# (Private) Preview | Snapshot-based backup for large SQL DBs in Azure VM

Azure Backup launched a [VDI-stream-based backup solution for SQL Server in Azure VMs](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms) in 2019. Today, this solution has become the choice of thousands of customers in Azure. While it scales up well for up to 4-6 TB databases (@ 200 MBps speed), enterprises are looking for even more performant backup and restore for large databases. Azure Backup has now come up with a unique snapshot-based backup solution that combines the goodness of snapshots for better RTO and the benefits from frequent log backups for low RPO:

* **Minimal impact on the source server:** Database needs to be quiesced to get an application-consistent snapshot. This process takes only a few seconds (as opposed to continuous resource sharing in case of streaming backups)
* **Cost-effective:** Incremental snapshots result in lower storage costs (as opposed to streaming full backups) but better redundancy since they are stored on zone-redundant storage by default.
* **Better RTO:** Restores are much faster since the snapshots are retained in the customer subscription.
* **15-min RPO:** As in the case of stream-based backup, log backups are streamed every 15 minutes and can be applied on top of the restored snapshot at the time of recovery.

## How does the snapshot-based backup solution work?

1. Azure Backup relies on the [managed-disk incremental snapshots](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms?tabs=azure-powershell) that are automated by the user-defined schedule (preview supports one snapshot a day). In preview, we only support **copy-only snapshots** which do not interfere with the on-going stream-based backups, if any.
2. **The snapshot is consistent with only one database at a time** (as per current VDI interface support, only one DB can be paused at the time of taking the snapshot)**.** For e.g.

* You have one 10 TB database and some 50 smaller databases (say, a couple of 100 GBs each) on a disk set: u*se snapshot backups for the 10 TB database to snapshot the underlying disks (combines size of 10TB+) and continue using stream-based backup for smaller DBs.*
* You have a 10 TB database, a 20 TB DB and some 50 smaller databases (say, a couple of 100 GBs each) on a disk set: u*se snapshot-based backup for the two large DBs and continue using stream-based backup for smaller DBs. Thus, you will end up with two initial full snapshots of 30TB+, each consistent with one of the 2 large databases only.*

1. The snapshots are then retained in the customer’s subscription in a specified resource group (RG) for a user-defined duration (max. 30 days). In preview, we do not support long term retention of the snapshots.
2. Log backups continue to stream such that at the time of recovery, first, the snapshot is restored as disk(s) (and attached to the target VM) and then the logs could be applied on top of it.

## Preview Scope

1. Supported for SQL Server 2016 (and above) on Windows Server 2016 and above.
2. In the backup policy, you could opt for:

* **snapshot + (weekly) streaming full + streaming logs:** In preview, weekly streaming fulls are mandatory if log backups are required. We would remove the dependency on streaming full backups going forward such that you could only have **snapshot + log** backups.
* **only snapshots (without logs)**: works if you are maintaining your own log backups outside of this solution and/or your database size is too big to support even weekly streaming full (@200 MBps),

1. Currently, the snapshots are stored in the customer subscription only and not in the vault tier (as in the case of stream-based backups). While it ensures faster restores, it may also run the risk of accidentally getting deleted by the customer.
2. **Billing impact:** All Managed disk snapshots will be charged to the customer as per Managed disk snapshot pricing ($0.05 per GB/Month) for the duration they are retained. The first snapshot will be a full snapshot and all subsequent snapshots are incremental. In preview, there is no additional backup management fee charged for only snapshot backup.
3. PowerShell support would be available at GA.
4. Not integrated with the Backup center yet, will be available at GA.
5. Restore to server which is part of windows cluster is not supported yet. This would be resolved going forward.
6. In preview, it is recommended to try out the solution only for **test workloads.**

## How to on-board to the preview?

Ensure that the **subscriptionID** is registered to our service provider **(Microsoft.RecoveryServices**) as explained [here](https://docs.microsoft.com/azure/azure-resource-manager/resource-manager-register-provider-errors#solution-3---azure-portal). Now on-board to the snapshot solution through the Powershell (PS) or the portal:

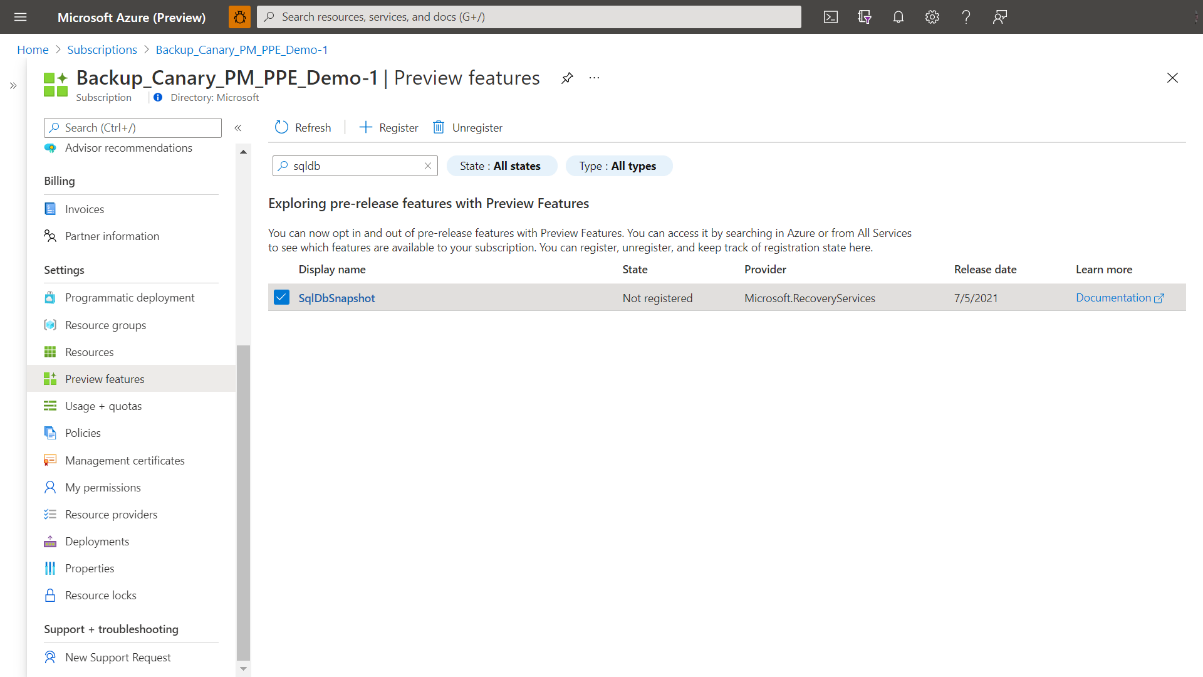
Run the following **PS command** under the subscription context. If successful, it returns “Registered”.

PS C:> Register-AzProviderFeature -FeatureName "SqlDbSnapshot" –ProviderNamespace Microsoft.RecoveryServices

**OR**

Go to the **Azure portal**

Subscription view >> Preview features >> **SqlDbSnapshot**



## Prerequisites

1. Identify or create a [Recovery Services vault](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms#create-a-recovery-services-vault) in the same region and subscription as the VM hosting the SQL Server instance.
2. Verify that the VM has [network connectivity](https://docs.microsoft.com/en-us/azure/backup/backup-azure-sql-database#establish-network-connectivity).
3. Make sure that the SQL Server databases follow the [database naming guidelines for Azure Backup](https://docs.microsoft.com/en-us/azure/virtual-machines/disks-incremental-snapshots#database-naming-guidelines-for-azure-backup).

Steps to Configure Backup

### Create Backup Policy with Snapshot backups:

As mentioned under [preview scope](#_Preview_Scope), you could opt for **only snapshots (without logs)** or **snapshot + (weekly) streaming full + streaming logs**.

Graphical user interface, text, application, email

Description automatically generated

### Set-up Permissions for Configure Backup (to be automated at GA):

Azure Backup extension (residing within the SQL VM) requires permissions to take snapshots of the managed disks and to place them in a user-specified Resource Group mentioned in the policy. To do this, Azure Backup leverages System assigned [Managed Service Identity](https://docs.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview) (**system** MSI) of the backed up VM.

During configure backup, we are dealing with 3 entities –

* Source Azure VM running the backed-up database
* Disk(s) attached to the source VM, that are getting snapshotted
* Resource group (RG) in which the snapshots taken would be stored

To simplify the assignment of roles and scope to the resources, use the following built-in roles. For exact granular roles, refer to the [appendix](#_Appendix:):

|  |  |  |
| --- | --- | --- |
| **Resource (Access control)** | **Role** | **User, group, or service principal** |
| Source Azure VM running the backed-up database | Virtual Machine Contributor | User configuring the backup |
| Disk(s) attached to the source VM (or the Disk RG), that are getting snapshotted | Disk backup reader | (system MSI of) Source Azure VM running the backed-up database |
| Resource group (RG) in which the snapshots taken would be stored (specified at the time of creating backup policy) | Disk snapshot contributor | (system MSI of) Source Azure VM running the backed-up database |

***Please do not change the resource groups once they are given/assigned to Azure Backup during preview***.

1. In the Azure Portal, go to [Recovery services vault](https://docs.microsoft.com/en-us/azure/backup/backup-sql-server-database-azure-vms) >> +Backup and choose **SQL Server in Azure VM**. *If you are familiar with the stream-based backup solution, you can ignore this section since the experience is similar for snapshot-based backup solution.*

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, application, email

Description automatically generated

1. Start [Discovery](https://docs.microsoft.com/en-us/azure/backup/backup-azure-recovery-services-vault-overview#discover-sql-server-databases) to search for unprotected VMs in the subscription. During this step:

* Azure Backup registers the VM with the vault for backup. All DBs on the registered VM can be backed up to this vault only.
* Azure Backup installs the AzureBackupWindowsWorkload extension on the VM and creates the service account NT Service\AzureWLBackupPluginSvc on the VM.
* NT Service\AzureWLBackupPluginSvc requires SQL sysadmin permissions. **While all SQL Server VMs with ‘SqlIaaSExtension’ get this permission automatically, for other VMs,** [**grant this permission manually**](https://docs.microsoft.com/en-us/azure/backup/backup-azure-sql-database#set-vm-permissions).

1. Go to Configure Backup.

Graphical user interface, application, Word

Description automatically generated

1. Create/select a **Backup policy** with ‘Snapshot Copy Only Full Backup’ enabled.

Graphical user interface, text, application, email

Description automatically generated

1. Select database(s) you want to backup with snapshot-based solution. **Auto-protection does not work** with snapshot-based backup solution since it is not an at-scale operation.

Table

Description automatically generated

1. Enable backup and track the job completion under **Backup Jobs.** In case you want, you can trigger an **ad-hoc snapshot** **backup** before the actual schedule gets kicked in to enable protection immediately.

Steps to Restore

### Set-up Permissions for Restore *(to be automated at GA):*

During restore, Azure Backup leverages Target VM’s MSI to read snapshot from user-specified RG, create disks in a target-RG and then attach them to the target VM. The Target VM’s MSI needs permissions at the user-specified RG scope and the Target RG scope. The granular list of resources, permissions, scope is present in [appendix](#_Appendix:).

***Once restore is completed, these permissions can be revoked***.

During restore, we are dealing with the following entities-

* Target VM (could be same as the source VM)
* Snapshot RG where the snapshots would be restored
* Target Disk RG where the disks should be created and then attached to target VM

|  |  |  |
| --- | --- | --- |
| **Resource (Access control)** | **Role** | **User, group, or service principal** |
| Target VM | Virtual Machine Contributor | User triggering the restore |
| Snapshot RG where the snapshots would be restored | Disk snapshot contributor | Target VM MSI |
| Target Disk RG where all disks will be created during restore | Disk Restore operator | Target VM MSI |
| Target VM | Virtual Machine Contributor  (Needed such that new disks could be added to the VM) | Target VM MSI |
| Source Disk RG (RG where all existing disks of target VM are present) | Disk restore operator | Target VM MSI |

1. Go to Recovery Service vault >> Backup Items

Graphical user interface

Description automatically generated

1. Click on **Restore**

Graphical user interface, application, table

Description automatically generated

1. Snapshot-based recovery is a 2-step process – **a. Restore the snapshot** **b. Apply logs over the restored snapshot**

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

4.b Restore logs over snapshot would return only those logs that are available corresponding to the latest restore snapshot for the target VM. **Ensure that the Target VM, instance name, DB name and Target physical path are same as in the first step of snapshot restore.**

Graphical user interface, application, Teams

Description automatically generated

Graphical user interface, application

Description automatically generated

Graphical user interface, text, application

Description automatically generated

Please note:

Modifying policy

While you can technically modify an existing stream-based backup policy to enable snapshot-based backup, it needs to be done with utmost care. If you edit an existing stream-based policy (with, say 10 protected databases) to a snapshot policy, you would end up getting 10 snapshots (with combined size of underlying disks), each consistent with only one database. Instead, try and change the associated policy for only one database at a time.

### Permission to delete snapshots (before retention duration)

|  |  |  |
| --- | --- | --- |
| **Resource** | **Role** | **User, group, or service principal** |
| Snapshot RG (for deleting snapshots) | Disk snapshot contributor | Backup Management Service |

Contact us @ [AskAzureBackupTeam@microsoft.com](mailto:AskAzureBackupTeam@microsoft.com) for any queries that you may have!

# Appendix:

**How to assign permission?**

* Go to the resource you want to assign role/permission to
* Go to Access control >> Add Roles assignments >> Input Role and user/principal name (VM or user)

Graphical user interface, application, Word

Description automatically generated

### Configure Backup

|  |  |  |
| --- | --- | --- |
| **Resource** | **Permission/Operation** | **Scope** |
| Backed up VM MSI | Microsoft.Authorization/permissions/read | Disk (for each VM disk) or Disk RG |
|  | Microsoft.Compute/snapshots/write | Snapshot RG mentioned in the policy |
|  | Microsoft.Compute/disks/read | Disk (for each VM disk) or Disk RG |
|  | Microsoft.Compute/disks/beginGetAccess/action | Disk (for each VM disk) or Disk RG |

### Restore

|  |  |  |
| --- | --- | --- |
| **Resource** | **Permission/Operation** | **Scope** |
| Target VM MSI | Microsoft.Authorization/permissions/read | Snapshot RG mentioned in the policy |
|  | Microsoft.Compute/disks/write | Target RG mentioned in the request where disks are created |
|  | Microsoft.Compute/snapshots/read | Snapshot RG mentioned in the policy |
|  | Microsoft.Compute/disks/beginGetAccess/action | Snapshot RG mentioned in the policy |
|  | Microsoft.Compute/virtualMachines/write | Target VM |
|  | Microsoft.Compute/virtualMachines/read | Target VM |