Disaster recovery planning in Google Cloud: Build a DRP

So far, you've learned that recovery is important as a last resource, and your last line of defense is the Disaster Recovery Plan (DRP). As a cloud security professional, you and your team need to build and manage a cloud-hosted DRP that outlines the steps your team needs to follow to recover critical cloud resources and defines Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO).

In this reading, you'll learn more about Google Cloud services and tools you can use to build and design a DRP with RPOs and RTOs.

Google Cloud services and tools for building a DRP

Here's a list of some of the services and tools Google Cloud offers, and when you can use each to build a DRP:

- **Cloud Storage:** Cloud Storage is a highly durable and scalable object storage service that can be used to store backups of your data and workloads. You can use Cloud Storage to create snapshots of your Compute Engine disks, which can then be restored in the event of a disaster. You can also use Cloud Storage to store backups of your Cloud SQL databases.
- **Cloud Backup and DR:** Cloud Backup and DR is a managed backup and disaster recovery service that provides a centralized way to protect your data and workloads running on Google Cloud and on-premises. Cloud Backup and DR can be used to create and manage backups of your Compute Engine disks, Cloud SQL databases, and Cloud Storage buckets. It can also be used to restore your backups to Google Cloud, or to an on-premises environment.
- **Cloud Spanner:** Cloud Spanner is a fully managed, mission-critical relational database service that offers transactional consistency at global scale, schemas; SQL (ANSI 2011); automatic, synchronous replication for high availability; and automatic, asynchronous global replication for disaster recovery. Cloud Spanner can be used to store your most critical data and ensure that it's always available and accessible, even in the event of a disaster.
- **Cloud Bigtable:** Cloud Bigtable is a fully managed, NoSQL database service for large analytical and operational workloads. Bigtable offers a pay-per-use model, in-memory storage, and in-memory analytics. It also supports synchronous cross-region

replication for disaster recovery. Cloud Bigtable can be used to store your large and complex datasets and ensure that they're always available and accessible, even in the event of a disaster.

- **Cloud Load Balancing:** Cloud Load Balancing is a load balancer that distributes traffic across multiple servers or instances. Load balancing can be used to improve the performance and availability of your applications. Cloud Load Balancing can be used to distribute traffic across your production and DR environments. This way, if there's a disaster in your production environment, you can quickly switch to your DR environment without any disruption to your users.

- **Cloud Interconnect:** Cloud Interconnect is a dedicated, high-performance connection between your on-premises network and Google Cloud. Cloud Interconnect can be used to replicate your data and workloads to Google Cloud for disaster recovery. You can also use Cloud Interconnect to connect your DR environment to your production environment. This way, if there's a disaster in your production environment, you can quickly switch to your DR environment without any disruption to your users.

Designing a DRP with RPOs and RTOs in Google Cloud

DRP design factors

When designing a DRP in Google Cloud, it's important to consider these factors:

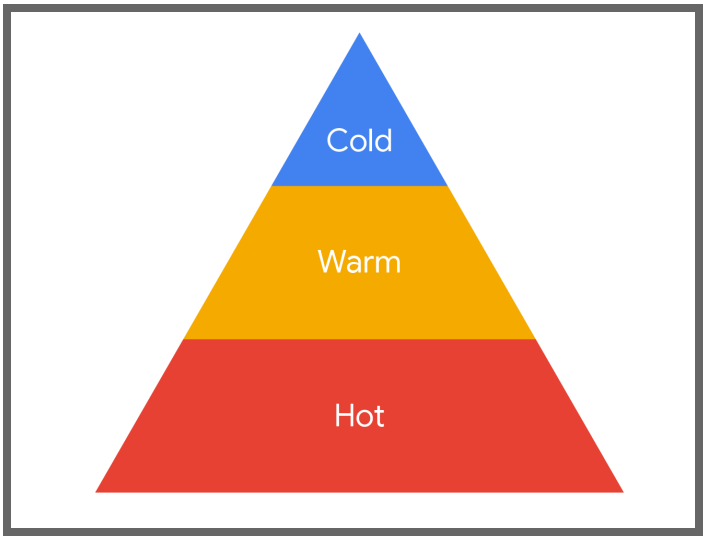
- **RPO:** the maximum acceptable amount of time for data to be lost from an application because of a major incident
    - A **low RPO**—less than 2 hours—indicates a business can afford little or no data loss time
    - A **medium RPO**—between 2 and 24 hours—indicates a business can afford little or some data loss time
    - A **high RPO**—between 1 and 7 days—indicates a business can afford a longer data loss time
- **RTO:** the target time allowed for the recovery of a service in the event of a disaster
    - A **low RTO**—between 5 and 60 minutes—indicates a business can afford little or no data loss time
    - A **medium RTO**—between—1 and 8 hours—indicates a business can afford little or some data loss time
    - A **high RTO**—between 8 and 24 hours—indicates a business can afford a longer data loss time
- **Workload requirements:** the requirements of your applications and workloads, including availability, performance, and security
- **Budget:** the amount of money that you're willing to spend on your DRP

DR patterns

Once you've considered the DRP design factors, you need to plan your responses to DR patterns. DR patterns indicate how your system's site environment can recover from a security incident. There are three parts to the DR pattern: cold, warm, and hot. Here's an explanation of each, according to the National Institute of Standards and Technology (NIST):

1. **A cold site** is a backup facility that has the necessary electrical and physical components of a computer facility, but doesn't have the computer equipment in place. The site is ready to receive the necessary replacement computer equipment in the event that the user has to move from their main computing location to an alternate site.
2. **A warm site** is an environmentally conditioned work space that's partially equipped with information systems and telecommunications equipment to support relocated operations in the event of a significant disruption.
3. **A hot site** is a fully operational offsite data processing facility equipped with hardware and software, to be used in the event of an information system disruption.

These three pattern levels are comparable to how you might respond to an unexpected weather cold front that moves in and turns the temperature outside to ice cold. Here's an example:



- **Cold** weather requires you to take immediate action. Your warm clothes are in a different location than you are, so you need to request their quick delivery from their local storage location. You also need time to clean the clothes before you wear them, since they haven't been used recently.
- **Warm** weather requires you to take action soon. You have a set of warm clothes at your location, but you need time to clean the clothes before you wear them, since they haven't been used recently.
- **Hot** weather requires you to schedule action in the near future. You have two sets of hot weather clothes at your location, and they're both kept clean and ready to wear. So if one set is damaged, you have a full, equal set of clothes that you can use right away.

For more information, please check out this resource: CISSP Study Guide: Disaster Recovery - Hot, Cold, and Warm Sites.

Connect DR patterns with RPO and RTO

Once you've chosen a site you're ready to choose the appropriate Google Cloud services and tools to implement your DRP. Here are some examples of how you can use Google Cloud services and tools to design a DRP with different RPOs and RTOs:

- **Low RPO and low RTO:** Use the **Cloud Backup and Data Recovery (DR) Continuous Data Protection (CDP)** feature, which provides continuous replication of data at the block level, ensuring that the most recent data is immediately available for recovery in the event of a disaster. You can also use the **Replication to Multiple Regions** feature, which provides redundancy and disaster protection. This way, if there's a disaster in your primary region, you can quickly switch to the secondary region without losing any data. These features are both **hot DR,** meaning they minimize data loss and help achieve a low RPO and RTO.
- **Medium RPO and medium RTO:** Use **Cloud Storage** to store daily backups of your data, as this is a **warm DR** that can tolerate a few hours of downtime. You can then schedule regular backups and restore your data from the backups in the event of a disaster.
- **High RPO and high RTO:** Use **Cloud Storage** to store weekly backups of your data to make use of a **cold DR** site. A cold DR site is a replica of your production environment that isn't kept up to date with your production data. You can then restore your data to the cold DR site in the event of a disaster and start your applications up.

Key takeaways

When designing a DRP, it's important to consider your needs related to your RPO and RTO, as well as your DR cold, warm, and hot patterns. Google Cloud offers a variety of services and tools that can help you build a DRP that meets your business' needs. When you build a DRP, you prepare for the worst. But remember, when your DRP is effective and resilient, you can expect the best outcome.

Resources for more information

For more information on DRP in Google Cloud, please visit these resources:

- Google Cloud Best Practices for Disaster Recovery: https://devops.com/cloud-disaster-recovery-best-practices/

- Google Cloud blog post on best practices for building a DRP: https://medium.com/google-cloud/disaster-recovery-on-google-cloud-for-data-part-1-9cf08782bac9
- Google Cloud Disaster Recovery: https://cloud.google.com/backup-disaster-recovery/docs
- Google Cloud Disaster Recovery Planning Guide: https://cloud.google.com/architecture/dr-scenarios-planning-guide
- Google Cloud Disaster Recovery Services: https://www.techtarget.com/searchdisasterrecovery/definition/cloud-disaster-recovery-cloud-DR