ORACLE | Partner

Oracle Integration Cloud

Disaster Recovery Solution by Conneqtion

conneqtion

ORACLE | Partner

OVERVIEW

ORACLE INTEGRATION CLOUD DISASTER RECOVERY

What is a Disaster?

A disaster is a temporary or permanent disruption, either caused by human error or through natural calamities that can partially or completely disrupt business operations.

Some of the disasters are:

- Force Majeure (earthquakes, floods, fires, etc)
- COVID-19 or similar epidemics
- Cyber attack (mostly intentional, to cause harm to business operations/data)
- Terrorist attacks or wars
- System failure (Hardware & Software)

Why does your business need Disaster Recovery solution?

Technology is an integral part of a business which allows organizations to collaborate and serve their customers in an efficient way. It is one of the main reasons why businesses have started the migration journey to the Cloud for development, growth and to offer better customer experience.

Cloud migration and remote work has posed a series of potential threats to organizations and hence a strategic disaster recovery plan is important to ensure business continuity. A system failure can have a negative impact for businesses depending on cloud applications for document storage and data.

Moreover, it is a must to have a disaster recovery plan ready as per the latest data privacy laws. Failure to adhere to these guidelines can result in compliance issues and a heavy penalty.

A business without a disaster recovery plan, is a business that is ready to disrupt with minor inconveniences, irrespective of the industry and size of business. It can lead to data loss, drop in productivity, increased expenditure and a lack of trust with their customers which impacts their bottom line.

How Disaster recovery works?

Disaster recovery works on the principle of assessing and building a plan of action to restore business critical applications and IT systems up and running after a natural or human error.

There are three different ways to prepare a DR for your business:

- **Preventive:** In this method, it is important to make sure your IT infrastructure is secure using external tools or applications to prevent a major disaster. It includes, but is not limited to, taking timely backup of business critical data or close monitoring of all systems.

- **Detective:** In this method, it is critical to identify when a response is required. It is different from the preventive method and focuses on identifying the problems rapidly as and when it occurs.

- **Corrective:** The third method focuses on planning for a potential disaster recovery plan so that the team as well as the system is ready with the backup to restore lost data and IT systems when needed.

A crucial factor of disaster recovery includes taking a backup of data and applications to a secondary location, also known as disaster recovery sites. A disaster recovery site is used to recover the most recent data. Alternately, businesses can also utilize a DR site if the primary IT system fails, until the primary site is restored.

Advantages of Disaster Recovery

Robust Operations

A disaster can impact your critical business operations which results in data loss, loss of productivity, user experience and more. Disaster recovery can help safeguard business operations and offer an enhanced customer experience.

Security

A carefully crafted DR plan leverages data backup and processes to improve your security posture and reduce the overall impact of an attack. For instance, businesses use advanced encryption, multiple authentication, identity and access management for enhanced security.

Rapid Recovery

Disaster recovery plan is used to get your IT infrastructure back online after an unforeseen attack or event. A good DR plan is built on the back of data replication and automated recovery to reduce the system down time.

Auto failsafe

Current cloud-based solutions have advanced features to support your DR plan. It comes with an auto failsafe and built-in redundancy features to protect business critical data at all times.

Enhanced Compliance

In the unforeseen event of an attack or a threat, DR planning helps define a list of processes and protection policies for your data and applications. It ensures that your business is well prepared and compliant with industry guidelines.

Uses of Disaster Recovery

A comprehensive disaster recovery strategy can help your business in the following ways:

Rapid Resolution

Irrespective of the type of attack/disaster, a good DR strategy can help the business return to normalcy, without jeopardizing data or financial transactions.

Data Protection

It is important to mitigate the risk of data loss and a comprehensive DR plan will ensure that by reducing the downtime.

Avoid Compliance Issues

Various industries have compliance laws that need to be adhered to, in terms of data storage and protection.

Repeat Customers

A robust DR plan can help businesses meet their SLAs, every single time and offer an exceptional customer experience, which often results in repeat business.

How to plan a disaster recovery strategy?

A proper disaster recovery plan must entail a list of emergency response requirements, data backup and failsafe procedures. The primary focus of any disaster recovery strategy is to prepare a process which includes a failsafe plan for IT infrastructure and enabling businesses to resume their operations as soon as possible, in times of distress.

The following key metrics should be considered while creating a successful disaster recovery strategy:

- **Recovery Time Objective (RTO)** - An estimated downtime, post which, a business data and workflow is restored.

- **Recovery Point Objective (RPO)** - Maximum amount of data loss that is tolerable for the business.

RTO and RPO can be better understood with the below examples:

1. For instance, a technical glitch in the Microsoft Exchange Server can hamper the communication exchange between Outlook, Microsoft Calendar and Microsoft Teams. If the RTO is set at one hour, it means that the tolerable downtime is one hour and hence the disaster recovery solution must be planned in a way so that the system is up and running again within an hour to mitigate any serious risk to the business.

2. For RPO, at the time of the disaster, if the most recent data backup is from 5 hours ago, and the standard RPO is 10 hours, then it is in compliance with the current BCDR plan. With the help of RPO, businesses can identify the time at which the recovery process can be adjusted, considering the data loss during that time frame.

How Conneqtion can help you with Disaster Recovery?

Conneqtion Disaster Recovery Plan leveraging OCI services can help reduce the cost related to RTO and RPO, as compared to meeting RTO and RPO requirements on premises. For instance, a conventional DR approach would need the following requirements:

- **Capacity** - Total number of resources for a scalable solution.
- **Security** - Offering security to safeguard physical assets.
- **Network Infrastructure** - Including but not limited to firewalls and load balancers.
- **Support** - Identify, assess and availability of skilled workforce to perform scheduled maintenance in a timely manner.
- **Bandwidth** - Suitable bandwidth to manage peak load.

Conneqtion's 3 Step Approach

Step 1: Planning

Creating a detailed DR plan

The following recommendations are essential to create a robust DR Plan.

1. Customize Your DR Plan

   Conneqtion will design a DR plan according to your recovery goals by assessing your current application and data recovery techniques, current RTO and RPO values and offer the feedback and guidance on which DR method is suitable for your business.

2. End-to-End Recovery Plan

   Taking timely backup of data is just half the battle won. It is essential that we prepare a dynamic DR plan that focuses on the complete recovery process including data backup and restoration.

3. **Identify Specific Tasks**

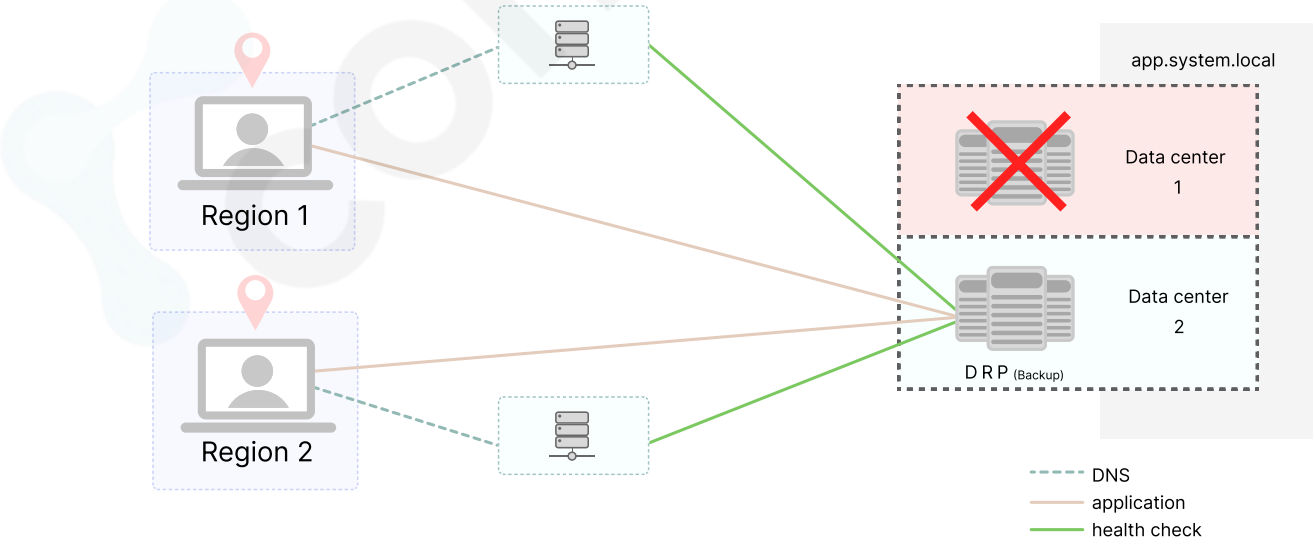
   We will help you identify each task in the DR plan to be performed along with the plan of action. It is best to have specific tasks which are not generic and are aligned to the DR plan.

4. **Finalize the Model**

   Conneqtion will help you finalize the DR model by choosing the environment type, plan, model and advising the switchover type (Auto or Manual).

Once the model is finalized, Conneqtion will work on the Disaster Recovery management architecture which is illustrated in the image below.

Disaster Recovery Management Architecture



5. Identify the RPO and RTO

In this step, Conneqtion will discuss the business critical applications and understand the actual RTO and RPO and advise the planned RTO and RPO based on a detailed analysis.

6. Notify users about the activity

In this step, we will share activity to be performed by Conneqtion where we will notify the business about the downtime.

7. Which Systems will be impacted?

Any application or service using OIC for integration and orchestration will be impacted by the downtime, though the underlying systems that OIC connects with will be accessible during the DR test. In this step, Conneqtion will notify the business about the applications that will be impacted along with the downtime.

8. What is the plan of action?

The systems using OIC for orchestration/integration will be impacted in this process and hence we will be working closely with the owner of the above systems to mitigate the risk and reduce the impact.

Step 2 : Execution

After the planning stage, Conneqtion will start executing the DR solution ensuring the below three key aspects.

1. **Matching RTO and RPO**

   It is important to ensure that your planning works, if and when a disaster occurs, the system works according to the plan.

2. **Multiple Data Recovery Path**

   It always pays to have an alternate solution. In case of a disaster, the connection method to OCI might be temporarily unavailable. In that case, it is best to plan and transfer the backup data to OCI and ensure that the backup path is functional.

3. **Regular Testing**

   Once a DR plan is put in place, it is critical to test it in a timely manner and flag the irregularities that come up during the process.

Step 3 : Calculate the actual RTO and RPO for timeline and cost

In this step, Conneqtion will connect with the business to fill the checklist and after a thorough analysis, come up with the actual RTO and RPO. This will help us identify the estimated timeline of the project.

- **Timeline & Cost :** Post a detailed analysis, we will be able to share the project timeline and cost.

Frequently Asked Questions (FAQs)

1. What are the advantages of the Oracle Disaster Recovery solution?

A disaster recovery (DR) solution enables you to recover quickly from natural or human-made disasters and continue to provide services to your users. In addition, you can use the DR set up for planned migrations and switch between different regions periodically.

2. What steps can be taken if the whole Data Centre goes down?

Conneqtion recommends to have backups in cross region and local peer region in order to avoid any downtimes.

3. Is there a possibility of database downtime while implementing a DR solution?

Yes, it will be minimal and that is where RTO and RPO will be planned with customer beforehand.

4. What if we are having Oracle DBaaS or DBCS instead of ATP?

Disaster recovery is possible with both Oracle Database.

5. Is it possible to use normal data guard so there is no data loss during database downtime?

Yes it can be used, but it would be better to know RTO and RPO which will help us understand which data guard is best suitable for the customer.

6. How will you ensure that RTO and RPO match as per our business requirements?

We follow certain standard operating procedures during the execution which ensures that customer's business is not impacted.

7. What is the estimated timeline of DR solution implementation?

The timeline will depend on various factors listed below like:

1. Number of integrations
2. Number of objects in the database
3. Number of VBCS applications
4. Number of PCS applications
5. Number of APEX applications

8. How much time does it take to conduct a DR drill? Will it impact business critical applications?

As per our past experience, it takes roughly 6 to 24 hours based on the criticality of business, number of regions and total objects involved.

9. Is it possible to implement the DR solution for both Non-Prod and Prod instances?

Yes, it is recommended to proceed with Non-Prod DR drill and then move to production environment.

10. Which applications will be impacted during the downtime?

Applications using Oracle Integration Cloud will be impacted as per RTO and RPO timelines.

11. Which applications/processes are not supported?

1. Processes under Process Cloud Service is not supported due to limitations from Oracle on CI/CD
2. Insights
3. B2B

12. What is the minimum BOM (bill of material) for Disaster recovery configuration?

It is recommended to have similar message packs for secondary instance as per the primary to support the transaction load during failover, however the minimum is 1 message pack is required in order to proceed with DR.

For any business inquiries
contact us on

business@conneqtiongroup.com
www.conneqtiongroup.com