KEY CONSIDERATIONS FOR MANAGING BACKUPS TO THE CLOUD

Some of the lowest hanging fruit when it comes to delivery excellent return on investment in the cloud world, is making use of cloud storage for backup and archival purposes, whether you're trying to protect on premise, or cloud storage.

Azure Backup comprehensively protects your data assets in Azure through a simple, secure, and cost-effective solution that requires zero-infrastructure.

It's Azure's built-in data protection solution for a wide range of workloads. It helps protect your mission critical workloads running in the cloud, and ensures your backups are always available and managed at scale across your entire backup estate.

This guide maps out the considerations you should work through as you build the perfect backup and archival solution for your business.

CONSIDERATION ONE:
SUBSCRIPTION DESIGN

Apart from having a clear roadmap to navigate through the Cloud Adoption Journey, you must plan your cloud deployment's subscription design and account structure to match your organization's ownership, billing, and management capabilities.

As the vault is scoped to a subscription, your Subscription design will highly influence your Vault design. **Learn more** about different Subscription Design Strategies and guidance on when to use them.

CONSIDERATION TWO:
BACKUP REQUIREMENTS

To get started with Azure Backup, its best to plan your backup needs.

A great place to start is with your workloads. Thankfully, most of your decisions are taken care of.

Azure Backup enables data protection for various workloads (on-premises and cloud) – you just need to choose from the array of options available. Azure Backup uses reliable Blob storage with in-built security and high availability features. You can choose LRS, GRS, or RA-GRS storages (covered in Guide 1) for your backup data.

It also features native integration with Azure Workloads (VMs, SAP HANA, SQL in Azure VMs and even Azure Files) without requiring you to manage automation or infrastructure to deploy agents, write new scripts or provision storage.

Learn more about supported workloads.

CONSIDERATION THREE:
VAULTS

Azure Backup uses vaults (Recovery Services and Backup vaults) to orchestrate, manage backups, and store backed-up data. Effective vault design helps organisations establish a structure to organise and manage the backup assets in Azure to support your business priorities.

The first consideration to look at is whether you'll need single or multiple vaults

One of the requirements of Azure Backup is that the vaults are required to be present in the same region as the resource to be backed-up. Therefore, you should create separate vaults for each geographic region to protect your resources.

Next, consider if your business operations are divided into separate Business Units and if each business unit has its own set of departments. Your business needs may require each department to manage and access their own backups and restores. And enable them to track their individual usage and cost expense.

You might want to create one vault for each department in a BU.

Another vital consideration is asking If you plan to protect different types of workloads.

If the answer is yes, then it's recommended that you create separate vaults for each type of workload. This helps you to separate access boundaries for the users by allowing you to grant access (using Azure role-based access control – Azure RBAC) to the relevant stakeholders.

If your operations require you to work on multiple environments, such as production, non-production, and developer, then it's similarly recommended you create separate vaults for each.

It's also key to understand limitations. Azure Backup allows only 1000 Azure VMs to be backed-up in one vault.

So, if you have more than that, you should create two different vaults and distribute the resources accordingly.

Similarly, vault limits allow you to back up 2000 workloads (with a restriction of 1000 VMs) in each vault.

Therefore, mathematically you can back up 2000 workloads in one vault (1000 VMs + 1000 workloads).

That said, this type of segregation isn't recommended as you won't be able to define access boundaries and the workloads won't be isolated from each other.

So, to distribute the workloads correctly, create separate vaults for workloads and VMs.

It's also wise to review the default settings for Storage Replication type and Security settings to meet your requirements before configuring backups in the vault.

Non-critical workloads like non-production and development are suitable for LRS storage replication.

Zone redundant storage (ZRS) is a good storage option for a high Data Durability along with Data Residency.

Geo-Redundant Storage (GRS) is recommended for mission-critical.

Before finalizing your vault design, review the **vault support matrixes** to understand the factors that might influence or limit your design choices.

CONSIDERATION FOUR:
BACKUP POLICIES

Azure Backup Policy has two components: Schedule (when to take backup) and Retention (how long to retain backup). You can define the policy based on the type of data that's being backed up, RTO/RPO requirements, operational or regulatory compliance needs and workload type. You can **learn more** about this in detail.

While scheduling your backup policy, consider scheduling the most frequently available automated backups per day for mission-critical resources.

For a resource that requires the same schedule start time, frequency, and retention settings, you need to group them under a single backup policy.

It's recommended that you keep the backup scheduled start time during non-peak production application time. And to distribute the backup traffic, its recommended that you back up different VMs at different times of the day.

CONSIDERATION FIVE:
RETENTION

In short, short-term retention can be "daily". Retention for "Weekly", "monthly" or "yearly" backup points is referred to as Long-term retention.

If you know in advance that data is required years from the current time, then use Long-term retention. If you don't know in advance, then use you can use on-demand with specific custom retention settings (these custom retention settings aren't impacted by policy settings).

If you need to take a backup not scheduled via backup policy, then you can use an on-demand backup. This can be useful for taking backups that don't fit your scheduled backup or for taking granular.

It's important to note that the retention policy defined in scheduled policy doesn't apply to on-demand backups.

As your business requirements change, you might need to extend or reduce retention duration.

If retention is extended, existing recovery points are marked and kept in accordance with the new policy. If retention is reduced, recovery points are marked for pruning in the next clean-up job, and subsequently deleted.

And remember, the latest retention rules apply for all retention points (excluding on-demand retention points).

So if the retention period is extended (for example to 100 days), then when the backup is taken, followed by retention reduction (for example from 100 days to seven days), all backup data will be retained according to the last specified retention period (that is, 7 days).

Azure Backup provides you with the flexibility to stop protecting and manage your backups. So if you're retiring or decommissioning your data source (VM, application), but need to retain data for audit or compliance purposes, then you can use this option to stop all future backup jobs from protecting your data source and retain the recovery points that have been backed up.

Stop protection and delete backup data will stop all future backup jobs from protecting your VM and delete all the recovery points. You won't be able to restore the VM nor use Resume backup option.

If you resume protection (of a data source that has been stopped with retain data), then the retention rules will apply. Any expired recovery points will be removed (at the scheduled time).

CONSIDERATION SIX:
SECURITY

To help you protect your backup data and meet the security needs of your business, Azure Backup provides confidentiality, integrity, and availability assurances against deliberate attacks and abuse of your valuable data and systems.

Azure role-based access control (Azure RBAC) enables fine-grained access management, segregation of duties within your team and granting only the amount of access to users necessary to perform their jobs. **Learn more here**.

If you've got multiple workloads to back and you've multiple stakeholders to manage those backups, it is important to segregate their responsibilities so that user has access to only those resources they're responsible for.

You can also segregate the duties by providing minimum required access to perform a particular task. For example, a person responsible for monitoring the workloads shouldn't have access to modify the backup policy or delete the backup items.

Azure Backup provides three built-in roles to control backup management operations: Backup contributors, operators, and readers.

Storage accounts used by Recovery Services vaults are isolated and can't be accessed by users for any malicious purposes. The access is only allowed through Azure Backup management operations, such as restore. You should also investigate encryption of data in transit and at rest.

Within Azure, data in transit between Azure storage and the vault is protected by HTTPS. This data remains within the Azure network.

Backup data is also automatically encrypted using Microsoft-managed keys.

When it comes to protection of backup data from unintentional deletes, Azure Backup looks after you with the **Soft-Delete** feature by allowing you to recover those resources after they are deleted.

With soft delete, if a user deletes the backup, the backup data is retained for 14 additional days, allowing the recovery of that backup item with no data loss. The additional **14 days retention** of backup data in the soft delete state doesn't incur any cost. Learn more

And what about rogue administrators?

A rogue administrator can delete all your business-critical data or even turn off all the security measures that may leave your system vulnerable to cyber-attacks.

Azure Backup provides you with the **Multi-User Authorization (MUA)** feature to protect you from such rogue administrator attacks. Multi-user authorization ensures that every privileged/destructive operation is done only after getting approval from a security administrator.

The same principles apply to ransomware protection. A malicious actor isn't able to encrypt your backup data as this can only be performed through Recovery-Services vault or Backup Vault, which can be secured by Azure role-based access control (Azure RBAC) and MUA.

Soft delete protects against deletion of backup data by a malicious actor. And by using longer retention (weeks, months, years) you can ensure clean backups (not encrypted by ransomware) don't expire prematurely.

Don't forget there's also strategies in place for early detection and mitigation of such attacks on source data.

Should any of these tactics be attempted by a malicious actor however, Azure Backup will send a critical alert over your preferred notification channel. **Learn more**

CONSIDERATION SEVEN:
NETWORKING

Azure Backup requires movement of data from your workload to the Recovery Services vault and provides several capabilities to protect backup data from being exposed inadvertently (such as a man-in-the-middle attack on the network).

For example, when it comes to VMs all the required communication and data transfer between storage and Azure Backup service happens within the Azure network without needing to access your virtual network.

For additional security that ensures your resources aren't available to the public interne, use **Azure Private Endpoint**. This is a network interface that connects you privately and securely to a service powered by Azure Private Link.

CONSIDERATION EIGHT:
GOVERNANCE

Governance in Azure is primarily implemented with Azure Policy and Azure Cost Management.

Azure Policy allows you to create, assign, and manage policy definitions to enforce rules for your resources. This feature keeps those resources in compliance with your corporate standards.

Azure Cost Management allows you to track cloud usage and expenditures for your Azure resources and other cloud providers.

CONSIDERATION NINE:
RETENTION

As a backup user or administrator, you should be able to monitor all backup solutions and get notified on important scenarios.

Azure Backup provides built-in job monitoring for operations such as configuring backup, back up, restore, delete backup, and so on. This is scoped to the vault, and ideal for monitoring a single vault. Learn more here.

If you need to monitor operational activities at scale, then Backup Explorer provides an aggregated view of your entire backup estate, enabling detailed drill-down analysis and troubleshooting. Learn more here.
If you need to retain and view the operational activities for long-term, then use Reports. A common requirement for backup admins is to obtain insights on backups based on data that spans an extended period.

You can also send data to the Log Analytics workspace or to an Azure event hub if you'd like to use a third-party Security Information and Event Management tool for detailed interrogation.

If you want to retain your log data longer than 90 days for audit, static analysis, or back up, you can use a Azure Storage account.

And for up to the minute, immediate feedback on the status of your backups, you can configure critical alerts and route them to any preferred notification channel.

Many of failure errors or outage scenarios are transient in nature. They can often be remediated by setting up the right Azure role-based access control (Azure RBAC) permissions or to just re-trigger the backup/restore job.

The smartest way to handle these scenarios is to automate the retry of failed jobs.