Backup-as-a-Service Choices for Protecting VMs Hosted in the Microsoft Azure Cloud: HYCU for Azure and Azure Backup

by DCIG President & Founder, Jerome Wendt

PRODUCTS

HYCU for Azure

URL ▶ **https://www.hycu.com/**

HYCU, Inc.
109 State Street
Boston, MA 02109
(617) 617-9100

Microsoft Azure Backup

URL ▶ **https://azure.microsoft.com/en-us/services/backup/**

Microsoft Corporation
One Microsoft Way
Redmond, CA 98052
(425) 882-8080

The Business Case for the Microsoft Azure Cloud

Many organizations in the 2020's expect to use a general-purpose cloud provider to host some or all their applications. As they contemplate their available cloud options, the Microsoft Azure cloud makes the short list for many organizations.

Enterprise familiarity with Microsoft products coupled with Azure's support for Microsoft's applications can drive the business case for Azure. Already the percentage of companies in 2019 that adopted Microsoft Azure nearly matches Amazon Web Services (AWS). Further, recent surveys suggest this trend will continue to grow in the coming decade.[1]

As companies adopt Azure, they will transition to and host Linux- and Windows-based applications in it. This cloud adoption will force them to re-examine how they manage and support applications and data once in the cloud.

Backup should rank near the top of the list of solutions that organizations re-evaluate as they move to the cloud. Their existing backup solutions may not work well or even break down once moved to the Azure cloud. This should come as no surprise. They were never originally designed nor intended to operate using Azure's architecture and resources. Organizations should therefore use their move to the Azure cloud as an opportunity to select a backup solution optimized for it.

Among available cloud backup solutions, organizations should prioritize those that deliver backup-as-a-service (BaaS). By selecting this approach, they consume backup services in the same way they consume other cloud resources. They only pay for the resources they use when they use them. Two such offerings already exist: Microsoft Azure Backup and HYCU for Azure.

BaaS in Microsoft Azure

Both Microsoft Azure Backup and HYCU for Azure (HYCU) deliver their respective solutions as a BaaS in Azure. Organizations may subscribe to either one of these solutions in the Microsoft marketplace. Using either of these backup services they only pay for these services when they use them with no up-front costs.

A BaaS architecture eliminates many of the hassles associated with deploying backup in the cloud. Both Microsoft and HYCU assume all responsibilities for the backend administration of their respective BaaS solutions. They do not require organizations to buy any backup software. Organizations also do not need to acquire any servers or VMs to host these solutions.

Microsoft and HYCU both assume much or all responsibility for the ongoing maintenance of their solutions. They handle all fixes, patches, and upgrades to their solution without requiring organizations to get involved in these activities.

Their BaaS solutions both leverage and integrate with Azure's identity and access management (IAM) services. Azure's IAM provides a single sign-on to Azure services and these two BaaS platforms. Within Azure IAM, organizations can create groups or individual roles, assign permissions to them, and then place users in the appropriate group or role.

This approach eliminates the need for separate backup management consoles for administrators and users to access. It automatically grants users access to backups that they may use to perform recoveries.

Despite both Azure Backup and HYCU for Azure sharing certain BaaS traits, they diverge in how they deliver many of their backup features. These differences surface in multiple areas to include administering backup policies, backup jobs, backup storage, pricing, recoveries, and support.

Backup Policy Administration

Once subscribed to either Azure Backup or HYCU for Azure, organizations can potentially skip the step of creating backup policies and schedule backups. Immediately scheduling backup jobs hinges on the usability of default backup policies included with the solution. While both solutions provide default backup policies, they differ in their number and quality.

1. Browning, Jack. "10 Cloud Adoption Stats IT Decision Makers Need to Know for 2020." Impact Networking. 13 Nov 2019. https://www.impactmybiz.com/blog-10-cloud-adoption-stats-it-decision-makers-2020/. Referenced 1/8/2020.

Default Backup Policies

Azure Backup provides one default backup policy. When applied to a virtual machine (VM), it will back up that VM by taking a snapshot of it daily. It then retains that backup for 30 days.

HYCU offers four different default backup policies: Bronze, Silver, Gold, and Platinum. HYCU's Bronze level backup resembles Azure Backup's single default policy. It backs up data once every 24 hours and retains each backup for a week.

Each tier above its Bronze policy backs up data more frequently. Its Silver policy backs up data every 12 hours, its Gold tier every four hours, and its Platinum policy once every two hours. All four policies have the same one-week retention period for each backup. These four default policies increase the odds that an organization can use HYCU to immediately schedule backup jobs.

New Policy Creation

Default policies notwithstanding, most organizations will eventually need to create a backup policy. In this respect, Azure Backup and HYCU share one important similarity: they both create global backup policies. Once created, anyone can apply any policy to any VM.

The differences between each solution become clearer during backup policy creation. A new Azure Backup policy only currently provides a choice between daily and weekly backups. It limits the number of recovery snapshots to 9,999 though it does permit the retention of any snapshot for an unlimited time.

Like Azure Backup, HYCU permits the retention of any backup for an unlimited period. HYCU differs in that it provides more granular choices for how frequently it can take snapshots. Using HYCU one can schedule snapshot to occur every hour. One may also configure a HYCU policy to take and retain an unlimited number of snapshots. (Figure 1.)

FIGURE 1

Backup Policy Administration

	HYCU for Azure	Azure Backup
Backup Policy Scope	Global	Global
Default Policies (Number)	4	1
Scheduled Backups—Frequency Options	Weekly, Daily, Hourly	Weekly, Daily
Backup Retention Period	No Limit	No Limit
Restoration Points (Max)	No Limit	9,999
VM Discovery	Automatic	Manual
Scans for Unprotected VMs	Every 5 Minutes	●
Central Backup Management Console	✔	●
Policy Assignment Options	Individual VM Group of VMs Auto-assigned User-assigned	Individual VM User-assigned

Policy Assignment

Both products require that organizations assign a policy to a VM for a backup to occur. They each differ in the process that organizations must follow to assign a policy.

Using Azure Backup, one must navigate to and select a VM from within Azure's central management console. After selecting a VM, a user must click on the Backup tab and assign a backup policy to a VM.

One may use Azure's central management console to assign an HYCU backup policy to a VM. However, HYCU provides its own dedicated console for centralized backup policy management.

Using HYCU's console, a user may apply a policy to multiple VMs at the same time. To do so, one first selects the policy to apply to the VM. HYCU's console then presents all the VMs that a user has permissions to view. A user may then select one or more VMs or search for the specific VMs. Finally, a user selects the VM or VMs to protect and applies the policy to them.

A user may also configure HYCU to automatically discover new VMs and assign a designated backup policy to them. Once enabled within HYCU's management console, HYCU will scan the environment every five minutes for unprotected VMs. HYCU will then automatically apply the designated backup policy to any unprotected VMs it discovers.

Key questions to ask:

- Do you need the backup solution to detect and protect unprotected VMs?
- Do different applications and VMs in your environment have different data protection and retention requirements?
- How frequently do you need to take backups? Once a day? More often?
- Do you need a central backup console that provides a consolidated view of the VMs in the environment and their protected status?
- Do you need a central backup console that can assign a backup policy to multiple VMs at the same time?

Backup Job Methodology

Once an organization assigns a backup policy to a VM, backups of the protected VMs begin. Both Azure Backup and HYCU use very similar processes to complete backups. Both:

- Use snapshots to perform backups
- Take an initial full backup of the VM
- Offer an option to kick off a backup job immediately when configuring a VM for backup
- Take incremental backups forever after the first backup

HYCU does differentiate itself in one notable way from Azure backup when performing its backups. Like Azure Backup, it makes a copy of the VM by performing a snapshot of it. Once the snapshot completes, HYCU mounts the copy of that VM.

This approach frees HYCU to use its own computing resources to back up the VM as well as index the data in It. Since HYCU uses its own

computing resources and not the VM's, it negates any potential performance impact to production applications during the backup. (Figure 2.)

FIGURE 2

Backup Job Performance

	HYCU for Azure	Azure Backup[2]
Backup Methodology	Snapshot	Snapshot
First Backup	Full	Full
Indexes Data During Backup	✔	●
Resources Used	HYCU's Cloud Compute	VM's Cloud Compute
Subsequent Backups	Incremental	Incremental

Key questions to ask:

- How much data is in each VM to protect?
- Can your production applications sustain performance hits during their backup?
- Do you have multiple VMs to backup initially?
- Do you need to perform granular file and folder recoveries?

Backup Storage Administration

As each solution completes its backup, they both, by default, adhere to the same two practices when storing backup data. They both store backup data on Azure Block Blob storage. They both place backup data in the same Azure region as where the VM resides.

These two practices facilitate faster backups, minimize costs, and preserve data integrity. Azure Block Blob storage acts as an immutable data store that protects against unauthorized data tampering by either users or ransomware.

Differences between Azure Backup and HYCU do surface in how they configure and manage the backend storage. Azure Backup places the responsibility of storage allocation, configuration, and management upon the user.

As part of configuring a backup policy, a user must select an Azure Block Blob backup target. The Azure backup policy defaults to geo-redundant storage (GRS) as the storage tier. A user may also choose Azure's locally redundant storage (LRS). LRS provides lower data availability and redundancy at a lower cost than GRS.

Using Azure Backup, organizations must choose the policy's underlying storage tier. Once they make a choice, they cannot change the backup target for that policy. Azure Backup then retains all backup data on that storage tier for the period defined in the policy.

In contrast, HYCU abstracts away the need for organizations to decide between storage tiers. HYCU automatically places data on the most appropriate storage tier in Azure based on the policy's data retention setting. HYCU decides where to place data based on variables such as speed of backup, speed of recovery, and cost.

HYCU mitigates the need for organizations to master storage management in Azure. HYCU handles all backend storage tasks such as managing backup vaults, available storage capacity, and Azure Resource Groups.

Finally, HYCU eliminates some of the guesswork around billing. HYCU only does capacity-based billing and its rates start at about thirteen cents per GB per month. Conversely, Azure Backup charges $5 per protected VM per month and for storage capacity. Its capacity-based rates start at two cents per GB per month. (Figure 3.)

FIGURE 3

Backup Storage Administration

	HYCU for Azure	Azure Backup
VM Backup Target	Azure Block Blob	Azure Block Blob
Default Blob Storage Type	Automatically distributes data across GRS & LRS based on policy	Geo-redundant storage (GRS) Locally redundant storage (LRS)
Storage Tiering	Auto tiering based on policy	User managed
Default Blob Region Target	Same region as VM	Same region as VM
Change Storage Target in Policy	Anytime	Only before first backup
Vault	HYCU managed	User sets up and configures
Billing	Capacity-based billing only Starts at .128 per GB per month for daily backups	$5+ per VM instance per month Starts at .02 per GB per month Storage costs in addition to per VM cost[3]

Key questions to ask:

- How familiar are you with configuring and managing Azure Block Blob storage?
- Do you know which backup storage tier is best for each application?
- Can you predict and track how many VMs will you protect?
- Do you need to accurately forecast your total monthly Azure bill?
- Would you prefer the BaaS automatically optimize backup data placement in Azure?
- Do you want or need to change backup data placement after creating the backup policy?

Monitoring, Recovery, and Support

Once organizations have backup jobs up and running, they must manage them. This includes monitoring backup jobs, recovering from backups, and accessing technical support when needed.

Azure Backup and HYCU both provide numerous options for monitoring and alerting on backups. They both generate alerts when backup jobs or restores fail as well as if someone suspends backups

2. https://docs.microsoft.com/en-us/azure/backup/backup-support-matrix. 12/27/2019.
3. https://azure.microsoft.com/en-us/pricing/details/backup/. 1/1/2020

on a VM. HYCU does differ in that it offers options to generate alerts if someone or some application modifies or deletes backup data.

The larger differences between the two solutions show up in how they respectively handle recoveries and technical support. Azure Backup currently only recovers full VMs. While HYCU supports full VM recoveries, it can also perform file and folder recoveries. It can, as well, provide more recovery points since it can back up a VM multiples times a day.

Organizations must also factor in HYCU's technical support when deciding between these two solutions. Though both offer "free" technical support, HYCU gives all its subscribers free access to its premium level of technical support. This includes email, phone, and web support.

To receive anything more than email support from Azure Backup, subscribers need to pay extra. Azure Backup's same day technical support starts at $100 per month and could easily exceed $1,000 per month. (Figure 4.)

FIGURE 4

Alerting, Recovery, and Support

	HYCU for Azure	Azure Backup
Backup Failure	✓	✓
Backup Data Deletion	✓	○
Backup Data Modification	✓	○
Exposes Logs to Azure Monitor	Roadmap	✓
Restore Failure	✓	✓
Stop Protection – Retain Data	✓	✓
Stop Protection – Delete Data	✓	✓
File Recovery w/o VM Mount	✓	○
Folder Recovery w/o VM Mount	✓	○
Support	Included	Free - $1,000+/ month
Production Tech Support	Included	Starts at $100/month[4]

Key questions to ask:

- Do you want to restore an entire VM and then navigate through it to find and recover specific files or folders?
- Do you want or need access to technical support in minutes or hours? Will you pay extra for it?
- Do you want the solution to generate an alert if someone or some application modifies or deletes existing backup data?

There's Azure Backup and then There's HYCU for Azure

Both Azure Backup and HYCU for Azure provide organizations the essential tools to backup and recover VMs hosted in Azure. Using either of these two solutions, organizations can successfully schedule and perform full VM backups and restores. However, they differ greatly in their respective abilities to provide a hassle-free backup and recovery experience in the Azure cloud.

HYCU packages the extra features that organizations need to streamline implementing backup and recovery in the Azure cloud. HYCU:

- Offers four default backup policies to match the backup needs of different VMs
- Scans Azure environments for new VMs and automatically applies a backup policy to them
- Backups do not impact the performance of the application running on the VM
- Optimally manages data placement and storage allocation on Azure Blob
- Only charges based on capacity usage to keep billing and forecasting simple
- Includes premium technical support at no extra charge

HYCU for Azure handles all the little, hidden administrative tasks associated with backup that frequently get overlooked. In so doing, HYCU takes the hassle out of performing and managing backups and recoveries in Azure. This simplicity frees organizations to focus on why they choose the Azure Cloud in the first place: to increase their productivity and drive down costs. ■

4. https://azure.microsoft.com/en-us/support/plans/. 1/1/2020.