QUISTOR
Is now broadpin

Quistor disaster recovery as a service

WHITEPAPER

ABOUT BROADPIN

At Broadpin, we empower enterprises through tailored Oracle solutions, combining global reach with local expertise. As a unified force of top-tier Oracle partners, we deliver AI-driven, cloud-enabled, and industry-specific strategies backed by world-class managed services. Our mission is to guide transformation with precision, helping businesses drive long-term success.

You might already know us as:

QUISTOR · Project Partners · PROMATIS · PITSS Simplifying Complexity · ITG International Technology Group

Mission

To be the most trusted Oracle partner in the world: a driving force that turns complexity into clarity, potential into progress, and technology into lasting business value.

Vision

To create a future where expertises worldwide are empowered to innovate confidently, operate resiliently, and thrive sustainably through Oracle technology.

broadpin
Your solution is here.

The key aspects of Disaster Recovery in the Cloud

In 2018 Schiphol Amsterdam Airport was hit by a power outage. All systems were down and many travelers were stuck at the airport for several hours. Also, many companies in this same region were impacted by this power outage causing system disruption. What would happen if your company was affected by a similar disaster? How would this impact your business and stakeholders?

For most companies' business continuity goes parallel with IT or Technology systems which are supporting critical business functions. In case of a disaster from a natural cause, human errors or cyber-attacks, companies must be able to safeguard business continuity in order to prevent major losses in revenue.

In general, “Disaster Recovery” consists of three main areas of attention:

- Prevention: avoidance of those disasters that are listed above.
- Anticipation: preparing effective responses to unavoidable disasters.
- Mitigation: ensuring a disaster and its aftermath to have the least negative impact.

When considering IT disaster recovery strategies, remember there is more to protect than just your server room. For example:

Hardware
Including your desktop computers, laptops, handheld devices, server racks, and other network equipment

Connectivity
Your primary and secondary connections internally and to your service provider: fiber, cable, wireless, Ethernet.

Software applications
ERP management, office productivity, databases, email, proprietary in-house applications.

Data and restoration

- How often is your data backed up? On what media?
- How soon after a disaster has been declared will you be able to access it?
- What is the time frame where some data might be unavoidably lost?

And, yes, your server room Is it contained in a secure, climate-controlled room with backup UPS?

The Basic Goals for Your Disaster Recovery Plan:

- Minimal disruption of core business operations
- Quickly restored operations to a pre-disaster state
- Maintained security levels before, during, and after a disaster
- Maintained, up-to-date backup systems

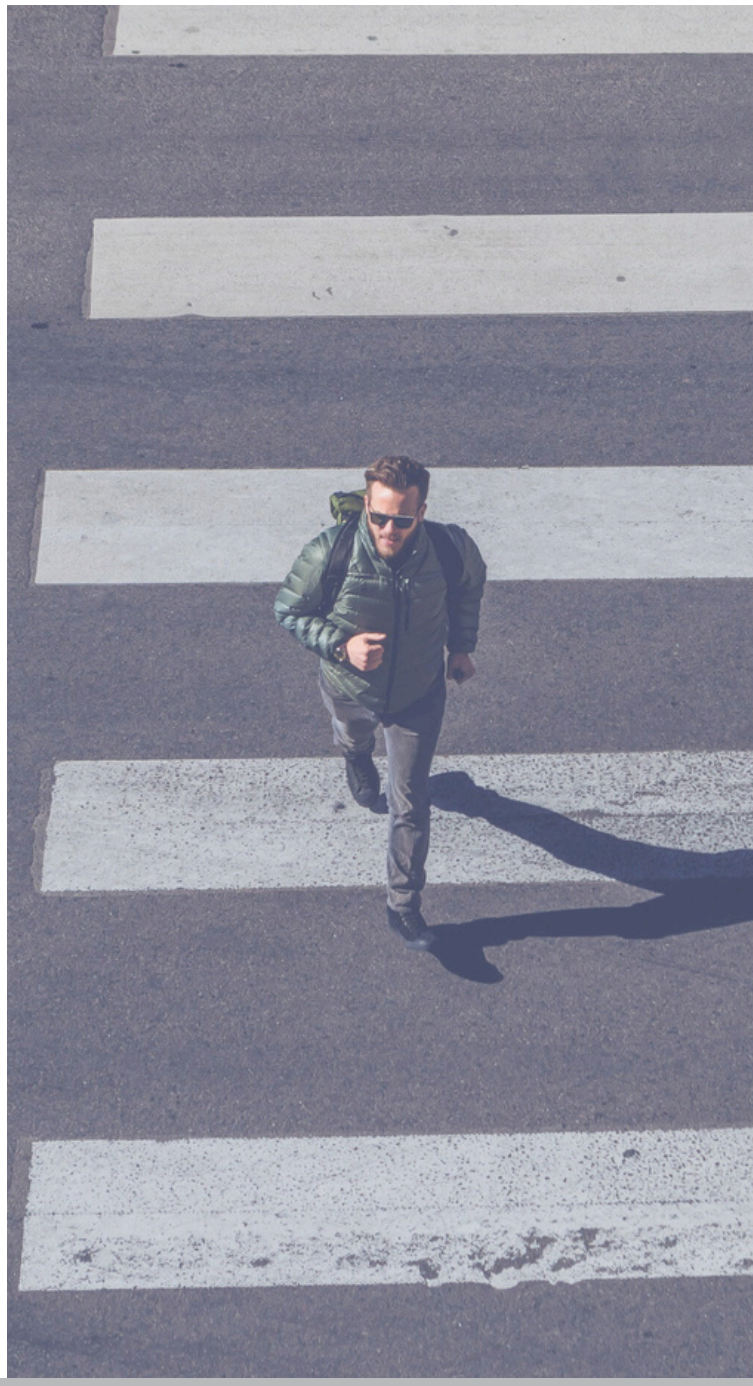
IT Disaster Recovery Plan (DRP)

Your Managed Services Provider (MSP) should work with you to prepare a comprehensive plan that details all of the steps to take before, during and after any particular catastrophe strikes. The MSP should plan a variety of Disaster Recovery Plans that should fit the needs of the company, not the other way around.

Different coverage levels generally fall into three main categories.

- This is for businesses that require real-time Disaster Recovery solution to have zero data loss or downtime. Usage of fully managed services, 24/7/365 monitoring and the latest technology solutions for data recovery and bringing up operations.
- When businesses can afford more downtime then data should be backed-up when transactions occur. Daily checks of operations are highly recommended.
- Businesses that can allow for interruptions and have fewer recovery timeline restrictions. Your data would be backed up on a regular basis in the cloud.

SHOULD A DISASTER OCCUR, THE MSP WOULD RESTORE YOUR DATA SO YOU CAN FOCUS ON



Disaster Recovery in the Oracle Cloud

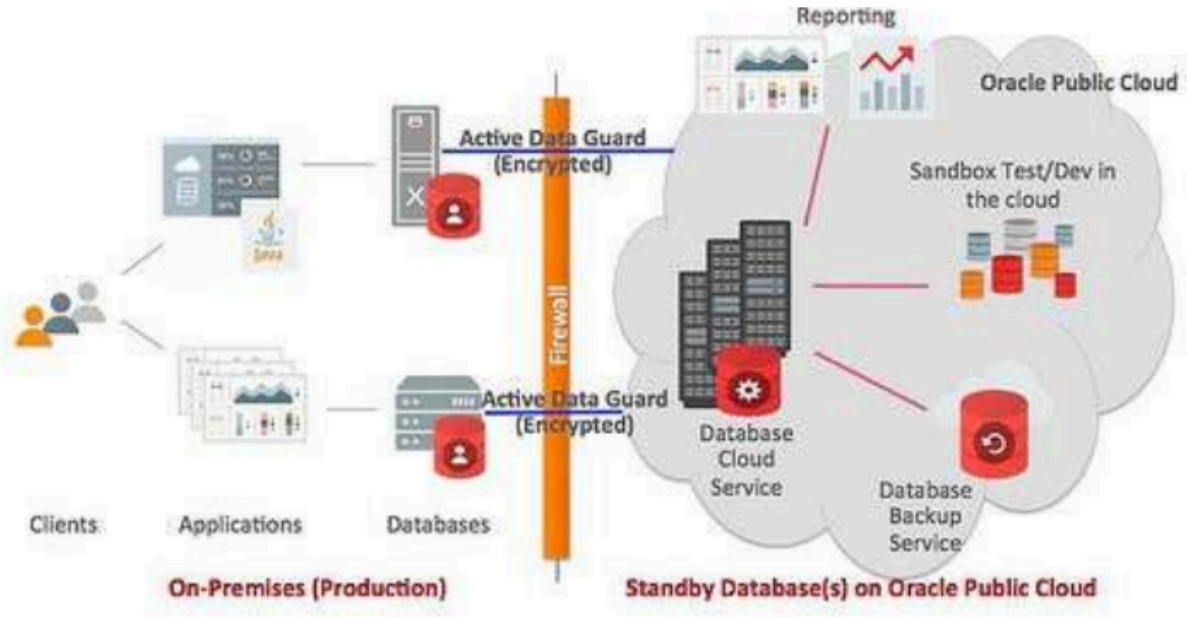
TStill, many companies run their DR environment On-Premise. An effective disaster recovery plan On-Premise can be costly due to the need to establish, equip and manage a remote data center. What makes the cloud so well suited for disaster recovery?

The following benefits are applicable:

- Saving resources as it does not require a huge upfront investment in setting up a duplicated datacenter.
- Faster response to a disaster, due to use of automation and orchestration tools to automate the in-cloud recovery process.
- More flexible, disaster recovery facilities can quickly and easily be moved to different parts of the world.
- No more resources needed for managing a remote datacenter.

The Oracle Cloud offers a great alternative for hosting standby databases for customers who do not have a DR site or who prefer not to deal with the cost and complexity of managing a remote data center. Existing production databases remain on-premises and standby databases used for DR are deployed on the Oracle Cloud. This mode of deployment is commonly referred to as a hybrid cloud implementation. Customers may choose to deploy either a Data Guard or an Active Data Guard standby on the cloud depending upon their requirements.

The following figure illustrates a hybrid architecture for DR:



We do understand that every company has different needs and business requirements regarding a DR and that the previous figure shows an example of an environment based on Oracle Technology.

What if you want to create a DR for non-oracle technology in the oracle cloud?

Recently we supported several customers moving critical applications towards a DR environment in the Oracle Cloud. One of our customers that is active in the tourism industry did not have any DR solution implemented for its most critical sales application. Once their production server would fail, all their sales, tour operators (B2B/B2C Channels) and many other teams would be affected by this.

What was the actual reason for not having a DR? The answer was simple, having a traditional DR was just too expensive because new hardware and licenses were necessary to duplicate the production environment. Simply said a DR environment is basically a standby environment. Why would you make this investment while you are not using the environment 24x7?

This particular customer was running in a Citrix Environment with Windows Servers several Tomcats, Apaches, SQL servers, Oracle Databases, Active Directory and some other less critical applications. To configure, install and implement the right DR environment it is very important to meet the customer expectations for the DR.

Many companies do have a Cloud strategy or an idea of moving to the Cloud but when it comes to a DR environment customers don't think directly about establishing it in the Cloud. Quistor, as a Managed Service Provider is pro-active, and is able to anticipate what is coming and to think about solutions which can really benefit our customer.

What were the main requirements for this customer?

- For the databases; Recovery Point Objective (RPO) and the Recovery Time Objective (RTO) must be close to zero. The closer these parameters are to zero (faster time to recovery, less amount of lost data), the more effective is the business continuity solution.
- Active - Passive data guard scenarios.
- Non-disruptive synchronization between applications

Competetive price based on the consumption.

- DR on the demand, no upfront investment needed for hardware, licenses etc.
- Scalability, if the recovery of the production environment is going to take more time than expected due to the disaster, you can easily up or downscale or add resources.
- Flexibility of resources. Free to change environments.
- High Performance. The performance must be equal to the performance of their production environment

Why was Oracle preferred?

For this customer, it was key that all their requirements were met, so they decided to test the Cloud solutions from vendors like Amazon, Microsoft and Oracle. In the end, they selected Oracle, but why? All vendors could meet most of the requirements but Oracle excelled in terms of performance and it offered the most competitive pricing. In the past, Oracle wasn't commonly known for being an affordable solution. Recently, Oracle has changed its strategy and now has one of the most competitive price ranges on the market.

THE DR SOLUTION WAS BUILT USING A VARIETY OF TECHNOLOGIES:

- Oracle Data Guard: For synchronizing the Oracle Databases

(In an Active-Active scenario Oracle Active Data Guard is applicable)
- Always On solution for SQL Server
- Rackware: used for synchronizing the applications

DR Installation and Implementation: What to Expect?

The total duration for implementing the DR in the Cloud took approximately 2 months. The installation took 3 weeks and followed by the testing phase.

Within these 2 months, a lot of time was spent on testing. As a managed service provider it is very crucial in this phase to exchange the information with a customer and understand the customers' requirements.

Due to the project`s strict timeline, Quistor and the customer had to follow a strict schedule to get the results we were looking for.

The key for Quistor as a managed service provider is to tightly collaborate with our customer during the installation phase and final implementation.

The following steps are applicable to the project:

1. First phase: Provisioning the environment in the Cloud, establishing a network, VPN, security rules etc.
2. Second phase: Migration of databases; applications servers; file servers; web servers etc. (In this phase you create an exact copy of the production environment). This migration takes place without stopping the current environment. 3. Third phase: Network configuration of the new cloud environment. Think about files shares; interfaces; load balancers etc.

4. Fourth phase: Technical test. Here we test if everything in the DR is functioning exactly the same as in the production environment. Close collaboration with the customer is crucial in this phase.
5. Fifth phase: Functional test. Check if all applications, environments, and services are working the same as they are used in the normal situation. (Functionalities and performance) Close collaboration with the customer is crucial in this phase too.
6. Sixth phase: Final test by switching over from Production to DR and vice versa.
7. Seventh phase: Go Live.

The wrap-up

Disaster recovery solutions are necessary to help businesses restore operations in the event of a worst-case scenario.

When businesses know they're covered in the event of a disaster, they can keep their focus on tactical and strategic business initiative to increase productivity and continue to develop as a company. As a certified managed service provider Quistor can provide the right tools, support, services, reporting, and analysis to achieve a highly optimized Disaster Recovery environment for both Oracle and Non-Oracle workloads. As a Service provider, we aim to deliver reliability, provide optimal pricing and insights that can help you make better decisions about your cloud strategy

In practice, what can you expect from us? We will help you to automate decisions on your infrastructure needs and acquisition, alert on performance issues, ensure compliance and help determine inefficient usage and optimization plan to reduce cloud costs. We will manage and monitor your systems on a 24/7 basis.

With Quistor as your strategic partner, you can focus on operations for your products and services.

To learn more about Quistor 's managed services and cloud offerings, schedule a free consultation today.

QUISTOR

Is now broadpin

info@quistor.com

www.quistor.com