N2W Backup & Recovery

Quick Start Guide for Azure

Version 5.0.2

docs.n2ws.com

Contents

1. Introduction 3

Requirements 3

2. Create a Custom Role and Permissions on Azure 4

3. Deploy the N2W Server on Azure 6

Assign the custom role to the N2W VM 10

4. Configure N2W with the Configuration Wizard 12

5. Creating an Azure Backup Policy 17

Adding and Confirming an Azure Account 17

Creating a Simple Backup Schedule 19

Creating a Simple Azure Backup Policy 20

Backing Up an Azure Policy 23

6. Recovering from an Azure Backup 24

Recovering a VM and Disks 24

Recovering Independent Disks 27

7. Additional Resources 28

1 Introduction

N2W Backup & Recovery is a powerful tool that's essentially plug-and-play. It takes about 20 minutes to set up the basic N2W configuration. The *Quick Start Guide for Azure* walks you through the core steps to get N2W up and running on the Azure cloud as a virtual machine with N2W installed on it.

Before installing N2W on Azure, review the basic N2W installation in the *N2W Backup & Recovery Quick Start Guide*.

> **Passwords.** N2W strongly recommends a strong password for the server. Make sure no one can access or guess it, and change it regularly. N2W enforces these rules:
>
> - Minimum length of 8 characters.
> - Not a common word or phrase.
> - Not numeric characters only.

Deploying N2W on Azure takes these procedures:

- Create a custom role on Azure
- Deploy the N2W VM on Azure and assign it the custom role
- Configure N2W with the Configuration Wizard
- Add an Azure account and create a backup policy
- Recover from an Azure backup

Requirements

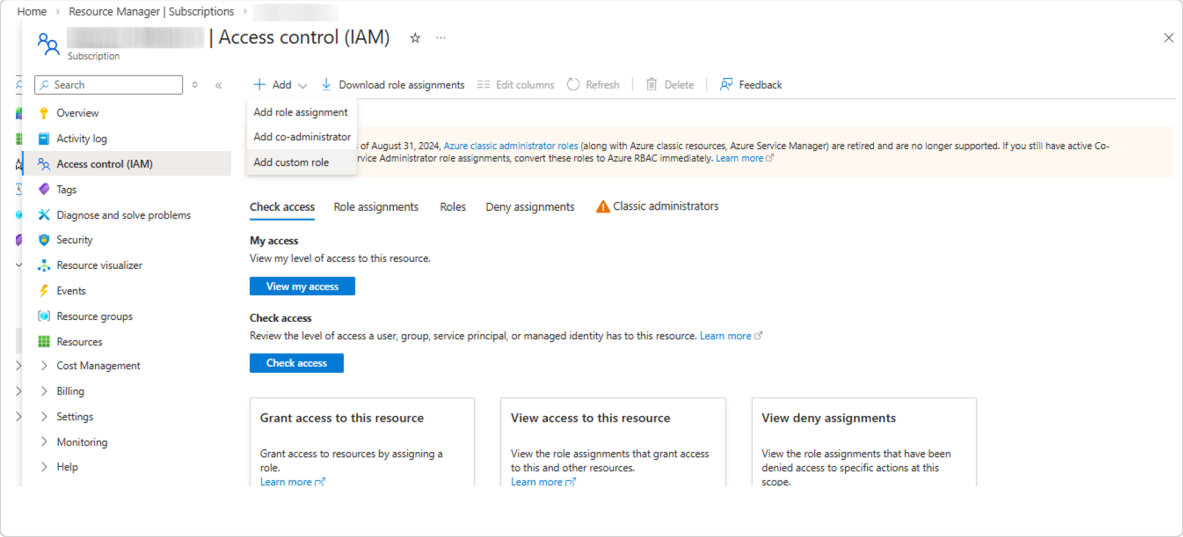
Before continuing, check that you meet the following requirements:

- You already have an Azure account and access to the Azure portal.
- You can access the Azure Marketplace and create virtual machines.

> **Note.** For the recommended virtual machine type and Azure disk size requirements of N2W for Azure, see the KB article Recommended VM Types for an N2W Server in Azure.

2 Create a Custom Role and Permissions on Azure

1. In Microsoft Azure, select **Subscriptions**.
2. Select your subscription, and then select **Access control**.
3. In the Access control (IAM) **+ Add** menu, select **Add custom role**.

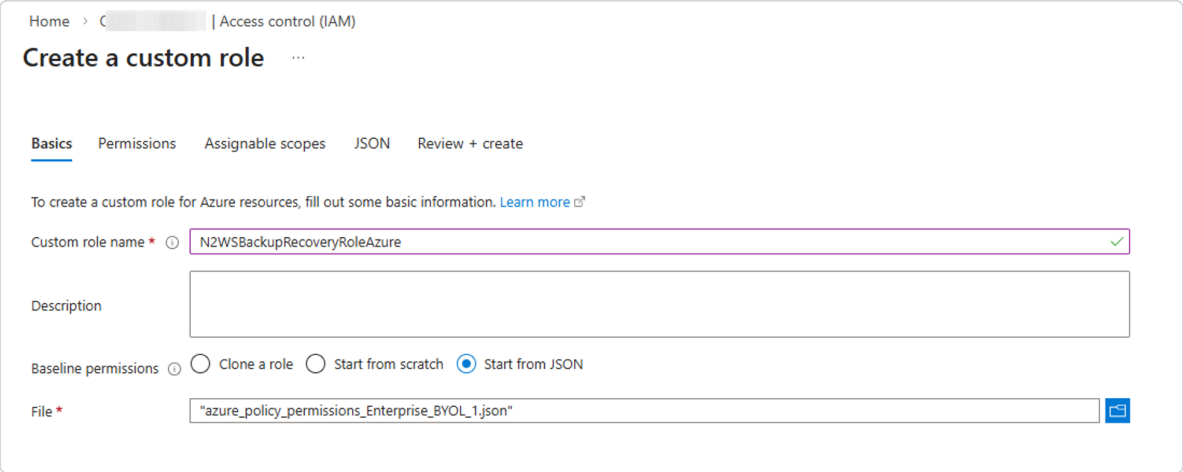


4. In the **Basics** tab, type a name for your custom role in the **Custom role name** box.
5. In the Baseline permissions section, select **Start from JSON**.
6. Download and extract the JSON files in **N2W-5.0.2-Azure-permissions.zip** from the KB article 5.0.2 Required Minimum Azure Permissions for N2W Operations. Add your subscription ID to the **subscriptions** attribute in the JSON file.

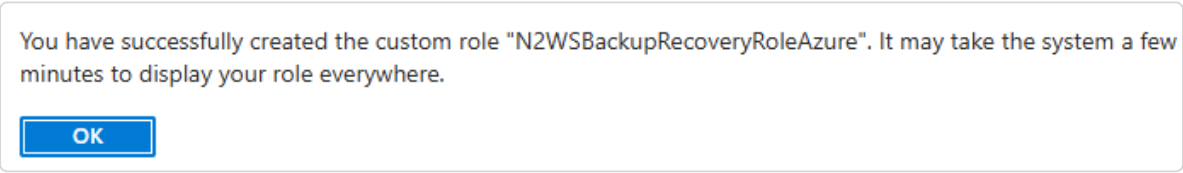
> **Note.** You can edit the file or change the configuration before selecting **Review + create**. If you have a newer N2W version, a matching permissions file is on our support site.

> **New in 5.0.2.** The custom role must include the **Microsoft.Compute/disks/beginGetAccess/action** permission, which is required for DR to a different location. The 5.0.2 permissions file already includes it. If you are upgrading, update your existing custom role with the new file.

7. In the **Select a file** box, select the downloaded JSON file relevant to your N2W license.



8. Select **Next**.
9. In the **Permissions** tab, review permissions if needed, and then select **Next**.
10. In the **Assignable scopes** tab, select **Assignable scope**.
11. In the **Type** list of the **Add assignable scopes** section, select **Subscription**.
12. From the subscription list in the right-hand column, select your subscription, and then select **Select**.
13. On the Assignable scopes page, select **Next**. The JSON tab opens with your custom role file.
14. Review and edit the JSON file as necessary, and then select **Next**.
15. In the **Review + create** tab, perform a final review, and then select **Create**.
16. When the custom role is created, select **OK**. It may take a few minutes for the new role to appear everywhere.

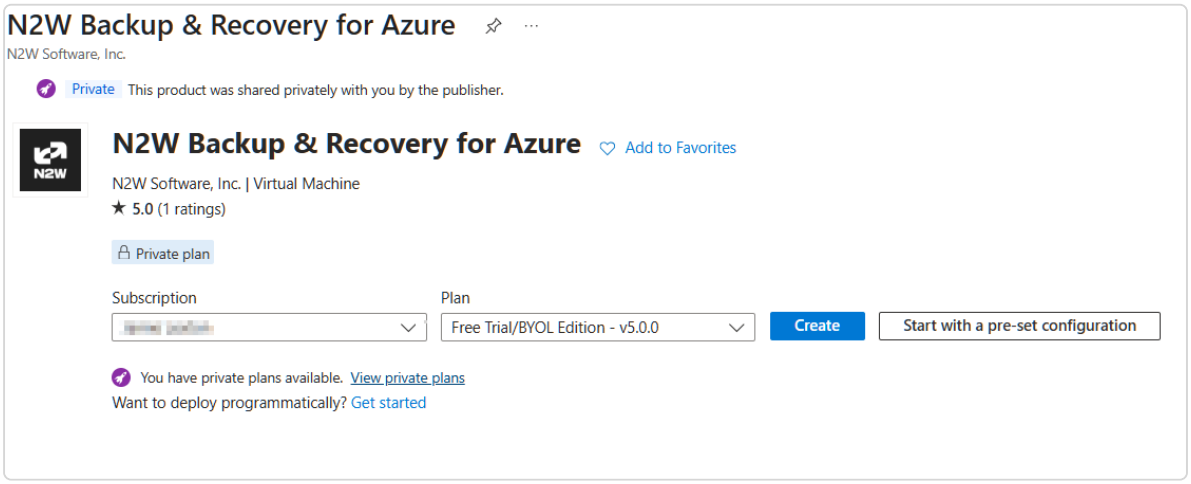


Note. Write down the name of this custom role. You need it when you deploy the N2W server.

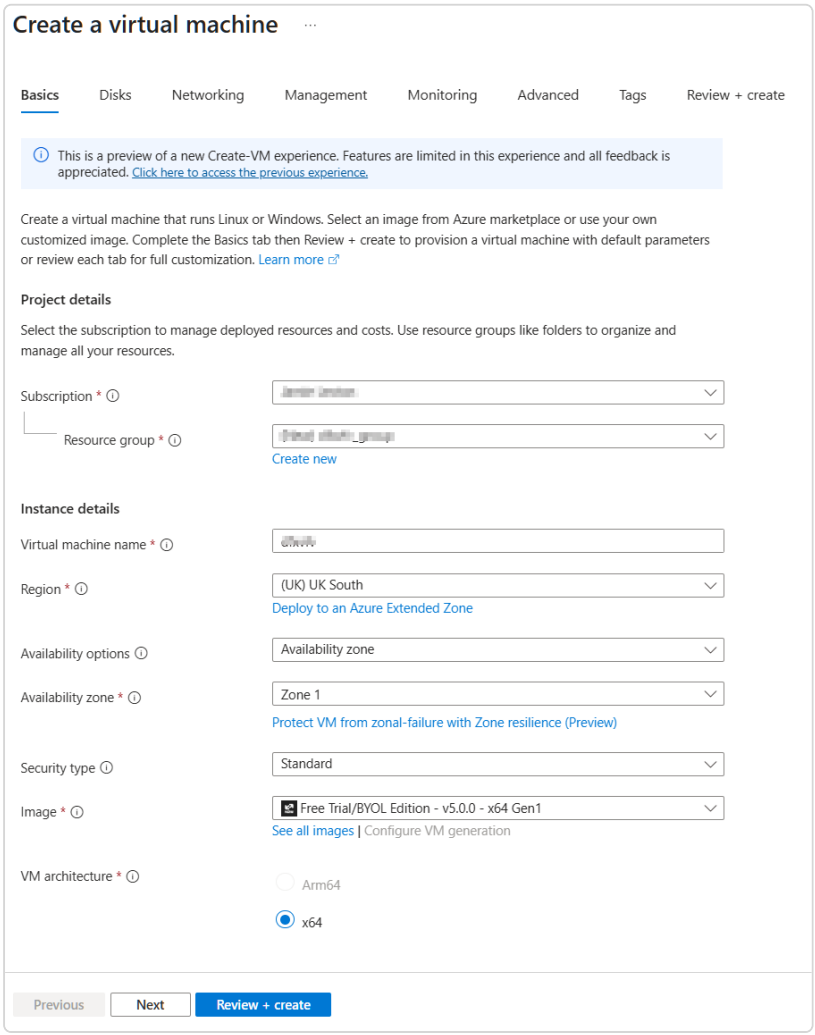
3 Deploy the N2W Server on Azure

To watch a video of the N2W deployment on Azure, see n2ws.com/support/install-guide.

1. In the Microsoft Azure Marketplace, search for **N2W**.
2. In the **Products** list, select **N2W Backup & Recovery for Azure**.
3. Select the latest version, and then select **Create**.
4. On the **N2W Backup & Recovery for Azure (preview)** page, in the **Plan** list, select **BYOL and Free Trial for the Latest Version** to start with a pre-set configuration, and then select **Create**.



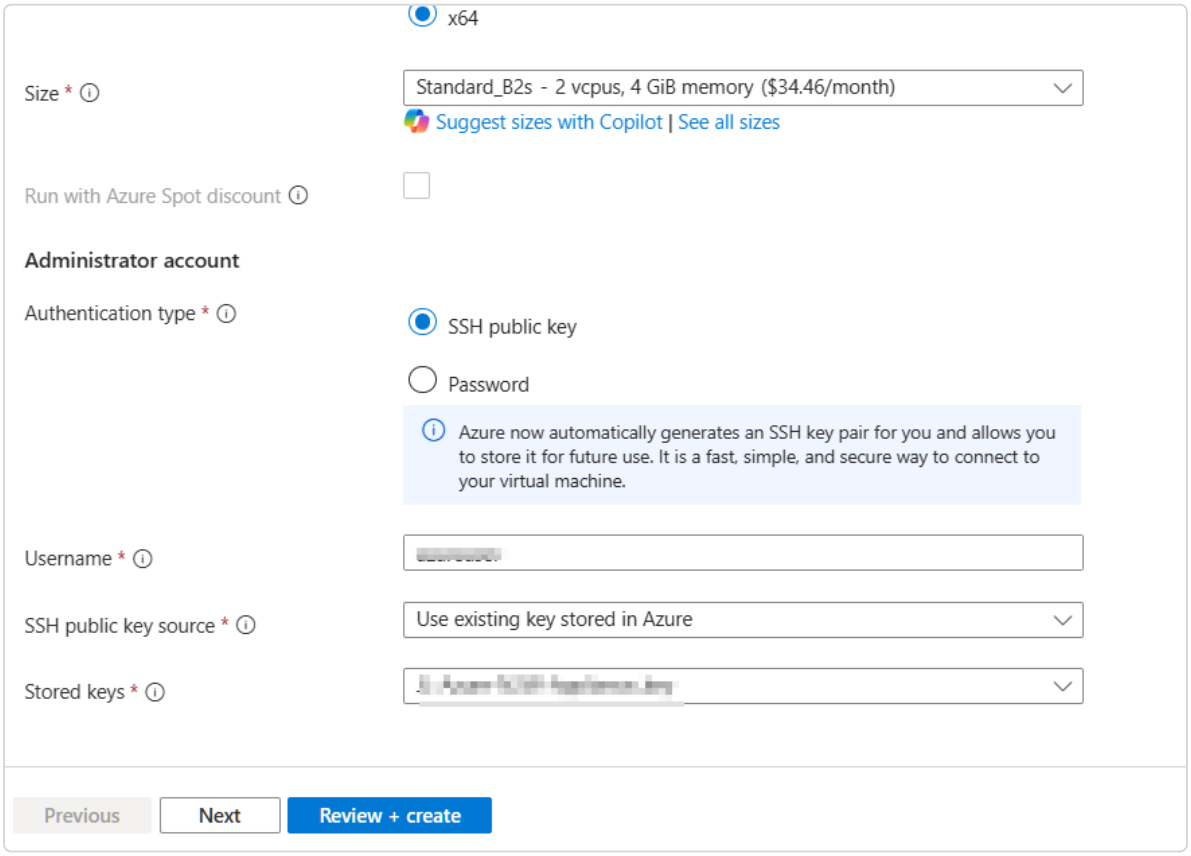
The Create a virtual machine wizard opens.



5. In the **Subscription** list, select the subscription to manage deployed resources. In the **Resource Group** list, select the resource group where you want to deploy the machine.

6. In the Instance details section:
   - Type the **Virtual machine name**.
   - Select the **Region** where the machine will be deployed.
   - Choose the **Security type**.
   - Select the **Size** of the virtual machine. **Standard_B2s** is the minimum requirement.
   - Set the authentication type: SSH or Password. For **Username**, we recommend **cpmuser**.

7. In the **SSH public key source** list, select **Use existing key stored in Azure**, or create a new key. In the **Stored Keys** list, select a key of your choice.



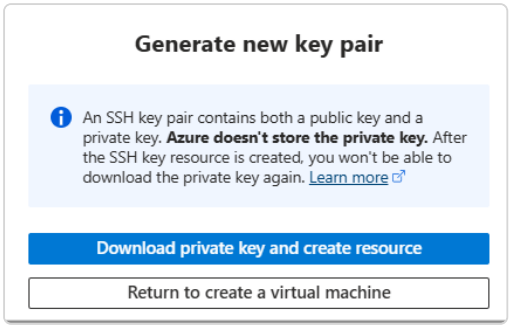
8. Select **Next: Disks**.
9. In the **Disks** tab, keep the defaults and select **Next: Networking**.
10. In the **Networking** tab, select the necessary network, subnet, public IP, and security group. Select **Delete public IP and NIC when VM is deleted**, and then select **Next: Management**.

> **Note.** The N2W server VM must have outbound HTTPS (TCP 443) connectivity to Azure service endpoints to perform backup and recovery operations. Make sure the selected VNet and subnet allow outbound internet access, and that DNS resolution is available to the VM. If your environment requires a proxy, you can configure it in the N2W Configuration Wizard.

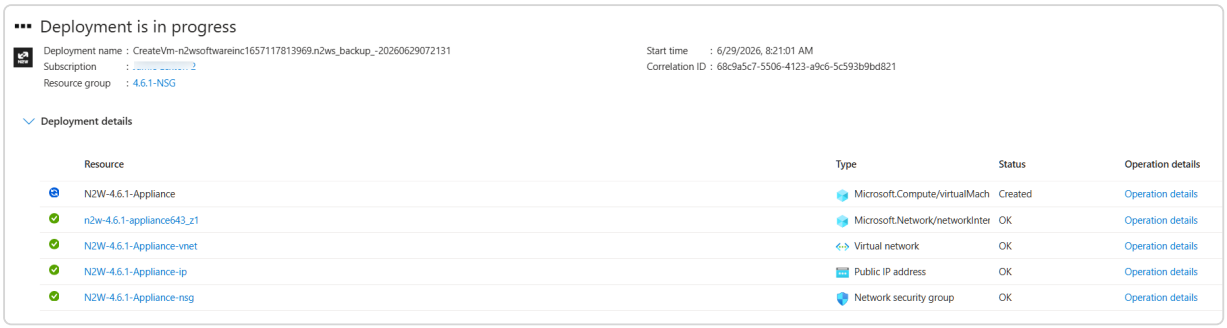
11. In the **Management** tab **Identity** section, select **Enable system-assigned managed identity**. To use a user-assigned managed identity instead, create and assign one using Microsoft's guide, Configure managed identities on Azure virtual machines. Then select **Next: Monitoring**.
12. In the **Monitoring** tab, select **Next: Advanced**.
13. In the **Advanced** tab **User data** section, select **Enable user data**, and then select **Next** to add **Tags** if necessary.
14. Select **Next: Review + create**.

15 At the bottom of the **Review + create** tab, select **Create** to start the deployment.

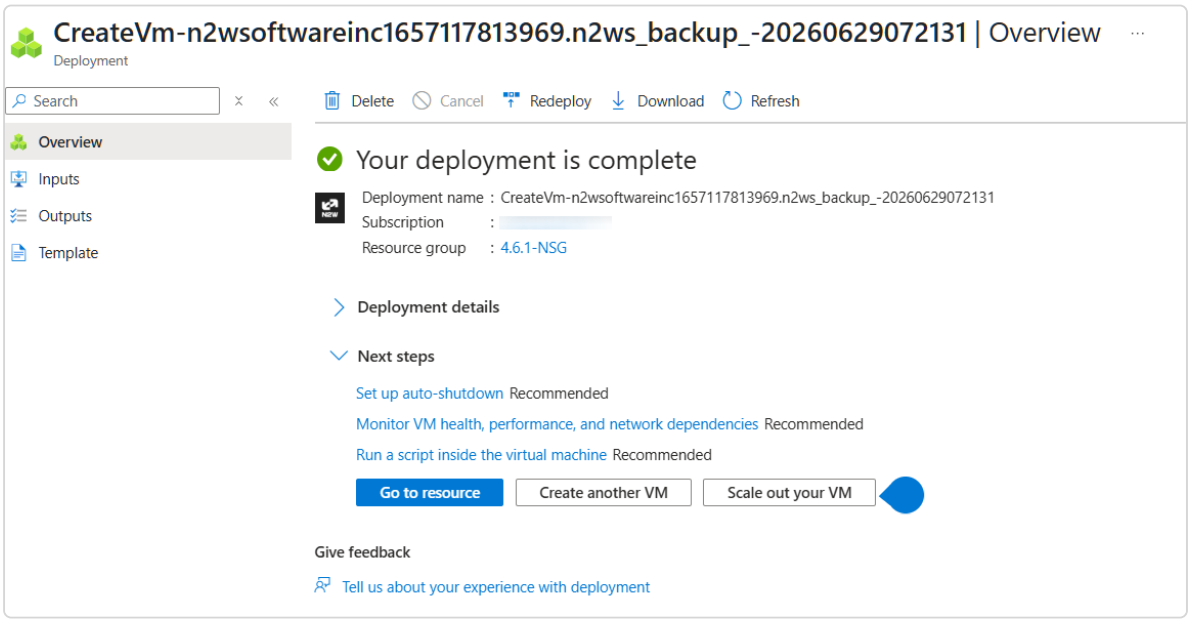
If you generated a new key pair, you are prompted to download the key:



Deployment stage messages appear in the upper-right corner, followed by the **Deployment is in progress** details.

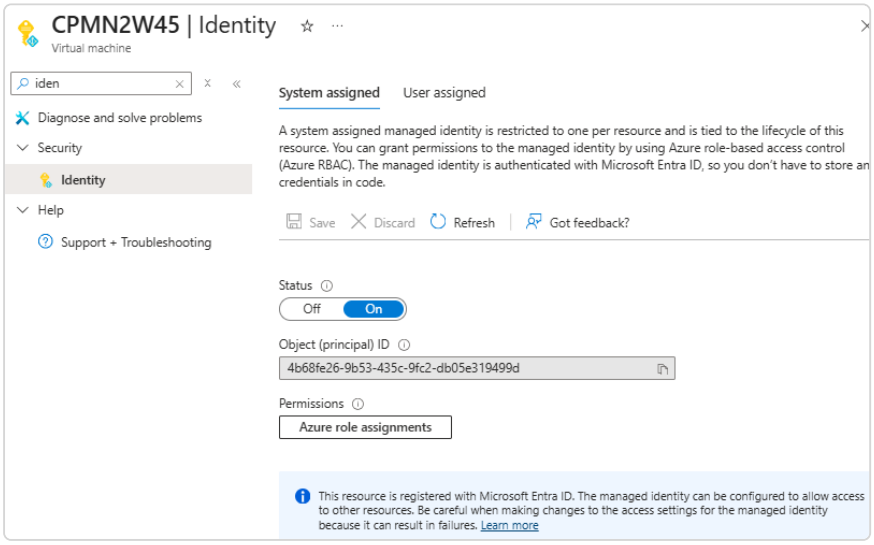


16 When the deployment is complete, select **Go to resource**.

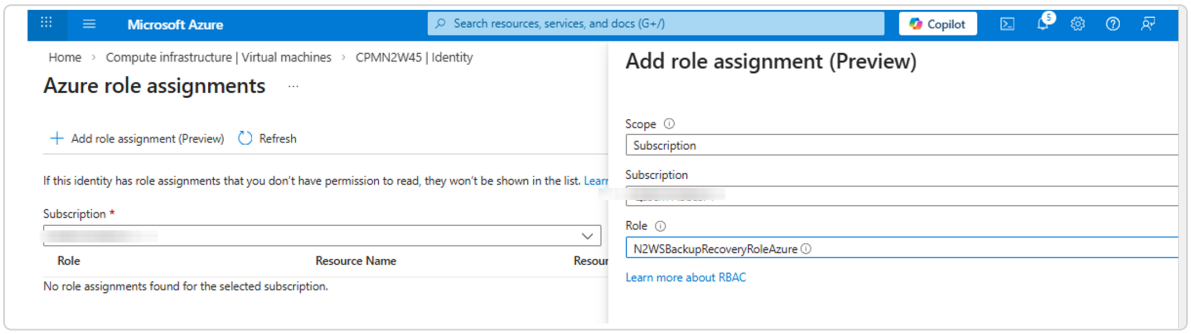


Assign the custom role to the N2W VM

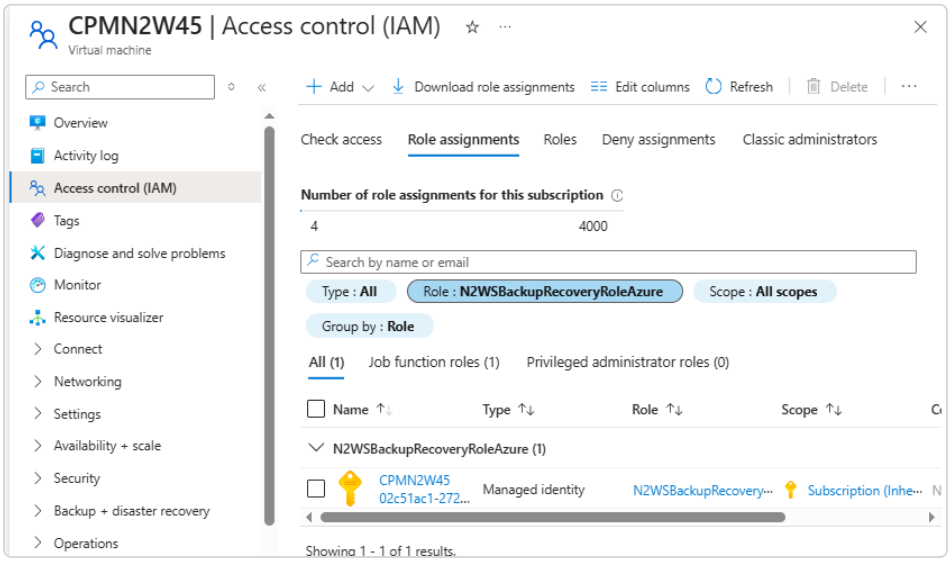
1. On the left menu, under **Security**, select **Identity**.
2. In the **Identity** tab, select **Azure role assignments**.



3. On the **Azure role assignments** page, select **+ Add role assignment (preview)**.
4. In the **Scope** list, select **Subscription**.
5. In the **Role** list, select the N2W custom role you created earlier. It contains the minimal permissions the VM needs to handle your resources. Then select **Save**.



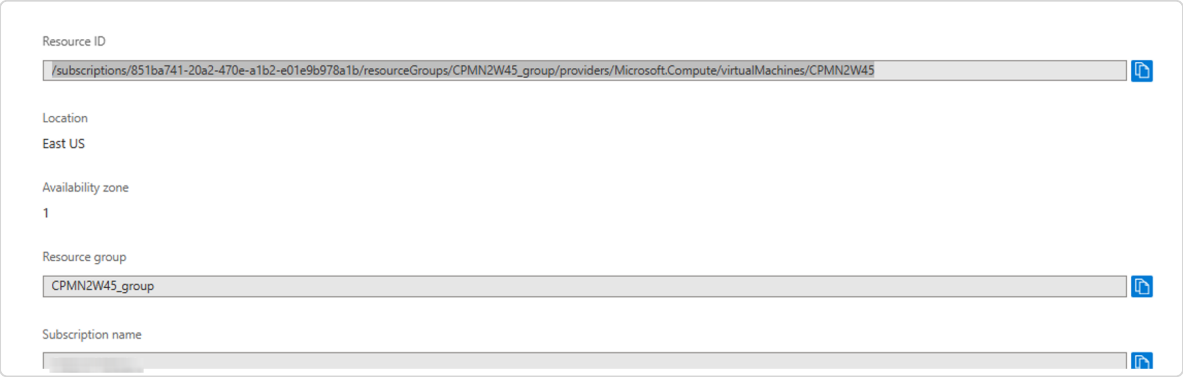
6. Role assignment messages appear in the upper-right corner. Confirm the role assignment in the **IAM** tab:


CPMN2W45 | Access control (IAM)
Virtual machine
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Monitor
Resource visualizer
Connect
Networking
Settings
Availability + scale
Security
Backup + disaster recovery
Operations
Add
Download role assignments
Edit columns
Refresh
Delete
Check access
Role assignments
Roles
Deny assignments
Classic administrators
Number of role assignments for this subscription
4
4000
Search by name or email
Type : All
Role : N2WSBackupRecoveryRoleAzure
Scope : All scopes
Group by : Role
All (1)
Job function roles (1)
Privileged administrator roles (0)
Name
Type
Role
Scope
N2WSBackupRecoveryRoleAzure (1)
CPMN2W45
02c51ac1-272...
Managed identity
N2WSBackupRecovery...
Subscription (Inhe...
Showing 1 - 1 of 1 results.

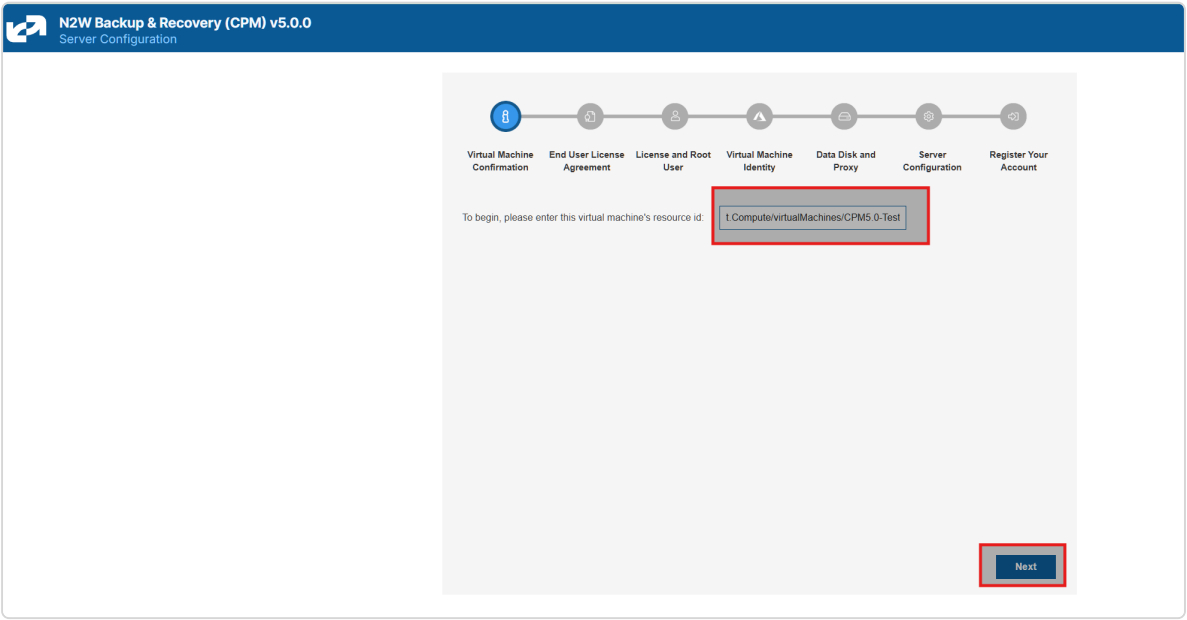
4 Configure N2W with the Configuration Wizard

To watch a video of the N2W configuration, see n2ws.com/support/install-guide.

1. In Microsoft Azure **Virtual machines**, select the N2W server VM.
2. In the **Properties** section, copy the **Public IP address**.
3. Open a new browser tab and paste the public IP address in the address bar. The N2W Server Configuration page opens.
4. Back in the Azure VM menu, scroll down to **Properties** and copy the **Resource ID**.

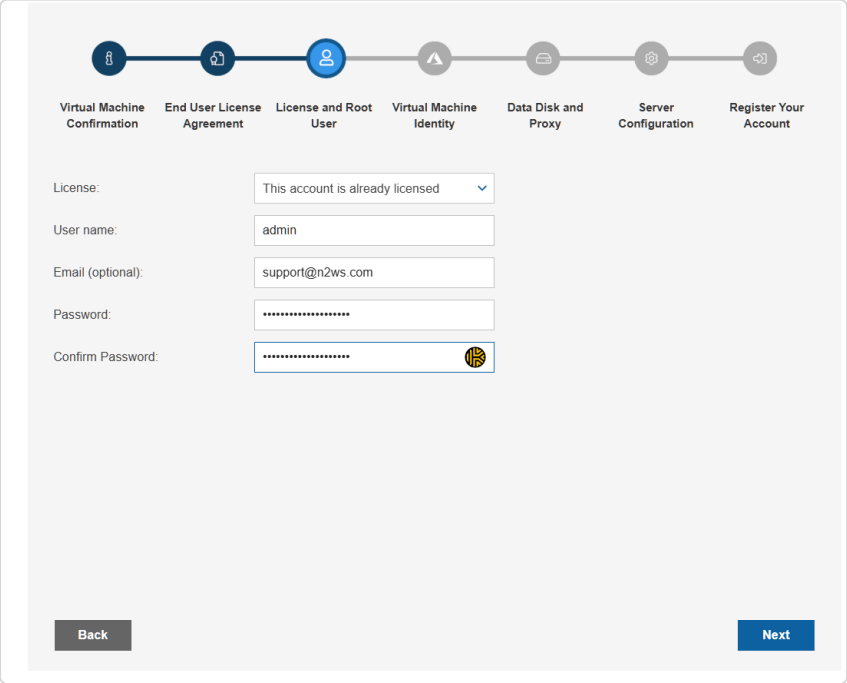


5. In the N2W configuration screen, paste the Resource ID in the **Virtual Machine Confirmation** step field, and then select **Next**.

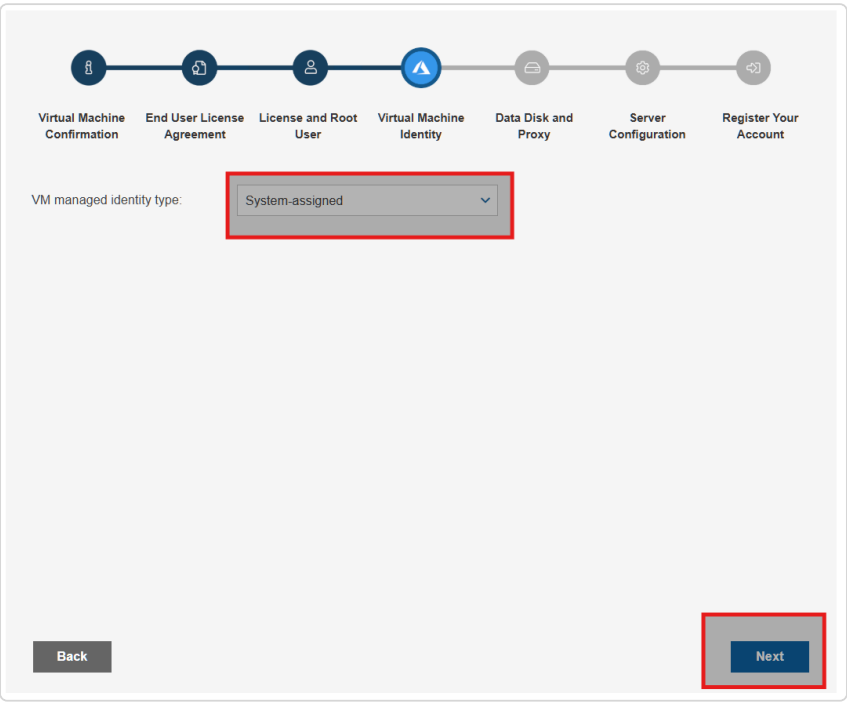


6. Accept the **End User License Agreement** terms and select **Next**.

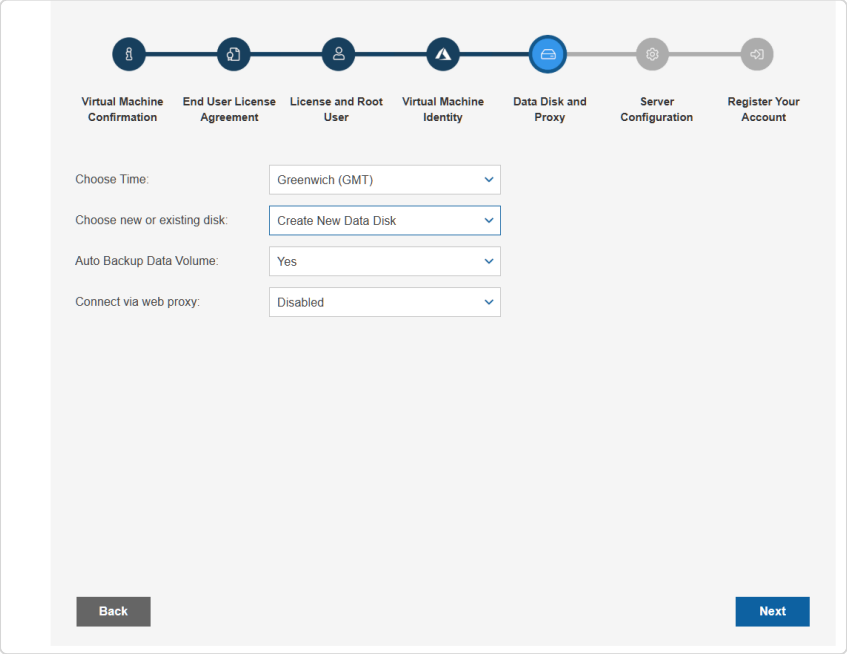
7. In the **License and Root User** step:
   - In the **License** list, select the license method.
   - Enter the root **Username**, an optional **Email**, and the **Password**, and then select **Next**. These are the admin credentials you will use to log in to N2W.



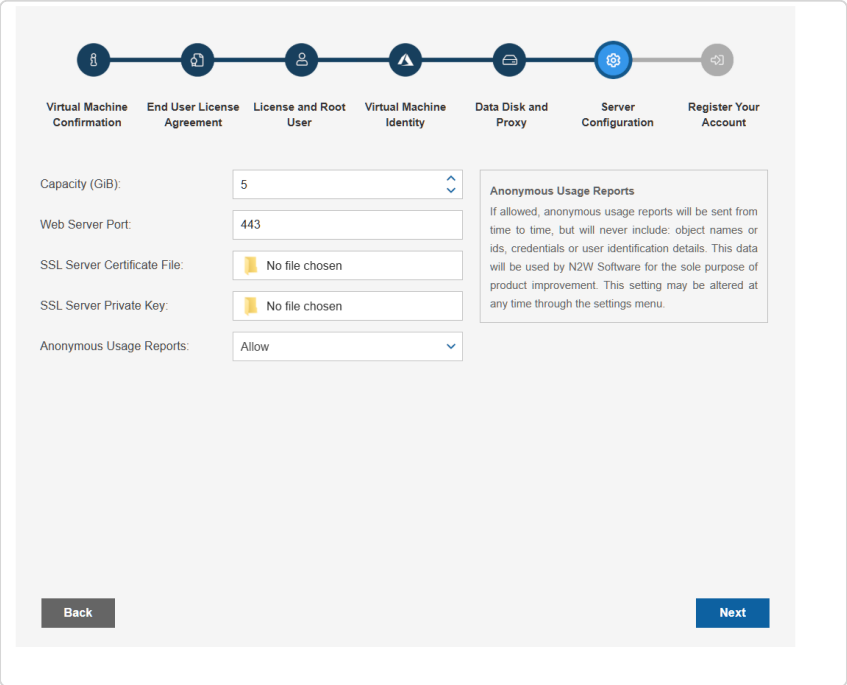
8. In the **Virtual Machine Identity** step, to use the system-assigned identity configured on Azure, select **System-assigned** in the **VM managed identity type** list, and then select **Next**.



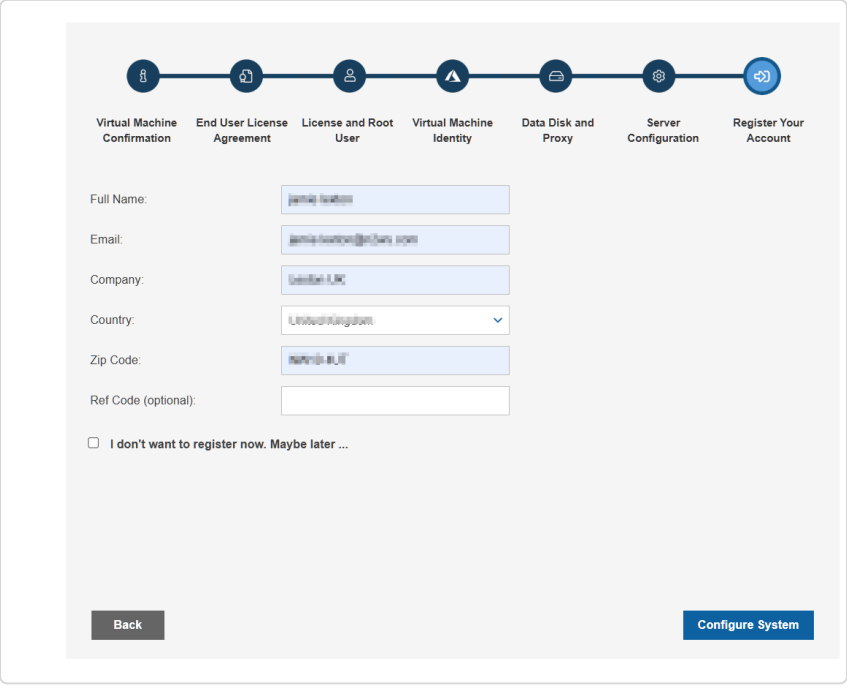
9. In the **Data Disk and Proxy** step:
   - In the **Choose Time** list, select your time zone.
   - In **Choose new or existing disk**, select **Create New Data Disk**.
   - Keep **Auto Backup** set to **Yes**. Add proxy details if required; otherwise leave the proxy disabled. Select **Next**.



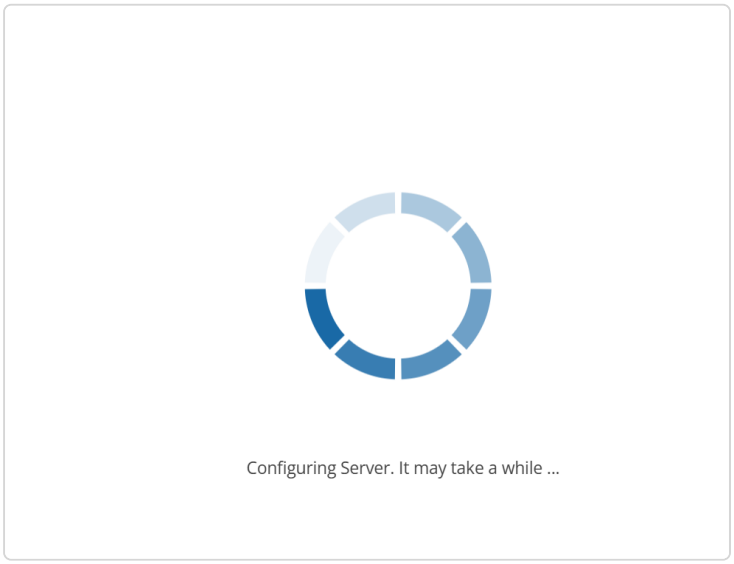
10. In the **Server Configuration** step, leave the fields as they are unless you want a non-standard web server port. Here you can also:
    - Add a custom SSL certificate (you need both the **.crt** and **.key** files).
    - Allow or deny anonymous usage reports.



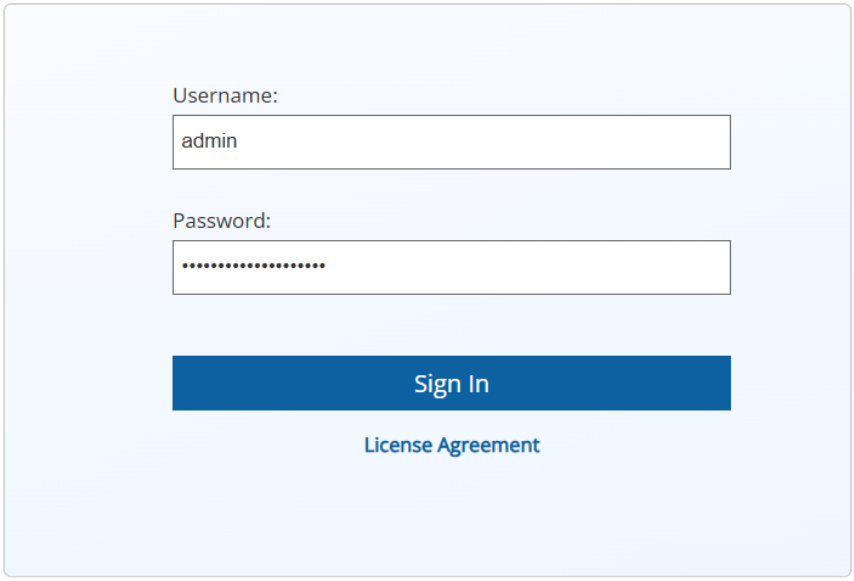
11 In the **Register Your Account** step, if you have not configured N2W before, enter the requested information and select **Configure System**.



12 The system configures itself. This can take up to 10 minutes.



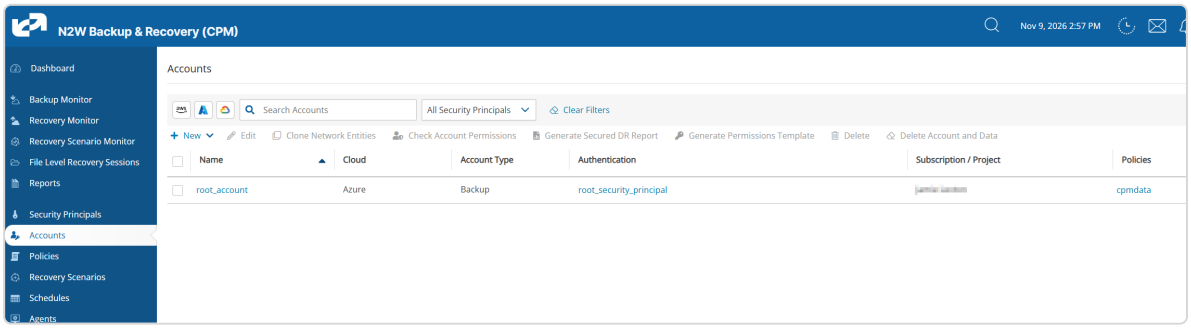
13 When configuration finishes, you are directed to the logon page and installation is complete. If you selected **I already have a license**, you may see the license server establishing a connection.



5 Creating an Azure Backup Policy

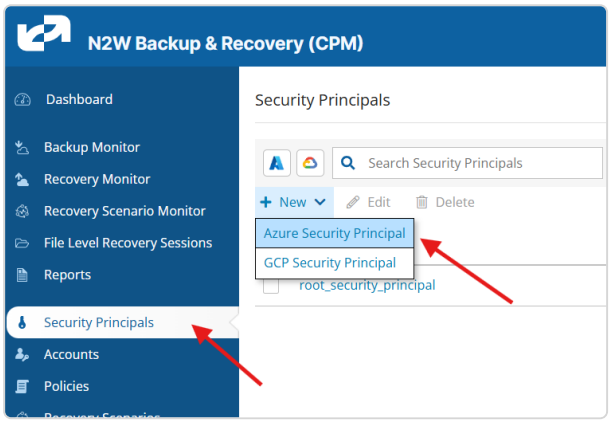
Adding and Confirming an Azure Account

1. Log in to N2W.
2. Go to **Accounts** and confirm that your account is listed.

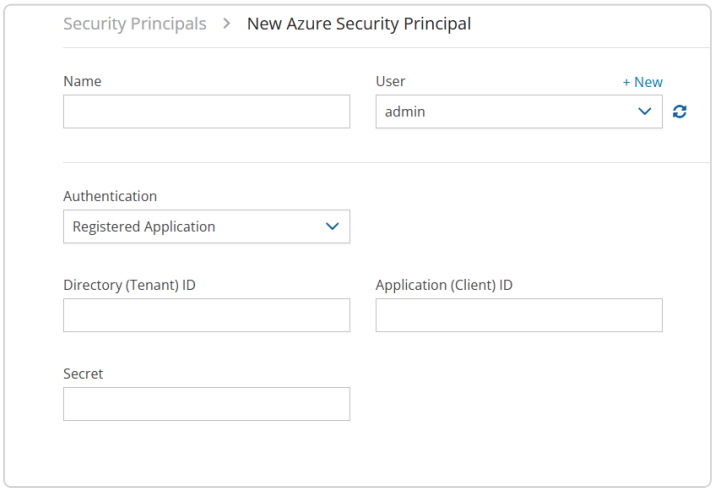


To add another account, such as a DR account, first define an Azure Security Principal. It holds the authentication details (an App registration or a managed identity) used by one or more subscription accounts.

1. In the main navigation menu, select **Security Principals**, and then select **New**.

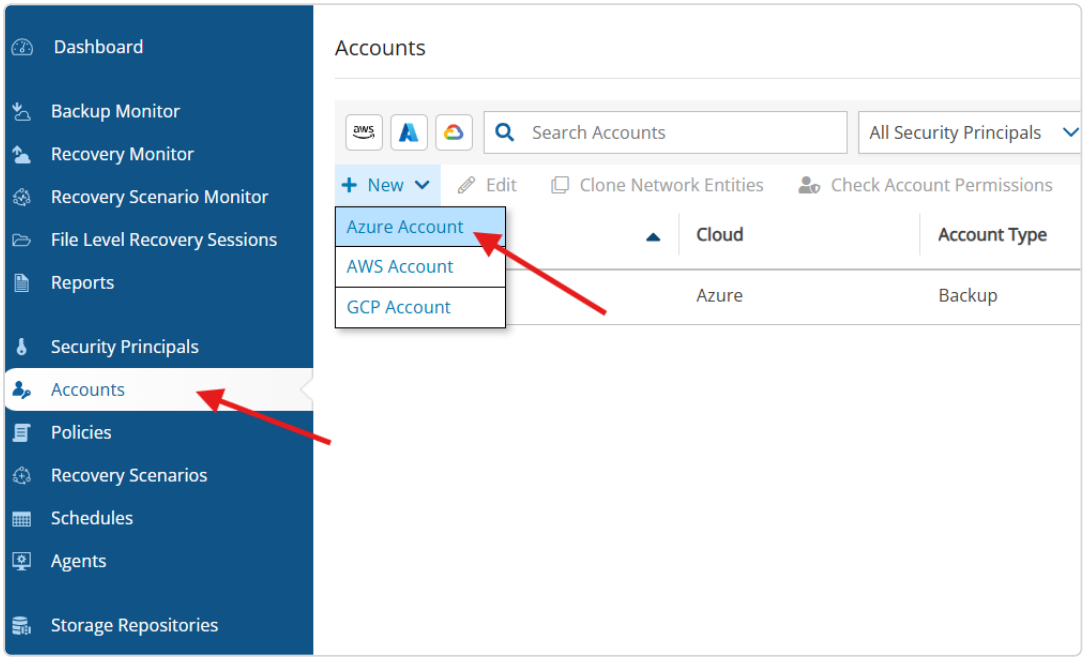


2. Complete the **New Azure Security Principal** screen: **Name**, **User**, **Directory (Tenant) ID**, **Application (Client) ID**, and **Secret**. Copy these values from your App registration in the Azure portal.

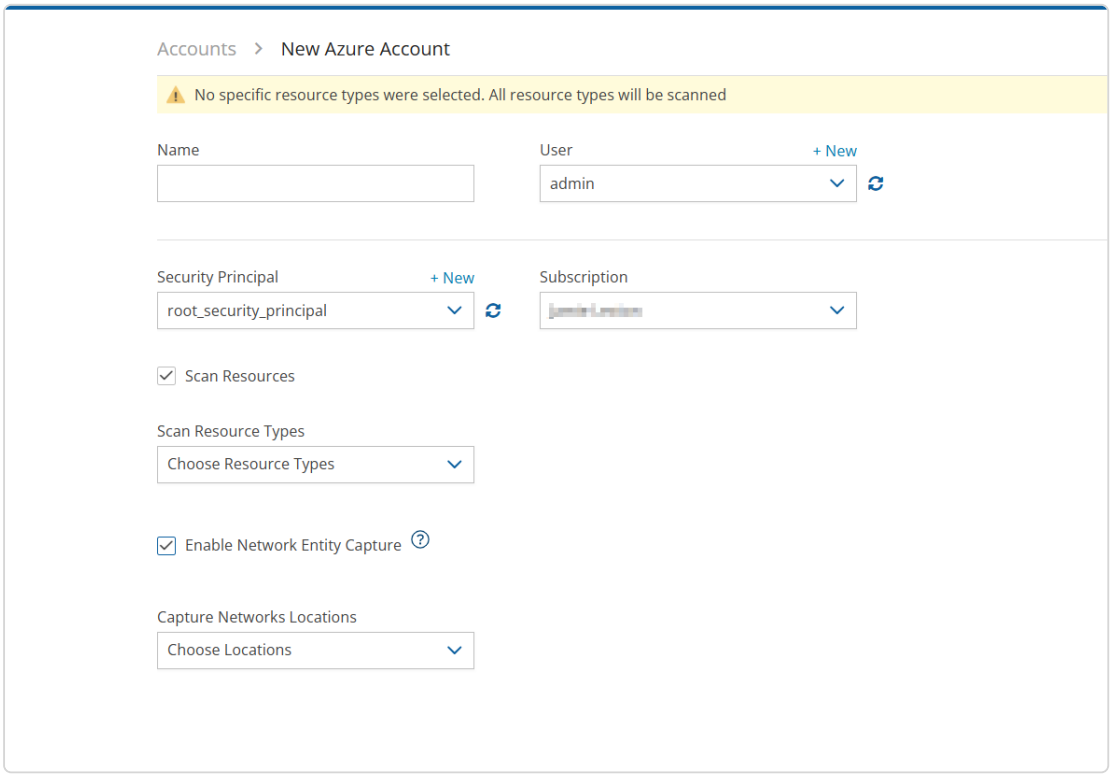


3. Select **Save**. N2W validates the credentials, and the new security principal appears in the **Security Principals** list.

4. Go to **Accounts**, and then select **+ New → Azure Account**.



5. Complete the **New Azure Account** screen: **Name** (must be unique), **User**, **Security Principal**, and **Subscription** (the subscription this account will manage; you can search by subscription ID). Optionally, select **Scan Resources** and **Enable Network Entity Capture**.



6. Select **Save**.

> **More on accounts.**
>
> - Microsoft: Register an application – exact steps to create an App registration and the supported account options.
> - N2W User Guide: Define an Azure Security Principal
> - N2W User Guide: Adding an Azure Account to N2W

Creating a Simple Backup Schedule

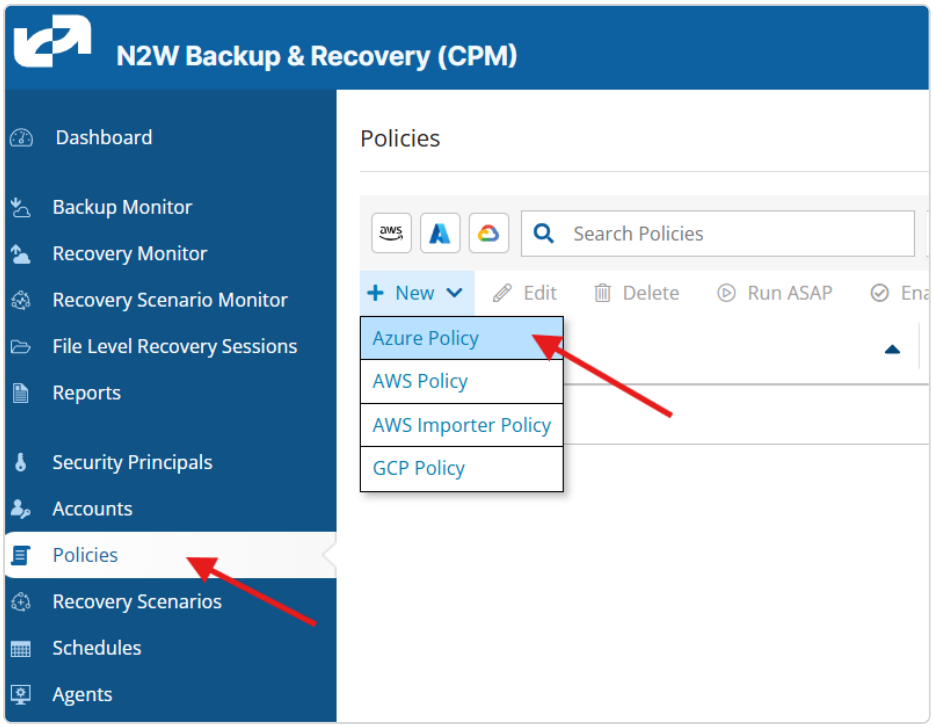
N2W includes default Daily, Hourly, Weekly, and Monthly schedules. To define a different one:

1. Go to **Schedules** and select **+ New**.
2. Define the **Name**, **First run time**, and **Frequency**.
3. Select **Save**.

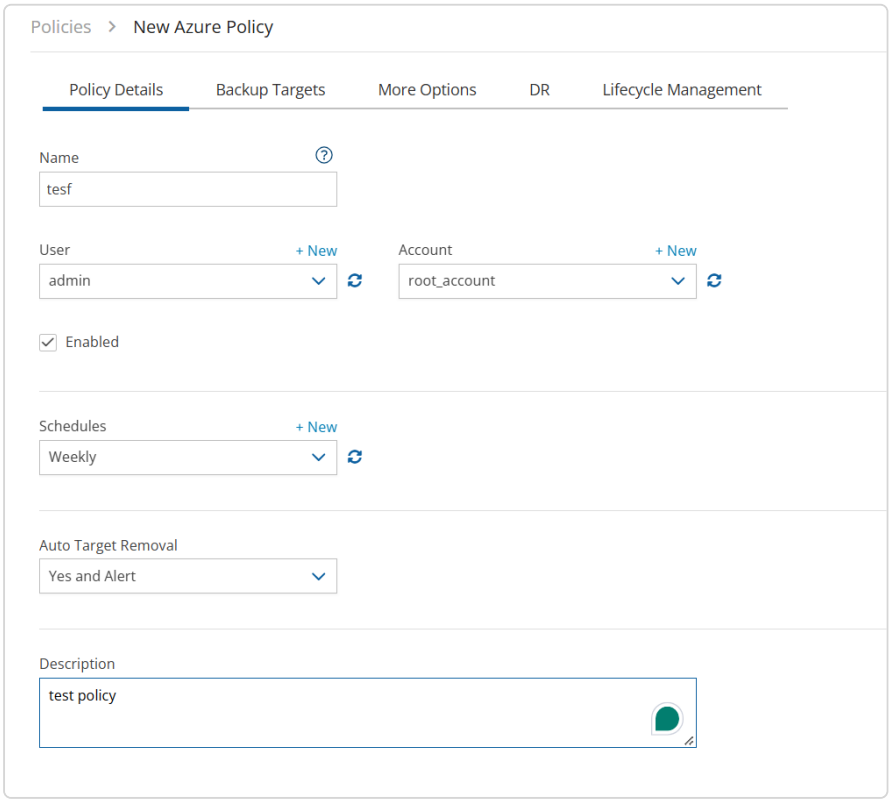
Creating a Simple Azure Backup Policy

To back up resources in Azure, create an N2W policy.

1. In N2W, select the **Policies** tab.
2. On the **New** menu, select **Azure policy**.

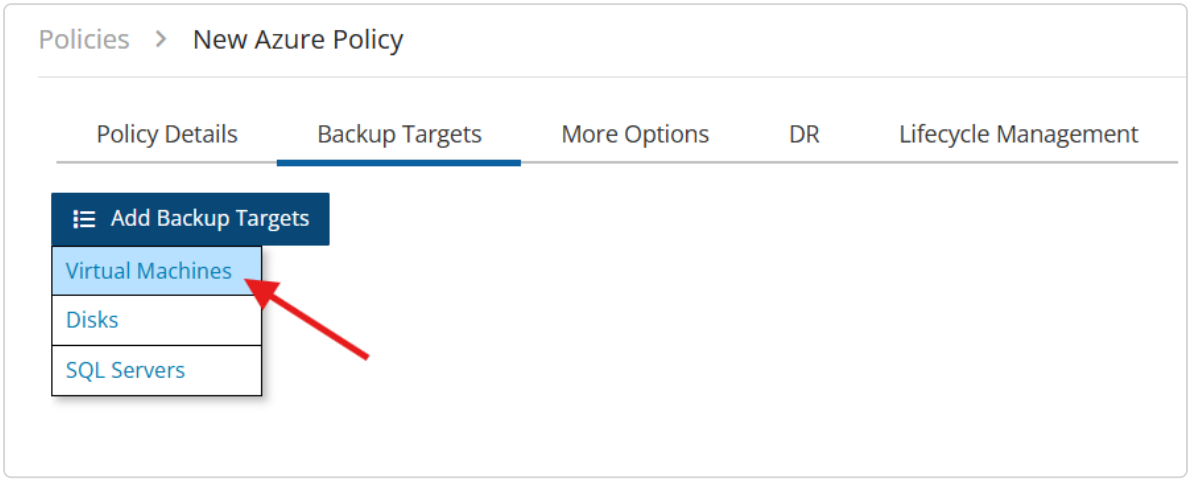


3. In the **New Azure Policy** screen, complete the fields:
   - **Name** – Enter a name for the policy.
   - **User** – Select from the list, or select **+ New** to add a user.
   - **Account** – Select from the list.
   - **Enabled** – Clear to disable the policy. You can also enable or disable a policy directly from the Policies page.
   - **Schedules** – Optionally select one or more schedules, or select **+ New** to add one.
   - **Auto Target Removal** – Select **Yes** to automatically remove a target that no longer exists from the policy.

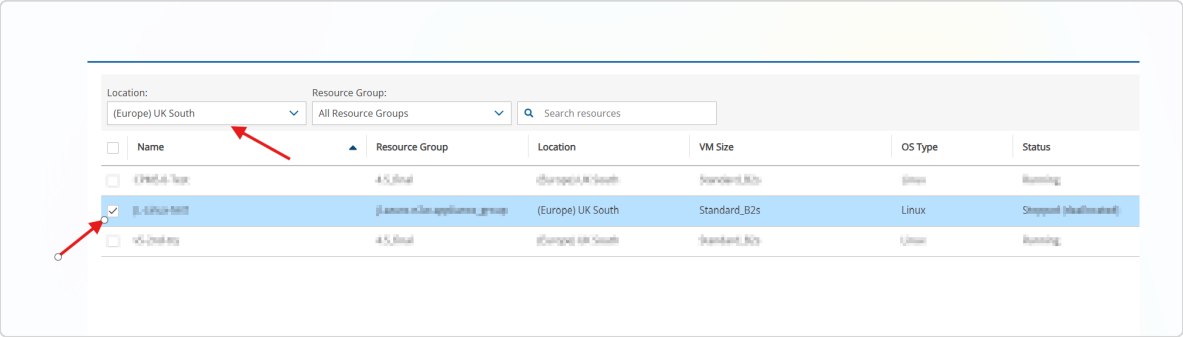


4. Select the **Backup Targets** tab.

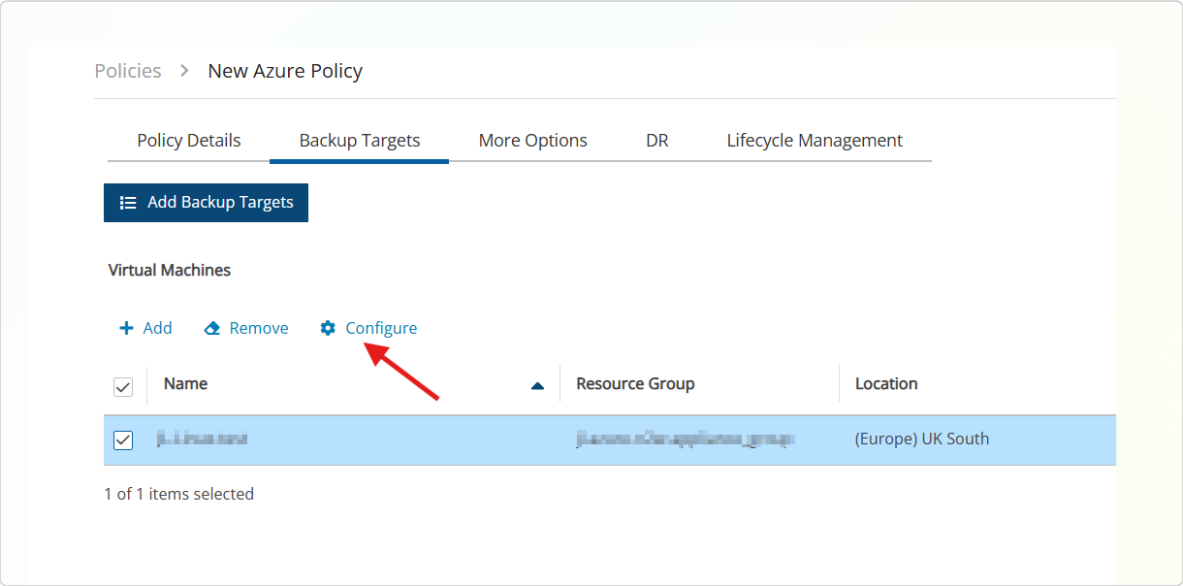
5. In the **Add Backup Targets** menu, select the targets to back up: **Disks** and/or **Virtual Machines**. The Add Virtual Machines / Disks screen opens.



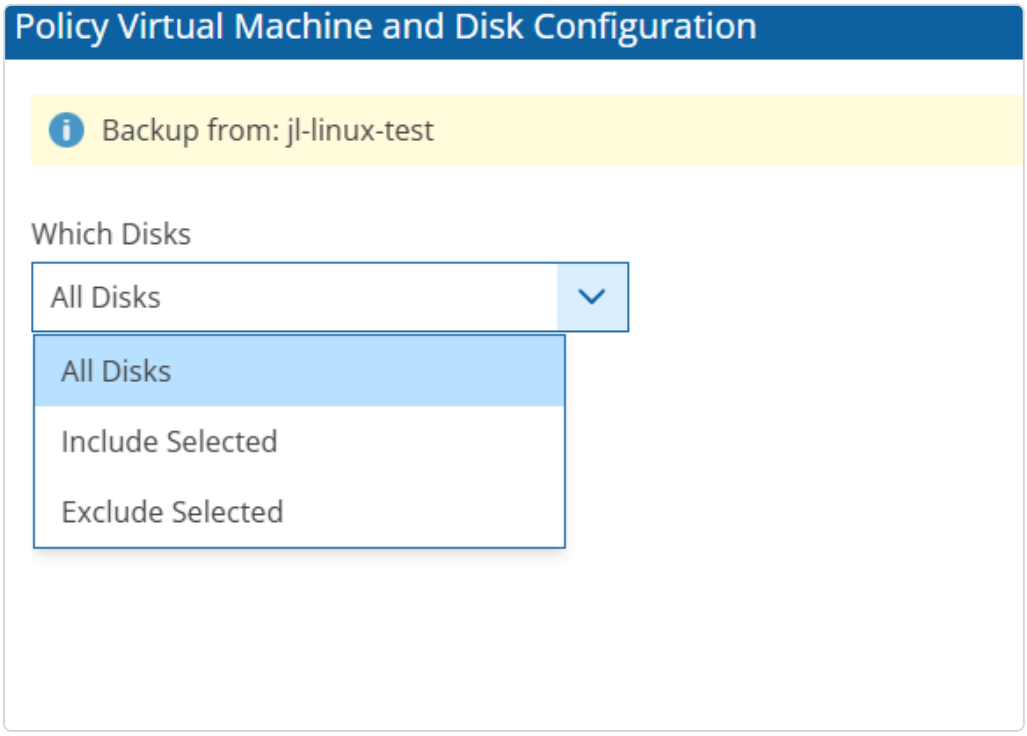
6. For Virtual Machines, you *must* filter by **Location** (list in the upper-left corner) *before* selecting individual targets. Filtering by Resource Group is optional.



7 When you're done selecting targets, select **Add selected**. The Backup Targets tab lists the selected targets.



8 To choose which disks to back up for each Virtual Machine target, select **Configure**. In the **Which Disks** list of the Policy Virtual Machine and Disk Configuration screen, select the disks to include or exclude.



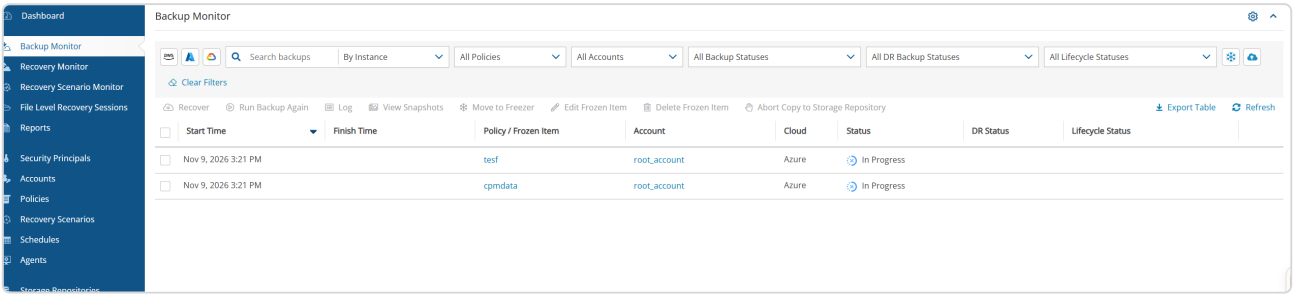
9 When finished, in the **Backup Targets** tab, select **Save**.

Backing Up an Azure Policy

If the policy has a schedule, it runs backups automatically according to that schedule. To run a policy right away, in the **Policies** view, select the policy and select **Run ASAP**.

To view the policy's progress and backups, select **Backup Monitor**:

- The backup progress is shown in the **Status** column.
- Use the Cloud buttons to display the Azure policies.



6 Recovering from an Azure Backup

After creating a backup, you can recover it from the **Backup Monitor**.

> **Note.** Only one VM can be recovered per recovery operation.

The VM recovery Basic Options include Azure options for replicating data to additional locations, to protect against data loss and unavailability:

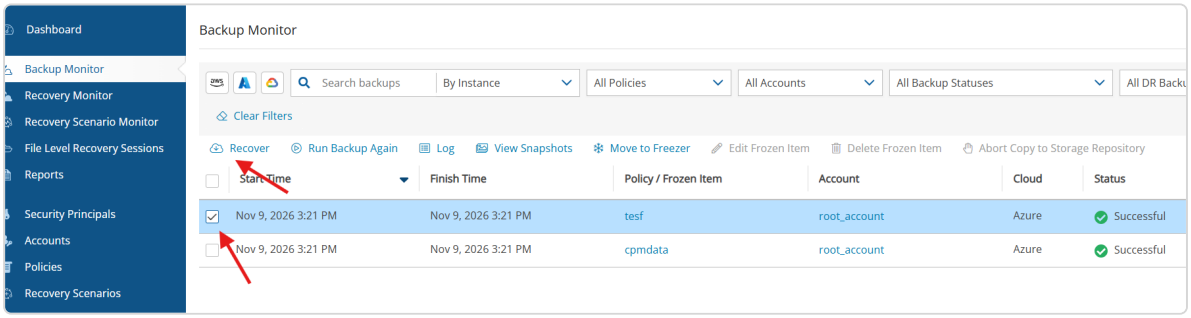
- **Availability Zone** – A redundant data center (different building, servers, power, etc.) within a geographic area managed by Azure.
- **Availability Set** – A redundant data center (different building, servers, power, etc.) that the customer launches, configures, and manages.
- **No Infrastructure Redundancy Required** – Data is not replicated to an additional zone or set. This saves money, but in rare cases you may experience some data loss or unavailability. (Azure typically provides 11 9s of durability and 99.9% availability.)

In the Disk Recovery screen, you may be offered the option to change the encryption when recovering certain disks. Disk encryption can be changed only when the disk is unattached or the VM is deallocated.

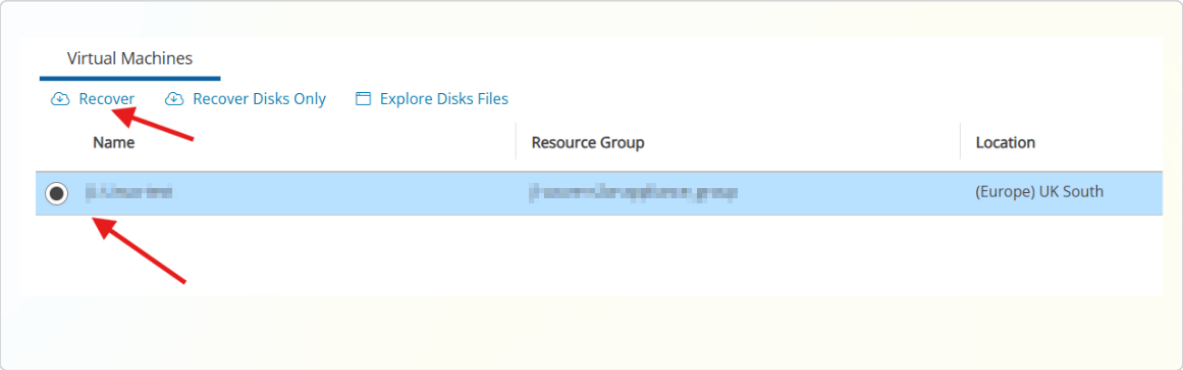
> **Note.** To add an additional layer of encryption during recovery, see Microsoft: Enable customer-managed keys for managed disks.

Recovering a VM and Disks

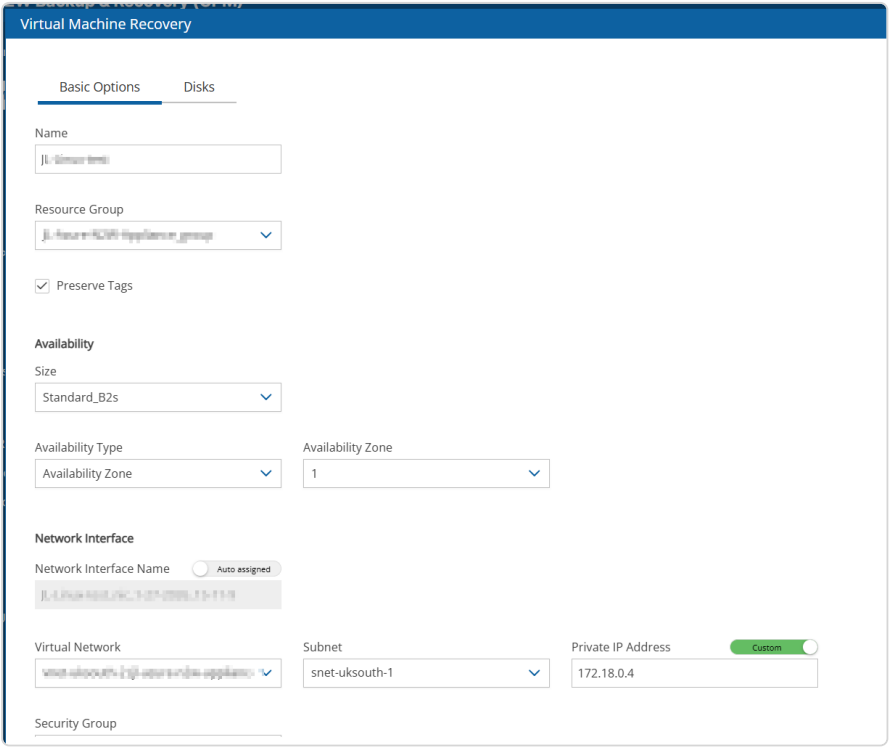
1. To recover a VM, with or without its attached disks, select the VM snapshot to recover from, and then select **Recover**.



2. In the **Virtual Machines** tab of the Recover screen, select one VM, and then select **Recover**.

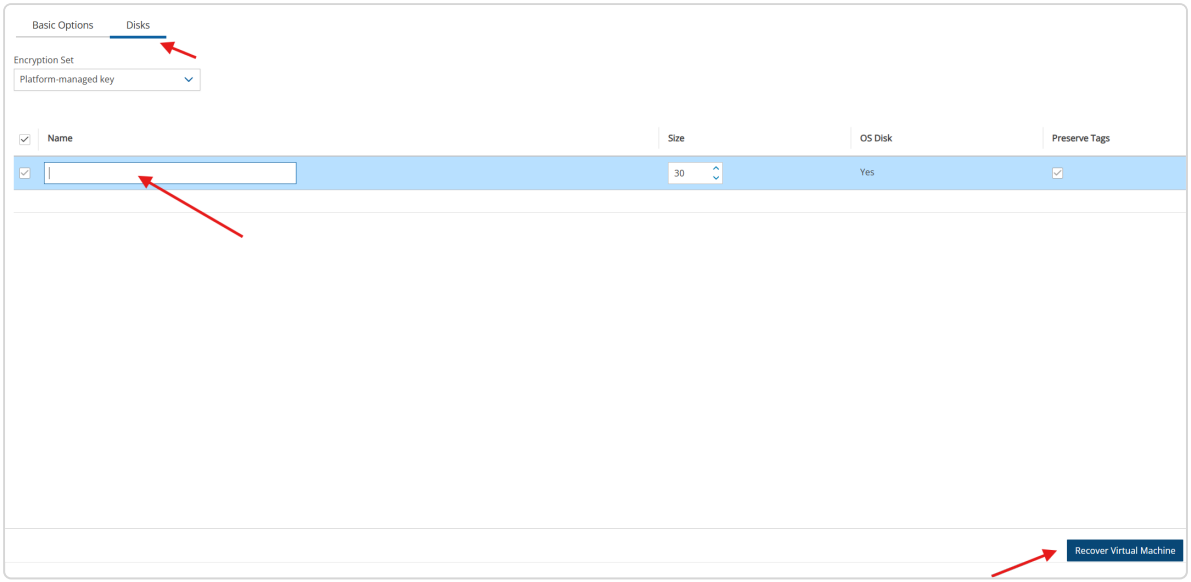


The **Basic Options** tab opens.



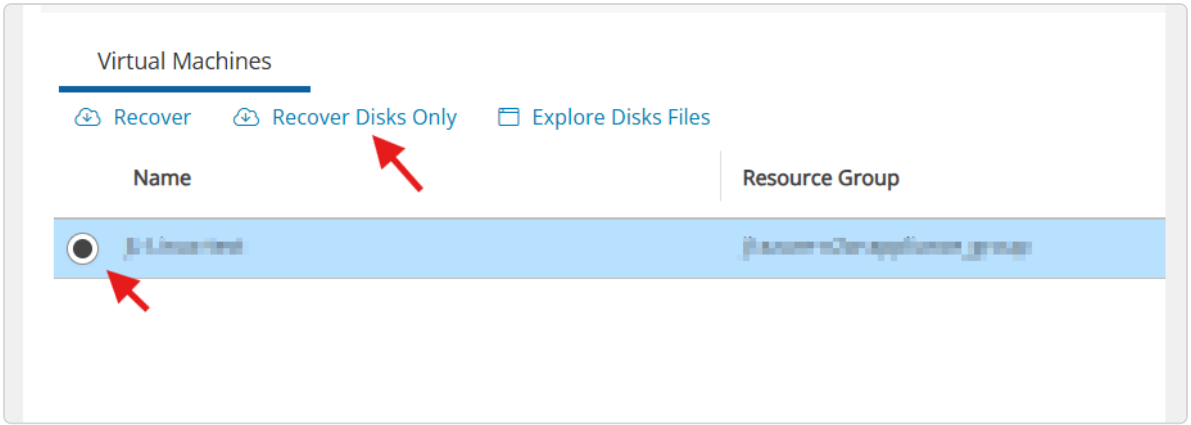
3. In the **Availability Type** list, select one of the following:
   - **No Infrastructure Redundancy Required** – Don't replicate data to a redundant location in another zone or set.
   - **Availability Zone** – Select a zone in the **Availability Zone** list.
   - **Availability Set** – Select a set in the **Availability Set** list.
4. In the **Virtual Network** and **Subnet** lists, select the network and subnet for the recovered VM. Optionally, select a **Network Security Group**; this field can be left empty.
5. In the **Private IP Address** box, assign an available IP address, or switch the **Custom** toggle to **Auto assigned**.

6. The default **Preserve Tags** action is **Preserve Original**. To manage tags, see the N2W User Guide.
7. In the **Disks** tab, enter a new **Name** for each disk. **Similar names will cause the recovery to fail.**
8. Select **Recover Virtual Machine**.

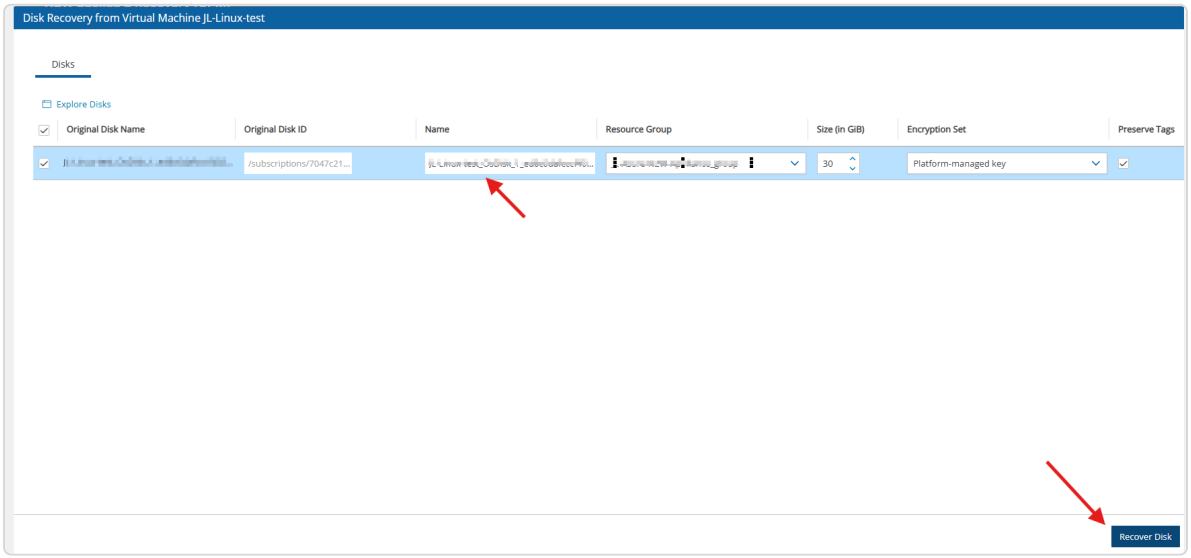


To recover only the disks attached to the VM:

1. Select **Recover Disks Only**.



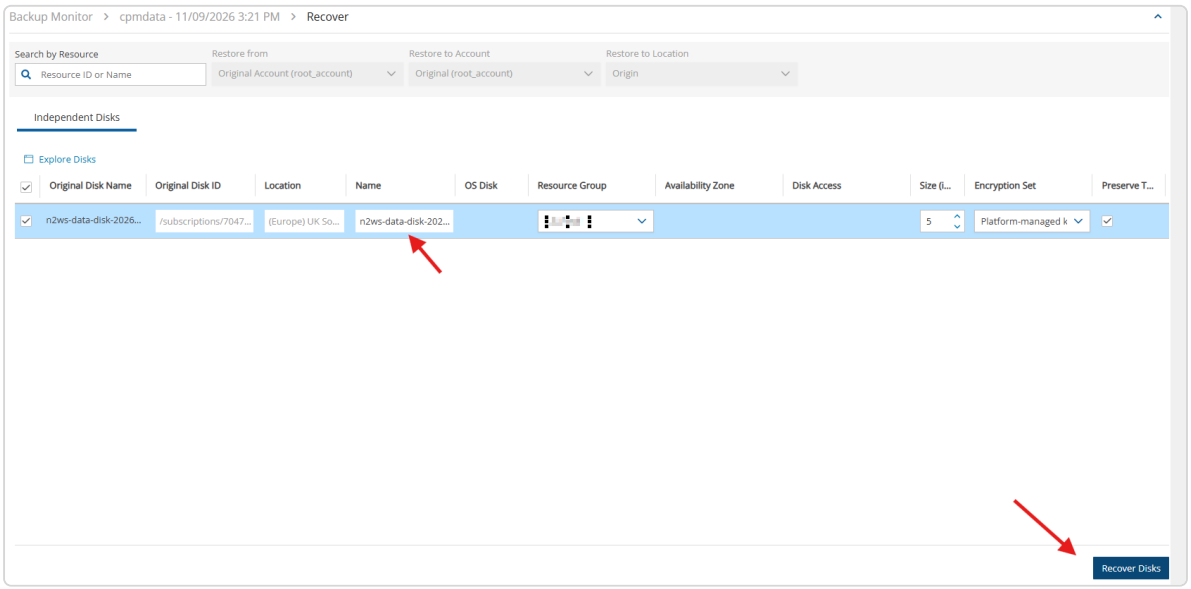
2. In the **Disks** tab, enter a new **Name** for each disk. **Similar names will cause the recovery to fail.**
3. Select **Recover Disk**.



4. To view recovery progress, select **Recovery Monitor**. Use the **Cloud** buttons to display Azure recoveries.

Recovering Independent Disks

1. Select the backup, and then select **Recover**, as in step 1 of Recovering a VM and Disks.
2. In the **Independent Disks** tab, enter a new **Name** for each disk to recover. Similar names will cause the recovery to fail.
3. Change other settings as needed.
4. Select **Recover Disk**.



5 To view recovery progress, select **Recovery Monitor**.

7 Additional Resources

N2W User Guide	docs.n2ws.com/user-guide
N2W Azure User Guide	docs.n2ws.com/user-guide/26-using-n2ws-with-azure
N2W Azure video tutorials	n2ws.com/support/video-tutorials