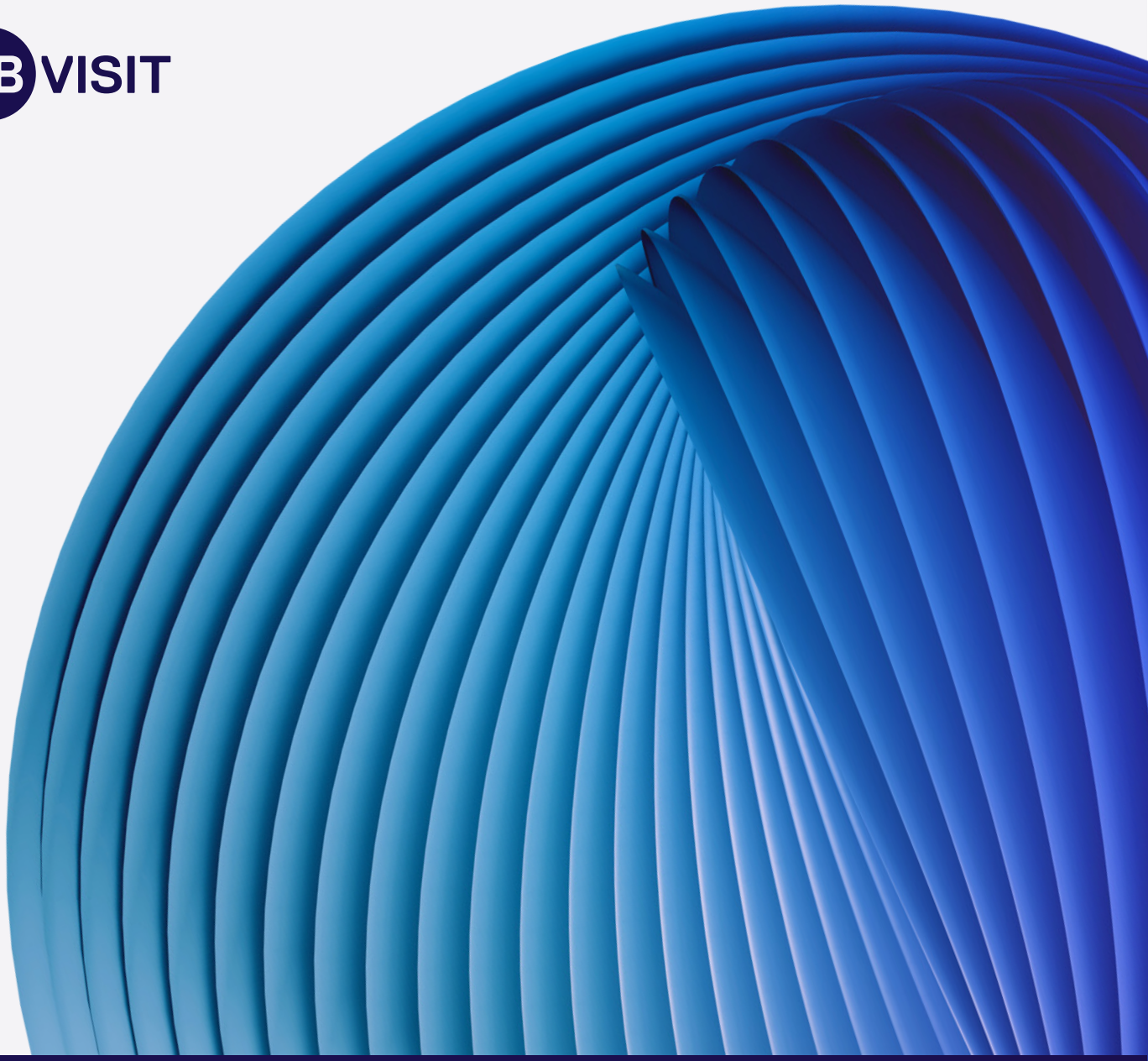


A DBVISIT WHITE PAPER

DO ALL CLOUDS HAVE A SILVER LINING?

Key considerations when migrating databases to the cloud.

INTRODUCTION

Migrating critical databases to the cloud can realize a variety of benefits including improved business efficiency, scale and performance. Cloud adoption can provide fast, efficient and often cost-effective ways to achieve a wide range of IT objectives.

While it is now common practice, migrating to the cloud can still be challenging. The services available are numerous, varied, and often shrouded in the type of 'marketing speak' that makes getting to the 'technical truth' challenging.

When planning your migration, careful consideration must be given to ensure database continuity. As with any on-premise solution, you must carefully evaluate your RPO/RTO requirements and then ensure that your cloud architecture can match these requirements across all disaster types.

In this paper, we will evaluate the key considerations that you must make when locating critical databases in the cloud. We will dispel some common myths surrounding databases in the cloud, and help you avoid some of the hurdles that are often hidden within the contractual small-print and marketing speak.

CLOUD ADOPTION IS GROWING

There is no denying that cloud adoption and migration are on the rise. But just how widespread is it? According to a recent study by Markets and Markets, cloud adoption will continue to grow at a compound annual growth rate (CAGR) of 16.3% between 2021 and 2026.

Similarly, according to Gartner's research, 95% of new data workloads will be hosted in the cloud by 2025, up from 30% in 2021. Gartner analysts said that more than 85% of organizations will embrace a cloud-first principle by 2025 and will not be able to fully execute on their digital strategies without the use of cloud-native architectures and technologies.

Whilst it is relatively easy to migrate noncritical application and workloads to the cloud, most organizations are slightly more resistant to migrate critical databases.

So why the discrepancy? Concerns around data integrity, availability, disaster recovery, sovereignty and performance are the key issues of concern. However, as cloud services have matured, native cloud databases (DBaaS) have become available and PaaS (Platform as a Service) and IaaS (Infrastructure as a Service) adoption has also grown, we are now seeing an acceleration in cloud adoption, even for critical database applications.

Cloud offers a way to scale fast, reduce costs, increase productivity, reduce operations and management overhead. For many organizations, it is not the question of "if" they need to move to the cloud; it is "what is the best strategy to move, and in what time frame".

DISPELLING COMMON CLOUD MYTHS

The trend of cloud adoption and migration is rapidly growing due to the many advantages that cloud computing offers over traditional on-premises approaches. However, **not all clouds are equal and not every cloud has a silver lining**. There are some commonly believed myths that you need to understand and dispel.

Myth 1 - "I'm in the cloud so I don't need Disaster Recovery (DR)"

Perhaps most importantly, moving to the cloud does not just fix all problems. If you have concerns about data integrity and availability risks, moving to the cloud will not instantly mitigate these risks. The reality is that no cloud is immune to downtime, and most people are actually less protected than they think.

As part of your cloud evaluation process, it is essential to deploy a parallel DR solution that meets your RTO/RPO needs. If you do not, then you are responsible for any issues that may arise, not your Cloud Service Provider (CSP).

Embarking on a cloud migration process is an ideal time to re-evaluate your DR strategy and ensure it is updated to reflect the needs of the business' RTO/RPO requirements. By doing this, you will be better placed to evaluate which cloud provider best suits your needs and what supplementary software or services will be required to complete the solution.

CSPs do not typically include resilient DR as part of their stack. Instead, they recommend that you implement out-of-region DR for any business-critical databases. This is very important and often lost in the glossy marketing speak. When evaluating CSPs, it is vital to dig deeper and read the small print. In our experience, many organizations that already have their databases in the cloud are blissfully unaware of how vulnerable they really are. This leads us to the next myth.

Myth 2 - "I'm safe because I have in-region high availability"

On the surface, CSPs will tout features such as "in-region high availability" as a panacea for most disaster recovery requirements. While in-region high availability can offer a good degree of resilience, it is far from being robust protection. So much so, that if you dig into the small print, most CSPs will recommend an out-of-region standby environment for business critical databases with strong RPO/RTO requirements.

Why is this? Well, the truth is that big is not always better and it is not uncommon for entire regions to go down, rendering in-region high availability null and void.

The most recent example (July 2022) occurred in London when the Google and Oracle cloud servers wilted during a record-breaking heatwave (40.3C), dropping networking, storage, and computing resources offline. This was a national phenomenon, taking down the whole region. However, this was just one example, some other notable examples include:

- **December 2021** - Amazon's AWS entire USA East Region experienced a major outage for five hours due to a networking issue.
- **November 2021** - Google Cloud experienced two hours downtime and users experienced 500/502 errors caused by a network configuration glitch.
- **July 2022** - Google Cloud's entire Europe-West2 region zones was impacted by the simultaneous failure of multiple cooling systems resulting in service unavailability for between 18 hours and 33 hours depending on the service.
- **March 2021** - Microsoft's Azure cloud suffered a widespread 14 hour outage due to issues in the rotation of security keys.
- **July 2022 -** Oracle Clouds' UK South (London) region suffered a 21hour service disruption caused by elevated temperatures and the failure of two coolers. This led to compute infrastructure going into protective shutdown.
- **June 2022** - Azure's East US 2 Data Center experienced a cooling failure caused by a power oscillation, resulting in a 12 hour outage of storage and compute resources in that particular availability zone.

"Ok, but my CSP offers me guaranteed uptime" I hear you say. While this is true, it is important not to be suckered in by the marketing hype. While some CSPs will advertise guaranteed uptime, the devil is in the detail. Most 'guarantees' merely offer small rebates if the SLA is not met, usually in the form of fee discounts. It is important to understand the differentiation here, CSPs are not guaranteeing that a service will be available, or ensuring access to your data; they are simply offering modest refunds should this eventuate.

The onus is on you as a user to evaluate your RTO and RPO requirements, and fully understand the cost of any down time to your business.

In addition, quality of service and uptime is not the same. While a region may be available, a host of technical reasons could mean that the service/user experience is temporally degraded. On top of this you have networking and internet backbone issues that can and do frequently occur.

When it comes to protecting your critical databases in the cloud, you need to be 100% confident. CSPs typically do not include resilient DR bundled into their offerings. Instead, they recommend you implement out-of-region DR for business-critical databases.

Myth 3 - "My data is protected because I have backups"

While backups are a necessary part of any DR plan, traditional backups no longer meet the data loss (RPO) and recovery speed (RTO) requirements of most businesses. Backups are also difficult to test and vulnerable to corruption.

WHAT APPROACH IS RECOMMENDED BY CLOUD SERVICE PROVIDERS?

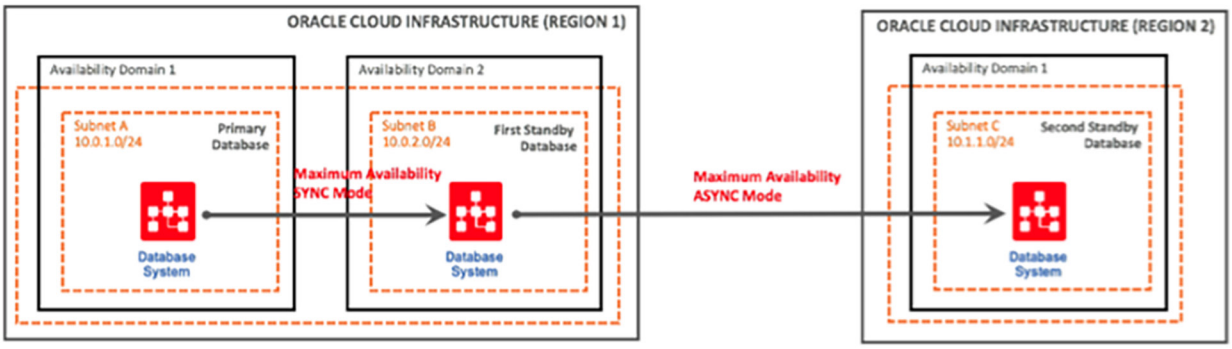
As previously discussed, while Multi-AZ deployments improve resiliency by providing high-availability capabilities to protect from a data center outage, it does not protect from a region-wide outage or performance issue. Multi-AZ configurations comprise of physically separate data centers that are in reasonable proximity to each other. This will provide protection from an outage at a single data center, but not from regional outages, and often not from data corruption.

These regional outages could be due to natural disasters, cloud vendor misconfiguration, malicious attacks, or a host of other factors. For this reason, most CSPs recommend out-of-region replication as the basis of best-practice DR. Because there are hundreds of cloud providers offering a variety of services, we will concentrate on two of the largest - AWS and Oracle - and examine their specific recommendations for highly resilient database architectures.

ORACLE CLOUD INFRASTRUCTURE BEST PRACTICE

Oracle Cloud Infrastructure (OCI) recommends a best practice configuration using Data Guard, where the first standby database is within the same region (using SYNC mode) and a second standby resides in a separate region (using ASYNC mode). This delivers in-region recovery, while also ensuring that the database can be recovered in the event of a complete region outage.

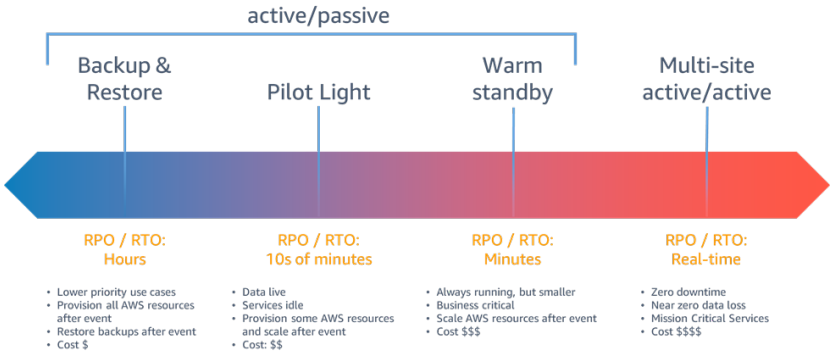
Best Practices for Disaster Recovery in Oracle Cloud Infrastructure – January 2020



For OCI customers running Standard Database Service with Oracle Standard Edition (SE), there is no support for Data Guard and no best practice provided by Oracle. Like Oracle Data Guard, Dbvisit's Standby MultiPlatform (StandbyMP) can be used to provide robust DR for Oracle SE implementations. Additionally, StandbyMP can be used for customers who wish to run a hybrid model, where their primary is on-premises and the standby is in OCI. This is just a summary; Oracle's recommended architecture can be viewed here ("Best practices for protecting your cloud topology against disasters").

AMAZON BEST PRACTICE

For organizations with short RTO/RPO needs, AWS, like Oracle, recommends deploying a standby environment in a separate region to mitigate a complete region outage. For AWS customers this need was highlighted in late 2021 after AWS suffered from multiple outages that took down an entire region.



AWS - Out of region Disaster Recovery Options in the Cloud

SQL Server Best Practice

For SQL Server DBaaS deployments, Amazon's Relational Database Service (RDS) does not support out of region replication. To achieve replication to another region, customers can deploy SQL Server using RDS Custom together with Log Shipping, Asynchronous Availability Groups or the more automated StandbyMP.

For SQL Server IaaS deployments on Amazon's Elastic Compute Cloud (EC2) customers should create a warm standby in a remote region that is continuously updated using Log Shipping, Asynchronous Availability Groups or the more automated StandbyMP. Complementary to this, in-region High Availability (HA) can also be implemented using Amazon's Multi Availability Zones.

Learn more about how StandbyMP compares to Log Shipping and Basic Availability Groups in our SQL Server Disaster Recovery methods whitepaper.

Oracle SE Best Practice

For Oracle SE deployments in AWS, RDS is not currently supported and customers must deploy on EC2 (IaaS). As Oracle Data Guard is not available for Oracle SE, the most trusted method for the creation of a remote warm standby is StandbyMP. Complementary to this, in-region HA can also be implemented using Amazon's Multi Availability Zones.

EVALUATING YOUR RTO/RPO REQUIREMENTS

Before evaluating which cloud provider and architecture is right for you, it is essential to understand your operational requirements in terms of RTO and RPO.

Recovery Point Objective (RPO)

RPO refers to your company's loss tolerance: the amount of data that can be lost before causing significant harm to the business. To put it another way, how much data can you afford to lose? This goal is defined as the time elapsed between the data loss event and the most recent preceding backup.

If you back up all your data daily, then in the worst-case scenario you will only lose 24 hours of data (RPO = 24hrs). This is acceptable for some businesses and applications, but it is disastrous for others. RPOs for business-critical databases will most likely be 30 minutes or less.

It is important you align your architecture with your RPO requirements. This may mean increasing the frequency of your backups or adding a warm standby database. Your architecture should also be resilient and meet your RPO requirements across all disasters.

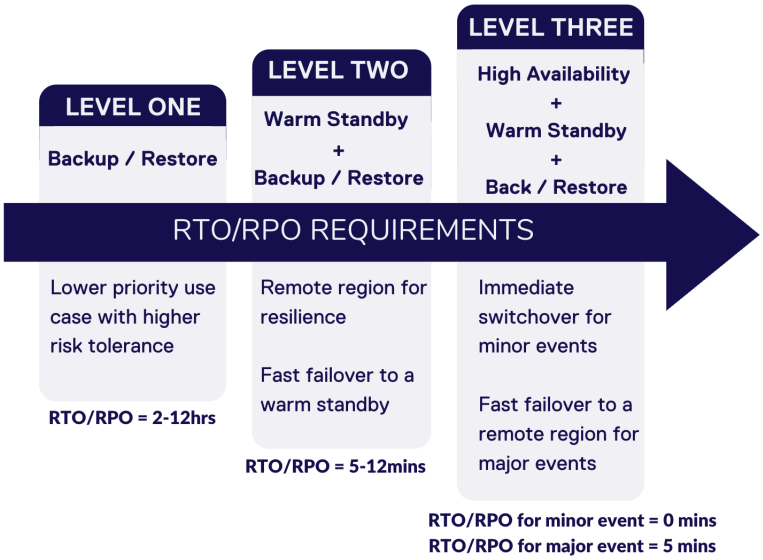
Recovery Time Objective (RTO)

RTO refers to how much time an application can be down without causing substantial damage to the business. That is, the amount of time from the disaster before you can resume business as usual. Note: RTO must take into consideration the steps that must be taken to restore your data and application.

Some applications can be down for days without significant consequences. Some high priority applications can only be down for a few seconds without incurring impact on employees, customers or lost business.

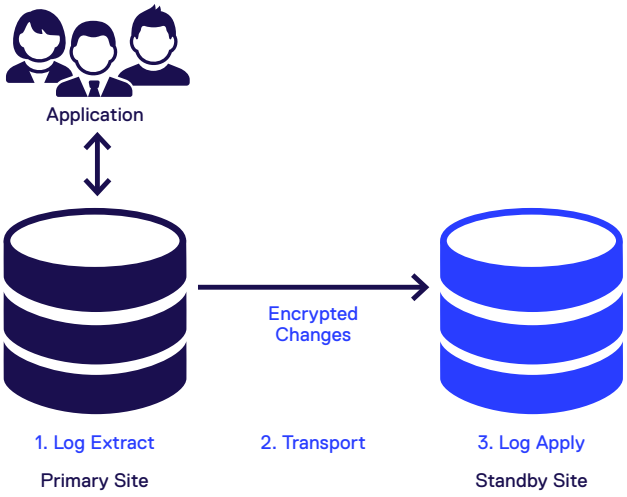
RTO/RPO In The Cloud

When it comes to providing DR capabilities for environments with short RTO/RPO timelines, CSPs identify (albeit in small print) cross-region replication as a best practise. In an ideal world, your data protection would restore all applications and data immediately upon failure. But this is the real world, and while you can design an infrastructure that allows an application to immediately failover and restore data with near-zero loss, these can be very resource-intensive and costly. As a result, businesses must set realistic recovery goals based on their budget, resources, and business priorities. Make sure you define the RPOs and RTOs with your business teams and talk about what they mean for the business in terms of data loss and financials.



USING A STANDBY DATABASE FOR GREAT RPO AND RTO

A warm standby database, either on-premises or in the cloud, is a resilient way to achieve minimal data loss (RPO) and fast recovery (RTO). To achieve this, third party software solutions such as StandbyMP offer cost effective and powerful solutions. StandbyMP for Oracle Standard Edition and SQL Server uses physical replication technology to create a standby database that is continuously verified and updated to ensure successful failover at any time.



StandbyMP delivers a Gold Standard level of Disaster Recovery, complementing CSP's in-region High Availability with a cross-region standby database, facilitation of DR Testing, and controlled switchovers for patching and testing.

Gold Standard Disaster Recovery must:

- Minimize RTO/RPO timeframes across all disasters.
- Ensure resilience through remote standby locations.
- Automate configuration and management to reduce risk of manual errors.
- Continually verify the standby database to guarantee recovery (be database aware).
- Facilitate regular DR testing to validate the end-to-end DR process.

Periodic testing of an organization's end-to-end DR strategy is considered best practice. This allows companies to validate that the system can be successfully recovered when called upon. StandbyMP provides built-in capabilities to streamline this process. DR Testing in the cloud is no different from DR testing an on-premises deployment.

- Utilize automated Graceful Switchovers (zero data loss planned switchovers) for more frequent patching and updates.
- Offer real-time replication and Smart Monitoring.

The standby monitoring components should be installed in a separate region from the primary database to reduce the risk of them being impacted if the primary database fails. For StandbyMP, this is achieved simply by deploying the Central Console on a VM in a different region than the primary.

A HYBRID APPROACH TO ACHIEVING GREAT DATABASE CONTINUITY

Customers who want to keep their primary database on-premises can achieve Gold Standard DR quickly and easily by eliminating local hardware requirements and allowing a database-aware standby environment to be located in a separate geographic region.

As we have already outlined, the key to effective DR is multi-regional support. Having your primary database onsite and a warm standby as a secondary in another region provides the basis of a resilient architecture. Leveraging the cloud for DR is a sensible strategy by removing the barriers of equipment acquisition and personnel shortages, while still allowing close control for your primary.

Solutions such as StandbyMP will offer:

- Implementation in hours, not days or weeks
- Guaranteed integrity
- Multi-threat resilience
- Minimal data loss
- Rapid recovery

CONCLUSION

The cloud is not immune from disasters, whether they are naturally occurring, man-made, or caused by human error. With so much of your organization's business value tied up in its data, it is critical that this data be backed up and protected. Backups, while important, cannot provide the RTOs and RPOs required by modern enterprises. While multiple availability zones improve reliance in cloud environments, they do not provide the necessary protection for environments with short RTO/RPO. As a result, multi-regional standby databases are critical to meeting organizational needs, and third-party software solutions are the best way to supplement existing cloud stacks.

StandbyMP provides that level of readiness for Oracle Standard Edition Databases and SQL Server databases hosted in the cloud. Having your standby database in the cloud makes perfect sense. You can place your DR environment in a different geographic location at a cost-effective price, without having to buy new hardware and worry about where to fit it into your data center.

Easily respond to the unexpected with StandbyMP.

Learn more here, or take StandbyMP for a Test Drive.