Building the Disaster Recovery Plan by configuring replication and testing recovery procedures.

Abstract:

Disaster recovery planning is essential for any business that relies on IT systems. By configuring replication and testing recovery procedures, businesses can ensure that they can quickly recover from a disaster and minimize disruption to their operations.

IBM Cloud virtual servers offer a number of features that make them ideal for disaster recovery planning, such as high availability, scalability, and security.

Step-by-step process for building a disaster recovery plan:

- Identify the critical virtual servers and data.
- Choose a replication solution:

  IBM Cloud offers a variety of replication solutions for virtual servers, including volume replication, instance replication, and live migration. Choose the solution that best meets our needs.
- Configure replication:

  The specific steps involved in configuring replication will vary depending on the solution that we choose. However, there are some general steps that are common to all replication solutions, such as creating a replication relationship between the source and target environments, selecting the virtual servers or data that you want to replicate, and configuring the replication schedule and other settings.

- Test the recovery procedures.

  Once we have configured replication, we need to test recovery procedures to make sure that they work. This involves simulating a disaster and then trying to recover the virtual servers from the replicated copy.
- Document the disaster recovery plan:

  The disaster recovery plan should include information such as a list of the critical virtual servers and data that are protected by the plan, a description of the replication solution that is used, and instructions on how to fail over to the test environment, fail back to the production environment, and restore the critical virtual servers and data from the replicated copy.
- Maintain and review the disaster recovery plan:

  The disaster recovery plan is a living document that should be maintained and reviewed on a regular basis to ensure that it is up-to-date and reflects the current state of IT environment.

By following these steps, can build a comprehensive disaster recovery plan that will help to protect the critical virtual servers and data from disaster and minimize disruption to business operations.

Brief explanation of the above steps

Step 1: Identify your critical virtual servers and data

The first step in building a disaster recovery plan is to identify the virtual servers and data that are essential to the business operations. These are the virtual servers and data that will need to protect with the disaster recovery plan.

To identify the critical virtual servers and data, can consider the following factors:

Impact on business operations:

How much would our business be impacted if a particular virtual server or data set were unavailable?

Compliance requirements:

Are there any compliance requirements that require to protect certain types of data?

Recovery time objective (RTO):

How quickly we need to be able to recover the virtual servers and data in the event of a disaster?

Recovery point objective (RPO):

How much data are we willing to lose in the event of a disaster?

Once you have identified your critical virtual servers and data, we can begin to develop

Step 2: Choose a replication solution

IBM Cloud offers a variety of replication solutions for virtual servers, including:

Volume replication:

Replicate volumes between two different IBM Cloud regions.

Instance replication:

Replicate entire virtual machine instances between two different IBM Cloud regions.

Live migration:

Live migrate virtual machine instances between two different IBM Cloud regions.

Choose the replication solution that best meets our needs.

Step 3: Configure replication

The specific steps involved in configuring replication will vary depending on the replication solution that we choose. However, there are some general steps that are common to all replication solutions:

- Create a replication relationship between the source and target environments.
- Select the virtual servers or data that we want to replicate.
- Configure the replication schedule and other settings.
- Start the replication process.

Example:

To configure volume replication between two different IBM Cloud regions using the IBM Cloud console:

1. Go to the Volumes page.
2. Select the volume that we want to replicate.
3. Click Actions > Replicate.
4. Select the target region and volume where we want to replicate the volume.
5. Click Replicate.

The replication process will begin immediately. Once the replication process is complete, we will have a copy of the source volume in the target region.

Step 4: Test the recovery procedures

Once we have configured replication, need to test our recovery procedures to make sure that they work. This involves simulating a disaster and then trying to recover our virtual servers from the replicated copy.

To test the recovery procedures:

- Create a test environment in the target region.
- Fail over to the test environment by stopping the virtual servers in the production environment and then starting the virtual servers in the test environment.
- Restore the most recent data from the replicated copy.
- Verify that the virtual servers in the test environment are working properly.
- Fail back to the production environment by stopping the virtual servers in the test environment and then starting the virtual servers in the production environment.

Step 5: Document the disaster recovery plan

Once we have tested our recovery procedures and documented the disaster recovery plan, we will have a comprehensive plan in place to protect our critical virtual servers and data from disaster.

The disaster recovery plan should include the following information:

- A list of the critical virtual servers and data that are protected by the disaster recovery plan.
- A description of the replication solution that is used to protect the critical virtual servers and data.
- Instructions on how to fail over to the test environment and how to fail back to the production environment.
- Instructions on how to restore the critical virtual servers and data from the replicated copy.

Step 6: Maintain and review the disaster recovery plan

The disaster recovery plan is a living document that should be maintained and reviewed on a regular basis. This will ensure that the plan is up-to-date and that it reflects the current state of the IT environment.

We should review our disaster recovery plan at least once per year, or more often if there are any significant changes to the IT environment.

Additional tips:

- When choosing a replication solution, consider your RTO and RPO requirements.
- Make sure to test our recovery procedures regularly to ensure that they work as expected.
- Document our disaster recovery plan and make it available to all relevant stakeholders.

Conclusion:

Building a disaster recovery plan is essential for any business that relies on IT systems. By configuring replication and testing recovery procedures using IBM Cloud virtual servers, businesses can ensure that they can quickly recover from a disaster and minimize disruption to their operations.

In short, IBM Cloud virtual servers provide a reliable and scalable platform for building a comprehensive disaster recovery plan. By following the steps outlined in this article, businesses can protect their critical data and applications, minimize disruption to their operations, and ensure that their business is prepared to handle any disaster.