THE TOP 10

Best Practices to Leverage the Public Cloud for Backup and Disaster Recovery

Many organizations want to improve their ability to recover from system failures and data loss, especially to protect themselves from natural and manmade disasters. Because building out a complete disaster recovery infrastructure can be cost prohibitive for many organizations we'll look at ways to leverage public cloud to supplement your backup and disaster recovery solutions. We'll also provide general backup best practices.

1 **Think of local protection as the first line of defense.** The public cloud is great; it offers virtually unlimited server and storage resources and can be extremely flexible because you can add and remove resources as needed and use operational budgets (OPEX) instead of capital budgets (CAPEX). However, when it comes to performing backup and recovery, the best performance—99 percent of the time—will be delivered by using resources local (on-premise) to the systems and data being protected.

2 **Identify the systems and the dependencies of those systems that are critical to the business.** If you think of local protection as your first line of defense, public cloud-based protection would be the second line of defense. You should prioritize the servers and data that need offsite disaster recovery protection by identifying key business services that are critical to your organization's day-to-day operations. Also make sure you understand the dependencies of those critical services, such as databases and middleware, and make sure those dependencies are also protected in the public cloud.

3 **Don't think only of traditional backup for disasters.** We always consider the possibility of large-scale disasters and of losing entire servers but many recovery operations are required after simple application crashes and data loss, which may be caused by accidental file deletion or file overwrite—and the data loss may not be realized initially. In addition to your traditional full backups, think about performing multiple point-in-time image or snapshot copies of your data. Infinite incremental image-based backups can complement or even replace traditional backups and allow you to achieve more frequent recovery points so you can easily restore data from 15 minutes ago, yesterday, from the day before, or from 4:00 p.m. last Wednesday. Also consider the ability to use replication technologies to provide continuous data protection locally and in the cloud, for those critical systems we talked about in point two. But remember that replication, although a great complement, is never a replacement for backups. Even high availability software solutions can be used with a public cloud for automated and push-button failover for the most critical systems and applications.

4 **Think about how you want to restore data and back up to meet that goal.** Backing up the system and all the storage will protect everything on that OS instance, which is perfect for when you need to restore the entire environment using bare metal recovery scenarios. If you are protect-

ing a service such as a database like Microsoft Exchange, you might want to restore only a specific mailbox or even a single email—so think about what you might want to restore then make sure you are backing up in a manner to facilitate your goals. This may require a backup agent that understands the service being protected.

5 **Backup at the hypervisor level may not always be enough.** Virtualization has brought us many wonderful capabilities, including the ability to perform backups at the hypervisor level of the virtual machines (VMs). But this type of backup typically will limit your restore to a VM-only level or, at best, to files within the VM. For rich services inside the VM—and for the best restoration experience—consider running backup agents within the VM OS instead of just on the virtualization host. And remember, if a virtual server fails, all VMs on that server are at risk so virtual servers make perfect candidates for a high availability solution.

6 **Long-term backup storage in the cloud.** Data is stored for many reasons, the most important of which is long-term archiving for corporate needs and to meet regulatory requirements. Maintaining long-term disk-based backups on a company's resources can be very costly; maintaining long-term backups or archiving old or infrequently used files in the public cloud can be a great, cost-effective alternative solution for many organizations.

7 **Ensuring security of the public cloud data.** Securing your organization's data is a major consideration for most organizations. If you are storing backup data or files in a public cloud, you should verify the security used in the solution—for example, the physical security of the public cloud locations, encryption of data at rest on the storage, and logical separation of your organization's data from other organizations using the same public cloud backup provider. You should also understand how your data is sent over the network to the public cloud and what encryption is used to protect the data during transmission.

8 **Running the recovery directly in the cloud.** With your systems, applications, and data protected and with backups stored in the public cloud, you have protection if you lose an entire site. But in case you do lose your site, where should you restore the data and operating system backups so that your organization can get up and running again? Look at options to run your systems in virtual environments in public cloud virtual machine hosting solutions using the systems and data backed up in the public cloud. This approach allows your operations to be up and running again even without your own datacenter.

9 **Unified backup and management.** Most organizations that leverage a public cloud for backup will still have local backup capabilities, which means potentially different management tools and even different backup agents on protected operating system instances. Consider leveraging a single solution that supports a hybrid model and enables a single management approach.

10 **Test the processes periodically and any time a significant change occurs in infrastructure.** The best solutions in the world will fail if you don't know how to use them correctly—and if you don't perform regular tests to ensure restore processes work and the data protected is valid. Get into the habit of performing regular tests.