CLUMIO
A Commvault Company

eBOOK

Removing Data Protection Roadblocks for Amazon RDS

Commvault®

INTRODUCTION

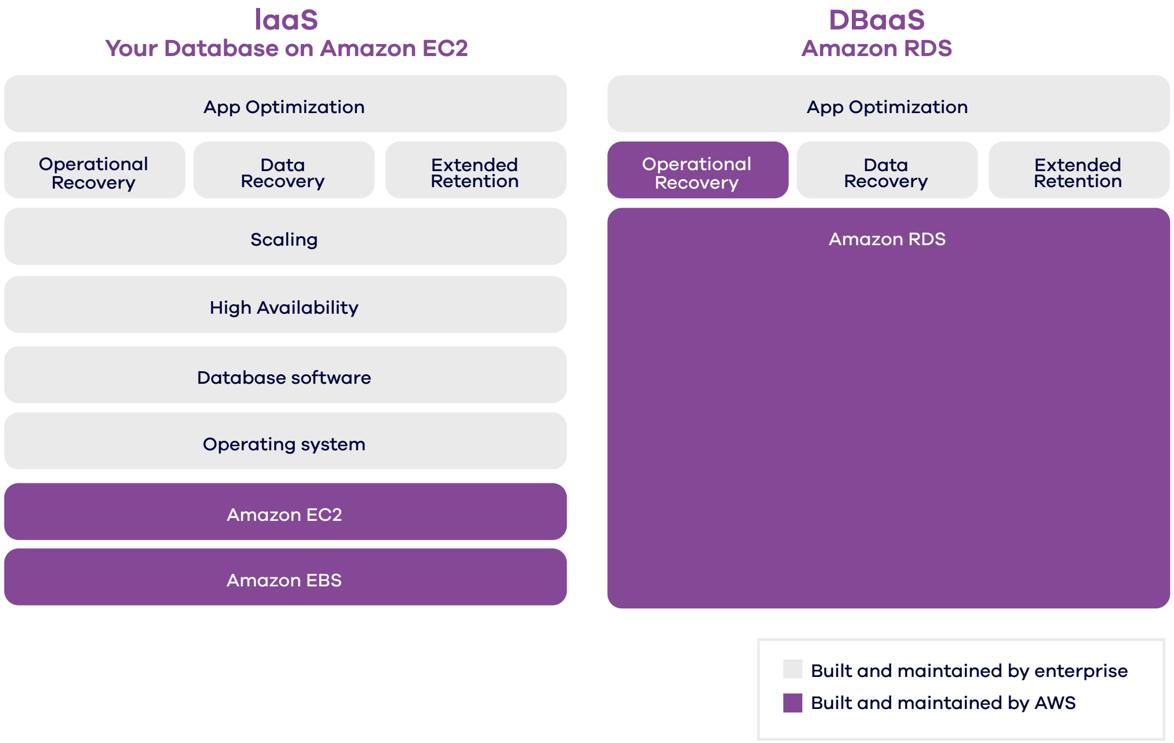
Traditionally, enterprises are known for building their own data centers and hosting operational database systems to store, process, and retrieve data for business applications. These databases were indispensable, could never go down, and had to be nurtured accordingly. These were meticulously built, managed, and upgraded with utmost care. Two megatrends – cloud computing and open-source software – have disrupted the way databases are set up and managed. The popularity of database as a service (DBaaS) offerings from cloud service providers (CSPs) has enabled organizations to treat database systems like a service utility – you spin up as many database instances as needed and spin them down when you are done.

The DBaaS delivery model liberates organizations from setting up and managing what is arguably the most complex and difficult-to-manage layer of enterprise applications – the database. Instead of worrying about provisioning, scaling, monitoring, and managing databases by employing dedicated database administrators (DBAs), now engineering teams can focus on building line-of-business applications with the agility and efficiency from these database engines managed by cloud service providers. Amazon Web Services (AWS) leads the market with Amazon Relational Database Service (RDS).

© 2025 Commvault

WHAT'S BEEN HOLDING RDS ADOPTION BACK?

Database Architectures in AWS



IaaS
Your Database on Amazon EC2

App Optimization
Operational Recovery
Data Recovery
Extended Retention
Scaling
High Availability
Database software
Operating system
Amazon EC2
Amazon EBS

DBaaS
Amazon RDS

App Optimization
Operational Recovery
Data Recovery
Extended Retention
Amazon RDS

□ Built and maintained by enterprise
■ Built and maintained by AWS

RDS has gone mainstream, but some enterprises continue to build their own databases in IaaS environments such as Amazon EC2. At the first look, it is easy to hypothesize that the trend here is to minimize modifications to existing applications. From our conversations with business leaders and cloud architects, we noticed a pattern on this last line of resistance in embracing DBaaS offerings such as RDS for enterprise applications. The bottom line is that customers have two main concerns regarding moving to DBaaS – the first is wanting to control their own data, and the second is concerns about exposure to security breaches and compromised accounts.

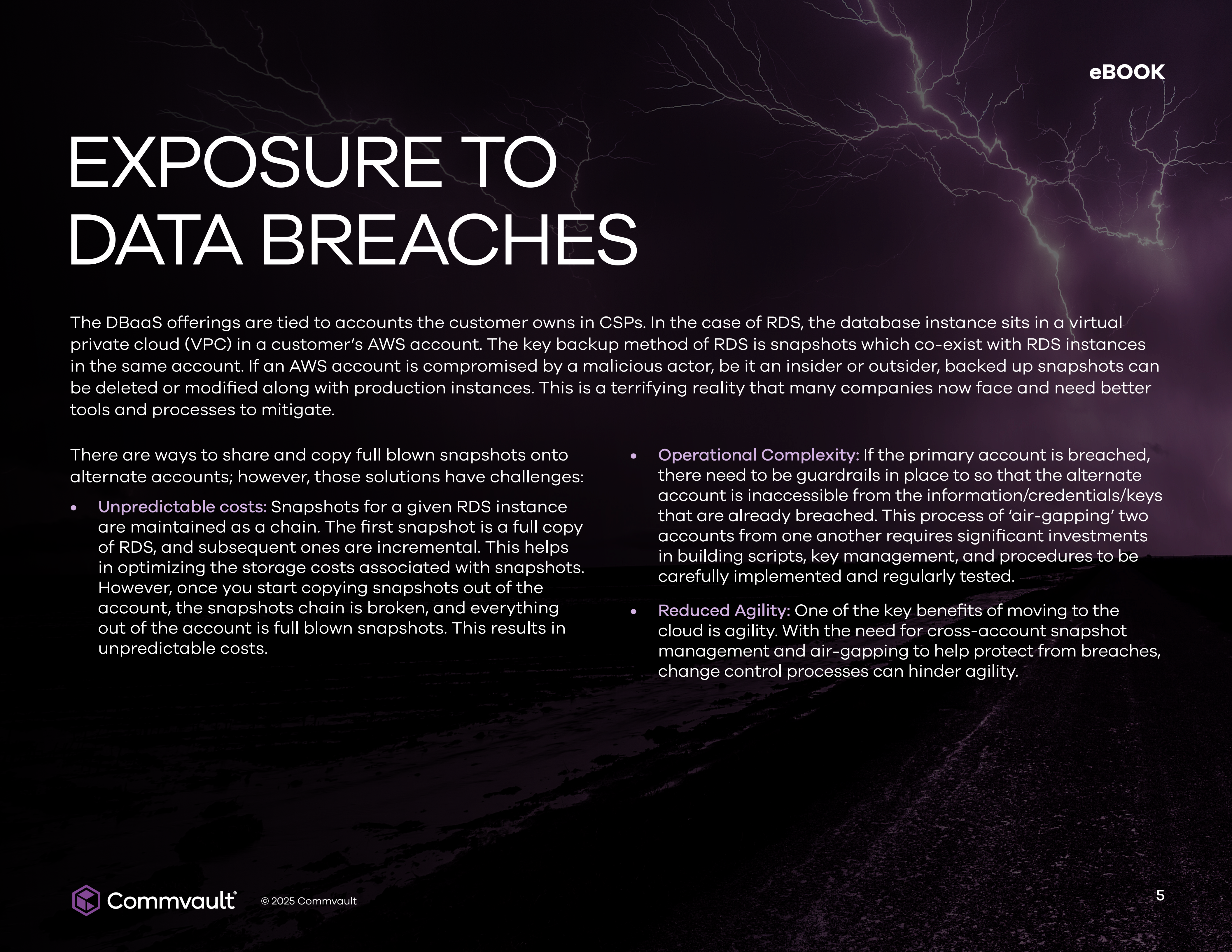
© 2025 Commvault

ENTERPRISES WANT TO CONTROL THEIR DATA

Data from business applications outlive the infrastructure where they currently reside. Enterprises want to ensure that the data is always in their control and may be ported across platforms. Some of the top concerns raised by enterprises tie into the fear of vendor lock-in. While enterprises welcome the agility of cloud computing and yearn to stay away from building and maintaining data centers, they worry that DBaaS may lock their data onto cloud services providers, thereby making it difficult to repatriate data off cloud or migrate to another cloud services provider.

This fear is further exacerbated by limitations in extended retention capabilities of data in DBaaS offerings to meet industry regulations and company policies. The way to perform backups for databases served by Amazon RDS is snapshots which, in turn, are tied to AWS platform. Thus, even if they managed to move off production data with the help of professional or specialized service offerings from third party vendors, they still need to worry that retrieval of data stored long term is still tied to AWS services. Hence, they need to maintain those accounts to meet compliance and respond to ad-hoc requests such as legal hold and eDiscovery.

© 2025 Commvault



EXPOSURE TO DATA BREACHES

The DBaaS offerings are tied to accounts the customer owns in CSPs. In the case of RDS, the database instance sits in a virtual private cloud (VPC) in a customer's AWS account. The key backup method of RDS is snapshots which co-exist with RDS instances in the same account. If an AWS account is compromised by a malicious actor, be it an insider or outsider, backed up snapshots can be deleted or modified along with production instances. This is a terrifying reality that many companies now face and need better tools and processes to mitigate.

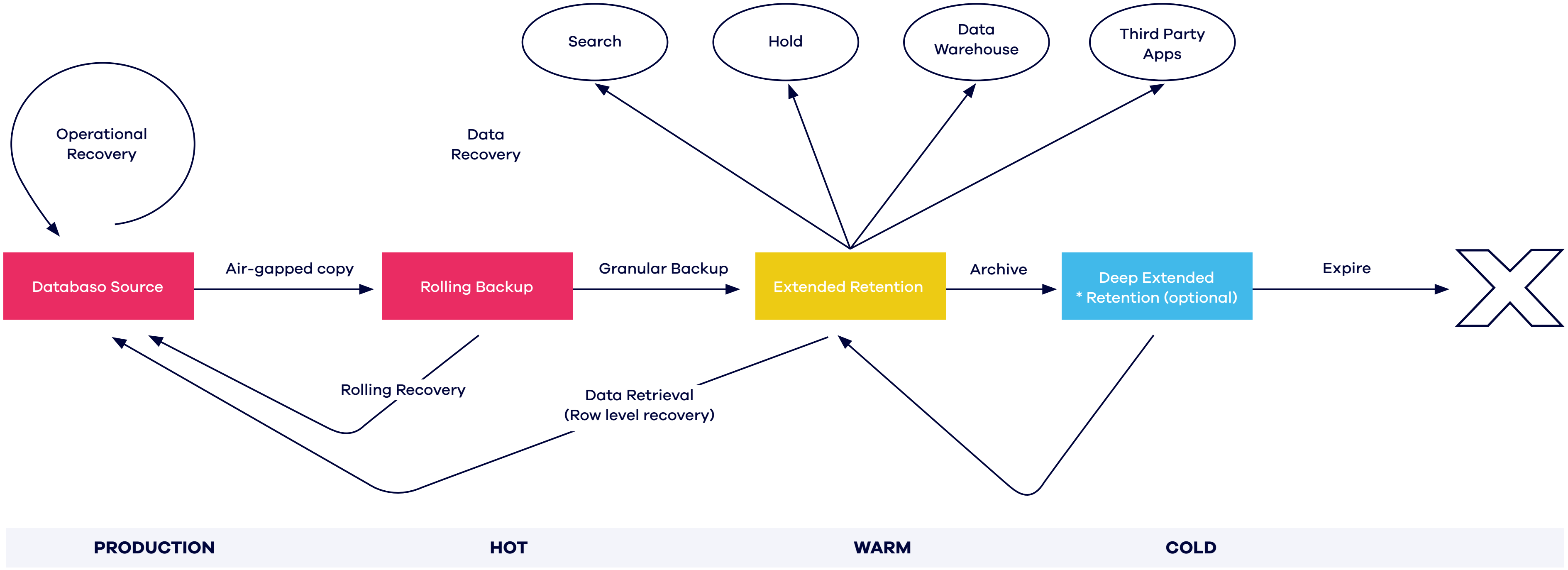
There are ways to share and copy full blown snapshots onto alternate accounts; however, those solutions have challenges:

- **Unpredictable costs:** Snapshots for a given RDS instance are maintained as a chain. The first snapshot is a full copy of RDS, and subsequent ones are incremental. This helps in optimizing the storage costs associated with snapshots. However, once you start copying snapshots out of the account, the snapshots chain is broken, and everything out of the account is full blown snapshots. This results in unpredictable costs.
- **Operational Complexity:** If the primary account is breached, there need to be guardrails in place to so that the alternate account is inaccessible from the information/credentials/keys that are already breached. This process of 'air-gapping' two accounts from one another requires significant investments in building scripts, key management, and procedures to be carefully implemented and regularly tested.
- **Reduced Agility:** One of the key benefits of moving to the cloud is agility. With the need for cross-account snapshot management and air-gapping to help protect from breaches, change control processes can hinder agility.

THE BEST OF BOTH WORLDS

RDS for Enterprises Without the Challenges

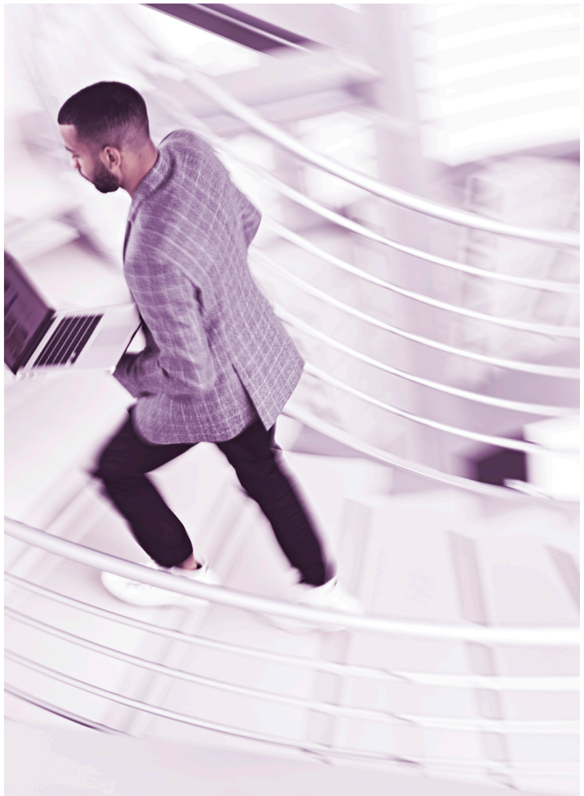
To design a data lifecycle management system, we need to look at the requirements of enterprises. Luckily, the requirements can be easily gleaned from how they used to manage data lifecycle on-premises. Data from production database systems goes through the following lifecycle.



© 2025 Commvault

BACKUPS FOR OPERATIONAL RECOVERY

If the availability of a database serving mission critical applications is affected due to software glitches, infrastructure failures, or human errors, backups stored close to the database act as the first line of defense. The recovery point objective here is minutes to days, while recovery time objective is minutes to hours – depending on the nature of the applications it is serving.



© 2025 Commvault

RECOVER QUICKLY FROM DATA BREACHES

Rolling backup is essentially a time-lagged standby of the production database. Transactions on production are replicated to a standby database in an alternate site, but deliberately time-lagged behind production by a predefined number of hours. This enables quick recovery without a full restore from backup, in case the production copy is affected by accidental or deliberate human intrusion.

© 2025 Commvault

EXTENDED RETENTION AND RECORDS RETRIEVAL

Enterprises store data beyond the operational recovery window to satisfy regulatory requirements, company policies, and historical data analytics. Organizations in regulated industries such as finance and healthcare create self-contained full backups on tapes on a periodic basis (e.g., every 14 days or every month) and store them offsite. They may also be making use of offsite storage services. Cloud-based object storage solutions such as Amazon S3 Glacier have become a viable alternative to tape storage.

For enterprises, data is the new oil. Many industries prefer to retain analytical data for extended periods. Extended retention copies are often used for historical data retrieval, not operational database recovery. Yet, to extract that data, organizations frequently restore entire databases into sandbox environments with the required software stack, allowing them to use standard access tools for data extraction. In this context, recovery is simply a step toward retrieving the desired historical data.

Amazon RDS includes built-in snapshot-based backup capabilities—automated backups that offer point-in-time recovery for up to 35 days. These provide a first line of defense. However, under the AWS shared responsibility model, customers must build additional safeguards and manage longer-term lifecycle needs. This is where third-party solutions can complement native RDS backups by simplifying management and enabling deeper control over retention, compliance, and cost.

© 2025 Commvault

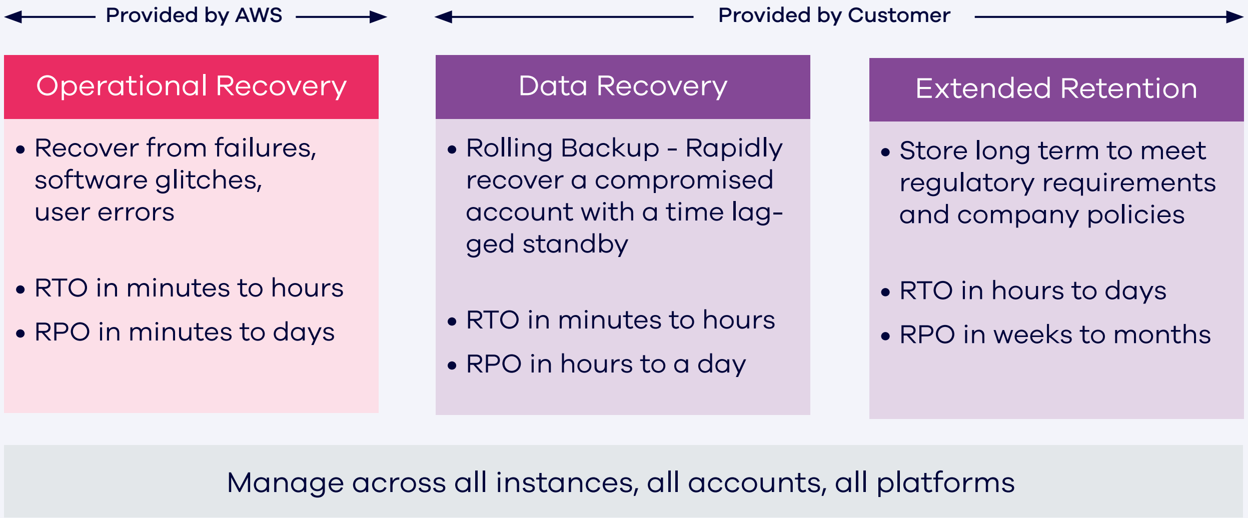
DEEP EXTENDED RETENTION

The last, and optional, phase of data is cold storage. Data is stored simply for the purpose of meeting regulatory requirements. The recall of data is a rare event. If and when data needs to be recalled, it is moved into a warm tier and thawed for data retrieval workflows.

The shared responsibility model dictates that native backup capabilities are AWS's responsibility. This is because operational recovery tools such as snapshots are part of the RDS platform itself. Once the data leaves the operational stage of its lifecycle, it is the responsibility of the customer to take care of data. Furthermore, as AWS accounts are the security perimeters of organizations or projects, rolling backups to alternate accounts is the customer's responsibility as well. This is depicted in the graphic below.

Making Amazon RDS Ready for Enterprise Applications

Meeting Enterprise Data Management Requirements



Provided by AWS

Provided by Customer

Operational Recovery

- Recover from failures, software glitches, user errors
- RTO in minutes to hours
- RPO in minutes to days

Data Recovery

- Rolling Backup - Rapidly recover a compromised account with a time lagged standby
- RTO in minutes to hours
- RPO in hours to a day

Extended Retention

- Store long term to meet regulatory requirements and company policies
- RTO in hours to days
- RPO in weeks to months

Manage across all instances, all accounts, all platforms

© 2025 Commvault

CONCLUSION

Amazon RDS brings agility and operational simplicity to operational database management systems. With the acceleration of workloads moving to the cloud, enterprises can make use of Amazon RDS to operational needs without compromising on regulatory and security requirements if they also adopt a database data lifecycle model that works in conjunction with the shared responsibility model of AWS.

Clumio helps to fulfill the customer's responsibility of data protection in the cloud by closing the gaps in data protection and lifecycle management tasks. Clumio also helps to recover quickly in case of account breaches with the use of backups that are air-gapped away from production accounts. And finally, the phases of data cycle management, from maintaining operational recovery copies to extended retention, are made possible by unified protection policies that can be applied across supported workloads, accounts, and platforms.

Learn more: **commvault.com/clumio-contact**

Commvault®

© 2025 Commvault. See here for information about our trademarks and patents. 05_25