COHESITY

Version 2.1

July 2024

Protect Your Azure VM Data with Cohesity

Cohesity for Azure Native Backup Configuration and Best Practices Guide

ABSTRACT

In the real world, the cloud is equal to a hosted data center. Like any data center, failures are commonplace in the cloud. With Cohesity Azure Native Backup, you can now protect your Azure Virtual Machines and associated volumes against data loss. Cohesity Data Cloud also provides the ability to restore data at granular levels, to the same or different Azure accounts.

Table of Contents

Figures

Tables

Azure VM Data Protection

Azure Virtual Machine (VM) is a service that provides secure and on-demand compute resources in the cloud. With more and more organizations using Azure VMs to deploy enterprise workloads, it's imperative to think about backing up data on Azure VMs. Now you can protect your Azure VM data while enjoying the recovery granularity and flexibility of Cohesity Data Cloud.

Cohesity supports the protection of Azure VMs for both Azure and Azure Government.

Backups Protect Azure VMs from Data Loss

Data loss is inevitable in any data center. The same rule applies to data centers hosted by cloud service providers. Table 1 describes some of the possible reasons for data loss in Azure VMs. Backing up Azure VMs helps mitigate such risks.

Table 1: Causes of Data Loss in Azure VMs

Reason for Data Loss	Data Loss Scenarios
Data loss due to platform issues	Azure is a very robust platform, but, like any other data center, hardware failure scenarios are unavoidable. Although Azure can maintain multiple copies of the data across different availability zones, there can be scenarios that cause data loss.
Administrative Errors/Mistakes	Azure VM provisioning and de-provisioning are day-to-day tasks, and prone to administrative errors. In a highly dynamic environment, the risk of an administrator deleting an Azure VM by mistake can be high.
Insider Threat	An insider with access can delete data residing in an Azure VM, or an entire Azure VM, from your infrastructure.
Application Error	There are cases where an application that was not tested properly wiped-out data in the Azure VM disks.
Hackers/ Ransomware/ Virus Attacks	Azure has checks and balances when it comes to external attacks. However, mistakes resulting from application deployment and network glitches can result in external attacks that compromise data.

Given the above scenarios, it becomes crucial to have automated point-in-time backups of the Azure VMs that can be used to restore your VMs or select data hosted by the VMs in cases of data loss. This approach can also be used for other use cases, such as cloning Azure VMs for test and dev projects.

Using Cohesity to perform your Azure VM backups gives you the ability to take control of your Azure infrastructure and associated data by providing the ability to do automated point-in-time backups of the Azure VMs and the associated volumes. It allows you to restore at different levels of granularity, from entire Azure VMs to individual files and folders. What's more, you can use the Cohesity Data Cloud to protect and recover your Azure data across multiple Azure accounts.

Cohesity's Azure VM Data Protection Methods

Cohesity platform offers two ways to protect Azure VM instances, Cohesity Native Snapshot and Cloud Snapshot Manager.

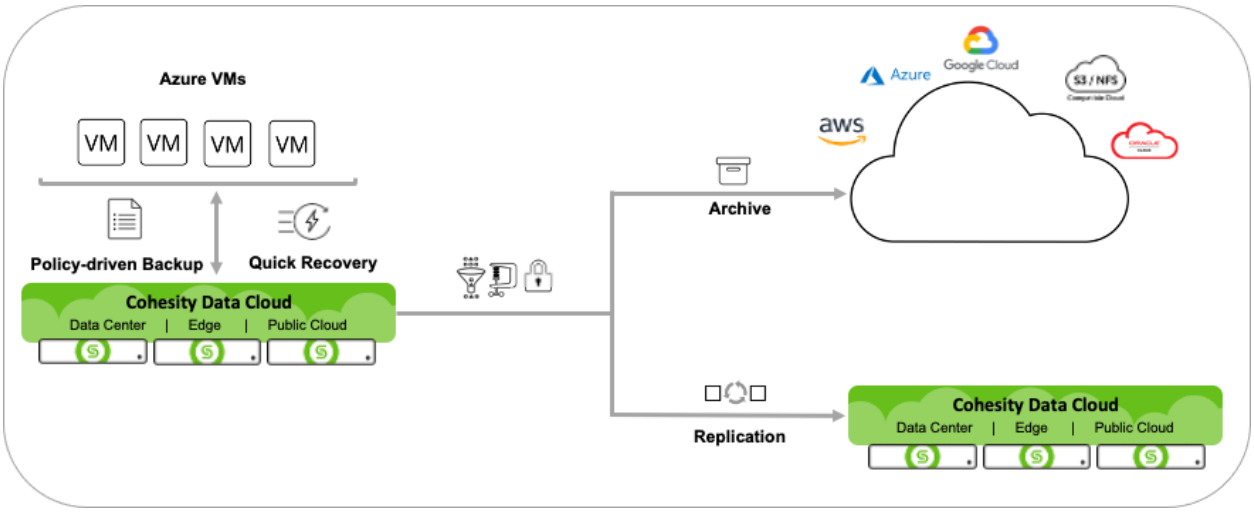
- **Native Snapshot**: The primary use case for Native Snapshot is the protection of native cloud VMs from within the cloud. Data and metadata are stored on the Cohesity cluster. Cohesity recommends using Native Snapshot as the default method for protecting native cloud VMs because data is stored on the Cohesity cluster. With Cohesity snapshots, we can extend the full benefits of using the Cohesity platform to the protected data.
    - From Cohesity version 7.0 onwards, the native backup method supports the backup and restore of Azure-managed disks using a private endpoint.
- **Cloud Snapshot Manager (CSM)**: The primary role of Cloud Snapshot Manager (CSM) is to protect native cloud VMs from on-prem (outside of the cloud) or across Cloud Service Provider (CSP) regions that would incur data egress charges. The CSM method manages native cloud snapshots, with only metadata being stored on the Cohesity cluster (no data is stored on the Cohesity cluster).

Cohesity's Azure Native Backup Solution

The Azure native backup feature in Cohesity gives you the ability to protect Azure VMs, along with their attached disks. The solution uses native Azure APIs for both backup and recovery of Azure VMs, without the need for agents. This helps you protect your entire Azure infrastructure with backup and restore features that keep your data safe. With your Azure VM backups on the Cohesity Platform, you can protect them further with flexible replication and archival to almost any storage platform.

NOTE: You can use any Cohesity platform (Physical, Virtual, or Cloud) for Azure native backups.

Figure 1: Use Cohesity to Protect Azure VMs with Backup, Archive, and Replication to Any Storage



How Azure Native Backups Work with Cohesity

Azure native backup works according to the type of disk used for the Azure VMs. Apart from some of the common steps, the workflow for VMs using managed disks differs from that for VMs using unmanaged disks. **Table 2** below compares an Azure-managed disk with an unmanaged disk.

Table 2: Azure Managed Disk vs Azure Unmanaged Disk

Azure Managed Disk	Azure Unmanaged Disk
Managed Disks, offered by Microsoft Azure, provide a seamless and simplified way to manage storage for your virtual machines. When creating new disks, Managed Disks eliminate the need for a separate storage account setup. Microsoft Azure takes care of the underlying storage infrastructure, reducing administrative overhead. However, this also means that you have limited direct control over the specifics of the storage configuration. See Azure managed disk overview.	Unmanaged disks are traditional types of disks used by VMs. With these disks, you create your own storage account and specify that storage account when you create the disk. In this option, customers need to be mindful of IOPS and other limits on the storage account

Backup Workflow Using Unmanaged Disks

In Azure, unmanaged disks are stored as blobs. Azure Storage provides the capability to take snapshots of blobs. Snapshots capture the blob state at that point in time. For unmanaged disks, Azure provides Azure Storage REST APIs, which makes it possible to trigger backups directly. The Cohesity Azure

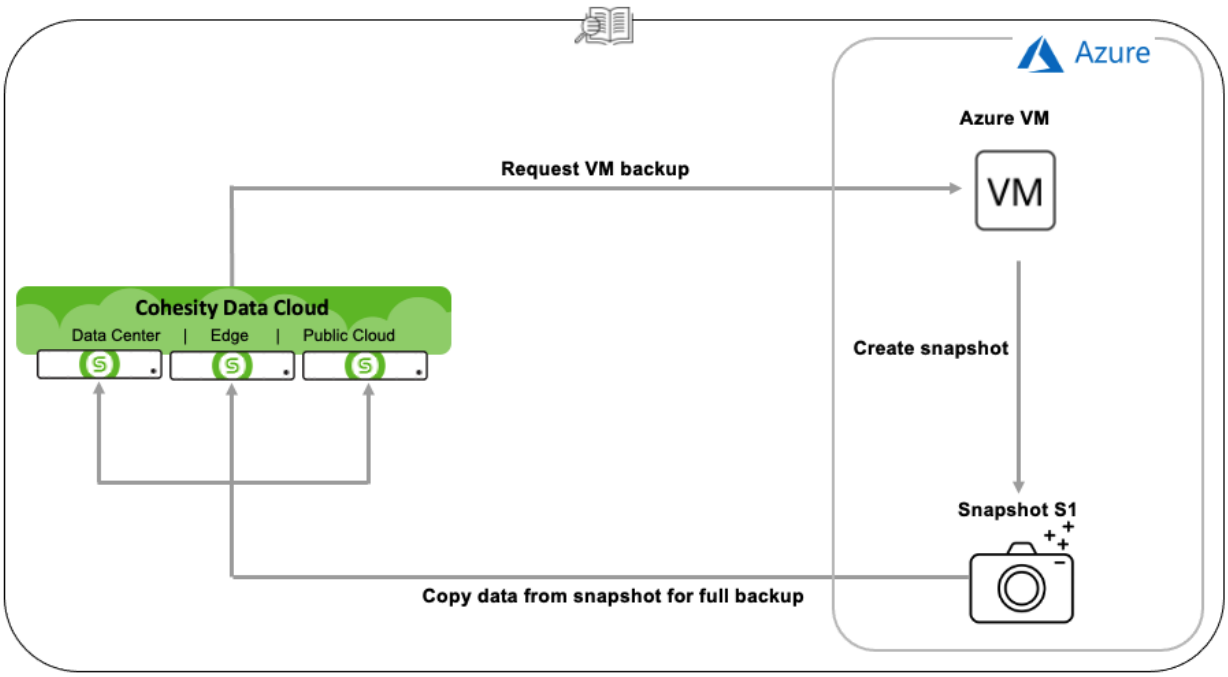
Native Backup option provides the ability to take full as well as incremental backups. The first backup is always full and successive backups can either be full or incremental, based on business needs.

Full Backup Workflow

To take a full backup of VMs that use unmanaged disks, Cohesity DataProtect:

1. Fetches the VM's information, along with details of every resource attached to that VM, such as disks and network details.
2. Creates a snapshot of the unmanaged disk, such as '*Snapshot S1*'.
3. Downloads the page ranges of that snapshot.
4. Fetches data from the snapshot. The first time the backup is run, the snapshot ('*Snapshot S1*') is retained, as it is used to take an incremental backup in the next run. For future runs, the most recent snapshot of the page blob is always retained for the next backup run.

Figure 2: Full Backup of Azure VMs Workflow



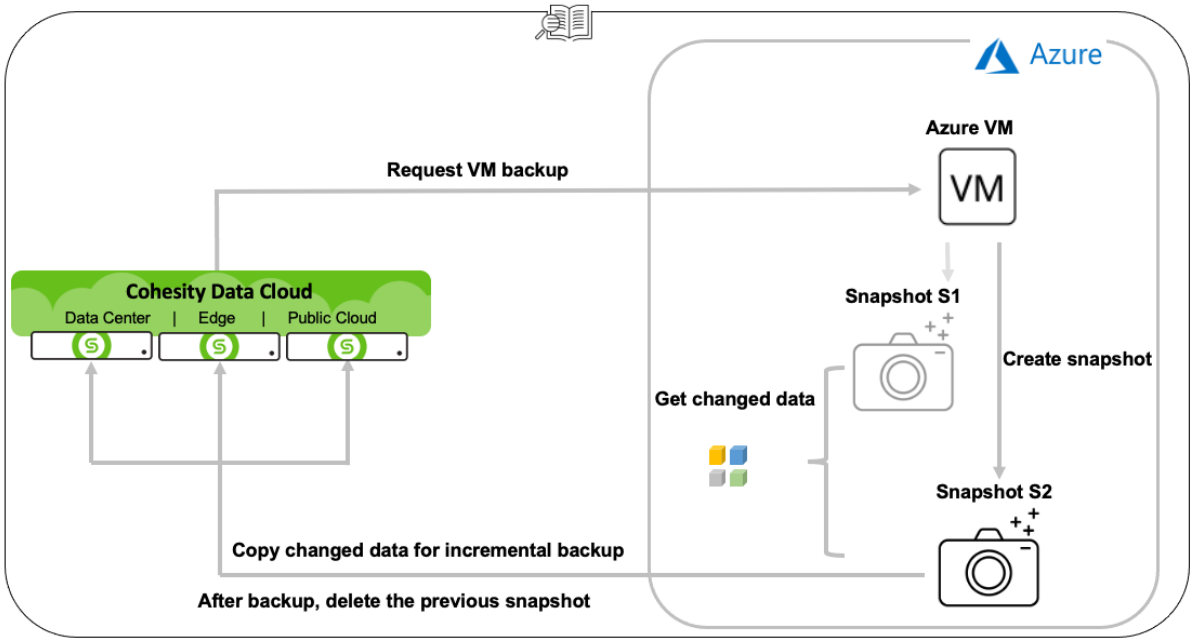
Incremental Backup Workflow

To take an incremental backup of VMs that use unmanaged disks, Cohesity DataProtect:

1. Fetches the VM's information, along with details of every resource attached to that VM, such as disks and network details.
2. Creates a new snapshot ('*Snapshot S2*').
3. Gets the delta page ranges (the changed data) between the previous snapshot ('*Snapshot1*') and the new snapshot ('*Snapshot S2*').
4. Fetches data from only the identified page ranges and downloads them onto the Cohesity cluster.

5. Deletes the previous snapshot (‘*Snapshot S1*’) and retains the new snapshot (‘*Snapshot S2*’) for the next incremental backup.

Figure 3: Incremental Backup of Azure VMs Workflow



Backup Workflow for VMs Using Managed Disks

The Native Snapshot backup process for Azure VM Managed disks is different from the backup process for unmanaged disks. Cohesity uses Azure APIs to create snapshots of the disks. The first snapshot is a full backup, and the subsequent ones are incremental backups.

With snapshots, a crash-consistent point-in-time capture of your managed disks is created. These snapshots are independent of the source disk and can be used to create new managed disks.

Backup Managed Disks

To take a backup of VMs that use managed disks, Cohesity Platform:

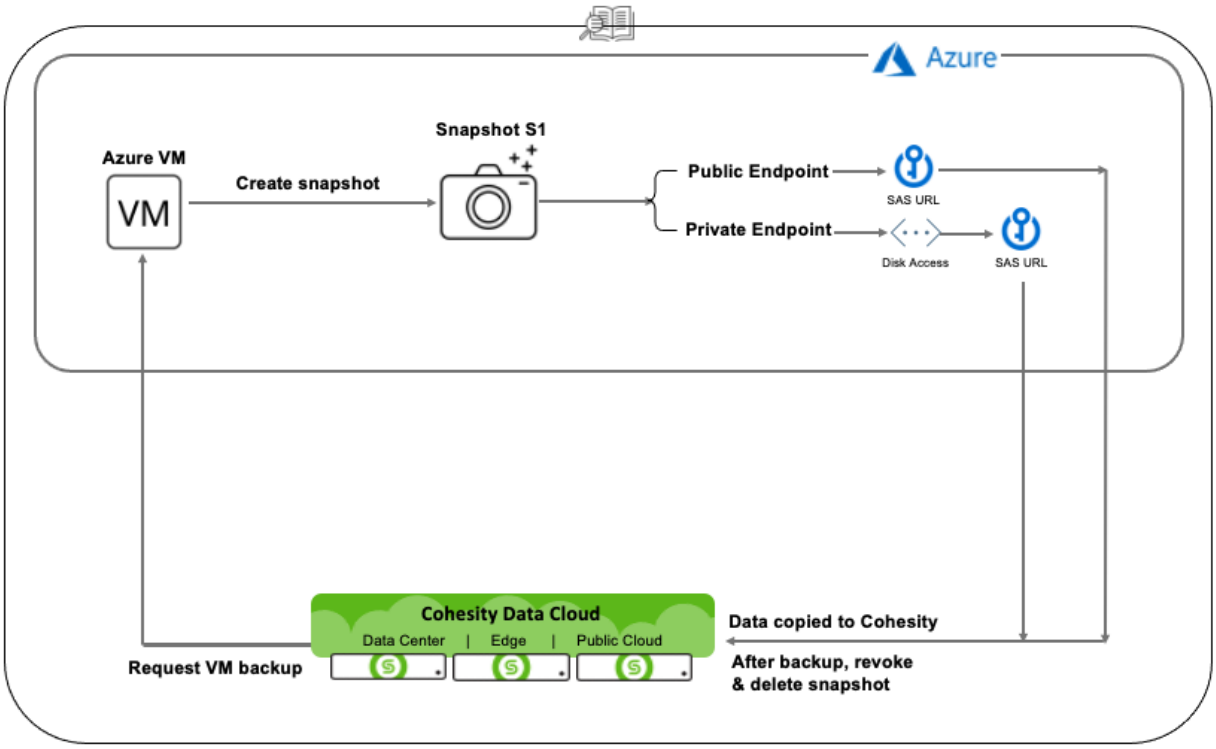
1. Fetches the VM info such as details of every resource attached to the VM, e.g. disks, network details.
2. Takes a snapshot (‘*Snapshot S1*’) of each managed disk attached to the VM.
    a. If you select Public Endpoint, Public SAS URLs are generated for each of the Azure snapshots, and data is copied to Cohesity using this SAS URL over the public internet.
    b. If you select Private Endpoint, the disks will get attached to Disk Access with private endpoint.
    c. Generates a SAS URL for the newly created snapshot.

d. Backs up the data using the SAS URL directly to the Cohesity cluster privately over the Azure network.

3. After the backup completes, revoke access to the snapshot (‘*Snapshot S1*’) and then delete the snapshot. Cohesity offers a feature that allows users to retain the last outstanding snapshot for efficient identification of incremental changes between snapshots. By keeping this snapshot, users can significantly speed up the process of performing incremental backups. However, it's essential to note that enabling this feature may come with an additional cost to the customer. Contact Cohesity Support to enable this feature.

NOTE: The Disk Access and Private Endpoint will be deleted only if they are not in use by any other backup or restore operations.

Figure 4: Backup of Azure VMs with Managed Disks Workflow



NOTE: Cohesity retains the most recent snapshot for each disk in the cloud to track incremental changes, which could result in additional costs depending on the size of the snapshots.

Configure Cohesity Platform for Azure VMs

You can set up Cohesity Platform to take backups of Azure VMs by completing the following steps.

1. Get Your Azure Subscription Details
2. Register Your Azure Subscription
3. Create a Protection Group

Get Your Azure Subscription Details

You will need the following information for registration.

Table 3: Get Azure Subscription Details

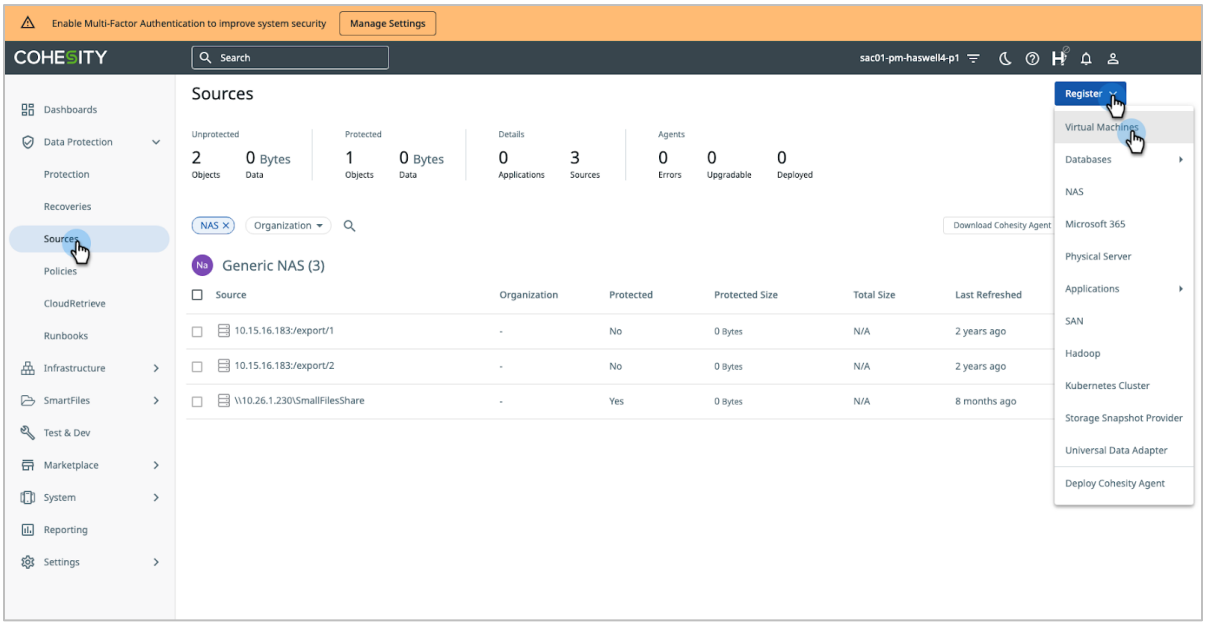
Field Name	Description
Category	Choose Standard Azure, Azure Government, or Azure Stack. All these categories are supported, but Azure Government provides additional security.
Subscription ID	Enter the Subscription ID for the subscription used. Log in to the Azure portal. In the left panel, click **Subscriptions** and copy the SUBSCRIPTION ID from the table.
Application ID	Enter the Application ID assigned by Azure during the service principal creation process. Learn how to get an application ID and authentication key in the Microsoft Azure documentation.
Authentication Key	Enter the Azure Authentication Key generated using the Legacy App Registration during the service principal creation process. Learn how to get an application ID and authentication key in the Microsoft Azure documentation.
Tenant ID	Enter the unique Tenant ID assigned by Azure. Learn how to get a tenant ID in the Microsoft Azure documentation.

For details on collecting this information, see Appendix C: Prepare Azure Subscription to Register with Cohesity Platform.

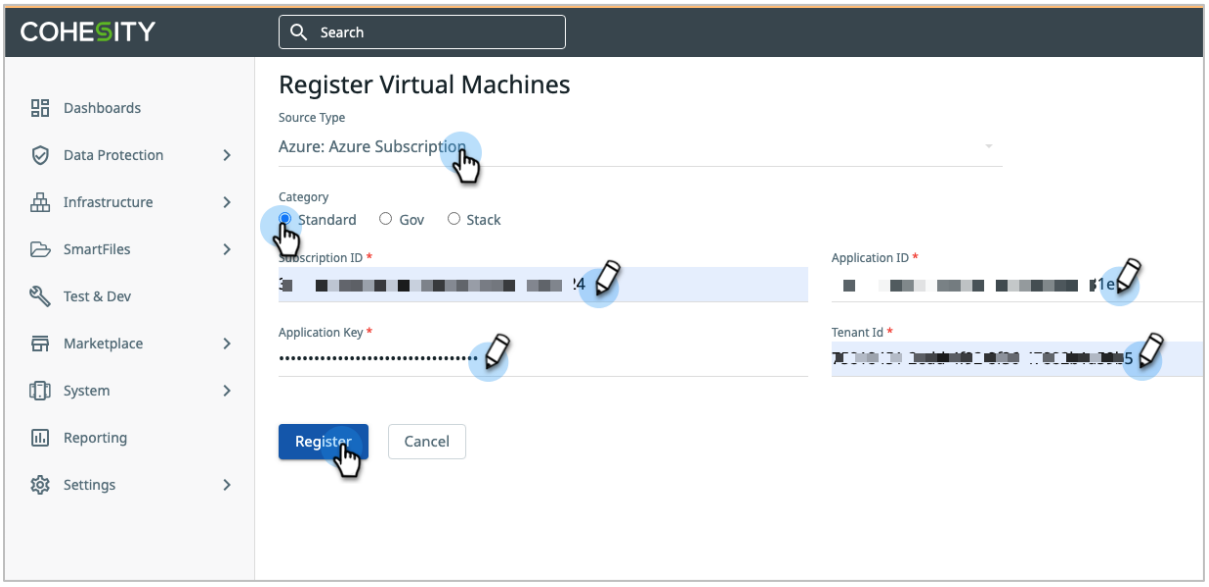
Register Your Azure Subscription

To register your Azure Subscription to Cohesity Platform:

1. Log in to Cohesity Platform and select **Data Protection > Sources** on the left. Then, select **Register > Virtual Machines**.



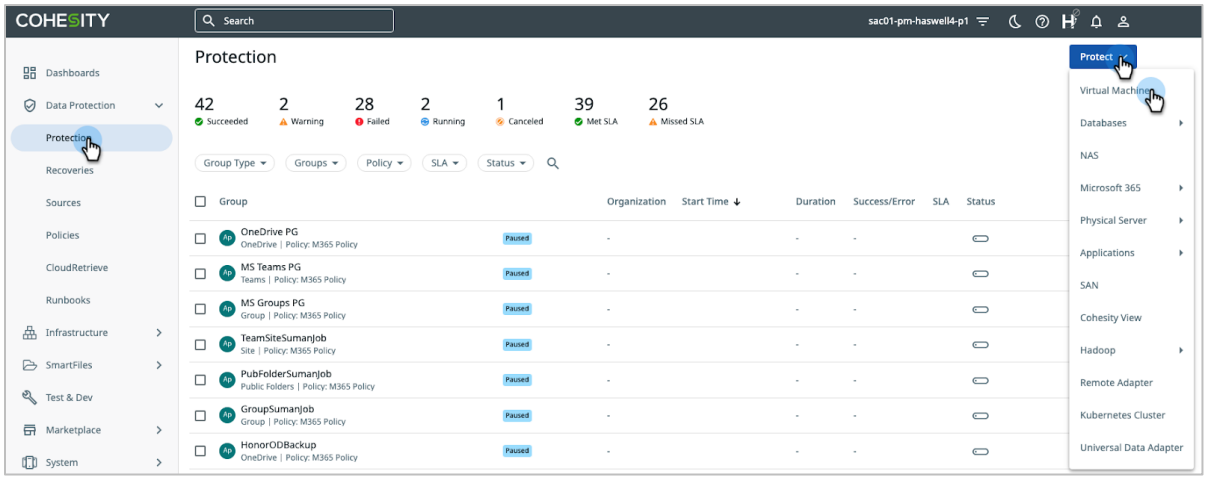
2. Select **Azure: Azure Subscription** Under **Source Type**, and select the **Category**, **Standard**, **Gov**, **or Stack.** Enter the **Subscription ID, Application ID, Application Key,** and **Tenant Id.** Click **Register** to proceed.



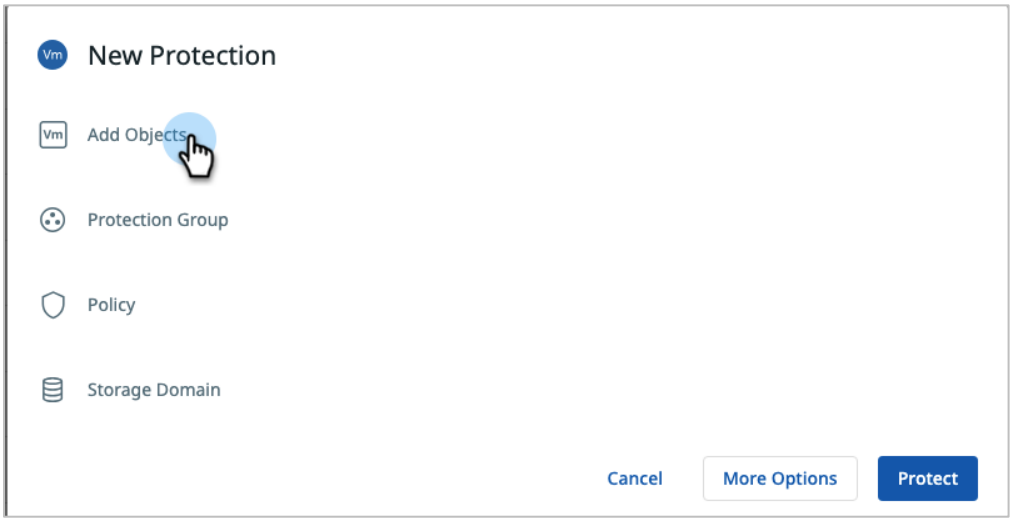
Create a Protection Group

Create a Protection Group by adding objects and assigning a Protection Policy to perform backups.

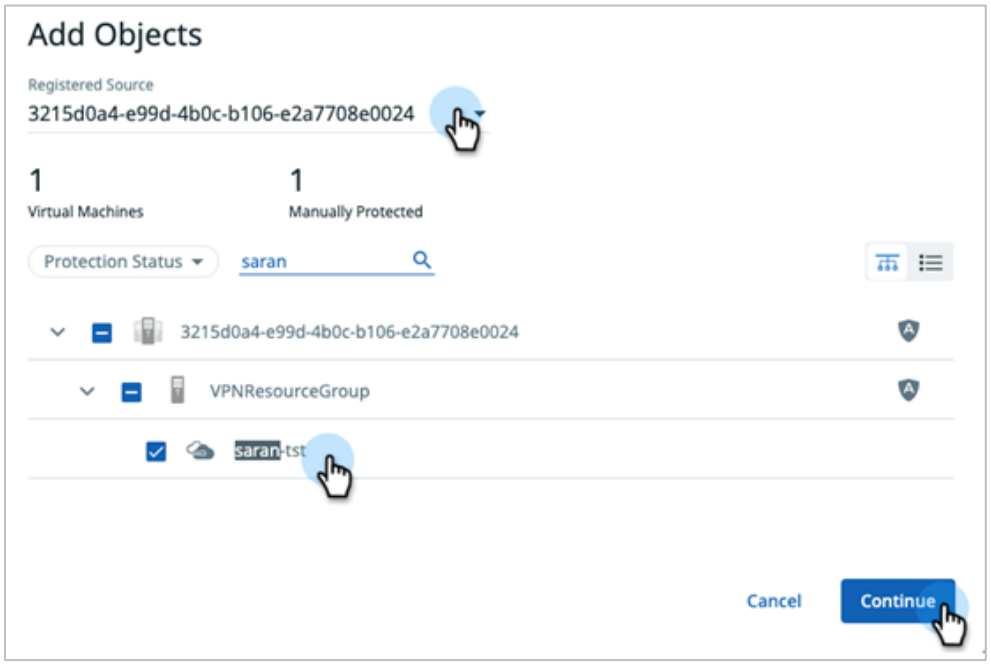
1. Log in to **Cohesity Platform** and select **Protection > Protect > Virtual Machines**.



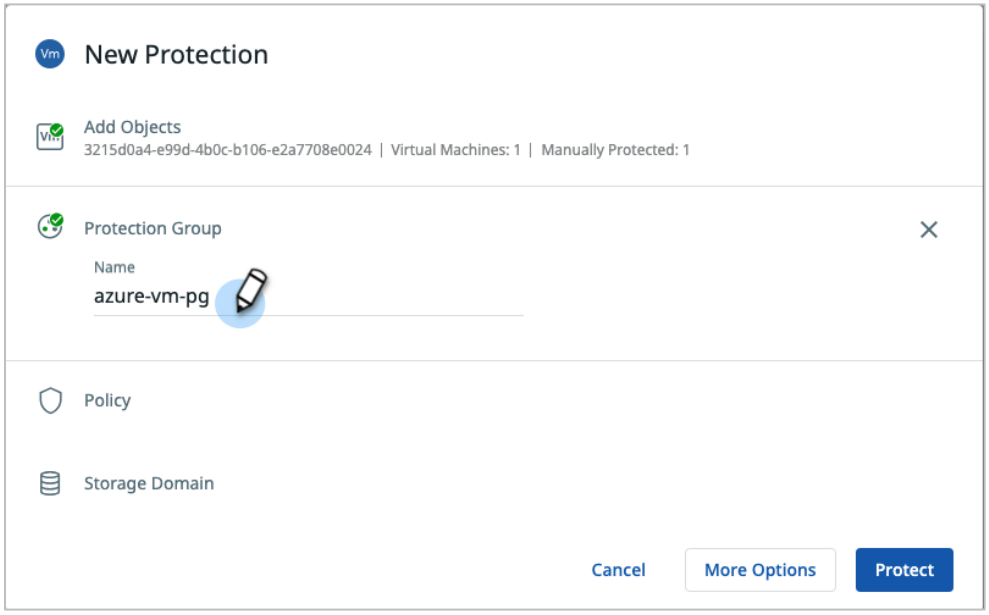
2. Click **Add Objects** to select a source to protect.



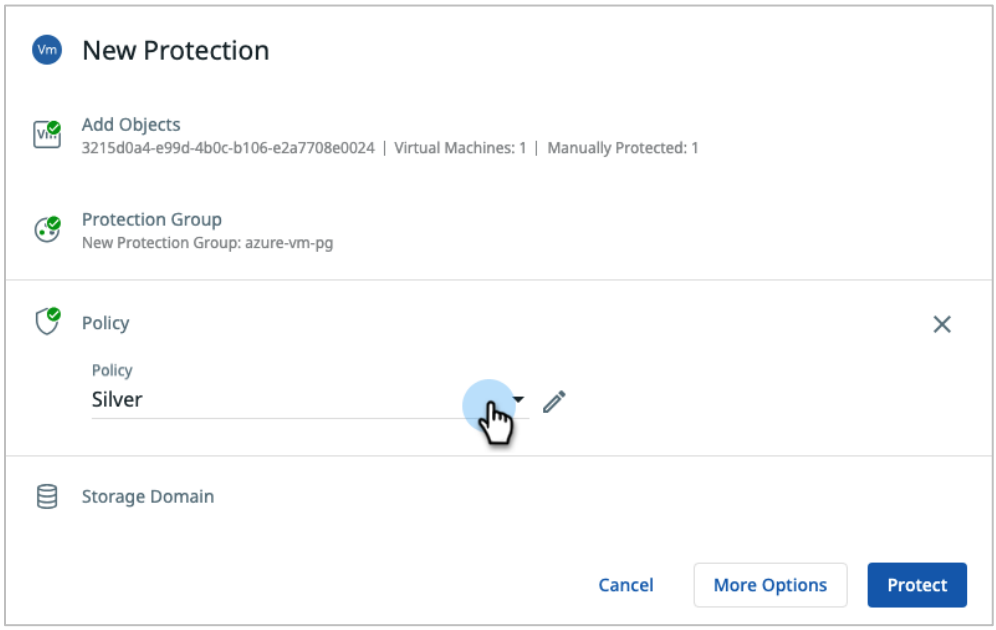
3. Select the Azure source and the VMs that need to be protected and click **Continue**.



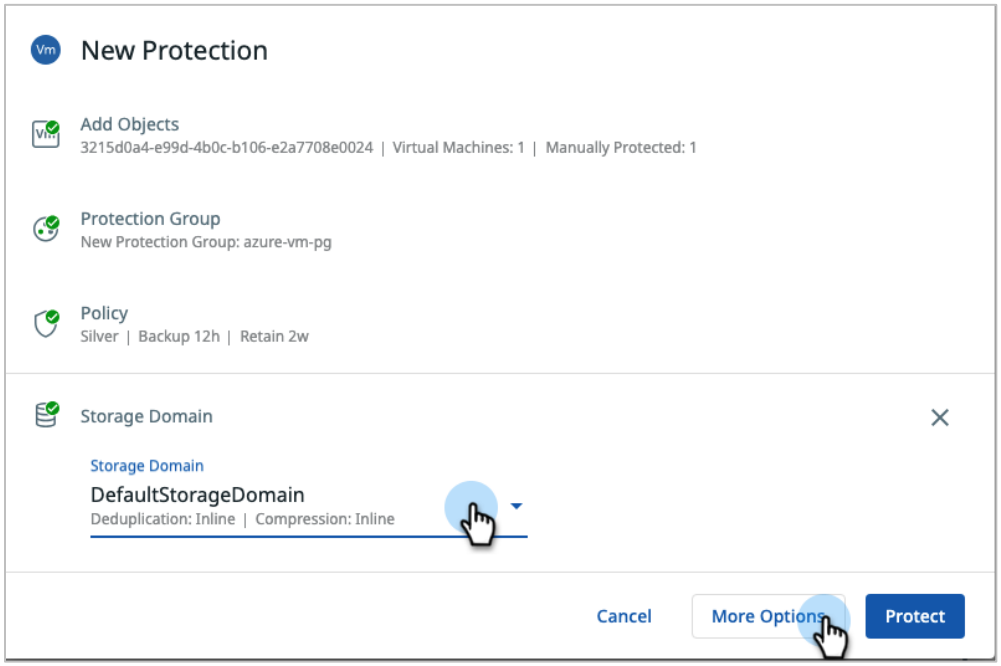
4. Enter a name for the Protection Group.



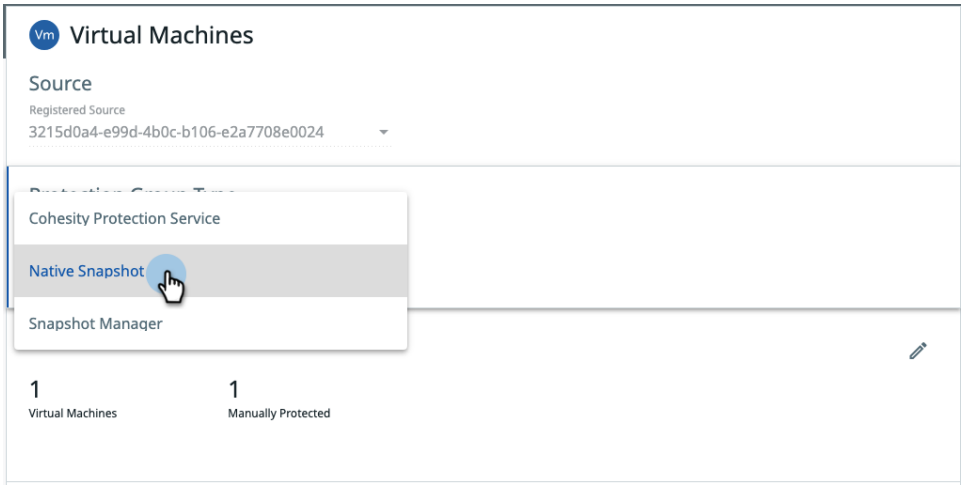
5. Select a Policy or create a new policy based on the backup requirements.



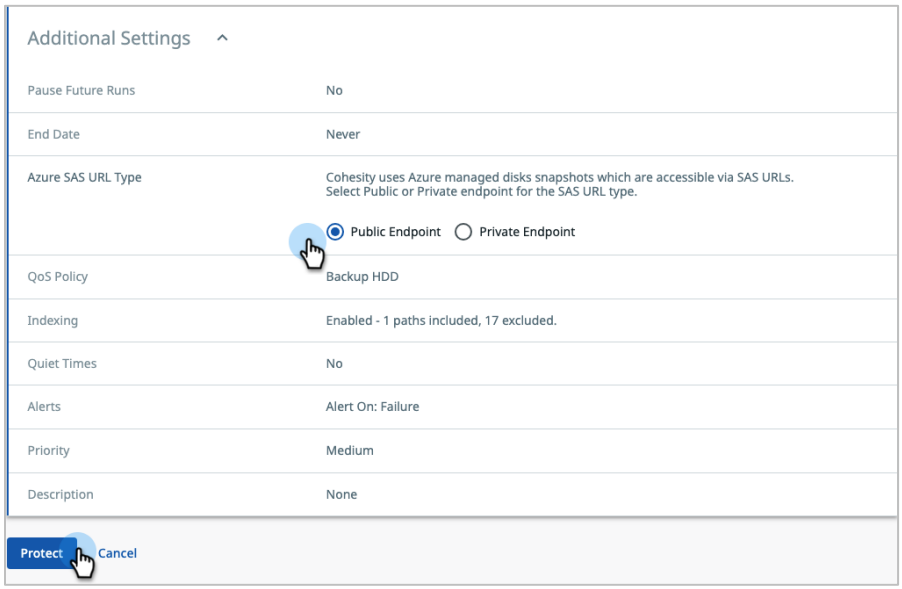
6. Select a Storage Domain and click **More Options** to review Additional settings.

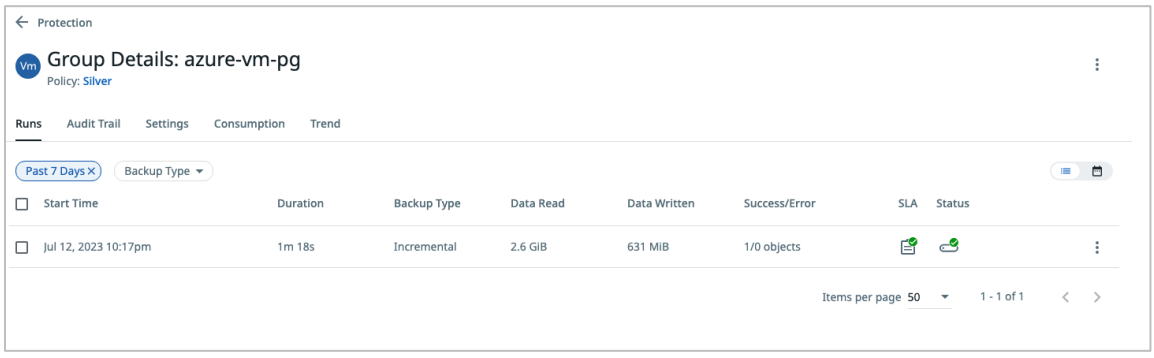


7. From the More Options page, you can specify the protection type, such as **Native Snapshot** or protect using **Snapshot Manager**. Please note that Cohesity does not recommend the Protection Service as Cohesity is planning to depreciate this service in future versions.



8. Expand Additional Settings to select how you want Cohesity to access the disk snapshots via SAS URLs through the public or private endpoint. Once the configuration is completed, click **Protect**. The Protection Group is now successfully created.





Recover Data with Cohesity Azure Native Backup

You can perform Recovery from Cohesity Azure native backups at different levels of granularity, and to both the original and alternate locations. Data can be restored across Azure accounts and regions.

The restore granularity levels are:

1. **Protection Group**. Recover all Azure VMs that are part of a Protection Group to a previous point in time using backup snapshots in a single click.
2. **Azure VM**. Search individual Azure VMs using their names, or the tags associated with them, and recover from a backup snapshot.
3. **Files and Folders**. Restore specific files and folders that reside in an Azure VM.

How Recovery Works with Azure Native Backup

Recovery is the most important aspect of any backup solution, and with Cohesity Platform, you can recover data at every level of granularity.

Although there are different workflows, they all involve these steps:

1. Go to **Protection** > **Recovery**, click **Recover**, and select **VMs**.
2. Search for an **Azure VM** using its name or assigned tags.
3. Select the **Azure VM** that you want to restore and initiate a restore.

Restore Workflows

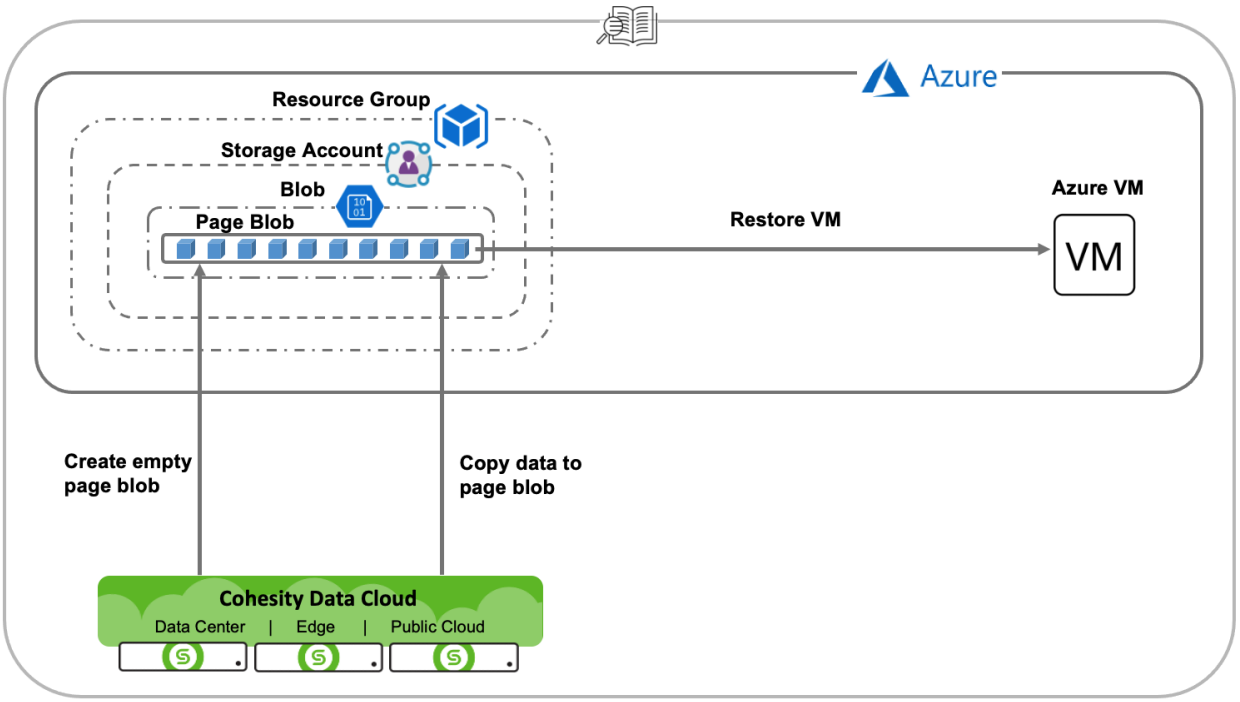
The workflow for data recovery for Azure VMs using an unmanaged disk is different from the recovery workflow for Azure VMs using a managed disk.

Restore Azure VMs Using Unmanaged Disks

The restore workflow for unmanaged disks involves the following sequence:

1. Identify the point in time at which you wish to restore and select a snapshot. Cohesity Platform creates a temporary View on the Cohesity cluster, and the data is cloned into the View.
2. Cohesity creates an empty page blob on Azure.
3. Cohesity DataProtect uploads the data from the temporary View to that page blob.
4. Finally, it creates the VM with the data uploaded to the page blob.

Figure 5: Restore Azure VM Using Unmanaged Disks

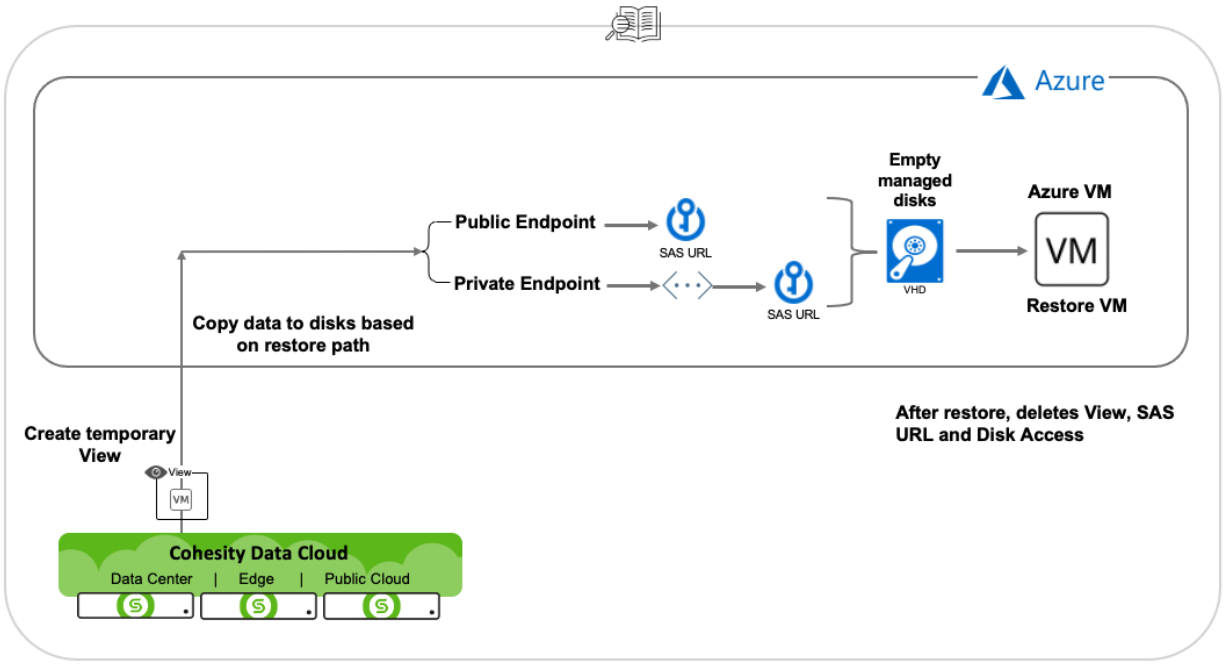


Restore Azure VMs Using Managed Disks

The restore workflow for managed disks involves the following sequence:

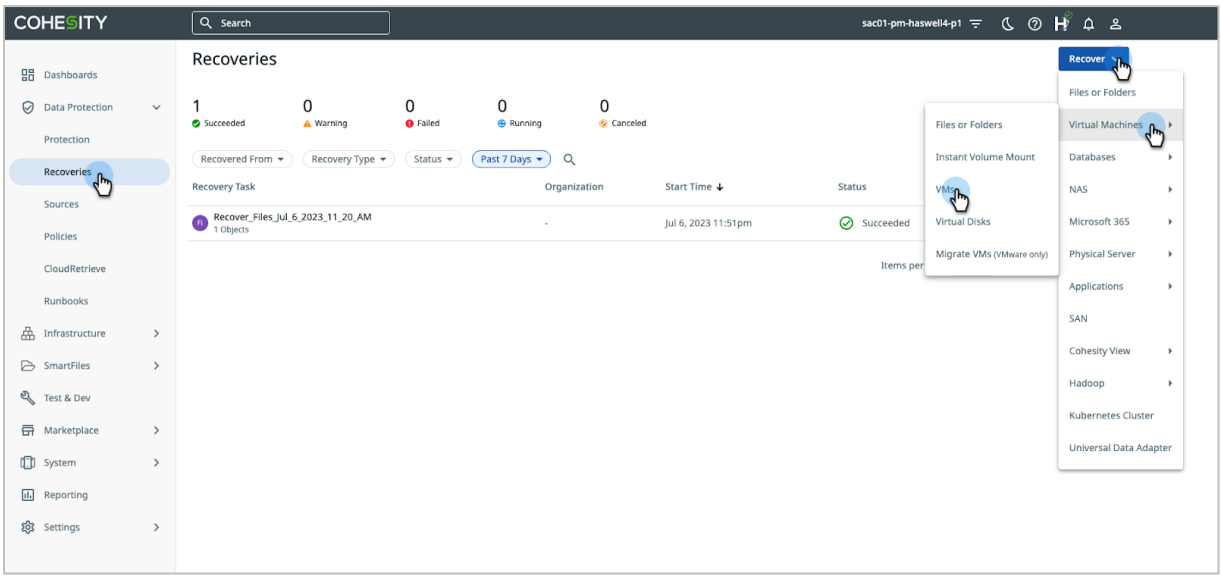
1. Identify the point in time which you wish to restore and select a snapshot. Cohesity creates a temporary View and clones the data from the snapshot to the View.
2. Cohesity creates empty managed disks of the same size as the disk size on Azure.
3. Based on the restore path selection, public or private endpoint, Cohesity updates the restore flow.
4. If the restore is using a Public endpoint, Cohesity creates a SAS URL for each disk, and the data gets copied to the disks using the SAS URL.
5. If the restore is using a Private endpoint, disks are attached to disk access with a private endpoint, and then creates a SAS URL for each disk to copy the data into it.
6. Next, it retrieves the ID of the created managed disk, and creates the VM using the managed disk.
7. Finally, after the restore is completed, Cohesity deletes the View, SAS URL, and Disk Access.

Figure 6: Restore Azure VM Using Managed Disks

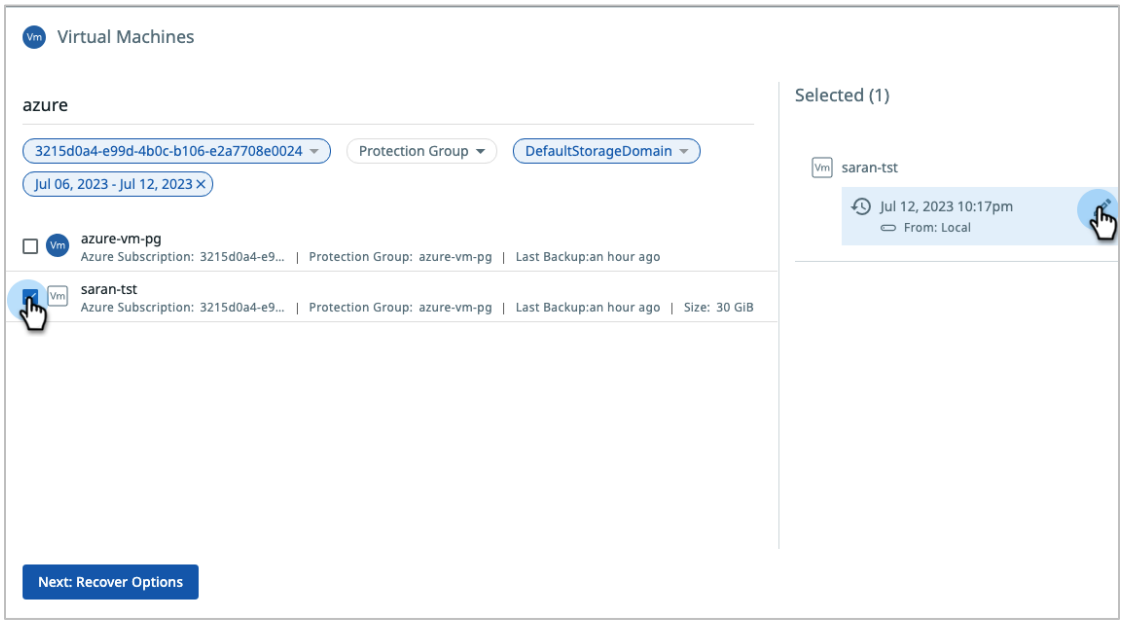


Perform VM Restore

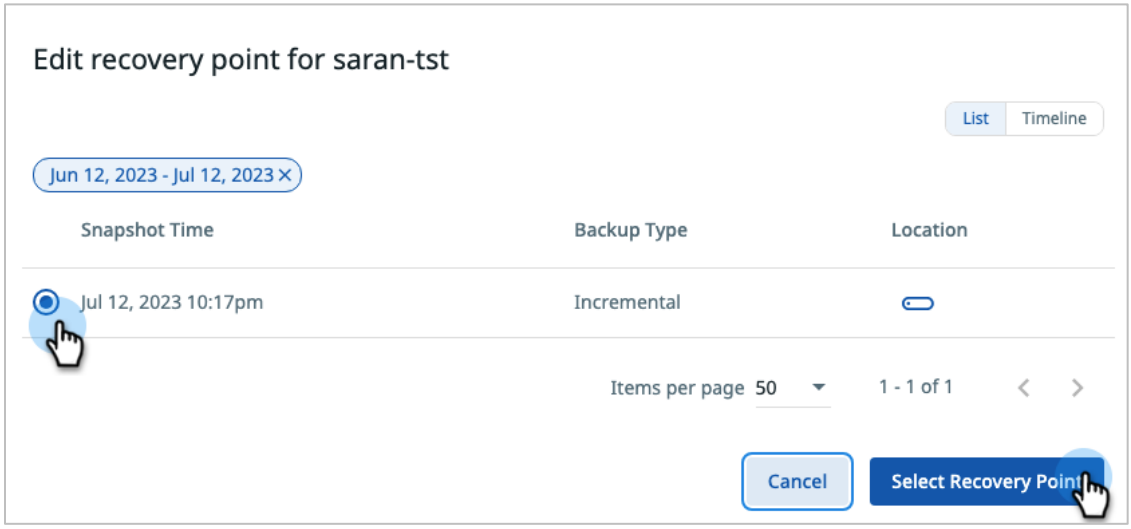
1. Log in to Cohesity Platform and select **Recoveries** > **Recover** > **Virtual Machines** > **VMs**.



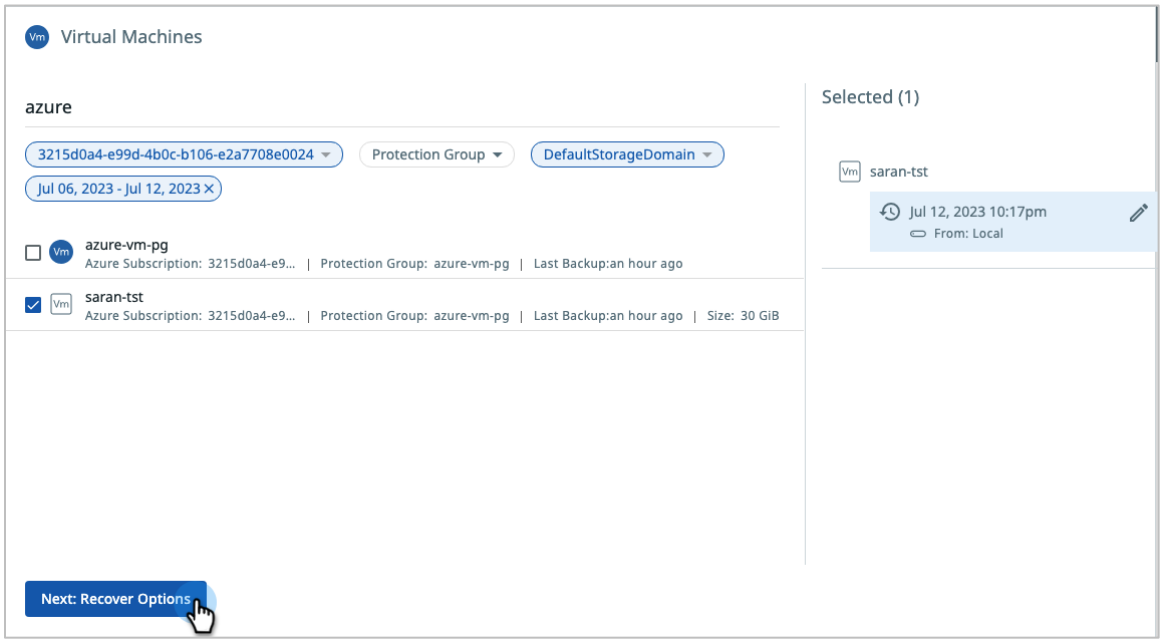
2. Search for the Protection Group, select the VM, and edit the recovery point to select a snapshot.



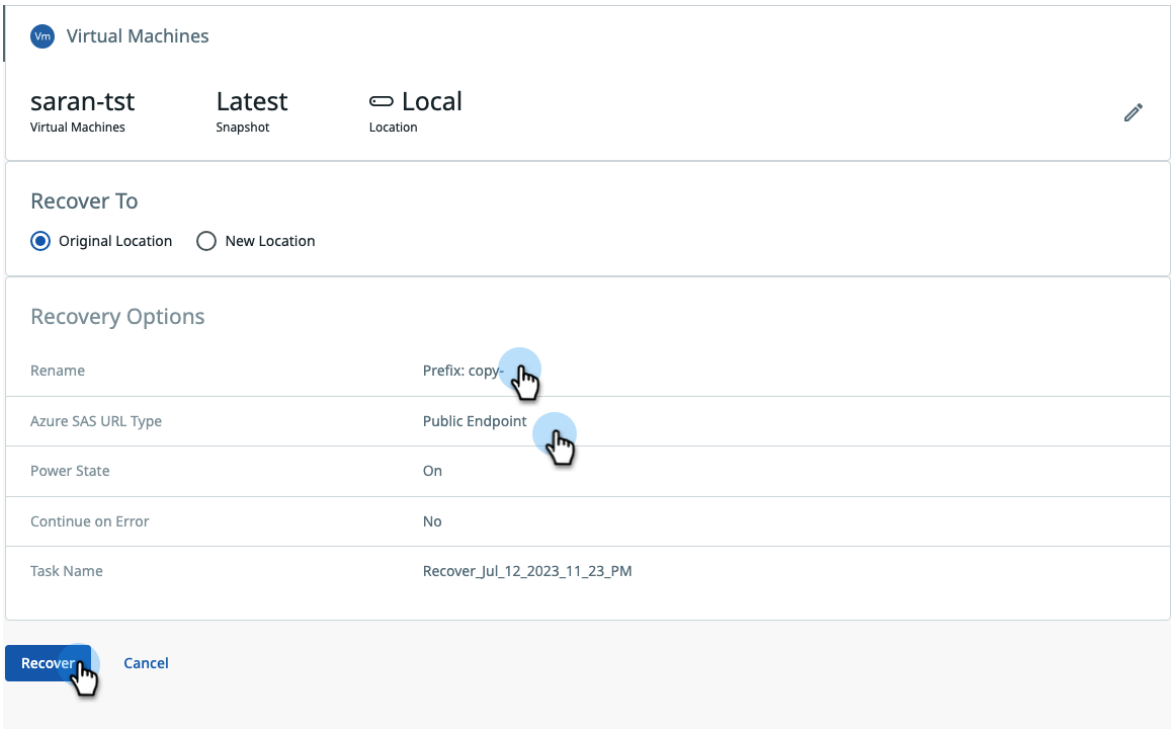
3. Select a snapshot from the list and click **Select Recovery Point**.



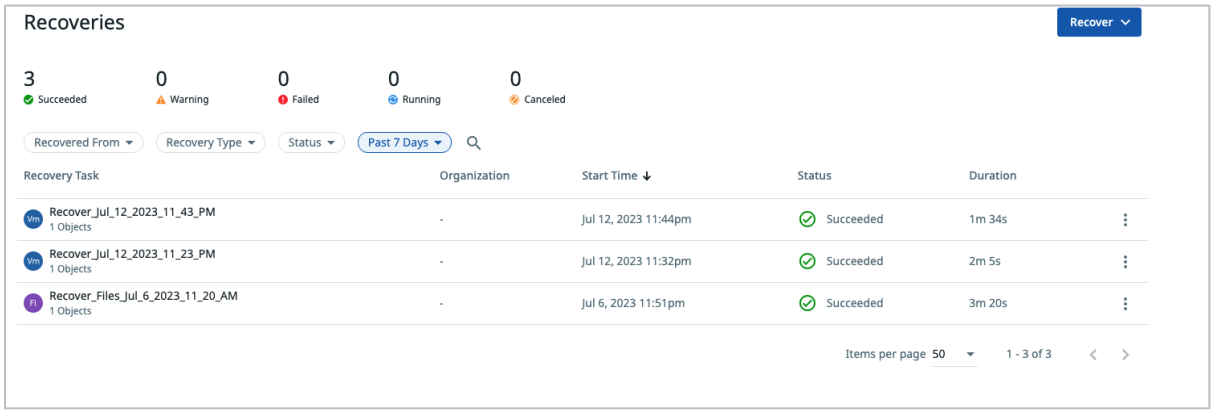
4. Click **Next: Recover Options** to proceed.



5. Select the location (**Original Location** or **New Location**) to recover the VM. Ensure that the correct **Azure SAS URL Type** is selected. Provide a prefix for the VM and click **Recover**.



6. The Recovery task is successfully completed.



Design Decisions and Best Practices

You must make important decisions about choosing a particular backup or recovery workflow that solves a given problem. This section provides a decision tree on when you should use a workflow and the best practices around that.

Backup Using Native Snapshot

You can use this workflow for Azure VM protection:

- If you are looking for Azure instance protection from within the cloud.
- If you want to recover file/folder-level granularity.
- If you want to reduce cloud storage costs with data deduplication and compression.
- If you want to leverage Cohesity archival & cluster level replication.

Backup Using Cloud Snapshot Manager

You can use this workflow for Azure VM protection:

- If you want to protect the Azure instances from outside of the cloud (e.g.: protect the Azure instances using an on-prem Cohesity cluster).
- If you want to recover only at the instance level (no granular recoveries).
- If you want the quickest protection/recovery of instances.
- When permissions for CSM-based backup are different from native snapshot backup. Review the list of permissions required for CSM backup and recovery before configuring the backup. Ensure that you add the required permissions to the Create a Custom Role and Assign Permissions using Azure Portal for CSM-based backup.

Backup Using a Combination of Native Snapshot and CSM Methods

If you have larger VMs and want to achieve quicker backup and require granular recoveries, then you can use both methods. The CSM method will provide a quicker backup compared to long-running backup operations in the native snapshot method. Along with the CSM method, many customers also enable the native snapshot method (in a different protection group) to leverage the granular recovery options as well.

Design Considerations

- Azure Commercial Native Snapshot backup requires the following URLs to be allowlisted in the firewall:
    - `Login.windows.net`
    - `management.azure.com`
    - `*.blob.core.windows.net`
- It's important to note that utilizing a private endpoint incurs additional costs. For detailed information about Azure Private Link pricing, please refer to Azure Private Link Pricing.
- If you are using a disk private endpoint, ensure to meet the following prerequisites:
    - The Cohesity cluster must have network connectivity to the subnet used for SAS URL private endpoints.
    - If your Cohesity cluster is in an on-prem data center, then you must set up VPN or use the Azure express route. If you are using the Cohesity Cloud edition cluster, you must ensure network connectivity between the Cloud edition subnet and the subnet used for SAS URL private endpoints.
    - If you are using a proxy server for the backup of Azure VM using disk private endpoint, then you must perform the following steps:
        - Create a private DNS zone and link to the virtual network of the proxy server.
        - Contact Cohesity support and provide the Private DNS Zone name.
        - Azure does not support SAS URI creation of a snapshot with a private endpoint if the size of the Azure disk is more than 8TB.
- Cohesity requires ports 443 and 50051 enabled on the target for File and Folder recovery.
- The target VM must be reachable with private IP.
- For Native Snapshot backup, Cohesity retains the most recent snapshot for each disk in the cloud to track incremental changes, which could result in additional costs depending on the size of the snapshots.

NOTE: During VM recovery, Cohesity adopts a precautionary approach by generating new resource names to avoid conflicts with existing resources that might hinder the recovery process. However, Cohesity also offers users the flexibility to restore VMs using their original resource names. Contact Cohesity support to enable this feature.

Azure Resources Created by Cohesity Platform During Restore

In the process of running restore, the Cohesity Platform creates resources on Azure.

Figure 7: Resources Created in Azure by Cohesity Platform

Resource	Workflow	Count	Reason	Life cycle	Naming convention
Resource Group	Restore	Per region per subscription	To restore VMs	Permanent	“cohesity” + <region of source vm> + “-rg”
Storage Account	Restore	Per region per subscription per cluster	To copy data from Cohesity to Azure	Permanent	“cohesity” + Hash(<cluster_id> + <region of vm > + <subscription_id>)
Storage Container	Restore	Per region per subscription per cluster	To copy data from Cohesity to Azure	Permanent	“cohesity” + <region of source vm> + “-sc”
VMName	Restore	Per Restore per VM	For VM restore	Permanent	Same as backed up VM name if no prefix and suffix are provided through UI.
Managed Disk Name	Restore	Per Restore per VM	For VM restore	Permanent	Creates a unique disk name. <VM name> + <unique_id>
Blob Name	Restore	Per Restore per VM	For VM restore	Permanent	“Cohesity_” + <cluster_id> + <job_id> + <task_id> + <backed_up blob name>

Resource	Workflow	Count	Reason	Life cycle	Naming convention
Network Interface Name	Restore	Per Restore per VM	For VM restore	Permanent	**For restoring in same location**: <VM Name > + Hash(<backed_up interface name> + <cluster_id> + <job_id> + <task_id>) **For restoring in different location**: <VM Name> + "-nic"

Appendix A: Azure Native Backup Terminology

There are several terms that are especially important to understand as you learn about the architecture of Azure native backups on Cohesity Platform.

Table 4: Azure Native Backup Terminology

Term	Definition
Azure Virtual Machines	Compute allocation in the cloud. The Azure VM being backed up is addressed as the “Source VM.”
Azure Disk Storage	Block storage allocated in the form of disks to an Azure VM.
Virtual Network	Virtual network dedicated to your Azure account.
Tags	A tag is a label that you or Azure assigns to an Azure resource. Each tag consists of a key and a value.

Appendix B: Egress Cost Considerations

Table 5 below outlines the deployment models and associated egress cost for backup and restore of data using Cohesity's Azure native backup solution.

Table 5: Egress Cost Considerations

Cohesity Platform	Region	Backup	Restore
On-Premise	NA	Yes	No
Cloud Edition	Same Region	No	No
	Different Region	Yes	Yes

Appendix C: Prepare Azure Subscription to Register with Cohesity Platform

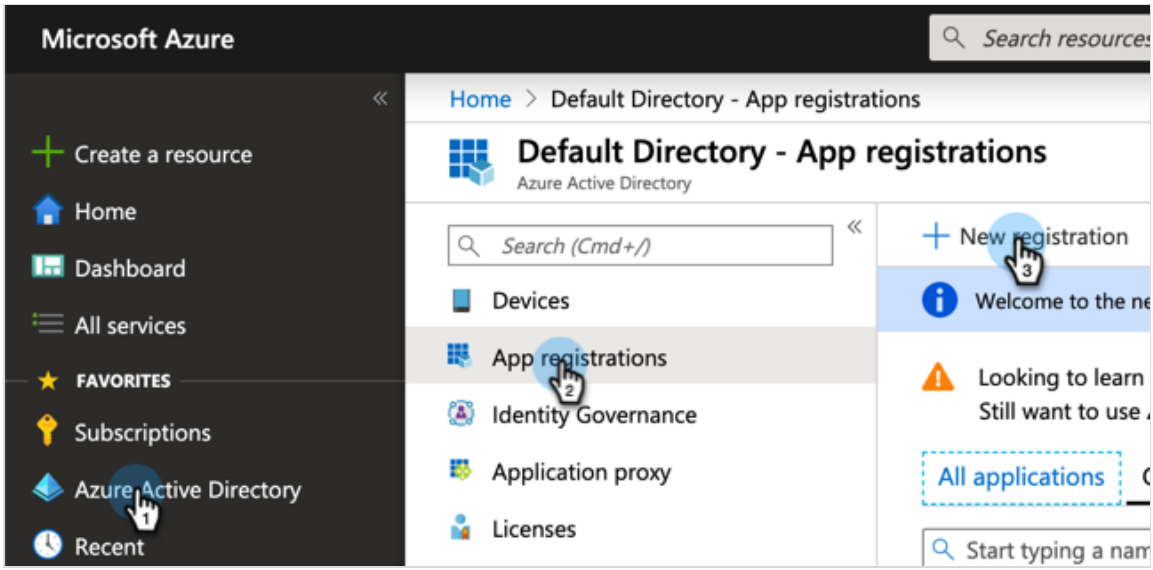
Before you register an Azure subscription with Cohesity Platform, some settings must be configured on Azure.

You'll need to:

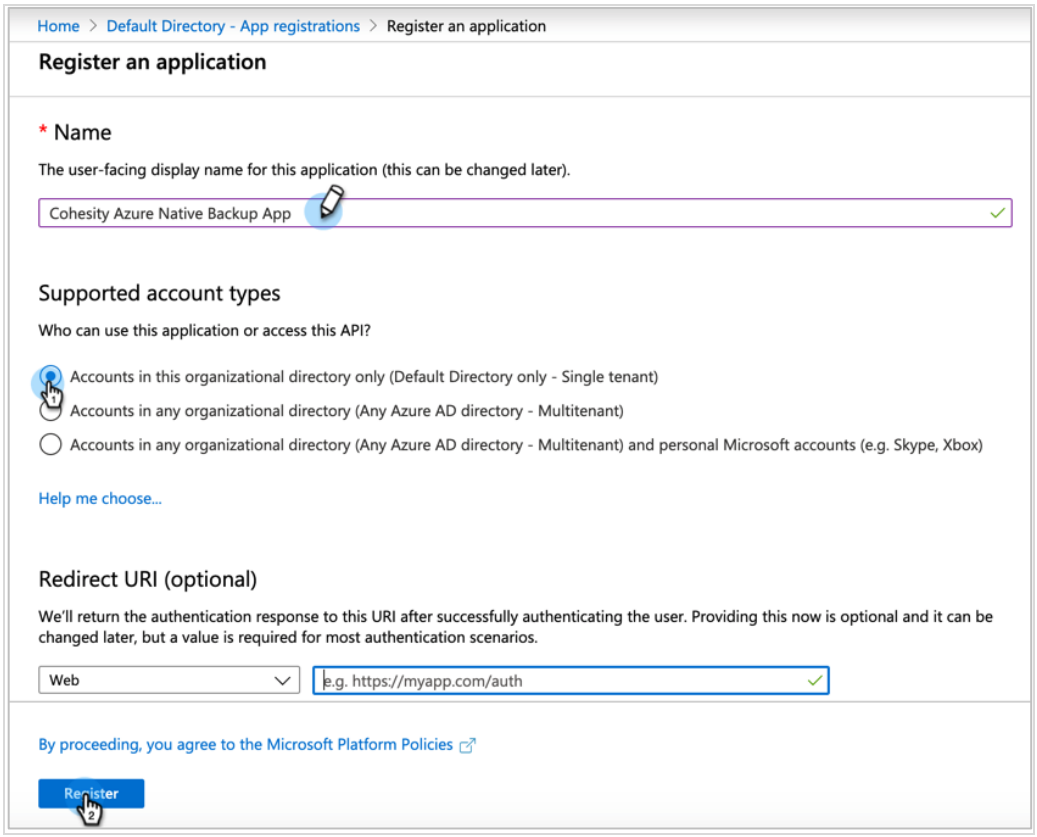
1. Register an App on Azure.
2. Create a Custom Role and Assign Permissions using Azure Portal.
3. Create a Custom Role and Assign Permissions Using the Azure CLI (optional).
4. Assign Custom Role to Registered Application for Subscription.

Register an App on Azure

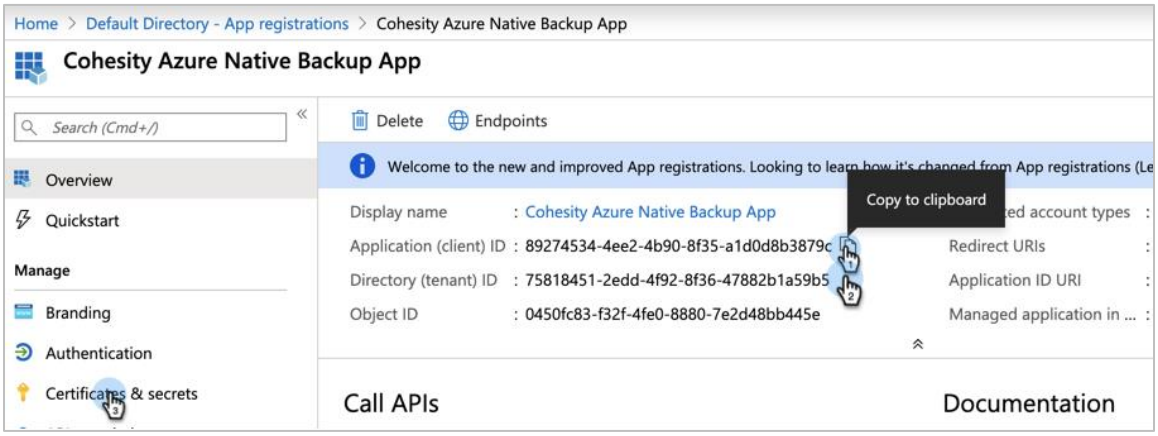
1. Log in to the Azure Portal at: https://portal.azure.com
2. Navigate to **Azure Active Directory > App registrations**. Click **New registration** to register a new App.



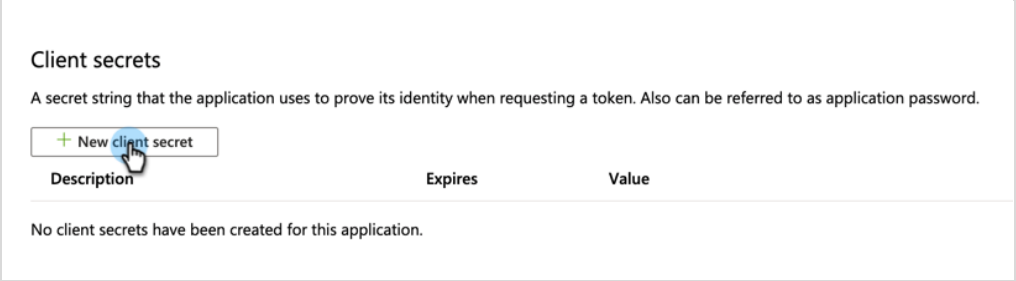
3. Enter the **Name, Supported account types**, and optionally the **Redirect URI**. Click **Register** to continue.



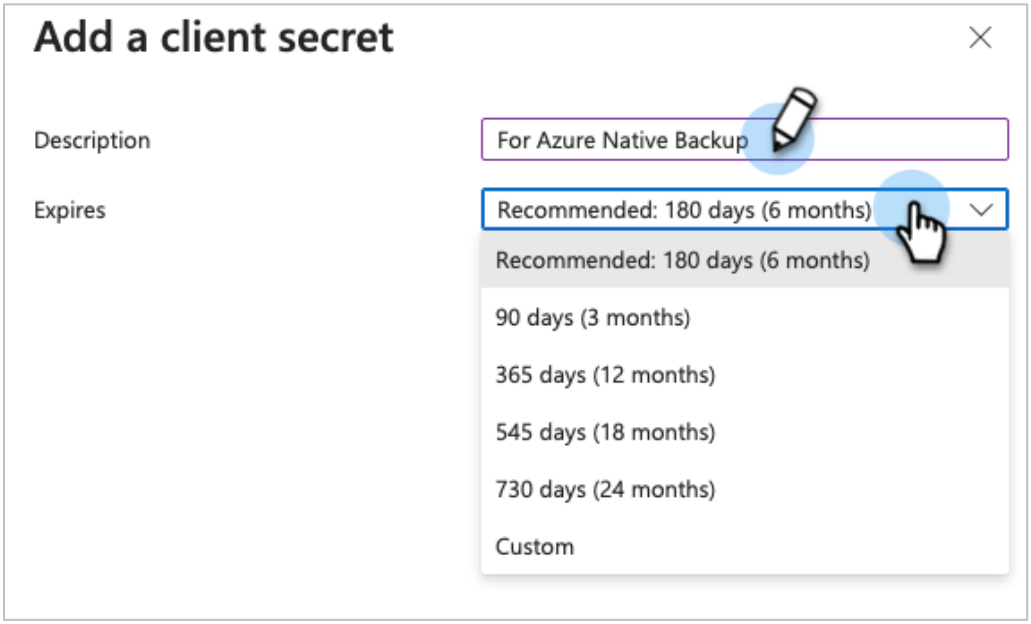
4. Copy the **Application (client) ID** and **Directory (tenant) ID** for the source registration process. Then click **Certificates & secrets.**



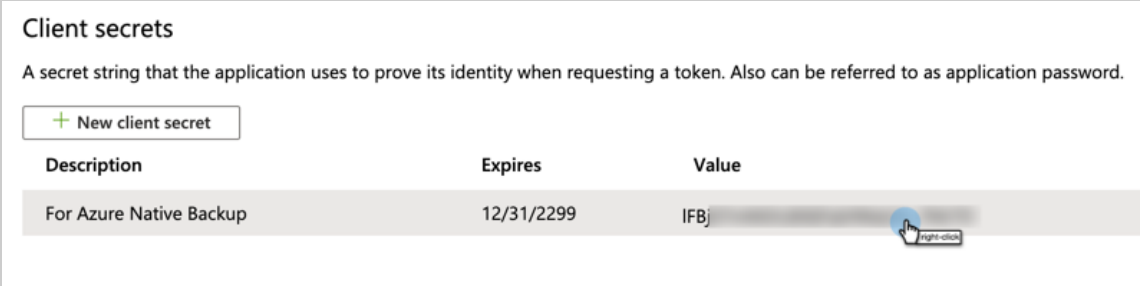
5. Click **New client secret**.



6. Enter a **Description** and select a period for **Expires**, then click **Add**.

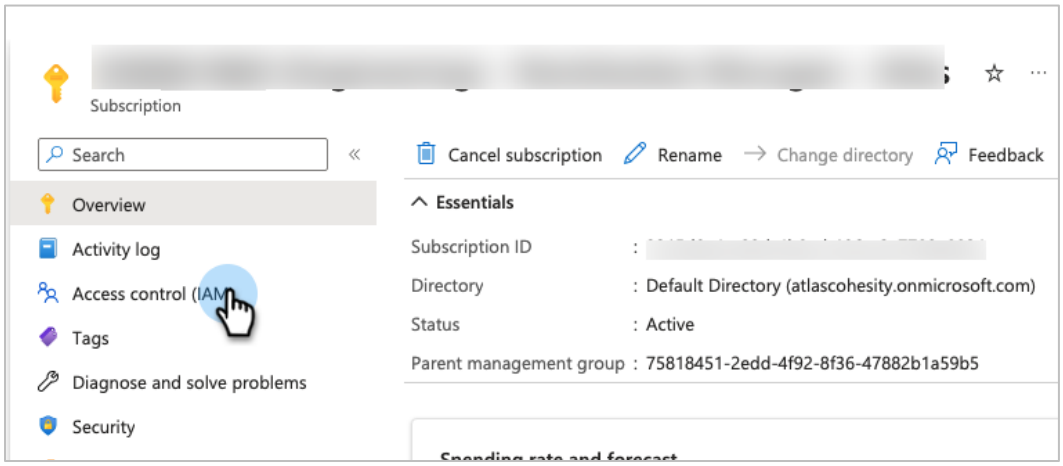


7. Copy the **App Secret** for source registration.

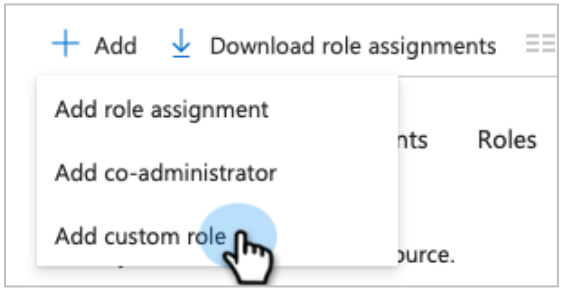


Create a Custom Role and Assign Permissions using Azure Portal

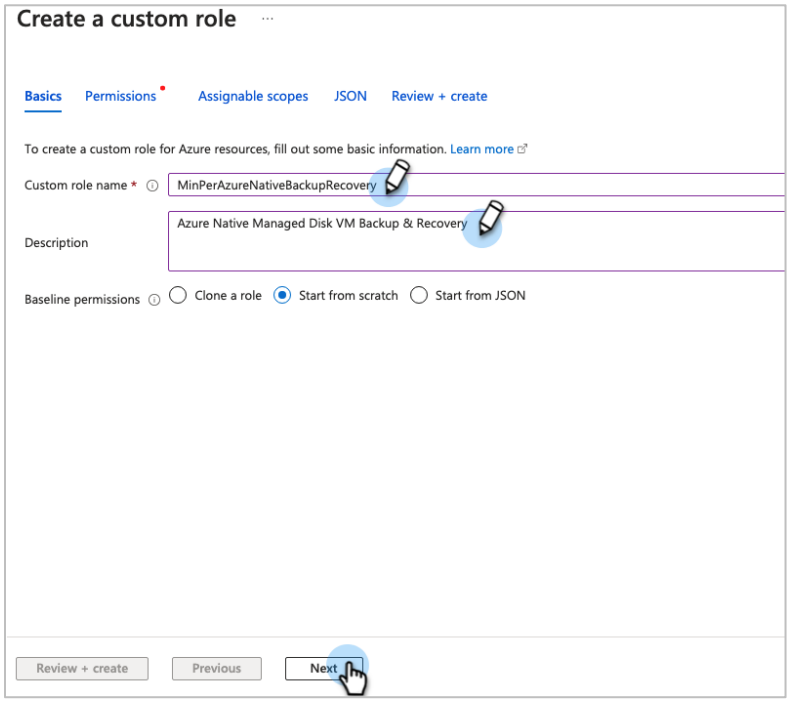
1. In the Azure portal, navigate to **Subscriptions,** click the **subscription**, and select **Access Control (IAM).**



2. Click **Add Custom role**.



3. Enter a **Custom role name** and description (optional) and click **Next**.



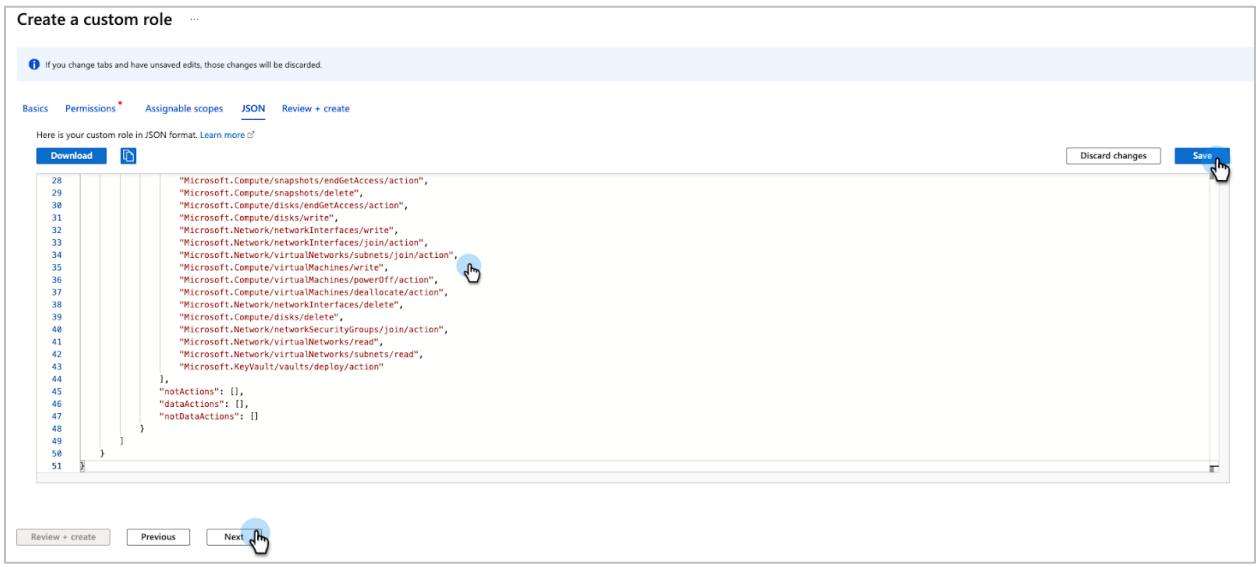
4. Click **JSON** and click **Edit**.

5. Copy the below-listed permissions and paste them into the JSON and click **Save**.

   a. Always refer to the documentation to verify if there are any changes in the minimum permissions required for Cloud-native backup and recovery.

```
    {
    "properties": {
        "roleName": "MinPerAzureNativeBackupRecovery",
        "description": "Azure Native Managed Disk VM Backup & Recovery ",
        "assignableScopes": [
            "/subscriptions/3215d0a4-e99d-4b0c-b106-e2a7708e0024"
        ],
        "permissions": [
            {
                "actions": [
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Network/networkInterfaces/ipconfigurations/read",
                    "Microsoft.Network/networkSecurityGroups/securityRules/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Resources/subscriptions/resourcegroups/read",
                    "Microsoft.Resources/subscriptions/resourcegroups/write",
                    "Microsoft.Storage/storageAccounts/write",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/wri
te",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/rea
d",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/disks/beginGetAccess/action",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Compute/snapshots/beginGetAccess/action",
                    "Microsoft.Compute/snapshots/endGetAccess/action",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Compute/disks/endGetAccess/action",
                    "Microsoft.Compute/disks/write",
```

```
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.KeyVault/vaults/deploy/action"
                ],
                "notActions": [],
                "dataActions": [],
                "notDataActions": []
            }
        ]
    }
}
```



6. Click **Create** to create the custom role.

Create a Custom Role and Assign Permissions Using the Azure CLI (optional)

You can also use Azure CLI to create a custom role and assign permissions.

1. In the Azure portal, navigate to **Subscriptions,** click the **subscription**, and copy the **Subscription ID** for source registration**.**
2. To create a custom role, download, install, and log in to the Azure command-line interface (CLI). For instructions, see Install the Azure CLI**.**

   NOTE: Custom roles can only be created using Azure CLI.

3. Log in to the Azure CLI and enter the command below.

   NOTE: In the JSON command below, you must replace <SUBSCRIPTION-ID> with your actual subscription ID

   a. Always refer to the documentation to verify if there are any changes in the minimum permissions required for Cloud-native backup and recovery.

```
    az role definition create --role-definition '{
   "Name": "MinPerAzureNativeBackupRecovery",
   "Description": "Azure Native Managed Disk VM Backup & Recovery " ,
   "IsCustom": true,
   "Actions": [
"Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/disks/read",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Network/networkInterfaces/ipconfigurations/read",
                    "Microsoft.Network/networkSecurityGroups/securityRules/read",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Resources/subscriptions/resourcegroups/read",
                    "Microsoft.Resources/subscriptions/resourcegroups/write",
                    "Microsoft.Storage/storageAccounts/write",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/write
",
                    "Microsoft.Storage/storageAccounts/blobServices/containers/read"
,
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/disks/beginGetAccess/action",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Compute/snapshots/beginGetAccess/action",
                    "Microsoft.Compute/snapshots/endGetAccess/action",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Compute/disks/endGetAccess/action",
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
```

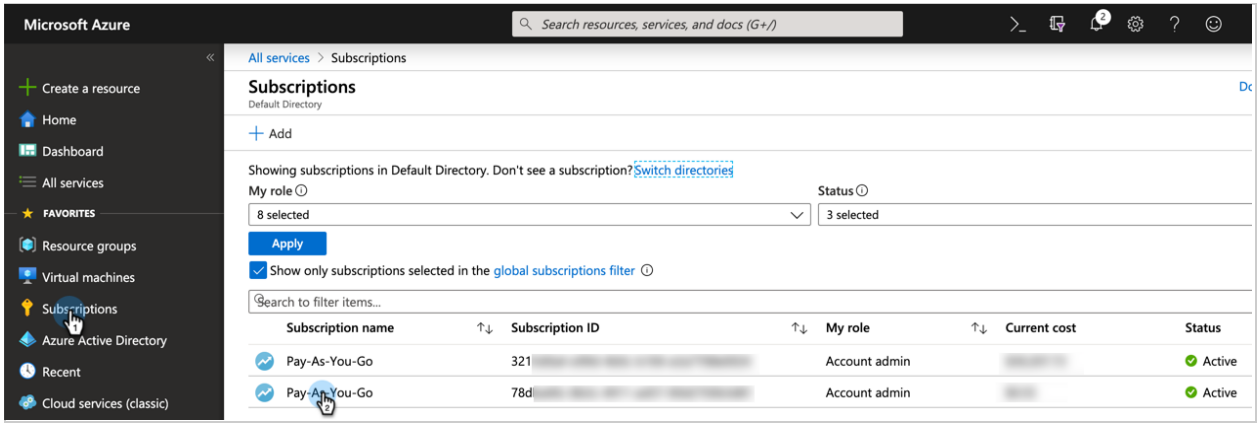
```
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.KeyVault/vaults/deploy/action"


    ],
    "DataActions": [],
    "NotActions": [],
    "NotDataActions": [],
    "AssignableScopes": ["/subscriptions/<SUBSCRIPTION-ID>"]
    }
```

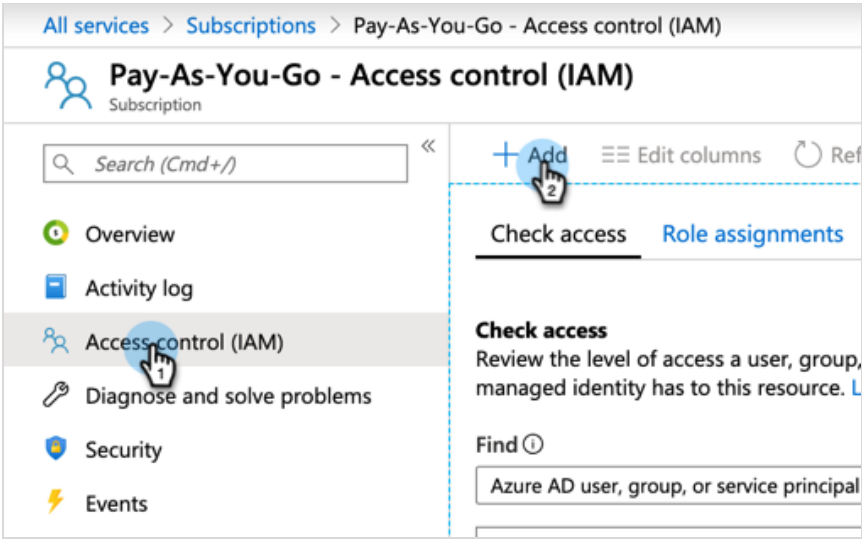
Assign Custom Role to Registered Application for Subscription

The custom role created above specifies the permissions that Cohesity requires to back up Azure VMs. We need to assign this role to the App we created under Register an App on Azure. Hence, when Cohesity uses this App for authorization, it can inherit the permissions specified in the custom role.

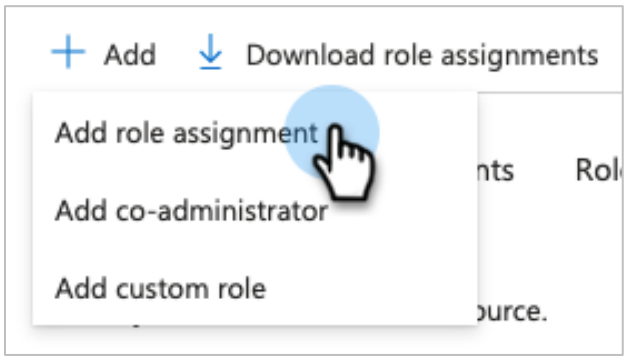
1. In the Azure portal, go to **Subscriptions > Pay-As-you-Go.**



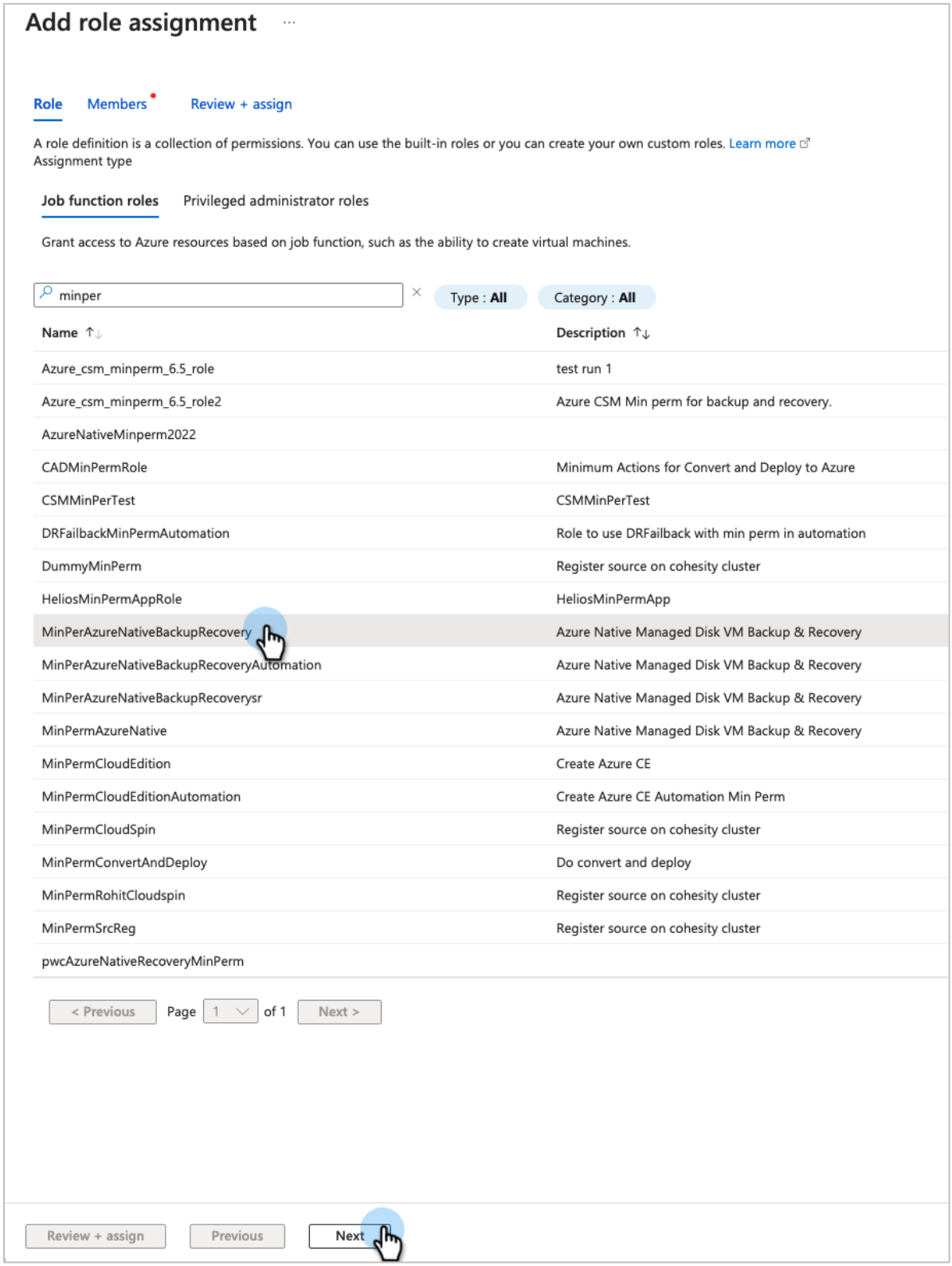
2. Click **Access control (IAM)** and then **Add**.



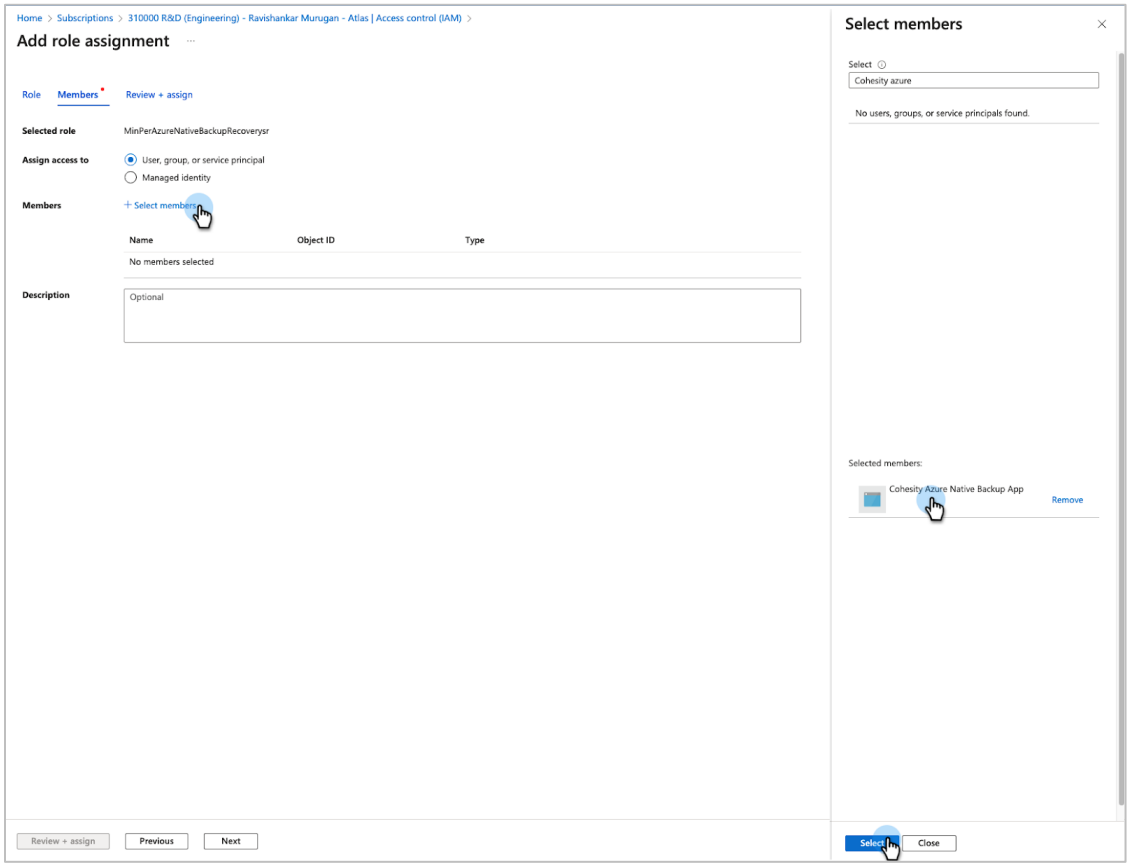
3. Click **Add role assignment**.



4. Select the custom role and click Next.



5. In the Members tab, click **Select Members** and search and select the created app.



6. Click **Review + Assign** to add the role assignment.

Considerations

Azure Native Snapshotting has the following considerations:

- For Azure VMs created using Azure marketplace images, the restored VM does not support logging in using a username and password present in the backed up VM. Login using SSH keys is supported.
- When the restored VM boots up for the first time, Azure images are pre-installed with cloud-init software that locks user accounts, which is the default behavior.

  TIP: Create an admin user from the Azure portal or log in through the root account if it was enabled in the source VM. Reinstate the user accounts using the following command:
  `passwd -u username`
- VMs encrypted through ADE can't boot up after being restored to a different location, unless the user replicates the keys that were used to encrypt the VM into the new location. VMs encrypted using Azure SSE do not have this issue.
- Managed disk VMs that are turned off are shown as 0 bytes in size in the entity hierarchy of Azure Source.
- Backup of Azure VMs that have Ephemeral Volumes is not supported.
- VMs with a static IP will not be recovered back with that static IP.
- Recovery of VMs from an Availability Set to a different location will not inherit the Availability Set parameters, as Availability Set parameters are tied to location.
- Recovery of an unmanaged disk with different SKU types depends on the storage container where the recovery is done.

Your Feedback

Was this document helpful? Send us your feedback!

About the Authors

Saran Ravi is a Staff Technical Marketing Engineer at Cohesity. In his role, he focuses on Cloud, Cohesity Cloud Services, and Kubernetes.

Other essential contributors included:

- Karthick Radhakrishnan, Director, Technical Solutions Engineering
- Himanshu Srivastava, Engineering
- Patibandla Harikrishna, Engineering
- Kevin Hill, Manager Solution Architects
- Subash Babu, Staff Technology Editor, Technical Solutions Engineering
- Mary Juliya, Technical Editor, Technical Solutions Engineering

Document Version History

VERSION	DATE	DOCUMENT HISTORY
2.1	July 2024	Republishing
2.0	Aug 2023	Updated to 7.0 release
1.0	Nov 2019	First full release

ABOUT COHESITY

Cohesity is a leader in AI-powered data security and management. Aided by an extensive ecosystem of partners, Cohesity makes it easier to protect, manage, and get value from data – across the data center, edge, and cloud. Cohesity helps organizations defend against cybersecurity threats with comprehensive data security and management capabilities, including immutable backup snapshots, AI-based threat detection, monitoring for malicious behavior, and rapid recovery at scale. Cohesity solutions are delivered as a service, self-managed, or provided by a Cohesity-powered partner. Cohesity is headquartered in San Jose, CA, and is trusted by the world's largest enterprises, including six of the Fortune 10 and 44 of the Fortune 100.

Visit our website and blog, follow us on Twitter and LinkedIn and like us on Facebook.