mount**.
4. Select **Mount as new GCE instance,** and update the configuration options according to the lab instructions.
5. Click **Mount**.

Allow time for the job to finish. Once it's complete, you can go to the **Compute Instance** page to see the new recovered VM.

Key takeaways

Recovery plays an important role in the incident response process. As a cloud security analyst, you'll perform recovery actions to effectively respond to security incidents and minimize the damage caused by a security incident. Being able to recover data quickly supports the continuity of critical business operations.

Resources for more information

- For more information about Backup and DR, check out the Backup and DR Service overview.