Innovation of Disaster recovery wid ibm Cloud virtual

1. **Cloud Resiliency Orchestration**:
IBM Cloud provides tools to automate the failover and failback processes, making disaster recovery more efficient and reliable.

2. **Global Data Centers**:
IBM Cloud has data centers located around the world, allowing for geographic redundancy. This means your data can be replicated to different regions for added protection.

3. **Multi-Cloud Integration**:
IBM Cloud supports multi-cloud strategies, so you can integrate with other cloud providers and on-premises systems for a more robust disaster recovery plan.

4. **Hybrid Cloud**:
You can use IBM Cloud for both public and private cloud solutions, which can be essential for hybrid cloud disaster recovery strategies.

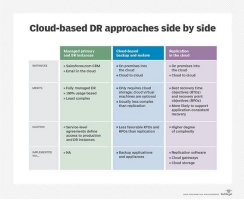
5. **AI and Automation**:
IBM Cloud uses artificial intelligence and automation to help predict and mitigate potential disasters, allowing for proactive disaster recovery planning.

6. **Security and Compliance**:
IBM Cloud offers robust security features and compliance certifications to help protect your data during disaster recovery.

7. **Disaster Recovery as a Service (DRaaS)**:
IBM Cloud provides DRaaS solutions, which means you can have a managed service to handle your disaster recovery needs.

cloud-based disaster recovery needed

With a cloud disaster recovery strategy, critical data and applications can be backed up to a cloud-based server. This enables quick data recovery for businesses in the wake of an event, thus reducing downtime and minimizing the effects of the outage.



cloud disaster recovery work

Cloud disaster recovery takes a very different approach than traditional DR. Instead of dedicated servers staged with the OS and application software and patching to the last configuration used in production, cloud disaster recovery captures the entire server Image in storage, which includes the operating system, applications, patches, and data into a single software bundle or virtual server image, waiting to be deployed in the event of a disaster.

The virtual server Image in the Cloud can be delta synced with the origin server during steady state and most importantly restored, or spun up, on a virtual machine in minutes.

Since the virtual server Image is not dependent on pre-installed hardware, the operating system, applications, patches, and data can be migrated from one data center to the Cloud much faster than traditional DR approaches.
age
What is Cloud Computing? Cloud Computing Concepts Hub Migration
What is Disaster Recovery?

What is Disaster Recovery?
Disaster recovery is the process by which an organization anticipates and addresses technology-related disasters. The process of preparing for and recovering from any event that prevents a workload or system from fulfilling its business objectives in its primary deployed location, such as power outages, natural events, or security issues. Disaster recovery targets are measured with Recovery Point Objectives (RPO) and Recovery Time Objectives (RTO). The failures handled by disaster recovery tend to be rarer than those covered by high availability and are larger scale disaster events. Disaster recovery includes an organization's procedures and policies to recover quickly from such events.

Why is disaster recovery important?
A disaster is an unexpected problem resulting in a slowdown, interruption, or network outage in an IT system. Outages come in many forms, including the following examples:

An earthquake or fire
Technology failures
System incompatibilities
Simple human error
Intentional unauthorized access by third parties
These disasters disrupt business operations, cause customer service problems, and result in revenue loss. A disaster recovery plan helps organizations respond promptly to disruptive events and provides key benefits.

Ensures business continuity
When a disaster strikes, it can be detrimental to all aspects of the business and is often costly. It also interrupts normal business operations, as the team’s productivity is reduced due to limited access to tools they require to work. A disaster recovery plan prompts the quick restart of backup systems and data so that operations can continue as scheduled.

Enhances system security
Integrating data protection, backup, and restoring processes into a disaster recovery plan limits the impact of ransomware, malware, or other security risks for business. For example, data backups to the cloud have numerous built-in security features to limit suspicious activity before it impacts the business.

Improves customer retention
If a disaster occurs, customers question the reliability of an organization's security practices and services. The longer a disaster impacts a business, the greater the customer frustration. A good disaster recovery plan mitigates this risk by training employees to handle customer inquiries. Customers gain confidence when they observe that the business is well-prepared to handle any disaster.

Reduces recovery costs
Depending on its severity, a disaster causes both loss of income and productivity. A robust disaster recovery plan avoids unnecessary losses as systems return to normal soon after the incident. For example, cloud storage solutions are a cost-effective data backup method. You can manage, monitor, and maintain data while the business operates as usual.

Prevention

To reduce the likelihood of a technology-related disaster, businesses need a plan to ensure that all key systems are as reliable and secure as possible. Because humans cannot control a natural disaster, prevention only applies to network problems, security risks, and human errors. You must set up the right tools and techniques to prevent disaster. For example, system-testing software that auto-checks all new configuration files before applying them can prevent configuration mistakes and failures.

Anticipation

Anticipation includes predicting possible future disasters, knowing the consequences, and planning appropriate disaster recovery procedures. It is challenging to predict what can happen, but you can come up with a disaster recovery solution with knowledge from previous situations and analysis. For example, backing up all critical business data to the cloud in anticipation of future hardware failure of on-premises devices is a pragmatic approach to data management.

Mitigation

Mitigation is how a business responds after a disaster scenario. A mitigation strategy aims to reduce the negative impact on normal business procedures. All key stakeholders know what to do in the event of a disaster, including the following steps.

Updating documentation

Conducting regular disaster recovery testing
Identifying manual operating procedures in the event of an outage
Coordinating a disaster recovery strategy with corresponding personnel

disaster recovery important

A disaster is an unexpected problem resulting in a slowdown, interruption, or network outage in an IT system. Outages come in many forms, including the following examples:

An earthquake or fire
Technology failures
System incompatibilities
Simple human error

Intentional unauthorized access by third parties
These disasters disrupt business operations, cause customer service problems, and result in revenue loss. A disaster recovery plan helps organizations respond promptly to disruptive events and provides key benefits.