Securing the Future of Government Data in the Cloud

MARKET TRENDS REPORT

govloop N2WS aws awsmarketplace

Executive Summary

Agencies continue to move workloads to the cloud, citing increased operational efficiency and agility, reduced costs and improved citizen services. While the cloud provides many benefits, it also delivers new challenges. For example, over time, most agencies have accumulated many different, often disconnected, cloud repositories. Accumulation makes it difficult to understand where all data is located and to recover quickly in the event of an emergency.

Additionally, many agencies are not backing up their data stored in the cloud. According to a recent survey, more than 90% of organizations already use Amazon Web Services (AWS) cloud technology in some form, yet many are not backing up their AWS environment. Without full infrastructure protection that includes image-based backups to multiple locations, full automation and the ability to define policies, agencies run the risk of data loss, slow recovery times, inability to access critical data in real time or non-compliance.

To learn more about how agencies can provide fast backup and recovery of data while maintaining and increasing manageability, GovLoop teamed with N2WS, an AWS-native backup, disaster recovery and archiving solution. This report will discuss why backup, recovery and disaster recovery are challenging for government agencies and the best ways to overcome those challenges. We gained additional insights from Sebastian Straub, a principal solutions architect with N2WS, and Julian Ware, a spatial data analyst for the city of Oakland.

By the Numbers

49%

of state governments are providing backup services to their local counterparts, while 47% are providing storage to their local counterparts.

Source: NASCIO

81%

of organizations say their move to the cloud is helping them better manage their data.

Source: DraaS survey

92%

of organizations already use AWS Cloud technology in some form.

Source: N2WS Cloud Data Protection Survey

32%

of organizations say they are not currently using any type of backup method for their AWS environment.

Source: N2WS Cloud Data Protection Survey

61%

of state CIOs say they rely on the cloud for better tools and insights.

Source: Report on NASCIO Midyear Conference

46%

of organizations still recover applications manually after an outage.

Source: N2WS Cloud Data Protection Survey

"New tools, technologies, and norms are creating opportunity to use data to bolster the Federal Government's mission delivery, service design, and tax-dollar stewardship for the public. In order to leverage these opportunities, the Government must address consistency in skills, interoperability, and best practices in how agencies use and manage data."

Source: OMB Memorandum

The Challenge: Data Sprawl in the Cloud

Backing up your cloud environment is an important first step to making sure that your data and infrastructure is always available, but it doesn't solve everything. Because agencies tend to deploy workloads across dozens of cloud platforms, for example, it can be difficult to quickly find the specific server or files required. Instead, administrators can spend hours examining the backups of each cloud platform to find what they need.

Speed of recovery is another challenge. With backups distributed across multiple clouds, it can be difficult to recover quickly in the event of an outage - what's known as Recovery Time Objective (RTO). Closely tied to RTO is Recovery Point Objective (RPO) — the time between backups. "If you back up once a day and have a failure after 23 hours, you have lost 23 hours' worth of data. Not too many agencies have that kind of tolerance for data loss," said Sebastian Straub, a principal solutions architect with N2WS, which specializes in data protection for cloud-based workloads.

With so many workloads spread across so many clouds, it also can be difficult to control who has access to your backups. And then there are concerns about data sovereignty — where the data actually lives — and whether vendors or other parties might be able to access that data. These security and compliance concerns constitute very real roadblocks for agencies storing workloads in the cloud.

It's also important to have confidence that backups are occurring consistently, and that the right people get notified when failures or other issues occur. For example, do you have the ability to carefully audit your environment to determine whether there are workloads that are not being backed up but should be?

The Solution: Automated, Policy-Driven Backup and Recovery

To protect against data loss, security breaches and slow recovery times while providing real-time data access, agencies need an automated, policy-driven, comprehensive backup and recovery plan that includes all data stores and infrastructure.

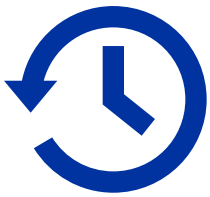
To provide fast availability and recovery time, choose a solution that prioritizes speed and automation. For example, the N2WS virtual appliance uses fast snapshot-based block storage, allowing it to recover an entire environment — all data, network configurations and servers — within about 30 seconds. That's particularly important when an entire region or data center fails.

If a disaster occurs, you should be able to recover everything at the same time instead of machine by machine. If a region fails, your solution also should support cross-region recovery. N2WS, for example, supports disaster recovery between AWS GovCloud (US) regions, so if one fails, everything is immediately available on the other site.

Providing full security and compliance is important with all backup scenarios. One way to do this in cloud environments is by using a solution that does not actually see or access any data it is backing up. Instead of filtering the data through a solution, for example, look for a solution that simply applies the instructions set by the organization to perform specific data manipulations. No third party, including the vendor, should have access or visibility into anything.

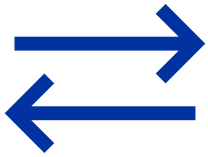
A comprehensive backup solution also should be able to automate how data is moved throughout tiers to save money. For example, data backed up to expensive Amazon Elastic Block Store (Amazon EBS) should be able to be moved to less expensive Amazon Simple Storage Service (Amazon S3) or even Amazon S3 Glacier Deep Archive, depending on its importance, relevance and how quickly it needs to be recovered.

Best Practices for Data Backup in the Cloud



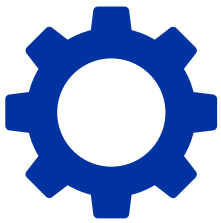
1. Don't assume that if you have resources in the cloud, they are fully backed up.

Despite what many people think, the cloud doesn't automatically back up your data and network infrastructure. "The only thing the cloud provides is virtual hardware, but the data is still your responsibility," Straub said. While cloud hosting providers like AWS do provide some basic backup tools, Straub says they can be difficult to use. Instead, use an automated backup and recovery solution optimized for your cloud environment.



2. Make sure your cloud-based backup solution prioritizes application consistency.

Cloud-based backups are extremely fast, which is a good thing. It can also mean, however, that your backups could miss important transactions that are occurring during the few minutes it takes that backup to complete. That can be a problem for both continuity and compliance. With backup solutions that prioritize application consistency, everything you back up — data, exchange servers, etc. — won't leave anything out, even transactions in process.



3. Automation is critical when backing up cloud workloads.

In addition to introducing the risk of human error, manual processes simply can't keep up with the speed of cloud-based backups. Automated solutions also enable administrators to configure what they want to back up, define targets and set frequency and retention periods. The intelligence in some of these solutions means that they can identify newly spun up resources and automatically back them up without being prompted by a human. In addition, these solutions can be set to conduct periodic disaster recovery drills automatically.

Finally, they can move data to different AWS tiers based on predefined rules, saving agencies money. "If you are in charge of database backups but I forgot to tell you that I just stood up a new database server, you might never find out about it," Straub said. "Experiencing a disaster six months later and needing to access a backup isn't the ideal way to find out about that database."

4. Choose a backup or recovery solution that positions you for the future.

Datasets will only get bigger, and requirements for recovery points and recovery times will only become tighter. To make sure that your agency can handle any mission requirement and incorporate any new technology and process that comes its way, prioritize a solution that keeps pace with changes your cloud provider makes. Backup solutions "born" in the cloud can be a good choice because they are built to work with the cloud.

Case Study: Recovery Time, Peace of Mind Prove Critical for City of Oakland

Known for its trendy neighborhoods, street festivals and major sports teams, Oakland, California, is as busy a city as you'll find. To keep up with maintenance, safety and citizen services, the city's IT staff began running a major geographic information system (GIS) in an AWS Cloud in 2012.

As the mapping system and associated data grew, the IT department realized it needed more comprehensive backup and recovery to guard against potential data loss. Access to mapping data is critical for many city services, including police and fire.

"AWS allows you to do a lot of things, but we were just too busy. We didn't have time to script out backup routines and make sure that everything was being consistently snapshotted and backed up," said Julian Ware, a spatial data analyst for the city of Oakland.

After evaluating the options, the team settled on N2WS, a backup and recovery tool designed for AWS workloads. When the team was a few days into the two-week pilot, Ware said he knew he had found the answer.

"There was a level of granularity in the backup scheduling that exceeds our ability internally, and we could do both incremental and full backups, which we couldn't easily do before," he said. Ware also noticed that recovery time improved dramatically, and that performing backups didn't significantly impact IT resources.

More than anything, Ware appreciates the peace of mind. "Being able to look at my email in the morning and know that backups ran at the time I scheduled them for and that there were no problems means I don't have to worry about it for the rest of the day," he said.

HOW N2WS AND AWS CAN HELP

N2WS technology was born in the cloud, built specifically to meet the backup and disaster recovery requirements of AWS workloads for some of the most demanding organizations, including state, local and federal government agencies. The Linux-based virtual appliance uses the AWS application programming interface (API) to access customers' AWS accounts, backing up not only file blocks that have changed, but network configurations and infrastructure. Intelligent automation and policy controls let agencies automatically move data sets to more economical tiers on any AWS platform: Amazon S3, Amazon Elastic Compute Cloud (Amazon EC2), Amazon S3 Glacier, Amazon S3 Glacier Deep Archive, Amazon EBS, Amazon Relational Database Service (Amazon RDS) and Amazon Redshift.

Because it is tied closely to AWS, the N2WS virtual appliance keeps pace with all AWS changes. Whenever AWS offers a new feature, N2WS immediately reflects that in its own technology. Notable features include one-click disaster recovery, data lifecycle management, automated policies and schedules, alerts and reporting, recovery scenarios and on-demand resource control. As a result, these organizations have been able to achieve near-instantaneous recovery, access critical data in real time and better manage data in AWS.

For more information, visit: www.n2ws.com/trial.

Conclusion

As agencies move more workloads to the cloud, they must find ways to make sure that their data and network configurations are fully backed up and can be quickly recovered. At the same time, they must make certain that security and compliance are not compromised, and that budgets stay under control.

An automated backup and recovery solution built specifically for the cloud will help agencies meet all of these goals. A "born in the cloud" approach to backup and recovery is better equipped to deal with workloads in multiple clouds, protect against data loss and security breaches, ensure compliance and enable real-time data access.

As mission requirements evolve, backup and recovery processes must change to keep pace. Using an automated, modern approach to backup, recovery and disaster recovery is the key to accomplishing these goals.

ABOUT GOVLOOP

GovLoop's mission is to "connect government to improve government." We aim to inspire public-sector professionals by serving as the knowledge network for government. GovLoop connects more than 300,000 members, fostering cross-government collaboration, solving common problems and advancing government careers. GovLoop is headquartered in Washington, D.C., with a team of dedicated professionals who share a commitment to connect and improve government.

For more information about this report, please reach out to **info@govloop.com**

ABOUT N2WS

N2WS is a leading provider of enterprise backup, recovery and disaster recovery solutions for Amazon Elastic Compute Cloud (Amazon EC2), Amazon Relational Database Services (Amazon RDS), Amazon Redshift, Amazon Elastic File System (Amazon EFS), and Amazon Simple Storage Service (S3), Amazon Aurora and Amazon DynamoDB. N2WS integrates seamlessly with AWS native technology, inherits strict security and compliance standards, and supports all AWS regions, including AWS GovCloud. N2WS was founded in 2012, with the mission to make enterprise-level Amazon Web Services (AWS) backup easy and reliable for AWS, and today serves thousands of customers around the world. N2WS Backup & Recovery is a preferred backup solution for public sector organizations, including: Government agencies, universities, service providers and system integrators running large-scale production environments on AWS. N2WS Backup & Recovery is available exclusively on AWS Marketplace.

To learn more, visit http://www.n2ws.com.

ABOUT AWS

With over 2,000 government agencies using AWS, we understand the requirements US government agencies have to balance economy and agility with security, compliance and reliability. In every instance, we have been among the first to solve government compliance challenges facing cloud computing and have consistently helped our customers navigate procurement and policy issues related to adoption of cloud computing. Cloud computing offers a pay-as-you-go model, delivering access to up-to-date technology resources that are managed by experts. Simply access AWS services over the internet, with no upfront costs (no capital investment), and pay only for the computing resources that you use, as your needs scale.

To learn more about AWS, please visit www.aws.amazon.com.

1152 15th St. NW Suite 800
Washington, DC 20005

P: (202) 407-7421 | F: (202) 407-7501

www.govloop.com
@GovLoop