

N2W Backup & Recovery

Quick Start Guide for Azure

V4.4.1



Contents

1	Introduction	3
1.1	Requirements.....	3
2	Create Custom Role and Permissions on Azure.....	4
3	Deploy N2W Server on Azure	5
4	Configure N2W on Azure with the Configuration Wizard	11
5	Creating an Azure Backup Policy	16
5.1	Backing Up an Azure Policy	18
6	Recovering from an Azure Backup.....	19
7	What to do After Deploying Your N2W Server on Azure	23



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* will walk you through the core steps to get N2W up and run 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](#).

A quick word about passwords before we get going. N2W strongly recommends that you create a strong password for the server. Make sure no one can access it or guess it. Change passwords regularly. N2W enforces the following password rules:

- Minimum length of 8 characters.
- Not a common word or phrase.
- Not numeric characters only.

After meeting the Requirements, you can install Azure on N2W with the following procedures:

1. Create a Custom Role on Azure
2. Deploy N2W VM on Azure
3. Configure N2W on Azure with the Configuration Wizard
4. Set permissions on the N2W instance for access to other targets in Azure.

1.1 Requirements

Before continuing, check that you have met the following requirements:

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

2 Create Custom Role and Permissions on Azure

Note: For complete information on setting permissions, see section 7, “Using Azure with N2W”, in the *N2W Backup & Recovery Quick Start Guide 4.1.0*.

1. In Microsoft Azure, select **Subscriptions**.
2. Select your subscription and then select **Access control**.
3. In the + **Add** menu, select **Add custom role**.
4. In the **Basics** tab, type the 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 the minimal_azure_iam_permissions_for_411.zip file at <https://n2ws.zendesk.com/hc/en-us/articles/28833036917021-Required-Minimum-Azure-permissions-for-N2W-operations>

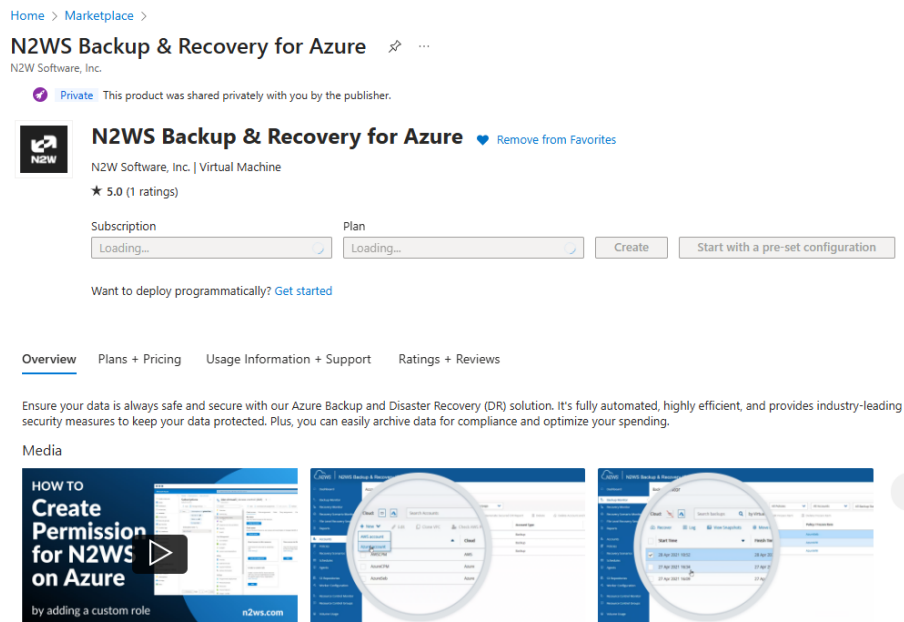
Note: You will be able to edit the file or change the configuration before selecting the **Review + create** button.

7. In the **Select a file** box, select the downloaded JSON file relevant for your N2W license.
8. Select **Next**.
9. In the **Permissions** tab, 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.
13. In 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 successfully created, select **OK**. It may take a few minutes to display the new role everywhere.

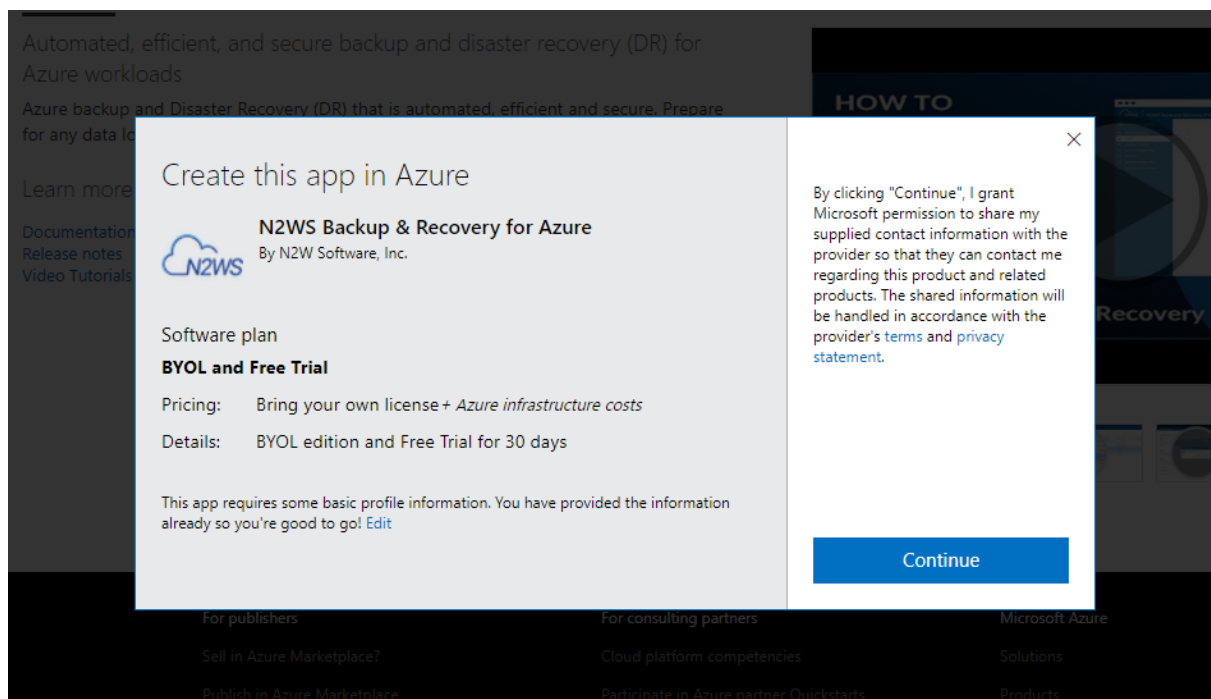
3 Deploy N2W Server on Azure

To view a video of the N2W deployment on Azure, see <https://n2ws.com/support/install-guide>

1. In Microsoft Azure Marketplace for Apps, select **Consulting Services**.
2. In the **Products** list, select **N2W Backup & Recovery for Azure**.
3. Select **Get it Now**.

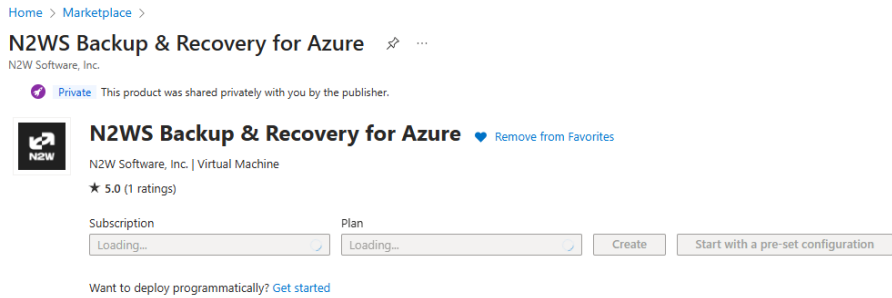


4. In the **Create this app in Azure** window for **BYOL and Free Trial**, select **Continue**.



The 'Taking you to N2W Backup & Recovery for Azure to complete this process' message opens.

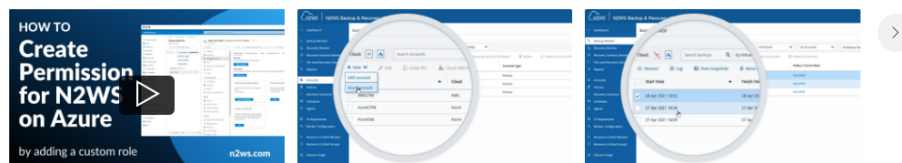
5. In the **N2W Backup & Recovery for Azure (preview)** page, select **BYOL and Free Trial** in the **Plan** list to start with a pre-set configuration; and then select **Create**.



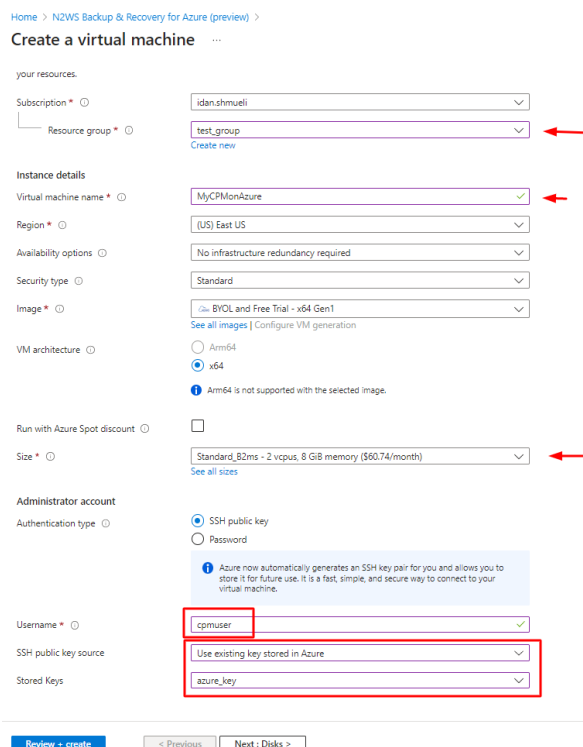
[Overview](#) [Plans + Pricing](#) [Usage Information + Support](#) [Ratings + Reviews](#)

Ensure your data is always safe and secure with our Azure Backup and Disaster Recovery (DR) solution. It's fully automated, highly efficient, and provides industry-leading security measures to keep your data protected. Plus, you can easily archive data for compliance and optimize your spending.

Media



6. In the **Create a virtual machine Basics** page, select the already defined username in the **Subscription** list.



7. In the **Resource Group** list, select the resource group where you want to deploy the machine.
8. In the Instance details section:
 - a. Type the **Virtual machine name**.
 - b. Select the **Region** where to deploy the machine.

9. Select the proper **Size** of the virtual machine. Two virtual CPUs and 8 GB RAM are the minimum required for a small company.
10. In the **Username** list, you can enter the Azure username, but it will be best to use 'cpmuser' as the **username**.
11. In the **SSH public key source** list, select **Use existing key stored in Azure** or you can create a new key.
12. In the **Stored Keys** list, select **azure_key**, and then select **Next: Disks**.
13. In the **Disks** tab, select **Review + create**, and then select **Next: Networking**.
14. In the **Networking** tab, select **Delete public IP and NIC when VM is deleted**, and then select **Next: Management**.
15. In the **Management** tab **Identity** section, you can select **Enable system assigned managed identity** or use a user-based identity later, and then select **Next: Monitoring**.

[Home](#) > [N2WS Backup & Recovery for Azure \(preview\)](#) >

Create a virtual machine ...

Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create


Configure management options for your VM.

Microsoft Defender for Cloud

Microsoft Defender for Cloud provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)


✔ Your subscription is protected by Microsoft Defender for Cloud basic plan.

Identity

Enable system assigned managed identity ☒ 

Azure AD

Login with Azure AD ☐


 This image does not support Login with Azure AD.

Auto-shutdown

Enable auto-shutdown ☐

Guest OS updates

Patch orchestration options


 Some patch orchestration options are not available for this image. [Learn more](#)

16. In the **Monitoring** tab, select **Next: Advanced**.
17. In the **Advanced** tab **User data** section, select **Enable user data**, and then select **Next** for **Tags**, if necessary.
18. Select **Next: Review + create**.


19. At the bottom of the **Review + create** tab, select **Create** to start the process.

[Home](#) > [N2WS Backup & Recovery for Azure \(preview\)](#) >




Create a virtual machine ...

 Validation passed

Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

 Cost given below is an estimate and not the final price. Please use [Pricing calculator](#) for all your pricing needs.

Price

<p>N2WS Backup & Recovery for Azure by N2W Software, Inc. Terms of use Privacy policy</p>	<p>Not covered by credits </p> <p>0.0000 USD/hr</p> <p> There was a problem showing prices from the Private Offers database. Custom pricing may apply.</p>
<p>1 X Standard B2ms by Microsoft Terms of use Privacy policy</p>	<p>Subscription credits apply </p> <p>0.0832 USD/hr</p> <p>Pricing for other VM sizes</p>

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Name

Preferred e-mail address

Preferred phone number

Basics

Subscription	idan.shmueli
Resource group	test_group
Virtual machine name	MyCPMonAzure
Region	East US
Availability options	No infrastructure redundancy required
Security type	Standard

Create

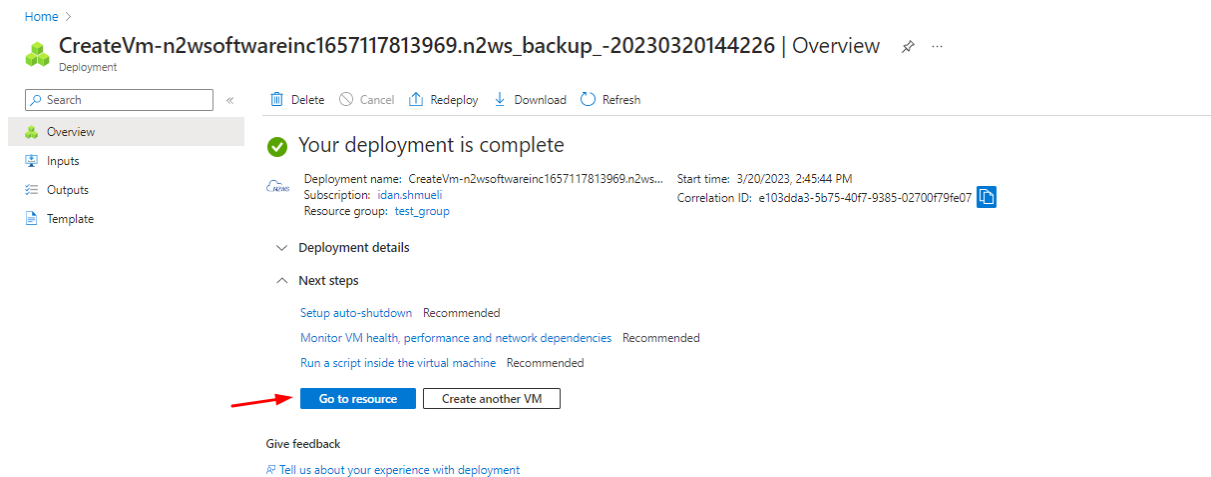
< Previous

Next >

Download a template for automation

Deployment stage messages appear in the upper right corner followed by 'Deployment is in progress' details.

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



Home > CreateVm-n2wsoftwareinc1657117813969.n2ws_backup_-20230320144226 | Overview

Deployment

Search

Overview

Inputs

Outputs

Template

✓ Your deployment is complete

Deployment name: CreateVm-n2wsoftwareinc1657117813969.n2ws... Start time: 3/20/2023, 2:45:44 PM
Subscription: idan.shmueli
Resource group: test_group Correlation ID: e103dda3-5b75-40f7-9385-02700f79fe07

Deployment details

Next steps

Setup auto-shutdown Recommended

Monitor VM health, performance and network dependencies Recommended

Run a script inside the virtual machine Recommended

Go to resource Create another VM

Give feedback

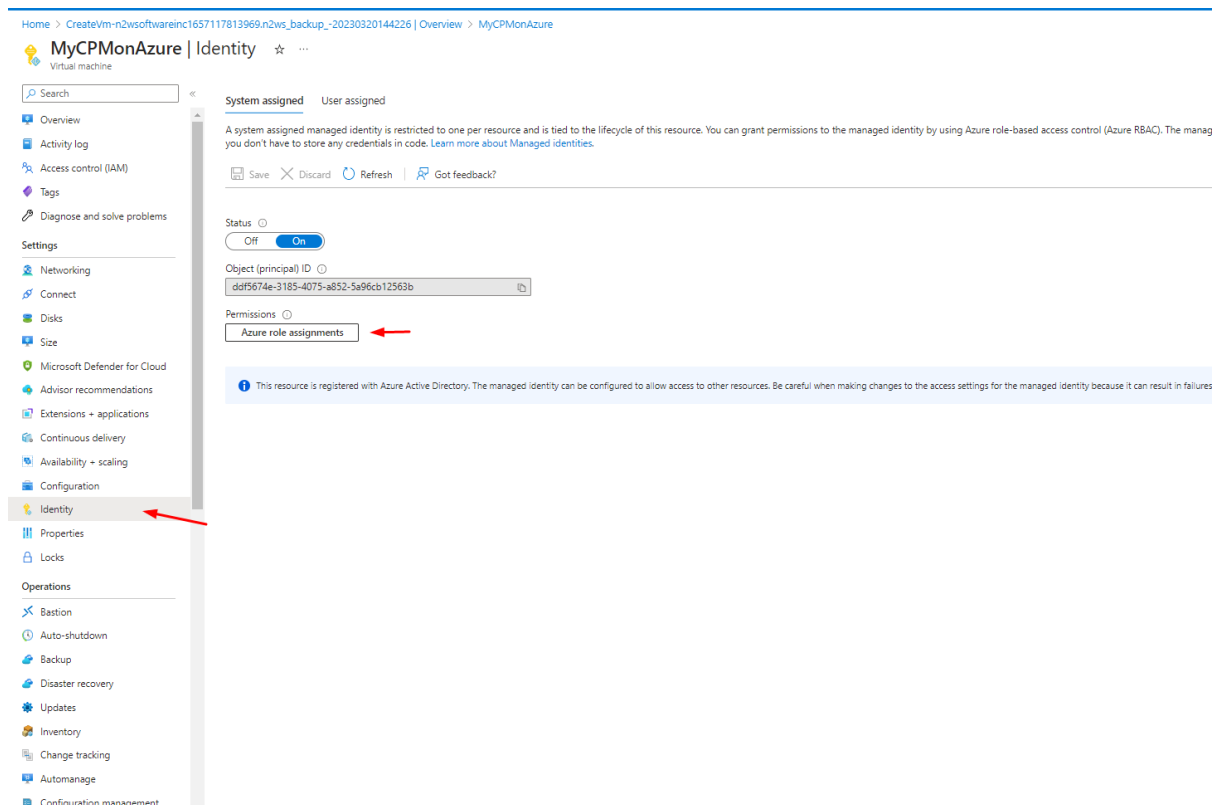
Tell us about your experience with deployment

The **CPMonAzure** screen opens.

21. In the **Networking** section of the **Properties** tab, copy the **Public IP address**.

22. In the **CPMonAzure** menu, select **Identity**.

23. In the **System assigned** tab, select **Azure role assignments** under **Permissions**.



Home > CreateVm-n2wsoftwareinc1657117813969.n2ws_backup_-20230320144226 | Overview > MyCPMonAzure

MyCPMonAzure | Identity

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

Locks

Operations

Bastion

Auto-shutdown

Backup

Disaster recovery

Updates

Inventory

Change tracking

Automanage

Configuration management

System assigned User assigned

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity you don't have to store any credentials in code. [Learn more about Managed identities.](#)

Save Discard Refresh Got feedback?

Status

Off On

Object (principal) ID

ddf5674e-3185-4075-a852-5a96cb12563b

Permissions

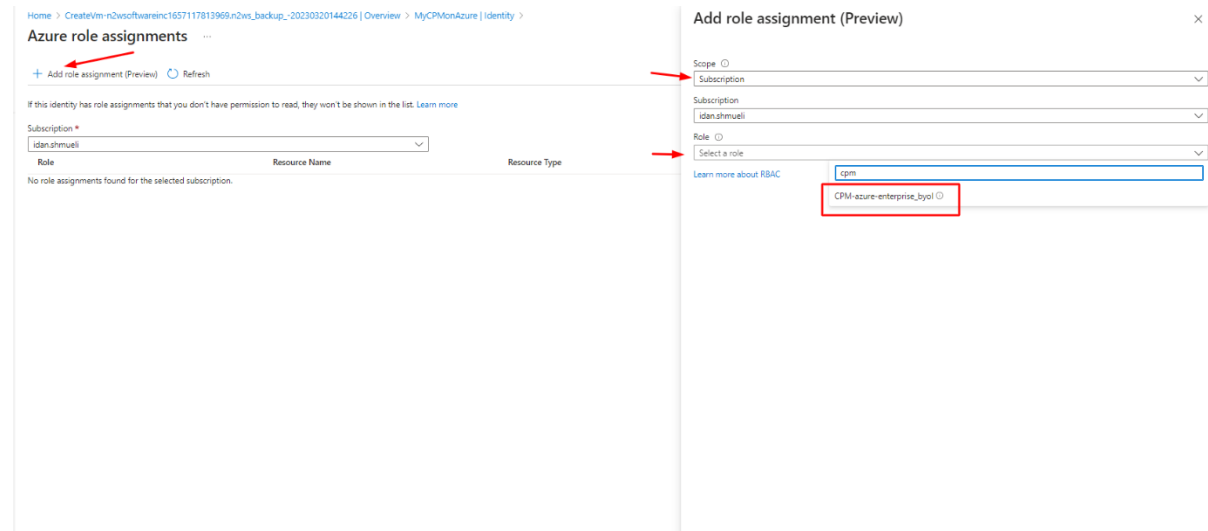
Azure role assignments

This resource is registered with Azure Active Directory. The managed identity can be configured to allow access to other resources. Be careful when making changes to the access settings for the managed identity because it can result in failures.

24. On the **Azure role assignments** page, select the pre-defined user in the **Subscription** list.

25. Select **+Add role assignment (preview)**.

The Add role assignment (Preview) window opens.



26. In the **Scope** list, select **Subscription**.

27. In the **Role** list, select **CPM-azure-enterprise_byol**, which should contain minimal permissions for the virtual machine to handle your resources. Then select **Save**.

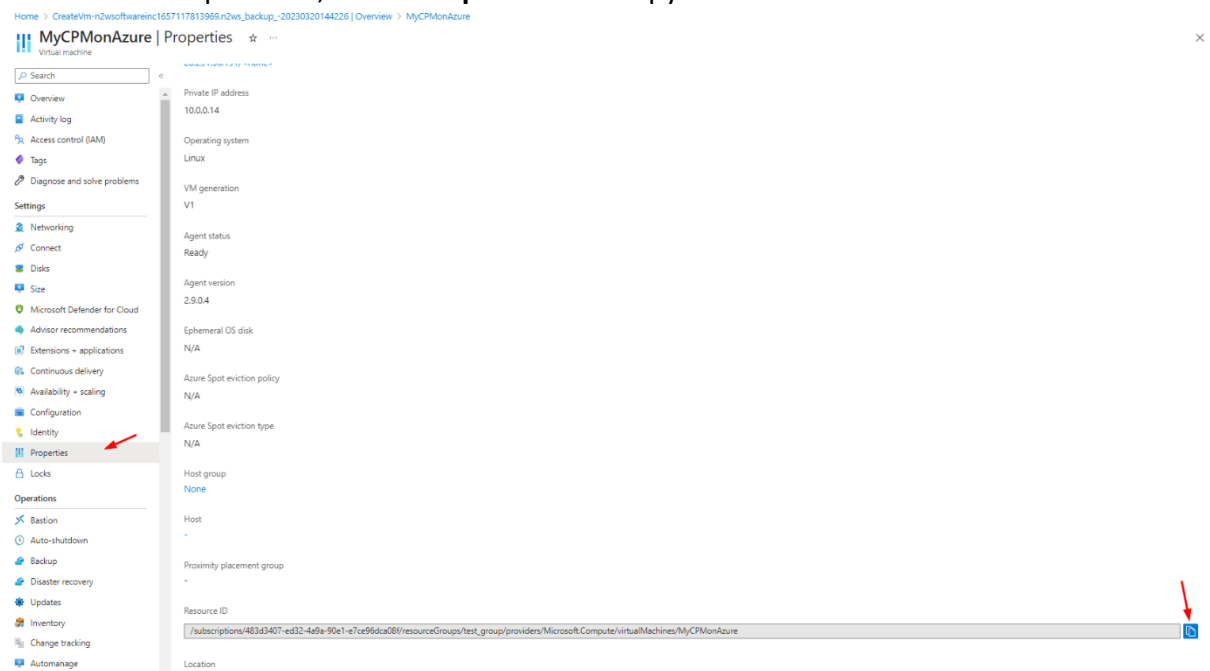
Role assignment messages appear in the upper right corner.

The Azure portion of the configuration is complete.


4 Configure N2W on Azure with the Configuration Wizard

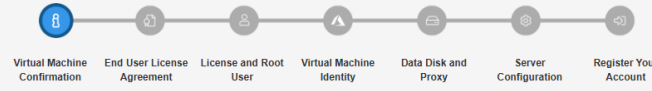
To view a video of the N2W configuration, see <https://n2ws.com/support/install-guide>

1. In Microsoft Azure, open a new tab and log on to N2W using the public IP address of the virtual machine over HTTPS.
2. In the menu select **Overview**.
3. In the Properties section, copy the Public IP address under Networking.
4. Open a new tab in the browser and paste the **Public IP address** in the address bar. The N2W Server Configuration page opens.
5. In the menu of the prior tab, select **Properties** and copy the **Resource ID**.




- In the N2W Configuration screen, paste the **Resource ID** in the **Virtual Machine Confirmation** step field and select **Next**.


 **N2W Backup & Recovery (CPM) v4.4.1**
 Server Configuration



To begin, please enter this virtual machine's resource id:

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

 **N2W Backup & Recovery (CPM) v4.4.1**
 Server Configuration



End User License Agreement
Version 4.4 – March 2025

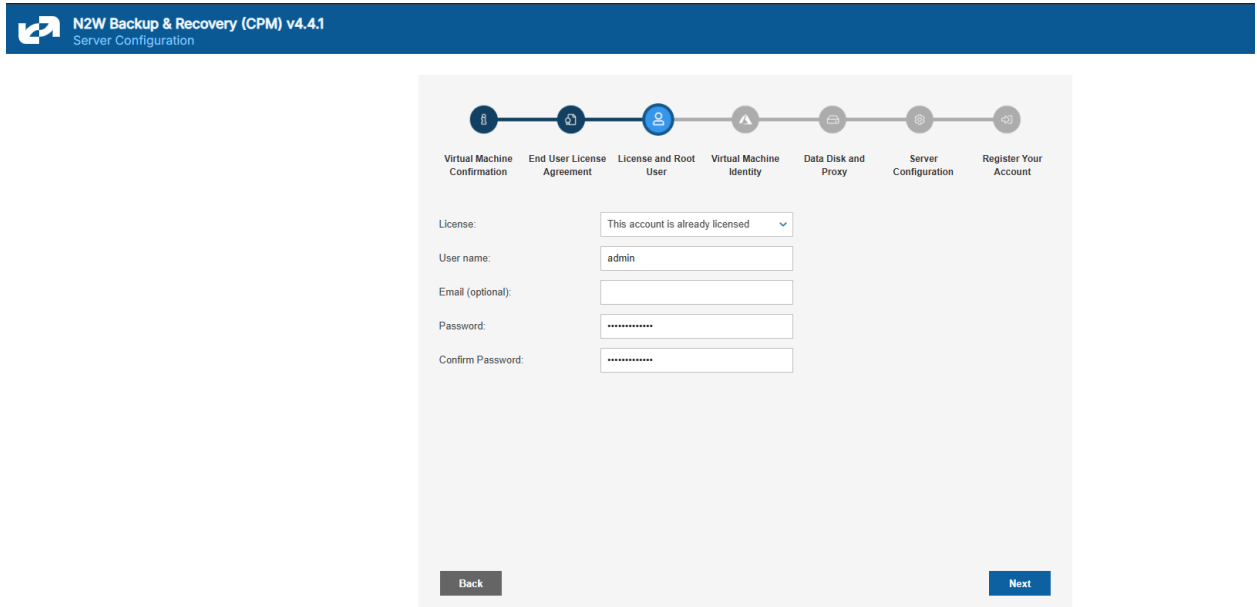
This License Agreement (the "Agreement") is made and entered into by and between Licensor (as defined below) and you as, or on behalf of, Licensee (as defined below). This Agreement governs Licensee's access to the Image and its use of the Licensee Instance (as these terms are defined below). Each of Licensor and Licensee is a "Party" to this Agreement and together they are indicated as the "Parties".

By either (a) submitting a signed Quote to Licensor; (b) providing to Licensor a purchase order complying with a Quote; (c) checking the "I read the License Terms and I Accept them" checkbox and subsequently clicking the "Next" button during the installation and configuration process of the Licensee Instance (as defined below); or (d) accessing or using the Licensee Instance, you as, or on behalf of, Licensee, are accepting and agreeing to be bound by the terms and conditions of this Agreement, which becomes effective as of the date you click the "Next" button (or first access or use the Image or the Licensee Instance) (the "Effective Date"). If you are accepting the terms of this Agreement on behalf of Licensee, you represent and warrant that: (i) you have full legal authority to bind Licensee to this Agreement; (ii) you have read and understand this Agreement; and (iii) you agree as, or on behalf of, Licensee to this Agreement. If you do not have the legal authority to bind Licensee, please do not click the "Next" button (or access or use the Licensee Instance).

1. License Grant. Licensor grants Licensee a limited, personal, revocable, non-exclusive, non-sublicensable, non-transferable license to do the following during the License Term: (i) install and configure the Image on a single Licensee Instance; (ii) create, copy, use, maintain and restore Provider Snapshots and Independent Backups of Licensee Information using Licensee Instance(s) for the internal business use of Licensee, subject to the attributes and usage limitations of Image or as set forth in the Quote; (iii) copy and use the Documentation solely for the above-mentioned purposes; and (iv) if and to the extent Licensee has been expressly authorized in writing by Seller in a Quote or otherwise, Licensee may either or both (a) install and configure the

☒ I read the license terms and I accept them

8. In the **License and Root User** step:
 - a. In the **License** list, select the proper license method.
 - b. Complete the logon root **Username**, optional **Email**, and **Password** sequence, and then select **Next**.



N2W Backup & Recovery (CPM) v4.4.1
Server Configuration

Progress bar: Virtual Machine Confirmation, End User License Agreement, **License and Root User**, Virtual Machine Identity, Data Disk and Proxy, Server Configuration, Register Your Account

License:

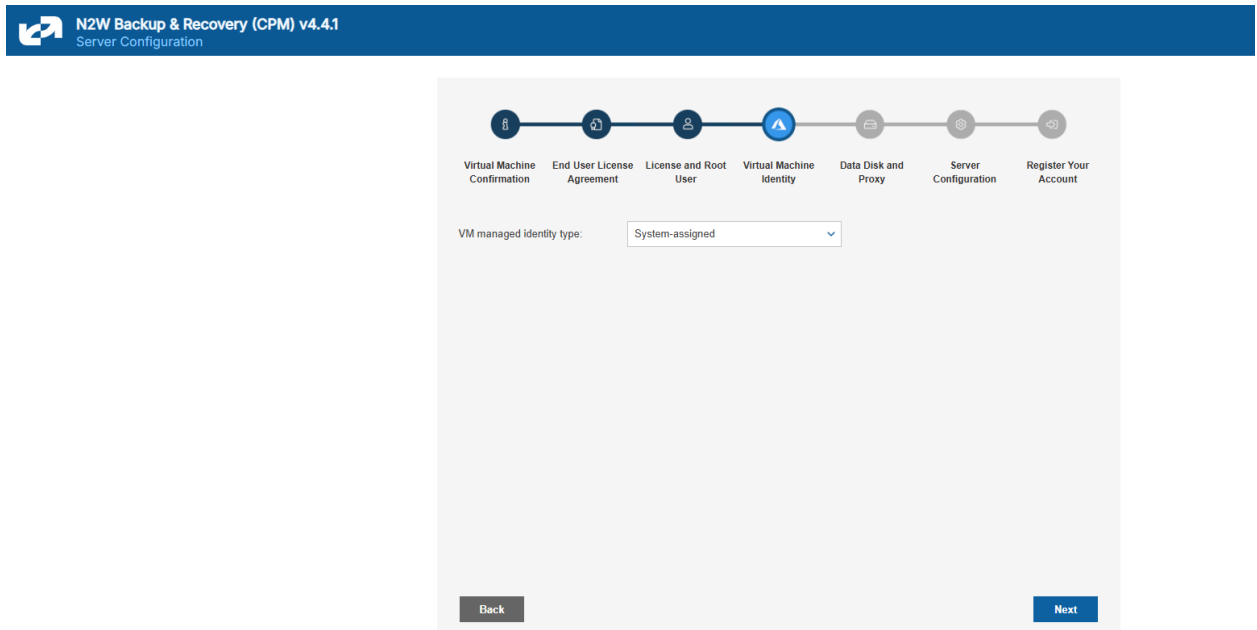
User name:

Email (optional):

Password:

Confirm Password:

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




N2W Backup & Recovery (CPM) v4.4.1
Server Configuration

Progress bar: Virtual Machine Confirmation, End User License Agreement, License and Root User, **Virtual Machine Identity**, Data Disk and Proxy, Server Configuration, Register Your Account

VM managed identity type:

10. In the **Data Disk and Proxy** step:

- In the **Choose Time** list, select the appropriate time zone.
- In the **Choose new or existing disk** list, select **Create New Data Disk**.


N2W Backup & Recovery (CPM) v4.4.1
 Server Configuration

Virtual Machine Confirmation
End User License Agreement
License and Root User
Virtual Machine Identity
Data Disk and Proxy
Server Configuration
Register Your Account

Choose Time: Greenwich (GMT) ▼


Choose new or existing disk: Create New Data Disk ▼

Auto Backup Data Volume: Yes ▼

Connect via web proxy: Disabled ▼

Back
Next

- Choose proxy settings as needed, and then select **Next**.


N2W Backup & Recovery (CPM) v4.4.1
 Server Configuration

Virtual Machine Confirmation
End User License Agreement
License and Root User
Virtual Machine Identity
Data Disk and Proxy
Server Configuration
Register Your Account

Choose Time: Greenwich (GMT) ▼

Choose new or existing disk: Create New Data Disk ▼

Auto Backup Data Volume: Yes ▼

Connect via web proxy: Enabled ▼

Proxy address:

Proxy port:

Proxy user:

Proxy password:

Back
Next (Connect Proxy)



11. In the Server Configuration step, review the disk defaults, and then select **Next**.

- **Capacity (GiB)** defaults to **10 GB**, which is the minimum size.

Note: This value may need to be increased depending on the number of VMs and disks you are protecting.

- **Volume Type** defaults to **Premium SSD**, which is the minimum disk type recommended.

Note: For more details on the recommended virtual machine type and Azure disk size requirements of N2W for Azure, see the following KB article:

<https://n2ws.zendesk.com/hc/en-us/articles/28857377102493-Recommended-VM-Types-for-an-N2W-Server-in-Azure>

12. In the **Register Your Account** step, if you have not configured N2W before, enter the requested information, and select **Register Now**. Otherwise, select **I don't want to register now**, and then select **Configure System**.

13. The system is now configuring; this may take up-to 10 minutes to finish. Once it does you will be automatically directed to the logon page, and the installation is finished.

5 Creating an Azure Backup Policy

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

1. In N2W, select the **Policies** tab.
2. In the **+ New** list, 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.
 - **Account** – Select from the list. Or, select **+ New** to add an account. See section [7.2](#).
 - **Enabled** – Clear to disable the policy.
 - **Subscription** – Select from the list.
 - **Schedules** – Optionally, select one or more schedules from the list, or select **+ New** to add a schedule. See section [4.3](#).
 - **Auto Target Removal** – Select **Yes** to automatically remove a non-existing target 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. When selecting Virtual Machines, it is *required* to filter by the **Location** of the target resources using the list in the upper left corner *before* selecting the individual targets. Filtering by Resource Group is optional.

Add Virtual Machines
✕

Location:

(Europe) North Europe
▼

Resource Group:

All Resource Groups
▼

🔍

↻ Refresh

	Name	Resource Group	Location	VM Size	OS Type
<input type="checkbox"/>	linux-ubuntu-europe	first-rg	northeurope	Standard_B1ls	Linux

0 of 1 items selected
▶

Add selected

Close

- When finished selecting targets, select **Add selected**. The Backup Targets tab lists the selected targets.

Policies > p2-azure

Last updated: Apr 5, 2021 10:59 PM Last recovery: Never

Policy Details Backup Targets

Add Backup Targets

Virtual Machines

Remove Configure

Search resources

<input type="checkbox"/>	Name	Resource Group	Location	VM Size	OS Type
<input type="checkbox"/>	linux-ubuntu-europe	first-rg	northeurope	Standard_B1ls	Linux

0 of 1 items selected

Disks


Remove

Search resources


<input type="checkbox"/>	Name	Status	Location	Resource Group	Size	Dis
<input type="checkbox"/>	linux-ubuntu-europe_disk1...	Reserved	northeurope	first-rg	30 GiB	Sta

0 of 1 items selected

Previous Save Cancel



- To determine which disks for each Virtual Machines target to back up, select  **Configure**. In the **Which Disks** list of the Policy Virtual Machine and Disk Configuration screen, select the disks to include or exclude in the backup.
- When finished, in the **Backup Targets** tab, select **Save**.


5.1 Backing Up an Azure Policy


If the policy has a schedule, the policy will back up automatically according to the schedule. To run a policy as soon as possible, in the **Policies** view, select the policy and select  **Run ASAP**. To view the policy progress and backups, select **Backup Monitor**.


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


Backup Monitor


Cloud:  



Search backups 


By Virtual Machine 








All Policies 


All Accounts 

All Backup Statuses 

Show:  

20 records/page 

 Recover
  Log
  View Snapshots
  Move to Freezer
  Edit Frozen Item
  Delete Frozen Item
  Refresh

Time	Finish Time	Policy / Frozen Item	Account	Status
3, 2021 4:07 PM		p2-azure	azure-account	 In Progress

0 of 1 items selected

6 Recovering from an Azure Backup

Note: Only one VM is recoverable during a recovery operation.

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

In the VM recovery Basic Options, there are Azure options for replicating data to additional locations to protect against potential data loss and data unavailability:

- **Availability Zone** – A redundant data center (different building, different servers, different power, etc.), within a geographical area that is managed by Azure.
- **Availability Set** – A redundant data center (different building, different servers, different power, etc.) that can be launched and fully configured by the customer and managed by the customer.
- **No Redundancy Infrastructure Required** – By selecting this option, the customer can choose not to replicate its data to an additional (redundant) location in another zone or set. By choosing this option, the customer would save some money, but in rare cases (usually 11 9s of durability and 99.9% of availability), the customer can experience some degree of data loss and availability.

In the Disk Recovery screen, you may be presented with an option to change the encryption when recovering certain disks.







Note: To add an additional layer of encryption during the recovery process, see <https://docs.microsoft.com/en-us/azure/virtual-machines/disks-enable-customer-managed-keys-portal>.





Disk encryption settings can be changed only when the disk is unattached or the owner VM is deallocated.

6.1.1 Recovering a VM and Disks

To recover a VM and/or attached disks:

Backup Monitor


Cloud:  
Search backups  By Virtual Machine  All Policies  All Accounts 

All Backup Statuses  Show:   20 records/page 

[Recover](#) [Log](#) [View Snapshots](#) [Move to Freezer](#) [Edit Frozen Item](#) [Delete Frozen Item](#) [Refresh](#)

<input type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status
<input type="checkbox"/>	Apr 6, 2021 7:51 PM	Apr 6, 2021 7:52 PM	p3-zure-disk	azure-account	✓ Succe
<input type="checkbox"/>	Apr 6, 2021 7:05 PM	Apr 6, 2021 7:05 PM	p2-azure	azure-account	✓ Succe
<input type="checkbox"/>	Apr 6, 2021 6:54 PM	Apr 6, 2021 6:54 PM	p2-azure	azure-account	✓ Succe
<input checked="" type="checkbox"/>	Apr 6, 2021 4:07 PM	Apr 6, 2021 4:07 PM	p2-azure	azure-account	✓ Succe

1 of 4 items selected



1. In the **Backup Monitor**, select the backup and then select  **Recover**.

Backup Monitor > p2-azure - 04/06/2021 4:07 PM > Recover



Search by Resource

Resource ID or name

Virtual Machines

 **Recover**  Recover Disks Only

Name	Resource Group	Location	Size	OS T
linux-ubuntu-europe	first-rg	(Europe) North Europe	Standard_B1ls	Lir

2. To recover a VM, with or without its attached disks, select the VM snapshot that you want to recover from and then select  **Recover**.
- d. In the **Virtual Machines** tab of the Recover screen, select 1 VM and then select  **Recover**. The **Basic Options** tab opens.

Virtual Machine Recovery

Basic Options Disks

Name
linux-ubuntu-europe

Resource Group
FIRST-RG

Size
Standard_B1ls

Availability

Availability Type
No Infrastructure Redundancy Required

Availability Zone

Availability Set

Virtual Network
FIRST-RG-vnet

Subnet
default


Private IP Address
10.0.0.4

☒ Preserve Tags

☐ Auto assigned

Recover Virtual Machine Close

- e. In the **Availability Type** list, select one of the following:
 - **No Infrastructure Redundancy Required** – Select to not replicate data at 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.
- f. In the **Private IP Address** box, assign an available IP address or switch the **Custom** toggle key to **Auto assigned**.
- g. In the **Disks** tab, enter a new **Name** for each disk. Similar names will cause the recovery to fail.

- h. Select **Recover Virtual Machine**.
3. To recover only Disks attached to the VM, select **Recover Disks Only**. a. In the **Disks** tab, enter a new **Name** for each disk. Similar names will cause the recovery to fail. b. See Note in section 7.5 about changing the **Encryption Set** for certain disks. c. Change other settings as needed. d. Select **Recover Disk**.
4. To view the recovery progress, select **Recovery Monitor**. Use the **Cloud** buttons to display the Azure () recoveries.

6.1.2 Recovering Independent Disks

To recover from backups with independent disks:

1. Select the backup and then select  **Recover** as in step 1 of the VM recovery.

Backup Monitor > p3-zure-disk - 04/06/2021 7:51 PM > Recover

Search by Resource
Resource ID or name

Independent Disks

<input checked="" type="checkbox"/>	Original Disk Name	Original Disk ID	Location	Name	Resource Group	Size	Encryption Set	Preserve Tags
<input checked="" type="checkbox"/>	run_disk1_db1b260c26964a20...	/subscriptions/cd...	(Europe) North Eu...	run_disk1_db1b2...	FIRST-RG	30	Don't Change Encrypt	<input checked="" type="checkbox"/>

2. In the Independent Disks tab:
 - i. Enter a new **Name** for each disk to recover as similar names will cause failure.
 - j. See Note in section 7 about changing the **Encryption Set** for certain disks.
 - k. Change other settings as needed.

Disk Recovery from Virtual Machine linux-ubuntu-europe

Disks

<input checked="" type="checkbox"/>	Original Disk Name	Original Disk ID	Name	Resource Group	Size	Encryption Set	Preserve Tags
<input checked="" type="checkbox"/>	linux-ubuntu-europe_...	/subscriptions/cd...	linux-ubuntu-eur...	FIRST-RG	30	Don't Change Encrypt	<input checked="" type="checkbox"/>

- l. Select **Recover Disk**.
3. To view the recovery progress, select **Recovery Monitor**. Use the **Cloud** buttons to display the Azure () recoveries.



7 What to do After Deploying Your N2W Server on Azure

Once your N2W server is deployed you can now start to configure your backup policies to start protecting your resources.

For Azure tutorial videos see the following link - https://n2ws.com/support/video-tutorials?e-filter-d7a0d74-post_tag=azure

Full User Guide manual can be found here - <https://docs.n2ws.com/user-guide>