ConversationalGeek®

Checklist of 10 Azure Backup Practical Tips

By Brien M. Posey, Microsoft MVP

Although backups have been around for as long as IT itself, cloud environments such as Microsoft Azure introduce new backup challenges. This list is designed to give you practical guidance for your Azure backups.

1 Make Sure that You Are Backing Up Your Data

The first step in formulating an Azure backup strategy is to figure out what it is that actually needs to be backed up. This means determining where your data resides within the Azure cloud and what is going to be required in order to protect that data. Remember, Azure data can reside in a variety of locations such as in virtual machines or in managed services such as Azure SQL. It's also possible that data might be scattered across multiple regions.

2 Use the Right Tool for the Job

As you work to protect your Azure data, it is important to make sure that you are using a modern Azure-aware backup solution. Legacy backup tools that were designed primarily for on premises use may be able to protect some of your Azure data, but chances are that they won't be able to protect all of it. For example, if you have data residing inside of a serverless database, then a legacy backup application probably won't be able to back that data up.

A legacy backup tool might also give you limited options for storing your backup data. For example, if you have made a conscious decision to run a particular workload in the cloud, then it might not make sense to store the workload's backups on premises. Even so, some legacy backup tools simply do not give you the option of using cloud-based backup targets.

3 Use Automation to Work Smarter, Not Harder

When it comes to backups, automation takes many different forms. For example, automation can consist of something as simple as scheduling backups to occur at a specific time. However, modern backup software gives IT pros the ability to automate more than just backup scheduling.

Historically, IT pros have had to cope with an entire laundry list of backup-related tasks that go well beyond just creating the backups themselves. Today, though, many of these tasks can be automated. For example, IT pros might consider automating backup lifecycle management or even backup testing.

4 Be Aware of Cloud Costs

From the very beginning, cloud service providers have marketed the public cloud as an inexpensive alternative to costly on-premises IT operations. In reality, however, organizations have often found that operating in Azure and other cloud environments can be just as expensive as maintaining workloads on premises.

When it comes to backing up Azure data, there are a few things that IT pros should keep in mind with regard to controlling costs. First, having an effective data lifecycle management policy is a must. Such a policy can help to limit the volume of data that is being backed up, as well as the size of the backups themselves. Second, be careful about using backup targets that reside on premises or in other cloud environments. Microsoft charges their subscribers a data egress fee for data leaving the Azure cloud, and these fees can be quite expensive for larger datasets.

Given the intricacies of managing costs in the cloud, it is important for your backup vendor to provide built-in backup cost calculation and data management tools that are aware of nuances of moving data in the cloud.

5 Use Storage Tiers Effectively

As you evaluate your backup storage options in Azure, you will inevitably have to select a storage tier. The available tiers vary considerably with regard to cost, availability, and performance. Higher performing storage tiers generally cost more.

It is worth noting that the tiers with the lowest cost per gigabyte might not necessarily give you the lowest overall costs, depending on how long you plan on keeping your backups. That's because the Cool tier has a minimum data storage duration of 30 days, while the Archive Tier has a minimum storage duration of 180 days. In other words, if you store data in these tiers, you will be paying to store that data for at least the minimum amount of time, even if you don't actually need to retain a backup for that long.

6 Isolate Your Backup Data

One of the most important things that an organization can do to protect its backups is to avoid keeping the backups online. A number of ransomware variants have been specifically designed to target backup servers, thereby leaving victims with little choice but to pay the ransom.

In the past, tape was the go-to mechanism for organizations that wanted to create an air gapped backup. Once the backup had been created, the tape could simply be removed from the tape drive. Although tape is not an option for cloud backups, another option does exist: Azure's Archive Tier is kept offline and has a latency of 2 hours.This can help to keep backup data out of harm's way. Another option is to simply ensure cloud storage is only accessible behind an account using multi-factor authentication; this keeps criminals from being able to use a leaked password or a brute force password attack from gaining access to your backups.

7 Consider the Importance of Data Mobility

Where you've got your cloud backup situated matters, business requirements around supporting hybrid/multi-cloud is on the rise, placing an emphasis on flexibility when it comes to both choosing and moving away from a given cloud vendor.

This, therefore, requires backup solutions that allow for a common control pane and portable backup formats. This helps facilitate the ability to move data across different platforms (on-premises to cloud, cloud back to on-prem, or from one cloud to another), avoiding platform lock-in.

8 Use a Single Backup Solution

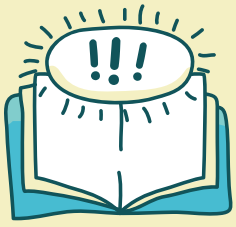
Today many organizations are using multiple backup products. An organization might use one backup tool to protect its on premises resources and another tool for protecting the resources residing in Azure. If at all possible, it's best to consolidate backup operations into a single backup tool. This helps to break down backup silos, giving organizations the ability to seamlessly move data between the cloud and its own datacenter. At the same time, using a single backup solution can greatly simplify backup operations while potentially also reducing licensing costs and reducing the chances that there are gaps that exist in the organization's data protection strategy.

9 Avoid Complexity Where You Can

The less complex a backup solution is, the more likely that it will work when you need it to. An overly complex backup solution is prone to human error, incorrect configurations, and compatibility issues as patches are released. As such, it is a good idea to look for a solution that not only has a simplified administrative interface, but that also simplifies the actual data protection process by not requiring agents. This means looking for a solution that can scale across environment of any size without the need for an admin to manually deploy agents for each new workload or to spend time writing automation scripts.

10 Having the Ability to Restore Matters

It is impossible to predict what the scope of a disaster will be or what systems will be impacted. As such, it is important to make sure that your backup solution will allow you to restore data to a dissimilar system or to the cloud. It is also important to be able to perform restores at a granular level. In the case of a virtual machine for example, you need to be able to restore the entire virtual machine, but you should also be able to restore a single file within the virtual machine just as easily.



To learn more about Azure Backup, visit

Veeam Backup for Microsoft Azure

Conversational Azure Backup Best Practices

Conversational Veeam Backup for Microsoft Azure