UNITRENDS
A Kaseya COMPANY

4 Best Practices for Protecting a Multicloud Enterprise

Are you ready to deal with the unique challenges of protecting multiple clouds?

INTRODUCTION

You probably already have a multicloud environment. If you have followed the path of most IT organizations you have SaaS applications such as Salesforce, Office 365, or G Suite, have data stored in the public cloud and perhaps use cloud resources for computing and disaster recovery. You may have grown through acquisition and inherited a cloud. Most organizations now use multiple clouds in their IT architecture.

The question is are you ready to deal with the unique challenges of protecting multiple clouds? How can you efficiently protect this multicloud environment with no gaps in coverage and avoid the risks of data loss and downtime?

WHY ARE MULTICLOUD INFRASTRUCTURES BECOMING MAINSTREAM?

The cloud is well suited to providing an expanding variety of computing services.

IDG (CIO Magazine, April, 2018) declared that – "In 2018, cloud computing went mainstream. Virtually all organizations (96 percent) use it in one way or another. However, studies show that as users gain cloud maturity, they tend to move from hybrid cloud scenarios – which comprise both private and public clouds – toward multicloud landscapes spread across a multitude of service providers. Indeed, according to a recent 2018 poll, 81 percent of enterprises already have a multicloud strategy in place."

The reasons are easy to understand – the economics and operational advantages of cloud makes great sense for many forms of computing. Cloud advantages include scalability, mobile access, security, and low capital expenditures. Increasing WAN capabilities also make cloud computing more responsive. And the use of multiple clouds will continue to expand. Gartner forecasts "that public cloud usage will double from 2016 to 2022, growing at a 16.6% CAGR." (Forecast: Public Cloud Services, Worldwide, 2016-2022, 3Q18 Update)

Having multiple clouds can mean having multiple different data protection and recovery strategies.

CHALLENGES OF PROTECTING A MULTICLOUD ENVIRONMENT

This shift from on-premises to cloud computing comes with challenges. Cloud disadvantages include a difficulty in accurate budgeting as unknown charges can arise, connectivity limitations as we are still dependent on WANs, compliance limitations, and most importantly for this report, clouds require different forms of protection..

Perhaps the greatest challenge is business continuity. Having multiple clouds can mean having multiple different data protection and recovery strategies. Technology can vary greatly across different types of clouds so that a protection solution that works in one scenario may not work somewhere else. You need to have a data protection and recovery process for each element of your computing strategy.

While you may believe that the cloud provider is backing up your data, the truth is that they are providing only rudimentary protections with no protection from deletions, ransomware, malicious employees or other user issues. Public cloud SLAs are limited to guarantees that the environment is operational – not that applications will recover as planned.

The challenge is that efficiencies of multicloud computing are quickly offset if you need a hodge-podge of backup solutions, each with its own user interface, service organization, and recovery procedure. You need an integrated backup and disaster recovery architecture that allows easy setup of automated tasks, complete and total recovery capabilities, advanced testing and data protection.

PROTECTION STRATEGIES FOR MULTICLOUD COMPONENTS

Each new compute environment requires its own protection strategy.

ON PREMISES / PRIVATE CLOUD

Your environment may be complicated, but protecting it doesn't have to be. You need to protect everything in your data center, whether it is physical or virtual, deployed on premises in your central data center, at a remote location, or on emerging hyperconverged infrastructures such as Nutanix and VMware VSAN. Using a private cloud purpose

built for data protection can provide a simple, all-in-one approach to backup, recovery automation, and continuity and makes IT administrators more productive as they can do more in less time.

Best-in-class organizations should deploy a single, complete solution, specifically designed to perform data and application protection - in other words, an appliance. A purpose-built, all-in-one appliance is easier to install, upgrade, and manage. Today's leading appliances protect all computing platforms, including virtual systems, physical Windows and Linux systems, legacy systems, and remote devices. Local recoveries can be run on the appliance itself. Appliances in different locations can act as backups for each other so that site level disasters such as electrical failures or flood do not bring down an entire enterprise. Cross-site monitoring and recovery by backup appliances can be nearly instantaneous.

PUBLIC CLOUDS

The best technology for protecting public cloud-based applications is the same as that which is used for your datacenter. Install a software appliance in the public cloud that automatically makes copies of the data, applications and system settings and replicates them to another area of the cloud, to your data center or even a different public cloud provider. Lost data files can be restored from the backups and the backups can be used to restore the entire computing infrastructure if needed.

The best tool to protect public cloud workloads is one that can interoperate with a recovery appliance in your data center. You should be able to manage all backup appliances –physical and virtual whether they are on-premises, in a remote physical site, in a public or private cloud from a single pane of glass without having to log off and on to different systems using different interfaces.

For recovery of cloud workloads it is better to use another cloud than to bring the apps to your on-premises data center. This would require extensive spare server and storage capacity which is probably one of the reasons you went to the cloud in the first place. For optimal recovery performance failover your public cloud workloads to a purpose-built Disaster Recovery service. This will give you the highest level of confidence in your ability to recover quickly from any cloud disaster event

While you may believe that the cloud provider is backing up your data, the truth is that they are providing only rudimentary protections.

It is most effective to administer a multicloud recovery strategy centrally. This means using a single devices to manage all backups and recoveries from a central location.

SAAS APPLICATIONS

You are as responsible to protect corporate data in the cloud as you are to protect it on premises. SaaS vendors such as Microsoft and Google protect you from data loss caused by system issues, but customers are responsible for data loss from accidental or malicious deletions, third party software, ran¬somware, and other user issues.

For example, SaaS apps have a Recycle Bin for basic recovery services. Deleted items are purged from the Exchange Recycle Bin, for example, and are unrecoverable after 14-30 days, depending on your settings. Similar limits exist for Google G Suite and Salesforce. It is impossible to recover a file once it has been deleted from the Recycle Bin unless you have optional backup capabilities.

For SaaS applications data protection is more about backup than continuity. It is highly unlikely that the entire Microsoft Azure O365 cloud goes down, but very likely the end user will delete a folder he believes is no longer important. It would be wiser to replicate the data from one cloud provider to another rather than establishing a traditional backup infrastructure to handle these apps.

A SaaS protection service can be purchased from third parties that, for a low monthly fee, can replicate files, folders, contacts lists and even entire shared drives to a different public cloud to protect them from catastrophic disasters and user errors. Recovery can be performed in seconds even if a user has permanently deleted data from his active account. You can even rollback to a specific version of a file, folder or document library.

WHAT 4 FEATURES SHOULD YOU HAVE IN A MULTICLOUD RECOVERY ARCHITECTURE

Managing these different cloud elements as a single platform requires products created as a single multicloud recovery architecture. What separates a collection of backup capabilities from different vendors from a best-in-class data protection and recovery architecture is that all elements can be interoperated and share these important attributes:

1 - CENTRALIZED MANAGEMENT

It is most effective to administer a multicloud recovery strategy centrally. This means using a single devices to manage all backups and recoveries from a central location. Rather than trust remote employees to follow a complex set of rules and regulations, a single team should be able to perform all protective functions using a single device.

The newest backup appliances enable a central device to manage any or all remote locations as easily as if they were on site. This ensures a consistent program covering all locations, even those where no IT resources may be located. A comprehensive and easy to use User Interface (UI) can automate a recovery strategy. It should always be possible to operate your backup system without having to refer to a manual so that managers can stand in when primary admins are unavailable.

2 - CENTRALIZED SUPPORT

When an element of your recovery architecture goes down you don't want to be the one trying to figure out which product is responsible and which service organization to call. You need to have your recovery architecture supported by a single team available by phone, chat, and email—24 hours a day, 7 days a week, 365 days a year. Ideally the support engineers should be located in the US and at the same location as central engineering to ensure easy access for advanced questions. Ask your vendor to document their satisfaction rating to see how satisfied existing customers are with their support.

3 - AUTOMATED RECOVERY TESTING

The only way to know if you can recover in an emergency is to test regularly and each time you make a change to your infrastructure. New, intelligent tools are available that can greatly ease your concerns by automatically testing to ensure all components are in place and capable of recovering or identifying issues. Additionally, you should receive an easy to read, formal report certifying that your disaster recovery solutions have been tested and show the results. The reports should be good enough be used in compliance audits to prove you have recovery procedures in place, they are regularly tested, and recoveries are performing at the required speed.

The only way to know if you can recover in an emergency is to test regularly and each time you make a change to your data center. New, intelligent tools are available that can greatly ease your concerns.

4 - COMPLETE DRAAS

Your recovery architecture should include the option of cloud-based Disaster Recovery-as-a-Service (DRaaS). DRaaS allows organizations to spin up their applications in an independent cloud if their datacenter or cloud-based applications go down for any reason. This is the ultimate level of protection as business critical applications can be run on remote infrastructure allowing business users to continue doing their jobs.

Using public clouds as a DR platform is a challenge. You have to become the DR expert, ensure the servers are properly configured, conduct the test and make all changes if testing shows an issue. Cobbling together a public cloud recovery process will leave gaps in coverage.

Look for DRaaS services that provide written guarantees that your applications will be restored within specific periods of time. You should be able to purchase premium DRaaS protection for the apps you determine to be critical and lower levels of protection for apps that are less important. DRaaS services should be able to protect cloud-based workloads as well.

CONCLUSION

Gone are the days of IT having all computing infrastructure in a single data center. Cloud computing offers advantages that cannot be ignored. A distributed computing infrastructure requires a new approach to data protection and recovery – a recovery architecture – that ensures all components are protected with no gaps in coverage.

For the greatest degree of confidence, you should partner with a specialist in data protection and disaster recovery. For more information on how to protect a multicloud computing architecture contact Unitrends and speak to a one of our solution experts.

unitrends.com
PART# WP-2089-ENG-A

UNITRENDS
A Kaseya COMPANY