Disaster Recovery with Huawei Cloud

Cloud Disaster Recovery Considerations and Options with Huawei Cloud

Cloud deployments are growing around the world. Indeed, analyst firm IDC expects spending on cloud IT infrastructure spending to reach $92 billion in 2023, or 58.1% of total IT infrastructure spend. Of this, public cloud data centres will account for 66.3% of this amount.

Properly designed, cloud deployments are known for their robustness. Yet regardless of how well systems are designed, they will inevitably fail. This can happen from various reasons ranging from inopportune hardware failures, insider attacks, or even human errors.

The onus is hence on users to establish the appropriate backup and disaster recovery plans to keep their cloud systems running.

Section A: Getting Started with Cloud Recovery

There is no question that a cloud deployment necessitates a cloud-based backup. In this section, we look at the advantages of cloud disaster recovery, common mistakes, and top considerations when it comes to cloud disaster recovery. The next section will cover specific Huawei Cloud services designed to support cloud backup and recovery.

Advantages of Cloud Disaster Recovery

Disaster recovery in the cloud is different from protecting a typical on-premises deployment. For a start, applications are typically encapsulated within a virtual machine (VM). Because the VMs are essentially hardware-independent, there is substantially greater flexibility and convenience in replicating VM images between storage repositories or even data centres.

Here are some of the advantages of cloud disaster recovery:

- **Rapid recovery:** The cloud offers speedier backup Recovery Time Objective (RTO) and Recovery Point Objective (RPO), allowing enterprises to get up and running again quickly in the event of a disaster. Of course, various configurations such as firewall rules and network topology must be correctly recorded for this to work.

- **Lower cost**: Unlike traditional infrastructure, enterprises do not have to acquire redundant physical servers or set up a new data centre for cloud disaster recovery. Costs are usually limited to backups and associated data transfers to guard against data corruption, and the cost of load balancers and architecture-level tweaks to facilitate disaster recovery.

- **Scalability**: With a cloud-based disaster recovery strategy, enterprises benefit from the inherent scalability and pay-as-you-go model of the cloud. With periodic tweaks, a well-designed disaster recovery strategy should continue to work as the enterprise grows.

Of course, the situation will evolve with the development of cloud-native applications. Newer cloud methodologies such as serverless architecture or containers will require a slightly different touch. Finally, managed cloud databases also require a different approach to backup that is not addressed in this white paper.

https://www.information-age.com/cloud-outages-cloud-security-123483558/

Common Mistakes with the Cloud

One common mistake with cloud backup is attempting to jump in too quickly. Drawing up a successful disaster recovery plan that works requires making a concerted effort to understand the capabilities of the chosen public cloud platform, working out how best to integrate them with your hybrid cloud deployment, and then implementing it.

Cloud vendor lock-in is a common fear of enterprises. For some, this culminates in attempts to reinvent the wheels by incorporating all systems within VMs for portability. Such an approach negates many of the advantages of the cloud, however, including cost effective services such as managed databases and data warehousing services – a managed cloud offering takes care of time-consuming tasks such as patching and data backups, greatly simplifying both maintenance and disaster recovery.

Finally, enterprises know that unmonitored systems are a receipt for bill shock. This applies to cloud disaster recovery, where ballooning storage use, frequent data backups of unimportant systems, and use of higher performance storage for mundane data archival can creep in over time.

Key Considerations to Cloud Recovery

Designing and deploying a cloud disaster recovery plan is a typically done as a team effort and cannot be fully covered within a single white paper. That said, we highlight some of the key considerations that should not be overlooked below.

Storage	It is vital to accurately size the storage requirements for your disaster recovery plan. There are templates and calculators that can be found online to estimate required storage space using information such as backup frequency and approach.
Hybrid Cloud	Hybrid cloud deployments are becoming increasingly common with the growth of the public cloud. This can offer more options for disaster recovery, but also adds to the complexity.
Cost	While the cloud offers cheaper disaster recovery, this can vary depending on the desired recovery window. If multiple availability zones and real-time database synchronisation is required, expect the cost to go up.

Section B: Huawei Cloud Backup and Recovery

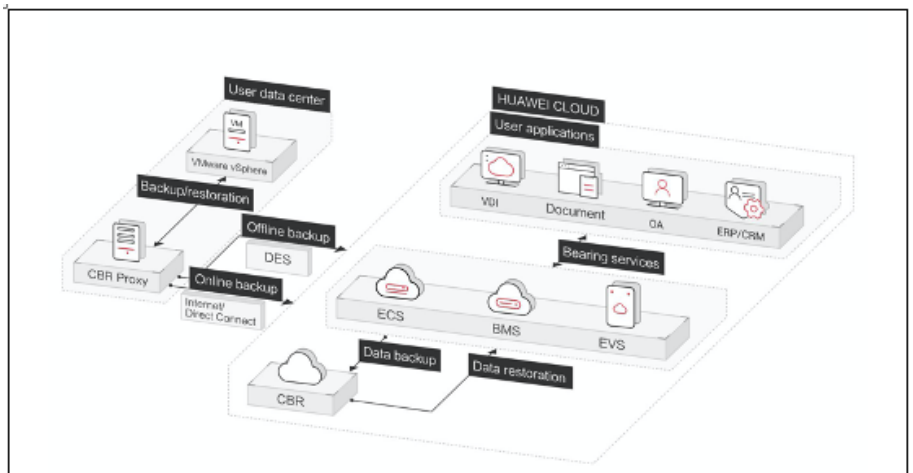
Designed to back up your Huawei Cloud infrastructure, the Cloud Backup and Recovery (CBR) service lets you back up a cloud and on-premises environment with ease. This allows enterprises to quickly recover from disasters such as malware infestations, system failures, corrupted data, or human errors.

Product Architecture

A CBR backup consists of three components: backups, vaults, and policies. The service can perform data backups of Elastic Cloud Servers (ECS), Bare Metal Servers (BMS), Elastic Volume Service (EVS), or Scalable File Service (SFS). It also works with on-premises VMware vSphere deployments through a proxy such as OceanStor BCManager. CBR uses vaults to store backups. Before initiating a backup, at least one vault must be available and associated with the server or disk. Note that the total capacity of the resource to be associated cannot be greater than the capacity of the vault.

There are four distinct types of backup types available.

- **Cloud Server Backup**: System and data disks on a server.
- **Cloud Disk Backup**: One or more specified data disks.
- **File System Backup**: SFS file systems (Used for shared file storage).
- **Hybrid Backup:** Synchronising on-premises VMs to the cloud.



Application scenarios for backup and restoration on Huawei Cloud

Performing a Backup

Backups are performed through backup policies. This can be configured by establishing the execution time of backup tasks, backup cycles, retention rules, and then binding a vault to the policy. Note that a vault can be bound to only one backup policy, and only a maximum of 32 backup policies can be created currently[1].

To set up a backup, a vault must first be purchased from the CBR Console. Once purchased, you will need to associate a resource with the vault to perform the backup. Note that the servers to be associated must be in the Running or Stopped state, while the disks to be associated must be in the Available or In-use state. The file systems to be associated must be in the Available or In-use state.

Vaults can be deleted, associated with a resource, expanded in capacity, or replicated from the CBR Console. Backups stored within a vault can similarly be deleted and replicated across more than one cloud region. Backups can also be shared with other projects, where they can be used to **c**reate a machine image or to create a file system. Finally, the use of Huawei Cloud's Identity and Access Management (IAM) service[1] is recommended for fine-grained permissions management. IAM provides identity authentication, permissions management, and access control, helping secure access to cloud resources.

A cost calculator for using CBR can be accessed here

Important tips:

- Use custom scripts to implement application-consistent backups for database management systems (DBMS).
- When backing up selected disks, ensure that all dependent volumes are backed up to avoid data inconsistency and cause applications to fail.
- Only single VMs are supported right now. Support for clustered databases will be implemented later .

https://www.huaweicloud.com/intl/en-us/product/cbr.html
https://support.huaweicloud.com/intl/en-us/bestpractice-cbr/cbr_07_0016.html
https://support.huaweicloud.com/intl/en-us/productdesc-cbr/cbr_01_0009.html
https://www.huaweicloud.com/intl/en-us/product/iam.html

Support for Hybrid Backup

As mentioned earlier, CBR also supports on-premises deployments through OceanStor BCManager[1]. Huawei OceanStor BCManager is a cloud-oriented disaster recovery and backup management software designed for enterprise-class data centres. It synchronises cloud backups and works with standard VMware VM to create disk snapshots and Changed Block Tracking (CBT) for incremental backups. This integration means Huawei can support hybrid cloud deployments, ensuring that on-premises deployments are always available in the cloud.

Start with Huawei Cloud

Get started on your cloud journey with Huawei Cloud. Let us help you build a hybrid IT deployment to empower your organisation. Contact us to find out more about Huawei Cloud and learn aboutour promotional bundles.

###

[1] https://support.huaweicloud.com/intl/en-us/hcbkp-fg-cbr/cbr_03_0054.html