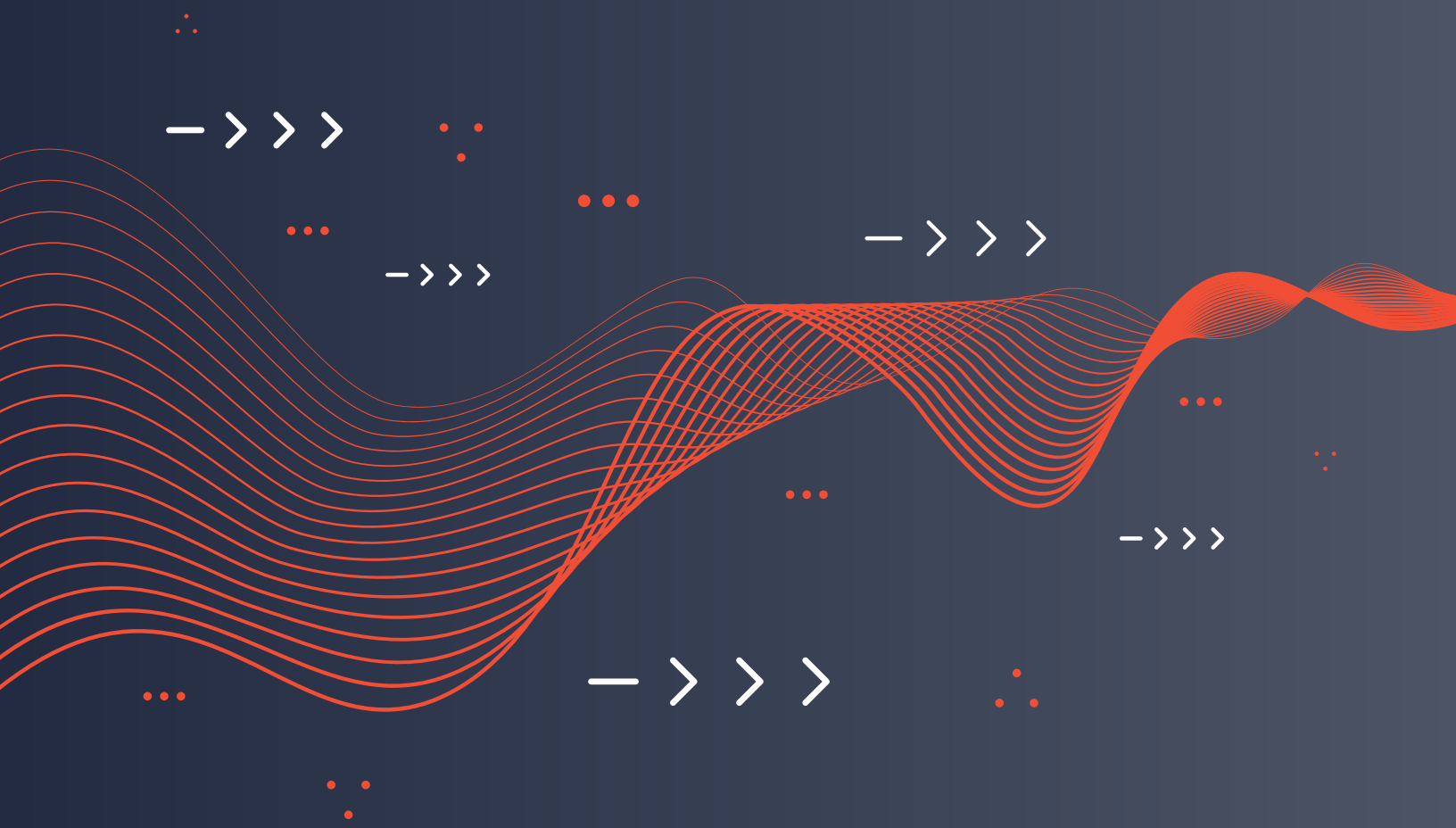

How the Cloud Powers Disaster Recovery for Government

govloop

Executive Summary

In recent years, federal, state, and local governments have faced unprecedented costs for disaster response and recovery efforts.

“The federal government obligated nearly $300 billion across numerous departments and agencies during fiscal years 2005 through 2014 for disaster assistance,” according to the Government Accountability Office. “Extreme disasters like hurricanes Katrina and Sandy caused billions of dollars in damage.”

The effects of these catastrophic storms and other disasters not only have immediate and direct impacts on citizens — such as damaged property or lost belongings — but they also have indirect consequences. For example, the very systems that government agencies depend on to serve citizens in the wake of a disaster are also at risk when disasters hit.

When government employees don’t have access to functioning hardware and software applications, they can’t disseminate timely information, disburse benefits to citizens, defend the homeland, or otherwise carry out their missions. Productivity could come to a grinding halt, resulting in lost time, wasted resources, and in some cases, major national security risks.

That’s why disaster recovery should be top of mind for governments at all levels. Disaster recovery, or DR for short, is the documented processes and procedures for how your agency will recover from a disaster that impacts IT infrastructure. Whether the culprit is a natural or manmade disaster, your agency needs a way to quickly recover and resume mission-focused activities.

GovLoop teamed with NetApp, which specializes in cloud-based and on-premises enterprise data management solutions, and cloud service provider Amazon Web Services (AWS) to produce this report. In it, we explore the state of DR in government, current challenges, the benefits of moving DR to the cloud and how to do it, as well as best practices that agencies at all levels should consider when implementing their DR strategy.

The State of DR in Government

There's a growing demand across government to manage massive amounts of data, whether it's citizen data for processing benefits claims, workforce data to make hiring decisions, or intelligence information for sensitive missions. The bottom line is federal, state, and local agencies increasingly rely on the availability of this data to make decisions that have far-reaching impacts.

Take state and local law enforcement agencies, for example. They rely on federal databases, such as sex offender registries and criminal background check systems to accurately identify individuals who may have carried out serious offenses. But what if law enforcement officers weren't able to properly identify a suspect because they couldn't access centralized databases? When lives and safety are at stake, there is no room for error or incomplete information.

To ensure data is accessible when and where they need it, a growing number of agencies have invested in IT disaster recovery solutions. In the event of a natural or manmade disaster, agencies still need to quickly recover. That's where disaster recovery planning and execution comes into play.

Think of DR as the documented processes and procedures for how your agency will recover from a disaster that impacts IT infrastructure. This includes networks, servers, desktops, laptops, wireless devices, data, and connectivity.

The two key drivers for any DR plan are recovery time objective (RTO) and recovery point objective (RPO). RTO is the time it takes after a disruption to restore a business process to its service level, as defined by the operational level agreement. RPO is the acceptable amount of data loss measured in time.

A thorough DR solution also enables agencies to maintain data compliance and protect against negative events that may result in data loss.

"Disaster recovery falls in line with the concept of business continuity planning, or the ability to continue to run, operate, and do business in the event your agency's data center is no longer operational for a variety of reasons," said Jerimiah Cox, a cloud solutions architect with NetApp. Think of DR as a subset of business continuity.

Considering the critical nature of disaster recovery planning, it's vital that agencies hash out the DR capabilities they need long before an incident occurs.

But from a cost standpoint, DR tends to be very expensive for agencies, said Lori Barber, a hybrid cloud business development manager at NetApp. Traditionally, the government's approach to DR has involved maintaining a separate facility with infrastructure that mirrors what's in an agency's primary data center. The concern is that agencies are paying to maintain such facilities even though they sit idle most of the time.

To better manage costs and move away from building and owning underutilized disaster recovery sites, agencies are exploring cloud computing as a viable option. With the cloud, agencies don't have to worry about paying for infrastructure that they rarely use. Instead they can benefit from AWS Cloud and NetApp solutions on AWS to quickly gain access to cloud resources.

In the next section, we detail some of the key benefits associated with moving disaster recovery operations to the cloud.

DR vs. Backup Recovery

In conversations about disaster recovery, you may have heard the term used interchangeably with backup recovery — but there is a difference. Backup recovery is the ability to selectively restore data or parts of an infrastructure, such as a virtual machine, a server, files, email, or things of that nature that have been lost, corrupted, or overwritten, Cox said. For example, backup recovery may involve replacing your email or contacts that you accidently deleted. Disaster recovery would entail you replacing or exchanging your entire email server in the event that it is no longer available.

Benefits of Moving DR to the Cloud

One of the major perks that agencies gain from moving to the cloud is the ability to have on-demand access to a virtual environment in the cloud that mirrors their physical environment.

This means agencies don't have to invest in additional servers, storage, or other infrastructure. They can reduce their physical footprint and move away from maintaining separate disaster recovery facilities, Barber said.

Because agency resources are stored in the cloud, they can have access to them when they need them. These resources don't have to be up and running 100 percent of the time like they would in a traditional DR facility that's owned and operated by government agencies. Instead, agencies only use the resources they need without incurring costs for idle resources.

Being able to integrate quickly to the cloud without having to install or configure new products creates ease of use during emergencies, making disaster recovery seamless. Agencies can easily schedule data snapshots, restore and do one-time migrations to the cloud, or continuously keep data in sync — with no added complexity.

A DR environment can also save money. Barber recommends agencies ensure they have contracts in place that enable them to take advantage of these benefits now, and properly prepare for any disasters down the road.

"The data is the most important piece," she said. "Agencies want to make sure that they always have access to their data and that it's always secure." With a cloud-based DR model, the data is always available in the cloud, even though servers are not always running.

With cloud-based DR, your agency can:

- Meet established RTO and RPO by storing data in a secure, remote, online facility that recovers data based on mission objectives
- Replicate data and quickly transition to a cloud site when an outage occurs
- Gain flexibility and cost savings by paying for your DR applications only in the event of a site or system failure
- Instantly resize storage capacity as your data requirements change

The ideal cloud-based DR plan is one that is optimized and properly tested to make sure any points of failure are discovered before a real disaster takes place.

Cloud-Based Solutions for DR

NetApp's Cloud Volumes ONTAP disaster recovery solution makes it easy for organizations to take advantage of cloud cost and efficiency benefits, while meeting critical DR requirements. Cloud Volumes ONTAP is a powerful, cost-effective, and easy-to-use data management solution for agencies' cloud workloads.

Using ONTAP, which runs on top of AWS infrastructure, agencies can easily deploy a DR environment in the cloud and rapidly recover when an outage occurs.

With Amazon Web Services, your agency can scale up its infrastructure on an as-needed, pay-as-you-go basis. You get access to the same highly secure, reliable, and fast infrastructure that Amazon uses to run its own global network of websites. AWS also gives you the flexibility to quickly change and optimize resources during a DR event, which can result in significant cost savings.

There are also security benefits that come with moving DR to the cloud. For example, AWS uses independent third party attestation of its facilities and compliance certifications are available within AWS.

3 Steps to Setting Up a Cloud-Based DR Solution

Standing up a cloud-based DR solution doesn't have to be complex. In fact, agencies can set up a DR environment in less than an hour. Below, we've outlined three high-level steps for moving to a cloud-based DR solution.

1. **Launch Cloud Manager from the AWS Marketplace.** Cloud Manager has several purposes, including serving as the interface to deploy Cloud Volumes ONTAP, managing ONTAP configurations, and adding capacity. Cloud Manager also allows you to centrally manage on-premises resources in a hybrid-cloud environment.

2. **Create a new Cloud Volumes ONTAP instance.** Using your management console, you can spin up a virtual instance of ONTAP and drag and drop from a variety of flexible cloud deployment models. ONTAP software provides a foundation for data management on the broadest range of deployment options — from engineered systems to commodity servers to the cloud.

3. **Drag and drop volumes to Cloud Volumes ONTAP to kick off the DR process.** Volumes are the partitions or compartments that enable agencies to store data. These volumes can support analytics, DevOps, enterprise applications and backup and disaster recovery.

Best Practices for Managing DR in the Cloud

For NetApp, the goal is to help agencies navigate the world of hybrid cloud, Cox said. "We reinforce the concept that with Cloud Volumes ONTAP they have more options and flexibility to consume services as they're developed and presented, such as those that AWS offers."

NetApp ONTAP directly integrates with Amazon S3 storage as a destination for backup data. Full DR sites can be stored on Amazon S3 and be on standby until they are needed. This approach significantly cuts costs, because users no longer need to invest in secondary data centers to protect against outages and other instances. Linkage with off-site systems, where you would replicate DR locations, bypasses the performance tiers (for example, Amazon EC2 or Amazon EBS) entirely and can go into colder tiers of storage until the DR site needs to be activated to optimize storage costs. In case of a disaster, SnapRestore®can leverage Snapshot®copies to restore entire file systems or data volumes on AWS.

Overall, storage efficiency technologies such as incremental Snapshot backups, deduplication, and compression minimize network latency, shorten transfer times, and depending on workload type, can save users up to 90 percent on storage capacity compared to on-premises storage.

When considering a cloud-based DR solution, these are the types of considerations that agencies should make in the early stages of the selection process. Doing so will help them benefit from current and future innovations around DR, whether that's in the cloud or across a hybrid environment.

Conclusion

Government agencies know that disaster can strike at any point, potentially impacting valuable data, information, and entire data centers. IT departments need to be proactive while planning for natural disasters, outages, cybercrime, and a host of other potential events that could jeopardize network accessibility. That's why an effective DR plan is critical.

The purpose of DR is to provide a replica of an organization's primary data and related infrastructure that can enable that agency to seamlessly continue operations. Whether it is a failure to the network, storage, infrastructure, communications, or virtual machine – or an outage caused by human error – agencies must have the necessary IT resources to continue their mission.

Cloud computing provides an affordable, secure, and user-friendly model for agencies to properly support DR. Moving DR operations to the cloud reduces the required data center space and storage infrastructure, resulting in cost savings and flexibility.

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 270,000 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 NetApp

NetApp is the data authority for hybrid cloud. We provide a full range of hybrid cloud data services that simplify management of applications and data across cloud and on-premises environments to accelerate digital transformation. Together with our partners, we empower global organizations to unleash the full potential of their data to expand customer touchpoints, foster greater innovation and optimize their operations.

For more information, visit www.netapp.com. #DataDriven

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, visit https://aws.amazon.com/government-education/government/

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

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

www.govloop.com
@GovLoop