



# Commvault Azure SQL Protection

**Copyright, Confidentiality and Non-Disclosure agreements apply.**

This document may contain forward-looking statements, including statements regarding financial projections, which are subject to risks and uncertainties, such as competitive factors, difficulties and delays inherent in the development, manufacturing, marketing and sale of software products and related services, general economic conditions, and others. Actual results may differ materially from anticipated results. The development and timing of any release, as well as any of its features or functionality, remain at our sole discretion. Any information about any software features or functionality is not a commitment, promise or legal obligation to deliver any material, code, or functionality.

## **Confidentiality**

This document contains information that is confidential and proprietary to Commvault. Without limiting rights under copyright or otherwise, this information is provided with the express understanding that it will be held in strict confidence and that no part of this document will be disclosed, used, reproduced, stored, or transmitted, in whole or in part, for any purpose other than as expressly approved or provided by Commvault in writing.

©1999-2023 Commvault

# Table of Contents

<b>INTRODUCTION .....</b>	<b>4</b>
<b>AUDIENCE .....</b>	<b>4</b>
<b>OBJECTIVES .....</b>	<b>4</b>
<b>OVERVIEW.....</b>	<b>4</b>
<b>CHALLENGES WITH AZURE AUTOMATED BACKUPS.....</b>	<b>4</b>
<b>THE COMMVAULT ADVANTAGE .....</b>	<b>5</b>
<b>SOLUTION ARCHITECTURE.....</b>	<b>5</b>
<b>CONFIGURATION.....</b>	<b>6</b>
<b>AZURE SQL BACKUP AND RESTORE PROCESS .....</b>	<b>11</b>
<b>AZURE SQL MANAGED INSTANCE BACKUP AND RESTORE PROCESS .....</b>	<b>13</b>
<b>AZURE SQL BACKUP METRICS.....</b>	<b>14</b>
<b>TEST LAB ENVIRONMENT.....</b>	<b>14</b>
<b>TEST PLAN AND TEST RESULTS.....</b>	<b>15</b>
<b>INFERENCE FROM TEST RESULTS.....</b>	<b>15</b>
<b>PERFORMANCE CONSIDERATIONS.....</b>	<b>15</b>

---

**SUMMARY..... 16**

## INTRODUCTION

In today's data-driven world, businesses rely heavily on reliable database solutions like Azure SQL Database to manage their critical information. However, relying solely on Azure's automated backup solutions may not be sufficient for many organizations. This whitepaper will explore how Commvault addresses these limitations by providing a comprehensive and robust backup solution for Azure SQL databases.

## AUDIENCE

This whitepaper is intended for:

- IT administrators and database professionals responsible for data availability and integrity of Azure SQL databases.
- Business decision-makers interested in understanding the benefits of Commvault's Azure SQL backup solution.

## OBJECTIVES

This whitepaper aims to achieve the following objectives:

- Explain the limitations of relying solely on Azure's automated backups.
- Introduce Commvault's Azure SQL backup solution and its key features.
- Provide a detailed overview of the architecture, configuration, and processes involved in backing up and restoring Azure SQL databases using Commvault.
- Highlight the benefits of using Commvault for Azure SQL backup, including performance metrics.

## OVERVIEW

Azure SQL is a managed cloud database service from Microsoft that provides a highly available, scalable, and secure platform for your applications. You can choose from a variety of pricing options to fit your budget, and Azure SQL automatically handles infrastructure management tasks such as upgrades, patching, backups, and monitoring.

Commvault provides robust Azure SQL backup and restore capabilities, encompassing entire instances, and full Azure subscriptions. Flexible scheduling options and retention policies automate your backups. De-duplicated and compressed air-gapped backups to make sure that customer is always ransomware ready.

## CHALLENGES WITH AZURE AUTOMATED BACKUPS

While Azure provides automated backups for SQL databases, relying solely on these has several limitations:

- **Predetermined Backup Frequency:** Azure's automated backups operate on a fixed schedule. Users lack the flexibility to adjust the frequency of backups to suit their specific needs.
- **Retention Limits:** There are limitations on how long Azure retains these backups. This might not align with the data retention requirements for compliance purposes of many businesses.

- **On-Demand Backups:** Users cannot trigger backups on-demand. This is a significant limitation in scenarios where an immediate backup is needed before critical operations.
- **Lack of Portability:** Azure automated backups cannot be restored to different clouds or on-premises SQL servers, restricting the ability to maintain hybrid/multi-cloud environments or to perform certain data recovery scenarios.

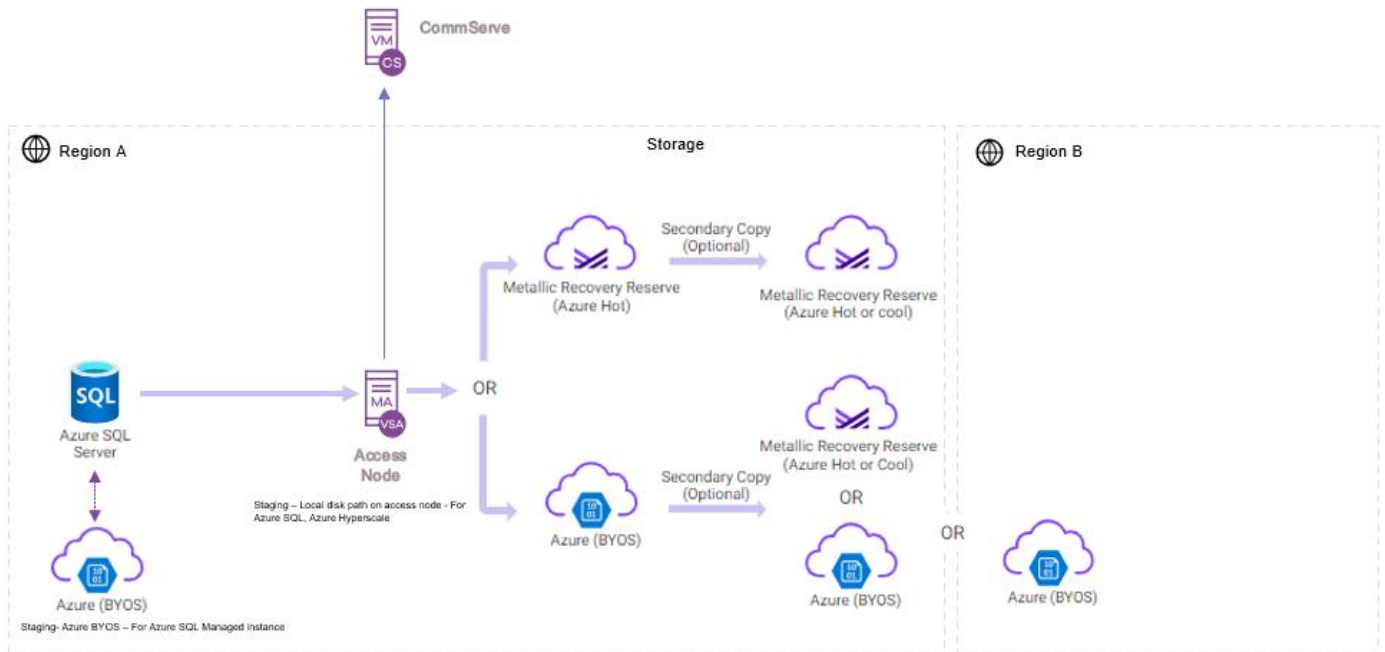
These limitations underline the importance of a more versatile and comprehensive backup solution like Commvault for Azure SQL databases.

## THE COMMVAULT ADVANTAGE

The growing trend of multi-cloud and hybrid deployments, while offering flexibility and vendor neutrality, presents a significant challenge: fragmented data protection. This fragmented landscape, combined with the shared responsibility model, demands a robust and integrated solution. Cloud native approaches, hampered by inflexibility and compliance concerns, are inadequate.

- **Single SLA policy/Plan:** Streamline data protection with one SLA policy that applies across all data sources and destinations, simplifying management and providing consistent service levels.
- **Flexible scheduling:** Schedule backups and archives based on your specific needs, including dynamic adjustments to optimize resource utilization and adapt to changing workloads.
- **Flexible Retention Periods:** Store backups for as long as needed, from days to years, meeting diverse regulatory and compliance requirements.
- **Immutable backups:** Protect against accidental deletion or ransomware attacks by creating immutable backups that cannot be modified or overwritten.
- **Portability across clouds and hybrid cloud:** Move data seamlessly between different cloud environments and hybrid deployments without vendor lock-in or data loss, allowing flexibility and resilience.
- **Simplified data protection:** Manage backups and archives across your entire environment from a single, centralized platform and user interface, reducing complexity and saving valuable time.

## SOLUTION ARCHITECTURE



CommServe – Responsible for configuration and scheduling.

MA(MediaAgent) – Manages deduplication database and communication to storage.

Access Node – Manages data transfer with Azure SQL

Storage – Azure Blob (BYOS - Bring Your Own Storage) or Commvault Metallic Recovery Reserve blob storage- Stores de-duplicated and compressed backups and air gapped copies of backups.

Azure SQL Server – Azure SQL or Azure Managed Instance or Azure Hyperscale

Staging – For staging backups during the backup and restore process

## CONFIGURATION

### PRE-REQUISITES

- **Network Requirements**

Verify that the following ports are open on the access node that has access to the Azure SQL:

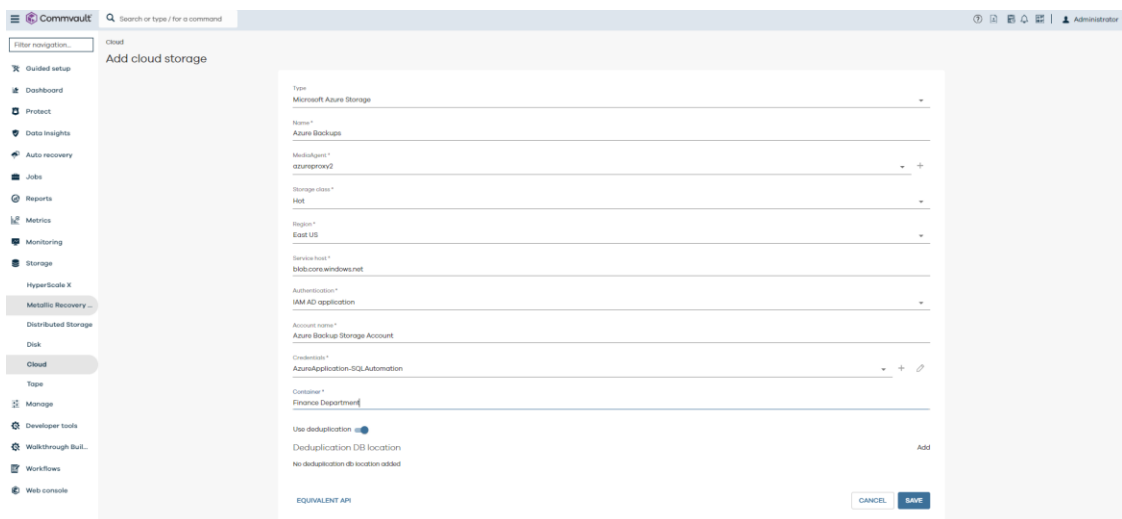
- 8443 to https://management.core.windows.net:8443
- 1433 to \*.database.windows.net

The Azure SQL configuration workflow from the Commvault UI seamlessly walks a customer through the following steps.

- Create a storage destination.
- Create a plan.
- Set up Azure SQL cloud account authentication.
- Discover SQL instances and databases.
- Associated discovered instances/databases to the plan.
- Run schedules backups or on demand backups and restores.

## Create a storage destination

A storage destination streamlines data protection by offering a centralized repository for backups and archives across your entire cloud environment. It eliminates the need for managing multiple cloud storage accounts and simplifies operations through a unified web-based interface. Configuration is straightforward, with flexible options for data placement and encryption with compliance and security. Additionally, Commvault provides global deduplication and compression, minimizing storage requirements and optimizing costs.



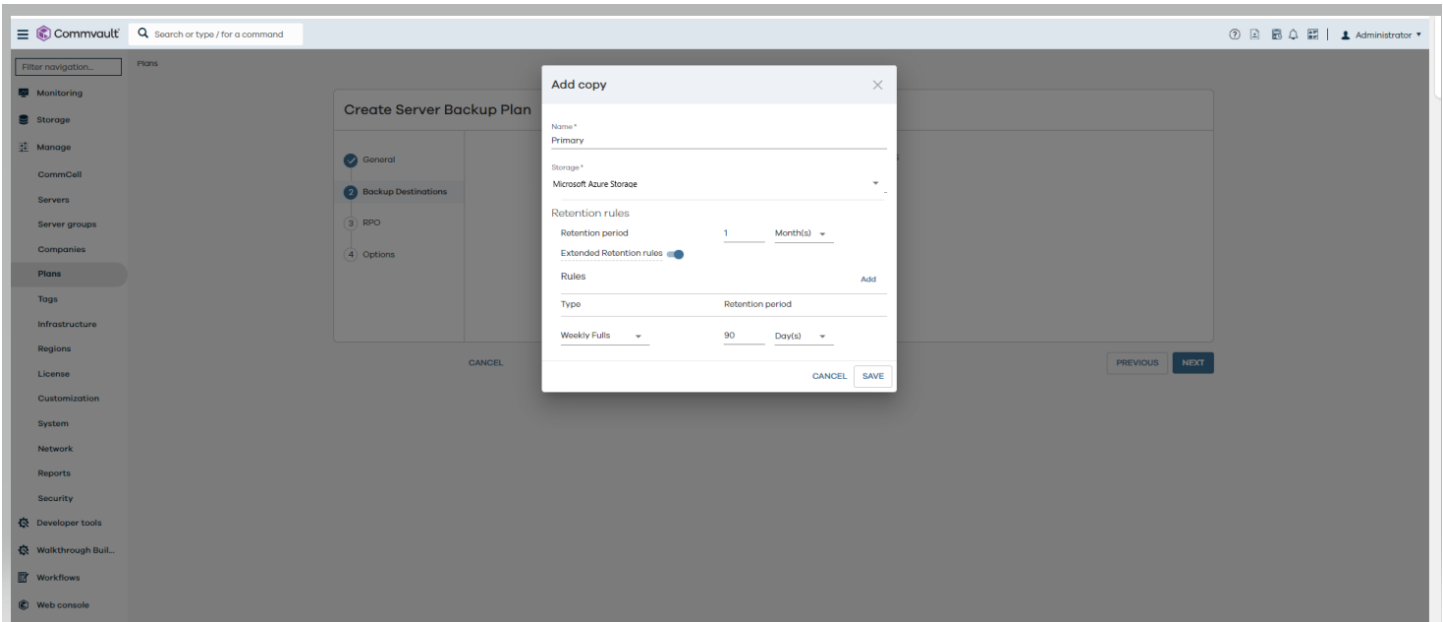
The screenshot shows the 'Add cloud storage' configuration page in the Commvault web interface. The page is titled 'Add cloud storage' and contains a form with the following fields:

- Type: Microsoft Azure Storage
- Name: Azure Backups
- Multiagent: storageproxy2
- Storage class: Hot
- Region: East US
- Service host: blob.core.windows.net
- Authentication: IAM AD application
- Account name: Azure Backup Storage Account
- Credentials: AzureApplication-SQL\_Automation
- Container: Finance Department

There is also a section for 'User deduplication' with a toggle switch and a 'Deduplication DB location' field with an 'Add' button. At the bottom, there is an 'EQUIVALENT API' label and 'CANCEL' and 'SAVE' buttons.

## Create a plan

A plan acts as a central orchestration tool, defining and automating backup workflows for a customer's entire IT environment, which eliminate manual configuration by encapsulating backup policies, schedules, and destinations within a single, reusable entity. This allows for easy deployment across diverse environments and provides consistent, reliable data protection. Additionally, plans also offer dynamic scheduling options.



## Set up Azure SQL cloud account authentication

Commvault needs a connection to the customer's Azure subscription(s) to protect Microsoft Azure SQL. Commvault utilizes the Microsoft Azure SQL Database REST APIs that are secured by Azure Active Directory, which in turn provides identity and access management for the Azure cloud. This allows for a secure and controlled interaction between Commvault and a customer's Azure SQL environment.

Two steps of configuration are required in Commvault to protect Azure SQL. The first step of the configuration allows Commvault to automatically discover all Azure SQL instances in each subscription. The second step of the configuration sets up authentication to discover databases and back them up.

Commvault recommends using managed identities for discovering Azure SQL instances. Azure Managed Identities are a feature of Azure Active Directory (Azure AD) that automatically manages credentials for Azure resources. They provide a secure and convenient way to authenticate to Azure resources without having to store or manage secrets in Commvault thus enhancing the overall security of the environment.

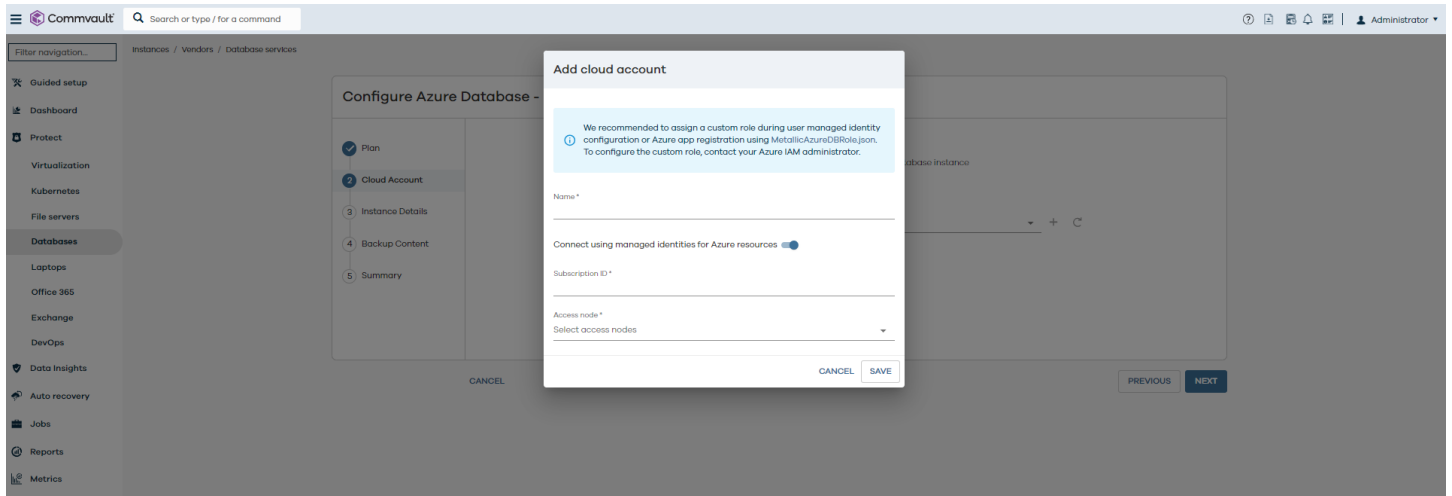
On the Azure portal ->access node VM-> Identity tab->system assigned->on->save.

On the Azure portal ->subscriptions-> Access control (IAM) ->role-> 'contributor role' (for more restricted roles check this link

[https://documentation.commvault.com/v11/expert/setting\\_up\\_managed\\_identities\\_for\\_azure\\_resources.html](https://documentation.commvault.com/v11/expert/setting_up_managed_identities_for_azure_resources.html))

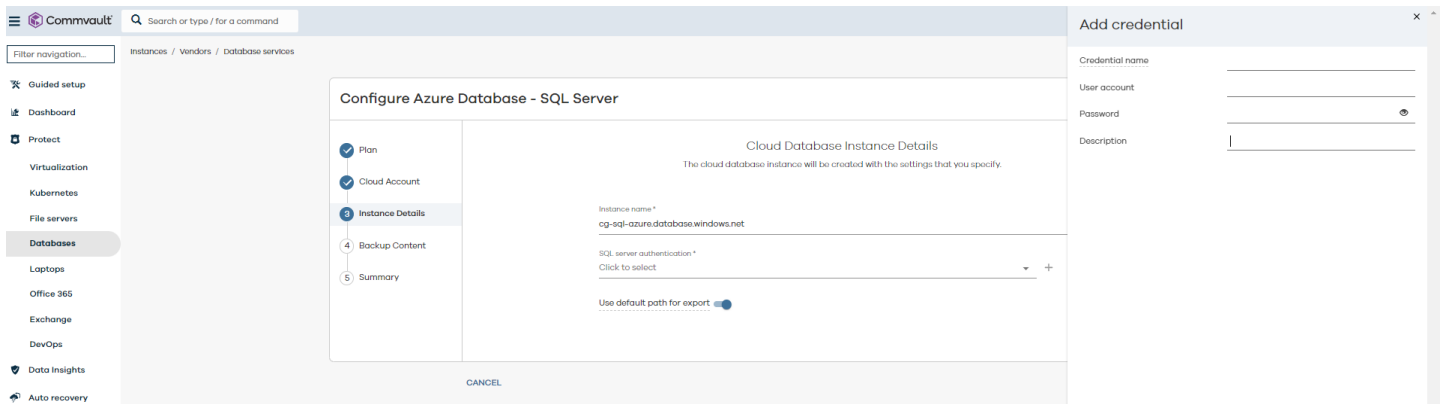
On the Azure portal ->subscriptions-> members ->assign access to 'Managed Identity'-> select members->subscription of the access node, managedidentity:access node





## Setup database authentication

AD authentication or SQL server authentication can be used for the database backups. Credentials can be created once and securely stored in a Commvault credential vault that allows for easy re-use for configuration and easy password rotation.



## Associated discovered instances/databases to the plan

**Configure Azure Database - SQL Server**

Summary

Congratulations! You have successfully configured a new cloud database instance. A backup job will be started in accordance with your selected backup plan.

Plan name	Cloud Clients Plan
Backup frequency	1 day
Cloud account	AzureChris_MI
Cloud database instance	vosqazurenw.database.windows.net

**FINISH**

## Run and On-Demand or Scheduled backups

**chrisazuresql.database.windows.net**

Overview Configuration Subclients Jobs

**Databases**

Protected	Not protected	Backup with errors
10	0	0

**General**

Cloud account	AzureChris_MI
Database engine	SQL Server
Server type	Azure Database Engine
Version	12.00.5249
Status	Ready
Total number of databases	10
Application size	0 B
A SQL Server account	AzureSQLServerAdmin - ADCreds - Windows Account
Plan	Cloud Clients Plan

**Recovery points**

December 2023

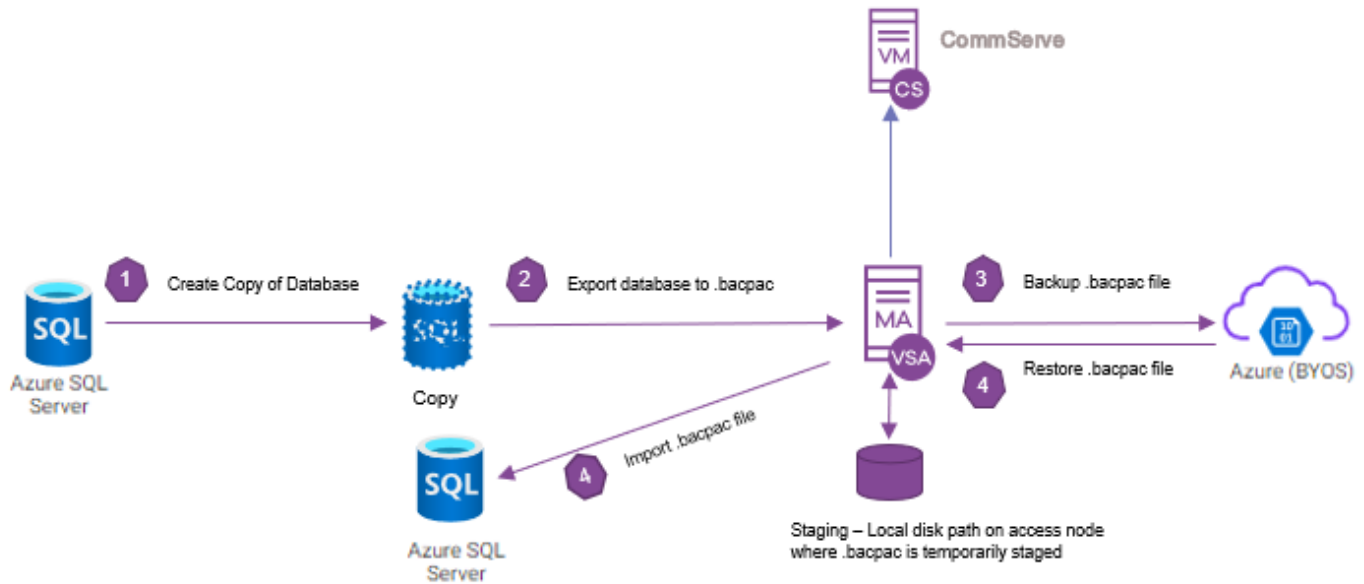
Sun	Mon	Tue	Wed	Thu	Fri	Sat
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31						

December 7 18:00:27

**Backup** **Deconfigure**

## AZURE SQL BACKUP AND RESTORE PROCESS

### Azure SQL Backup and Restore Flow



#### Backup Process:

1. The CommServe starts backup based on the schedule defined in the plan or a user can start an on-demand backup.
2. The CommServe sends the backup request to the Commvault SQL agent on the access node.
3. The Commvault SQL agent on the access node uses Azure SQL REST APIs to first create a transactionally consistent copy of the Azure SQL database under the same server as the original database. This is the method recommended by Microsoft.

<https://learn.microsoft.com/en-us/azure/azure-sql/database/database-copy?view=azuresql&tabs=azure-powershell>

- The copy has the same access controls as the source database. For e.g., if the source is accessed with a private end point, then the copy will continue to be accessed with a private end point.

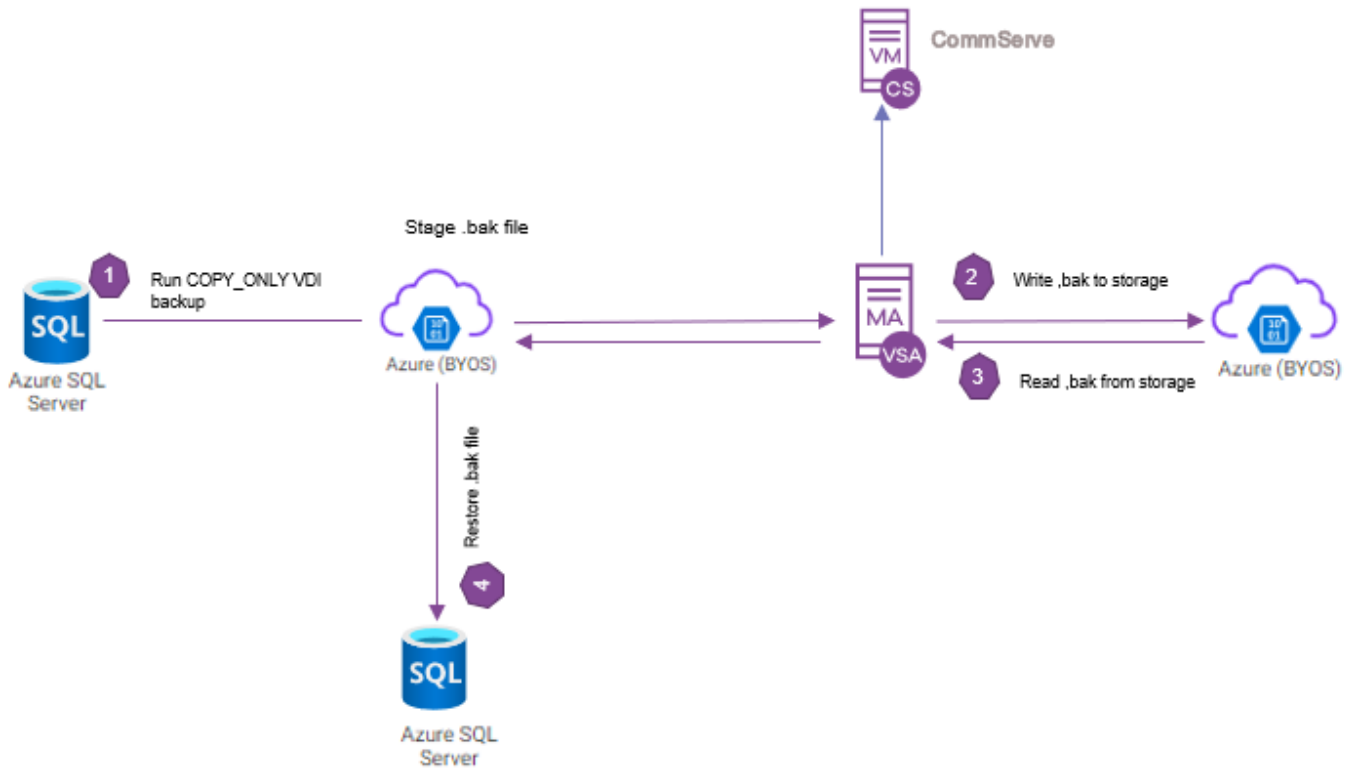
- Copy is named with prefix cv\_copy\_xxxx. The copy database should be excluded from any locking policies that may be in place since this copy is deleted as soon as the export process completes.
4. An export operation is then run on the copied database and the resulting .bacpac file is copied to a preconfigured staging location on the access node.
    - Commvault uses the [DacFx API](#) to export the database.
    - Please check this link to see [limitations and restrictions](#) with DacFX
    - [Sizing of the staging location](#) – Access nodes processing import/export requests need to store the BACPAC file as well as temporary files generated by the Data-Tier Application Framework (DacFX). The disk space required varies significantly among databases with the same size and can require disk space up to three times the size of the database. As a result, some requests may fail with the error There is not enough space on the disk. The workaround is to increase the staging space on the access node.
    - TEMP/TMP system variables - If by chance you receive a failing with Out of Disk space message, it's advisable to configure the %TEMP% folder of the system to reside on a distinct data disk. By doing so, you can confirm sufficient space for the export process to execute smoothly, avoiding potential disk space complications.
      - i. To configure the system's %TEMP% folder:
      - ii. Open the System Properties window by pressing the Windows key + Pause/Break or right-clicking on This PC and selecting Properties.
      - iii. Select the link labeled Advanced system settings on the left-hand side.
      - iv. In the ensuing System Properties window, navigate to the bottom and select Environment Variables.
      - v. Under the section labeled System Variables, locate the **TEMP and TMP variables**, then select Edit associated **with each**.
      - vi. Modify the values of both variables to point to a pathway on the separate data disk you have established. For instance, if your data disk is designated as D:, set the values as D:\Temp.
      - vii. Confirm the changes by selecting OK and closing all open windows.
  5. The database copy is deleted immediately after an export operation.
  6. The access node then writes the .bacpac in Commvault proprietary, compressed, and de-duped format to the storage destination.
  7. Backup ends after the .bacpac is successfully copied.
  8. The backup is always a full backup of the database.

#### **Restore Process:**

1. The user kicks off a manual out of place restore of a database to another SQL server.
2. A restore operation restores the .bacpac file to the staging location on the access node.
3. The access node then imports the .bacpac file to the destination server.
4. A restore always restores the full database.

## AZURE SQL MANAGED INSTANCE BACKUP AND RESTORE PROCESS

### Azure SQL Managed Instance Backup and Restore flow



#### Backup Process:

1. The CommServe starts backup based on the schedule defined in the plan or a user can kick off an on-demand backup.
2. The CommServe sends the backup request to the Commvault SQL agent on the access node.
3. The Commvault SQL agent on the access node uses AD authentication or SQL SRVER authentication to connect to the Azure SQL Managed instance and kick off a COPY\_ONLY VDI backup to an azure blob end point that acts as a staging location.
4. Copy-only backups are independent of the sequence of conventional SQL Server backups. This means they don't affect the existing backup chain.
5. The access node then reads the .bak from the staging azure blob and writes it in Commvault proprietary, compressed, and de-duped format to the storage destination.
6. Backup ends after the .bak is successfully written.
7. The backup is always a full backup of the database.

### Restore Process:

1. The user kicks off a manual out of place restore of a database to another SQL server.
2. The access node restores the .bak file to the Azure staging blob.
3. The SQL server is further restored from the .bak file. Restore always restores the full database.

## AZURE SQL BACKUP METRICS

The purpose of the following tests is to guide the user to the optimal database tier for their Azure SQL databases such that backups can meet the required SLAs without impacting the performance of the production database.

### TEST LAB ENVIRONMENT

1. Database instance, access node and Media agent were deployed in the same Azure region.
2. Network speeds used for testing were at least 10Gbps between all Commvault infrastructure components and the DB instance.
3. Backups were stored on destination storage that was Azure Blob storage (hot tier) that was configured in the same region as the production Azure SQL Database.
4. Access Node and Mediagent were installed on the same Azure VM.
5. Access Node sizing – Windows 2016 Datacenter, 8vCPUs, 32GB RAM
6. Access node had staging space = 20% of total DB workload set aside.

### CAVEATS

- The results shown below demonstrate the performance of Commvault within a set environment to show what results are achievable within similar environments.
- Due to the variations in all environments, results will be varied compared to the results achieved within this paper. While some environments can and will achieve better performance, other environments may not match the performance metrics captured in this paper.
- This paper is not meant to show the maximum or minimum performance of the solution, but a snapshot of performance based on conditions used in this testing. This paper, including any results or statements herein, does not guarantee or warrant performance.

## TEST PLAN AND RESULTS

Database size (GB)	Run DB backup one at a time? (Y/N?)	vCores for PaaS SQL instance <a href="#">Database tiers</a> (General purpose, Gen5, serverless, V5)	Total Backup time (hh:mm:ss)	Time to copy (hh:mm:ss)	Time to Export (hh:mm:ss)	Time to write to media (hh:mm:ss)	Cost of copy (\$)
50GB	Y	2	1:59:31	0:12:52	1:45:39	0:01:10	\$0.50
50GB	Y	4	1:04:52	0:11:42	0:51:42	00:00:56	\$1.34
50GB	Y	8	1:04:19	0:11:37	0:51:20	0:01:08	\$2.13
50GB	Y	16	1:04:27	0:11:36	0:51:19	0:01:01	\$2.55
100GB	Y	2	2:05:12	0:21:27	1:41:36	0:01:37	\$1.47
100GB	Y	4	2:03:27	0:21:27	1:39:57	0:01:32	\$2.93
100GB	Y	8	2:03:34	0:21:27	1:39:58	0:01:34	\$4.89
100GB	Y	16	2:02:54	0:21:22	1:39:19	0:01:34	\$5.74
500GB	Y	2	15:10:34	1:54:43	13:07:15	0:08:00	\$11.87
500GB	Y	4	14:52:45	1:54:43	12:49:18	0:08:09	\$17.01
500GB	Y	16	14:47:42	1:54:43	12:44:07	0:08:10	\$25.47

## INFERENCE FROM TEST RESULTS

- Comparable Copy, export and write to media times are seen when vCores are increased beyond 4 vCores.

## PERFORMANCE CONSIDERATIONS for AZURE SQL BACKUPS

- The copy is created with the same pricing/sizing tier as the production database.
- Performance data collected from customer environments has shown that having the production database run on a minimum of 4 cores helps meet the backup SLA while keeping costs down for database sizes of up to 500GB.
- For the best performance Azure SQL DB, access node, media agent and destination storage should be in the same region to avoid network latency.
- Copy and export operations are managed by Azure and hence there is not much that we can control in terms of performance for those operations from the Commvault end.
- Time for export also depends on the actual data being exported.
- Performance of write to destination storage/media is already tweaked to perform optimally for most use cases. For further fine tuning refer to -  
[https://documentation.commvault.com/2023e/expert/improving\\_throughput\\_to\\_storage\\_media.html](https://documentation.commvault.com/2023e/expert/improving_throughput_to_storage_media.html)
- Please check this link to see [limitations and restrictions](#) with DacFX
- Exporting a database using DacFX causes [throttling](#) by the Azure SQL Database service. You can [view the DTU stats for the database on the Azure portal](#). If the database has reached its resource limits, [upgrade the service tier](#) to add more resources.
- Exporting large tables without clustered indexes can be very slow or even cause failure. This behavior occurs because the table can't be split up and exported in parallel. Instead, it must be exported in a single transaction, and that causes slow performance and potential failure during export, especially for large tables.
- [Sizing of the staging location](#) – Access nodes processing import/export requests need to store the BACPAC file as well as temporary files generated by the Data-Tier Application Framework (DacFX). The disk space required varies significantly among databases with the same size and can require disk space up to three times the size of the database. As a result, some requests may fail with the error- There is not enough space on the disk. The workaround is to increase the staging space on the access node. It is recommended that this staging space be created on SSD disks for optimal performance.
- TEMP/TMP system variables - If by chance you receive a failing with Out of Disk space message, it's advisable to configure the %TEMP% folder of the system to reside on a distinct data disk. By doing so, you can confirm sufficient space for the export process to execute smoothly, avoiding potential disk space complications.  
To configure the system's %TEMP% folder:
  - Open the System Properties window by pressing the Windows key + Pause/Break or right-clicking on This PC and selecting Properties.
  - Select the link labeled Advanced system settings on the left-hand side.
  - In the ensuing System Properties window, navigate to the bottom and select Environment Variables.
  - Under the section labeled System Variables, locate the **TEMP and TMP variables**, then select Edit associated **with each**.
  - Modify the values of both variables to point to a pathway on the separate data disk you have established. For instance, if your data disk is designated as D:, set the values as D:\Temp.
  - Confirm the changes by selecting OK and closing all open windows.



- 
- Restore operation restores the data to the lowest pricing tier by default. This may lead to slow restores. Use the UI options to select the pricing tier for the restored database such that required restore RTO is met.

## SUMMARY

Commvault's Azure SQL protection safeguards your Azure SQL data with flexible retention policies, flexible scheduling policies and cross cloud mobility. It seamlessly integrates with Azure SQL and allows for data availability and integrity for your critical databases.