# AWS

# Best Practices: DATA PROTECTION

BY N2WS

# TABLE OF CONTENTS

aws partner network

**Advanced**
Technology Partner

Storage Competency

Marketplace Seller

# INTRO

## Executive Summary

**In a data-driven society, downtime is the last thing organizations want to experience**.

Outages of any kind push businesses to lose data and a failure to recover that data can expose them to losses in productivity, reputation and revenue.

In their effort to embrace IT modernization, enterprises are moving their IT systems to the cloud, looking to manage costs, be more efficient and keep data safe. However, the cloud approach is not a one-time action, but rather a long-term commitment, a change in strategy, and a whole new set of rules.

One of the biggest advantages of cloud computing is that it cuts out the burden of maintaining an on-premises infrastructure, charging on the pay-as-you-go model. Many enterprises are choosing Infrastructure as a Service (IaaS) providers, however this doesn't solve all the issues.

Most cloud providers, including Amazon Web Services (AWS), operate on the **Shared Responsibility Model**. This means that the provider takes care of the infrastructure's security and integrity, while the protection of data stored in the cloud falls under the customers' duty.

Cloud services are not spared the need for doing backups and having a backup & disaster recovery (DR) strategy in place.

***Such measures are imperative to ensure availability and to prevent data loss.***

This whitepaper presents some aspects that IT Professionals need to take into consideration when they set up a data protection strategy for data and applications stored in AWS.

# 1. Minimize Recovery Time Objective (RTO)

**When protecting your data, both the recovery and backup sides of the equation are critical.**

How long will it take your organization to recover and to be fully up and running again after a system failure, a cyberattack, a human error or a natural disaster?

A complex organization with many locations and large amounts of data stored in the cloud and many EC2 instances running needs the assurance of a backup and recovery solution that allows full recovery within moments of a failure or outage.

Consider, too, the possibility that you may need to simply recover a single file or folder without needing to restore an entire instance.

Your backup and recovery solution should address normal business operational data retrieval needs, as well as disaster recovery for major emergencies, with **a simple way to retrieve snapshots, volumes or single files quickly.**

**WATCH OUT!**

Avoid “homegrown” solutions that are notoriously error prone and provide job security for the script creator.

**BEST PRACTICE!**

Choose a solution that is user friendly and can be adopted by other members of the IT team. In the event of an outage or failure, you don’t want to have to rely on 1-person on the IT team.

# 2. Run application-consistent backups

**Nothing is more frustrating than a corrupted backup file when you need to recover your systems.**

One of the biggest benefits of a dedicated backup management solution is application-awareness. It should remove a problem with AWS snapshot scheduling that otherwise presents a burden for the user: **backing up data while maintaining its integrity**.

Static data, such as pictures and documents that may not change much, can be backed up relatively easily but backing up and restoring live application-specific data is more challenging. Unlike static data, application data constantly changes as the application processes new transactions.

**In these scenarios, the application and the backup solution must work in concert to ensure that the application data is backed up according to the policies laid down by the business**. This calls for a key feature that you should look for in a backup automation solution: quiescence.

The backup process should 'quiet' an application just before it takes a snapshot of its data. This temporarily pauses the application, preventing transactions that may otherwise be in flux at the instant the snapshot is made. Pausing an application without affecting its availability to allow a snapshot ensures that the backup represents the true state of the application in its most current, stable state. No transactions are left hanging in limbo.

**WATCH OUT!**

Avoid solutions that require extensive downtime or regular maintenance windows to achieve application consistent backups.

**BEST PRACTICE!**

Choose a solution that adopts and enhances cloud-native technologies like EBS snapshots, allowing you to achieve consistency without maintenance windows.

# 3. Restrict permissions for IT staff

When using a dedicated system with built-in permission and credential management, only authorized people can set and change those policies. This eliminates one of the biggest problems when managing AWS backups manually: insecure permissions.

**Instead of granting high-level privileges to any storage admin that needs to run a backup, a dedicated system manages permissions itself, granting policy management privileges to user accounts on a least-privilege basis.**

This means that members of the team scheduling and checking backups have access to do only what they need to do, and nothing more. One person may need to change a policy, while another need only check a report to assess a backup job's status. The system logs whatever they do, creating a paper trail that will be invaluable in event of an audit.

For companies with a large IT staff monitoring and performing backups, finding a tool that integrates with SAML based identity providers such as Okta, LDAP and Microsoft Active Directory Federation Services (AD FS) both simplifies the lives of end users and provides additional security. By implementing centralized control, a company can manage the login process and rest assured that employees who are terminated will have privileged access removed in an automated way, even from disparate systems.

**WATCH OUT!**

Avoid solutions that grant the same level of privileges to any type of user, groups or roles.

**BEST PRACTICE!**

Look for a solution that has a built-in user management system that allows you to assign users specific privileges based on their responsibilities.

# 4. Move snapshots to another AWS region

## Snapshots protect company data, but what protects the snapshots?

A disaster recovery strategy is only as good as its ability to quickly recover, so a backup and restore strategy must protect it from harm and keep it as available as possible. Amazon's manual tools make it possible to backup snapshots between different regions in the AWS service, but **a dedicated tool can automate that process, allowing customers to set the regions that they want to use as DR sites**.

This makes it possible to recover files, applications, or even an entire environment in the rare case that an AWS region goes down. A sophisticated tool will also enable administrators to copy snapshot backups across different AWS accounts for added security, in case of a malicious attack, ransomware, malware, or insider threat.

Look to third-party solutions for functions that manage AWS snapshots along their entire lifecycle. A backup management system should automatically delete expired snapshots in line with predefined retention policies.

**WATCH OUT!**

Avoid relying solely on the standard AWS snapshot tools that provide limited restore capabilities.

**BEST PRACTICE!**

Choose a solution that leverages the native AWS technologies and is able to automate backup jobs, offer granular recovery and define backup policies.

# 5. Monitoring and reporting

To make their lives easier, IT administrators need to schedule automated reports and alerts that show at a glance whether the backups have been successful and warn of potential problems.

When they monitor the backup and recovery processes in real time, it's important to have access to all backup metrics: alerts, daily summaries, and information about how, when, and by whom data can be accessed.

**Dashboards, comprehensive reports, and push notifications are critical for monitoring how your backup solution is performing in real time**.

Understanding and being aware of everything that's happening under the hood can make the difference between taking the right proactive measures and a system failure.

**WATCH OUT!**

Leaving your workloads unattended can lead to downtime, data loss and unauthorized access.

**BEST PRACTICE!**

Choose a user-friendly solution, with an interface designed to provide all key status information for your environment at a moment's notice.

# 6. Keep your data inside the AWS environment

To help ensure that your security requirements are being met, consider solutions that run entirely inside your AWS environment and don't have access to your data.

**A solution that does not require you to move data out of your AWS accounts is more auditable, making it easier to demonstrate compliance**.

Such a solution is also more customizable, simpler to align with security policies, and easier to integrate with existing compliance and audit tooling and frameworks.

Finally, a solution that runs entirely within AWS gives you complete control of your data and does not require any external networking flows to monitor and document.

**WATCH OUT!**

Public cloud providers charge egress fees to transfer data out of their clouds.

**BEST PRACTICE!**

Find a solution that operates in the AWS environment to avoid security issues, high costs and to address compliance requirements.