



N2W Backup & Recovery

AWS Quick Start Guide

V4.5.1

Content

1	Introduction.....	3
2	Launching N2W Backup & Recovery.....	4
2.1	Launching with CloudFormation.....	4
3	N2W Server Instance Configuration	5
3.1	N2W Server Instance Connectivity.....	5
3.2	Creating an Instance When Launching through EC2.....	5
3.3	N2W Server Instance Configuration.....	8
3.4	N2W Server Configuration Wizard.....	9
4	Creating a Simple Backup Policy.....	17
4.1	Adding an AWS Account	18
4.2	Creating a Simple Backup Schedule.....	19
4.3	Creating a Simple AWS Backup Policy.....	20
5	Performing a Basic Recovery.....	24
6	How to Configure N2W with CloudFormation.....	28
7	Using Azure with N2W	34
7.1	Setting Up Your Azure Subscription.....	34
7.2	Adding an Azure Account to N2W	37
7.3	Creating an Azure Policy	38
7.4	Backing Up an Azure Policy.....	40
7.5	Recovering from an Azure Backup.....	40
	Appendix A - AWS Authentication.....	44
	Appendix B - Adding Exception for Default Browser	48



1 Introduction

Quickly install N2W, set up your server, and configure your first automated backup.

N2W Backup & Recovery is a powerful tool that's essentially "plug-and-play". It takes about 20 minutes to set up and works in your existing AWS environment. N2W plays well with other platforms for making backup and recovery worry-free. This Quick Start Guide will walk you through the core steps to get N2W up and running.

A quick word about passwords before we get going. N2W Software 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.

Prefer a video tutorial? Follow along at <https://n2ws.com/support/install-guide> and you'll be set in ~12 minutes.



2 Launching N2W Backup & Recovery

You have 2 options to launch: via the 8 steps below or using CloudFormation.

To launch N2W as part of a 30-day free trial or as a BYOL edition:

1. Go to <https://aws.amazon.com/marketplace/>
2. Search for 'n2w'.
3. Select your edition of **N2W Backup & Recovery (CPM)**.
4. Select **Continue to Subscribe**.
5. In the AWS logon page, enter your AWS account information, and select **Continue to Configuration**.
6. Under **Configure this software**:
 - a. Change the fulfillment option to **Amazon Machine Image (AMI)**.
 - b. Select the latest version in the **Software Version** list.
 - c. Select the **Region** you want to deploy to.
7. Select **Continue to Launch**.
8. In the **Choose Action** list, select **Launch through EC2**.

2.1 Launching with CloudFormation

CloudFormation is an AWS service that allows you to treat a collection of AWS resources as one logical unit. CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment, across all regions and accounts in an automated and secure manner.

Note: The IAM role will automatically contain the required permissions for N2W operations.

To configure N2W using CloudFormation, see section 6.

3 N2W Server Instance Configuration

3.1 N2W Server Instance Connectivity

For the configuration process to work, as well as N2W’s normal operations, N2W needs to be able to “talk” with AWS APIs. Thus, it needs to have outbound connectivity to the Internet. Verify that the N2W instance has Internet connectivity; this can be achieved by placing the instance in a public subnet with a public IP address, by assigning an Elastic IP to the instance, using a NAT instance or by using an Internet Gateway. You also need to make sure DNS is configured properly and that HTTPS protocol is open for outbound traffic in the VPC security group settings. It is by default.

3.2 Creating an Instance When Launching through EC2

1. Under the **Name and tags** section, enter a name for your instance in the **Name** box.

Name and tags [Info](#)

Name

N2WS

Add additional tags

If required, select **Add additional tags**.

2. Under **Application and OS images (Amazon Machine Image)**, leave all default values, as this section shows what AMI we are using for the EC2 instance image.

▼ Application and OS Images (Amazon Machine Image) [Info](#)

An AMI contains the operating system, application server, and applications for your instance. If you don't see a suitable AMI below, use the search field or choose [Browse more AMIs](#).

AMI from catalog

Recents

My AMIs

Quick Start

<p>Name</p> <p>N2W-CPM-4.4.1-RELEASE-14807ff7-6eb0-4030-9b61-8782f8e8e834 Verified provider</p> <p>Description</p> <p>N2W-CPM-4.4.1-RELEASE</p> <p>Image ID</p> <p>ami-0495ac7f39eb60935</p> <p>Username ⓘ</p> <p>root (Check with the AMI provider.)</p>	<p style="text-align: center; color: #0070C0;">🔍</p> <p style="color: #0070C0; font-size: 0.8em;">Browse more AMIs</p> <p style="font-size: 0.7em; color: #666;">Including AMIs from AWS, Marketplace and the Community</p>												
<table style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left; border-bottom: 1px solid #ccc;">Catalog</th> <th style="text-align: left; border-bottom: 1px solid #ccc;">Published</th> <th style="text-align: left; border-bottom: 1px solid #ccc;">Architecture</th> <th style="text-align: left; border-bottom: 1px solid #ccc;">Virtualization</th> <th style="text-align: left; border-bottom: 1px solid #ccc;">Root device type</th> <th style="text-align: left; border-bottom: 1px solid #ccc;">ENA Enabled</th> </tr> </thead> <tbody> <tr> <td>AWS Marketplace AMIs</td> <td>2025-08-20T18:57:44.000Z</td> <td>x86_64</td> <td>hvm</td> <td>ebs</td> <td>Yes</td> </tr> </tbody> </table>	Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled	AWS Marketplace AMIs	2025-08-20T18:57:44.000Z	x86_64	hvm	ebs	Yes	
Catalog	Published	Architecture	Virtualization	Root device type	ENA Enabled								
AWS Marketplace AMIs	2025-08-20T18:57:44.000Z	x86_64	hvm	ebs	Yes								

If you have an existing license entitlement to use this software, then you can launch this software without creating a new subscription. If you do not have an existing entitlement, then by launching this software, you will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's [End User License Agreement](#) ⓘ

ⓘ The Image has a newer version. Would you like to view the newest version?

- Under **Instance type**, the recommended minimum size is **t3.medium**. However, for bigger environments, the type may need to be larger.

Note: For information on choosing the appropriate size, see

<https://n2ws.zendesk.com/hc/en-us/articles/28811725028125-Recommended-instance-sizes-and-volume-types-for-N2W-Servers>

▼ **Instance type** [Info](#) | [Get advice](#)

Instance type

t3.medium
Family: t3 2 vCPU 4 GiB Memory Current generation: true

All generations

[Compare instance types](#)

The AMI vendor recommends using a t2.small instance (or larger) for the best experience with this product.

- Under **Key pair**, you can create a new key pair or use an existing one. The key pair is used when connecting to the instance's CLI.

▼ **Key pair (login)** [Info](#)

You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*


N2WS_Virginia

[Create new key pair](#)




5. Under **Network settings**, select a relevant **VPC**, **Subnet**, and **Security group** for the instance. For the configuration process to work, as well as for normal N2W operations, N2W needs outbound connectivity to the Internet for the HTTPS protocol. Needed are:
- A public IP, or
 - An Elastic IP attached to the instance, or
 - Connectivity via a NAT setup, Internet Gateway, or HTTP proxy,

▼ Network settings [Info](#)


VPC - *required* [Info](#)

vpc-0d5ca26ed8e0ef938 (default) 
172.31.0.0/16

Subnet [Info](#)

No preference   [Create new subnet](#) 

Auto-assign public IP [Info](#)

Enable 

[Additional charges apply](#) when outside of [free tier allowance](#)

Firewall (security groups) [Info](#)

A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

Create security group Select existing security group

Security group name - *required*

N2WS Backup & Recovery for AWS Free Trial/BYOL-4.3.0-AutogenByAWSMP--1

This security group will be added to all network interfaces. The name can't be edited after the security group is created. Max length is 255 characters. Valid characters: a-z, A-Z, 0-9, spaces, and ._-:/()#,@[]+=&;{}!\$*

Description - *required* [Info](#)

N2WS Backup & Recovery for AWS Free Trial/BYOL-4.3.0-AutogenByAWSMP--1crea

Inbound Security Group Rules

▶ Security group rule 1 (TCP, 443, 0.0.0.0/0)	Remove
▶ Security group rule 2 (TCP, 22, 0.0.0.0/0)	Remove

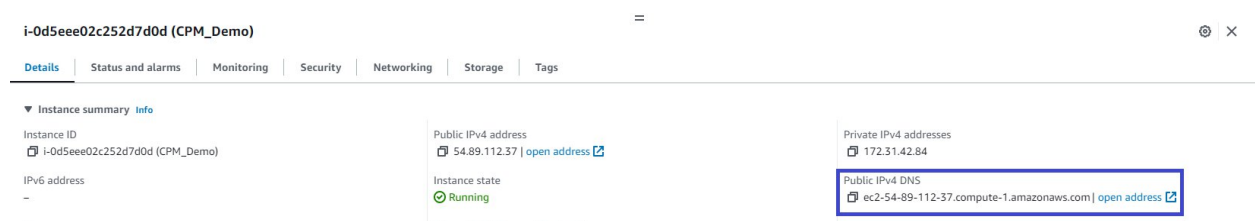
- Under **Advanced details**, the only mandatory field to change is the IAM instance profile. Create a new role to give the EC2 instance the minimum permissions needed to perform its functions. See <https://n2ws.zendesk.com/hc/en-us/articles/33252616725533--4-5-0-Required-Minimum-AWS-permissions-for-N2W-operations>
- Select **Launch instance**.

3.3 N2W Server Instance Configuration

N2W has a browser-based management console. N2W supports Chrome, Edge, Firefox and Safari.

Note: For N2W to work, Java Script needs to be enabled on your browser.

After launching the N2W AWS instance, use AWS Management Console or any other management tool to obtain the IP address of the new instance:



Note: Use the IP address to connect to the N2W Server using the HTTPS protocol in your browser (<https://<server address>>).

When a new N2W Server boots for the first time, it will automatically create a self-signed SSL certificate. After initial configuration, it is possible to upload a different certificate. Since the certificate is unique to this server, it is perfectly safe to use. However, since the certificate is self-signed, you will need to approve it as an exception for the browser. To add an exception for the default certificate in Chrome and Firefox, see Appendix B – Adding Exception for Default Browser (page 48).

After adding the exception, you get the first screen of the N2W configuration application.

3.4 N2W Server Configuration Wizard

The N2W Server Configuration wizard takes you through the process step by step. There are a few differences between configuring N2W for the Free Trial and other paid editions.

For the Free Trial edition:

- A new volume must be defined for the N2W server.
- You will need to enter a user name, a valid email address, and enter a strong password and verify it.

For other N2W Editions:

Step 1: Verify ownership of new instance

On the first screen you will be asked to type or paste the instance ID of this new N2W instance. This step is required to verify that you are indeed the owner of this instance.



Instance Confirmation End User License Agreement License and Root User Data Volume and Proxy Server Configuration Register Your Account

To begin, please enter the instance ID of this instance:

Next

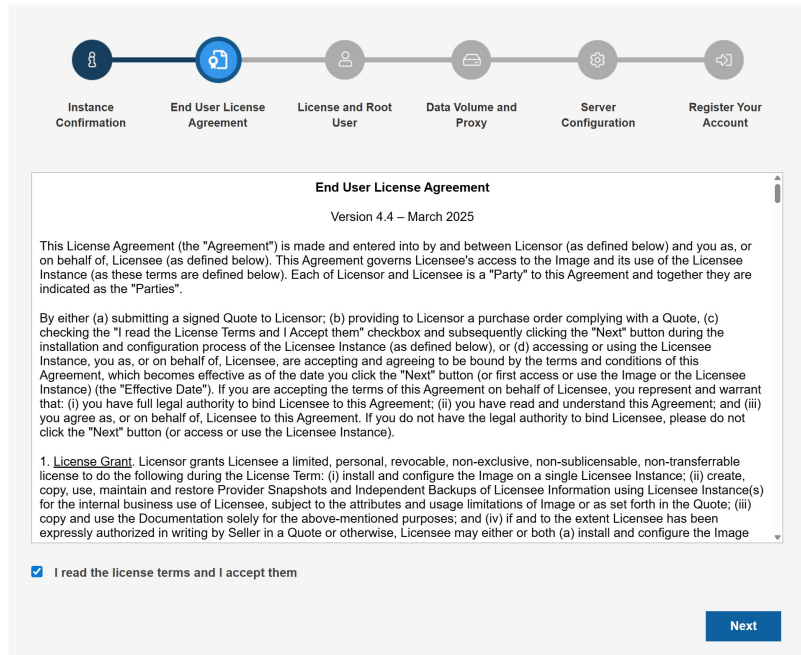
Select **Next**. In the next step the N2W configuration procedure begins.

Step 2: Approve the N2W license agreement.

Review the end user license terms, select the acceptance checkbox, and then 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 License 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 Image

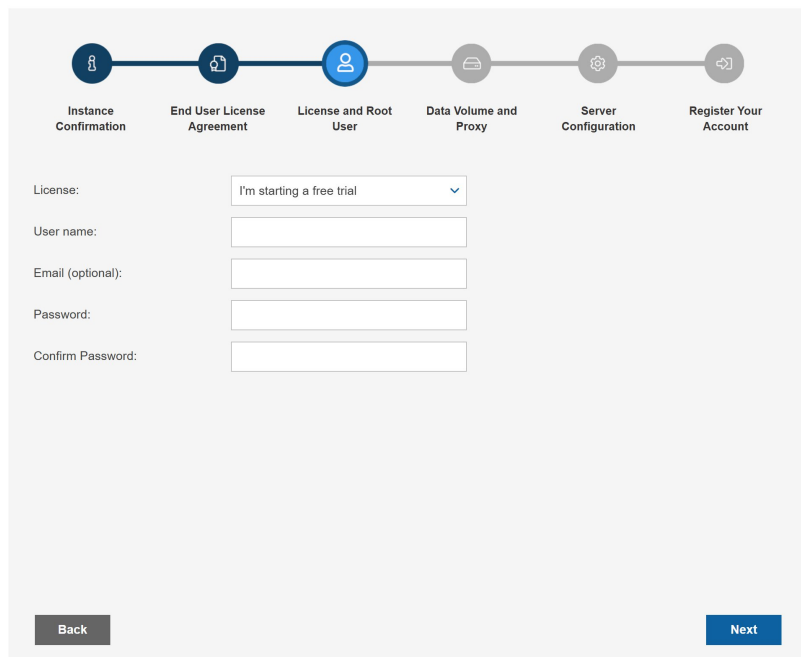
I read the license terms and I accept them

Next

Step 3: Configure the license type, N2W "root" account password, and user information.



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



License and Root User

License:

User name:

Email (optional):

Password:

Confirm Password:

Back

Next

For the Free Trial, leave the **License** list with the default. If you purchased a license directly from N2W Software, choose one of the **License** options, according to the instructions you received.

Note: If anyone in your organization already installed a N2W Free Trial in the past on the same AWS account, you may receive an error message when trying to configure or connect to N2W. Contact support@n2ws.com to resolve.

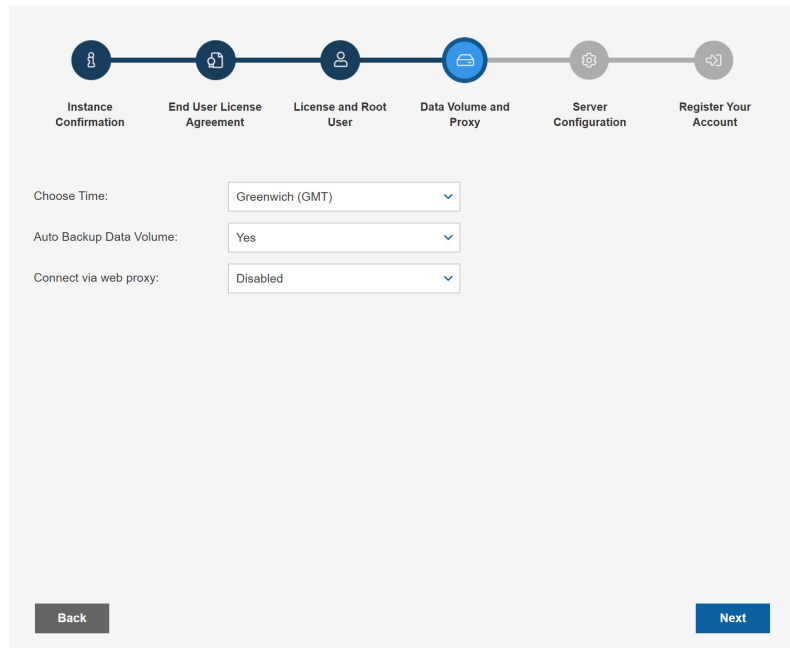
Note: If you are using one of the N2W paid products on AWS Marketplace, you will not see the License field.

If this is an upgrade, the username must remain as it was before the upgrade, but the password can be modified.

Note: Passwords: N2W does not enforce password rules. However, N2W recommends that you use passwords that are difficult to guess and to change them regularly.

When you have completed entering the details for Step 3, select **Next**.

Step 4: Time zone, new volume, force recovery mode, and web proxy settings



Instance Confirmation End User License Agreement License and Root User **Data Volume and Proxy** Server Configuration Register Your Account

Choose Time:

Auto Backup Data Volume:

Connect via web proxy:

1. Choose your time zone.

2. If configuring a paid edition, choose whether to create a new data volume or use an existing one. To configure an additional N2W server, in recovery mode only, choose an existing data volume and select **Force Recovery Mode**. In Step 5, you will be presented with a list of existing N2W data volumes.

The screenshot shows the 'Data Volume and Proxy' step of the configuration wizard. At the top, a progress bar indicates the current step is highlighted in blue. Below the progress bar, four configuration options are listed, each with a dropdown menu:

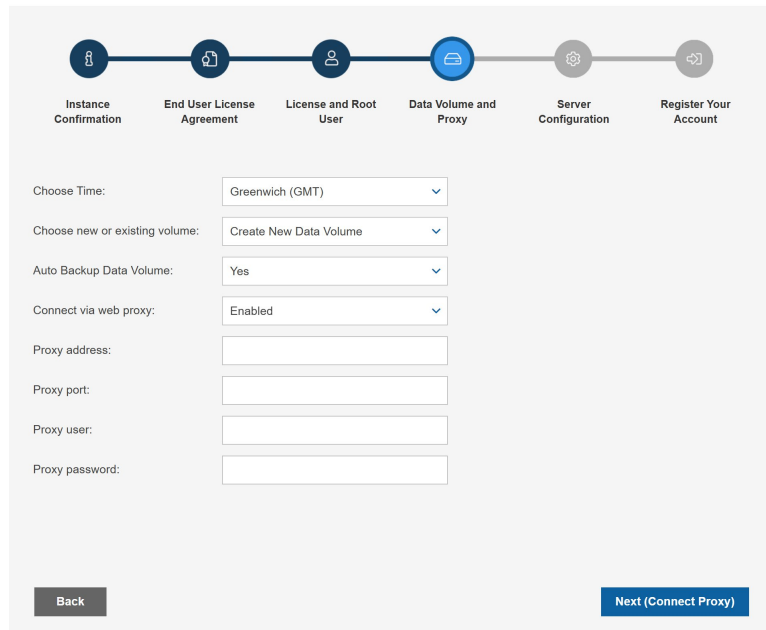
- Choose Time: Greenwich (GMT)
- Choose new or existing volume: Create New Data Volume
- Auto Backup Data Volume: Yes
- Connect via web proxy: Disabled

At the bottom of the form, there are 'Back' and 'Next' buttons.

Note: The N2W server configured for recovery mode will NOT:

- Perform backups.
- Copy to S3.
- Have Resource Control management.
- Perform any scheduled operations.

3. If you select **Enabled** for **Connect via Web proxy**, additional boxes appear for defining the proxy:



The screenshot shows the 'Data Volume and Proxy' step of the N2W Backup & Recovery (CPM) v4.4.1 Server Configuration wizard. At the top, a progress bar indicates the current step is 'Data Volume and Proxy', with other steps being 'Instance Confirmation', 'End User License Agreement', 'License and Root User', 'Server Configuration', and 'Register Your Account'. The main configuration area includes the following fields:

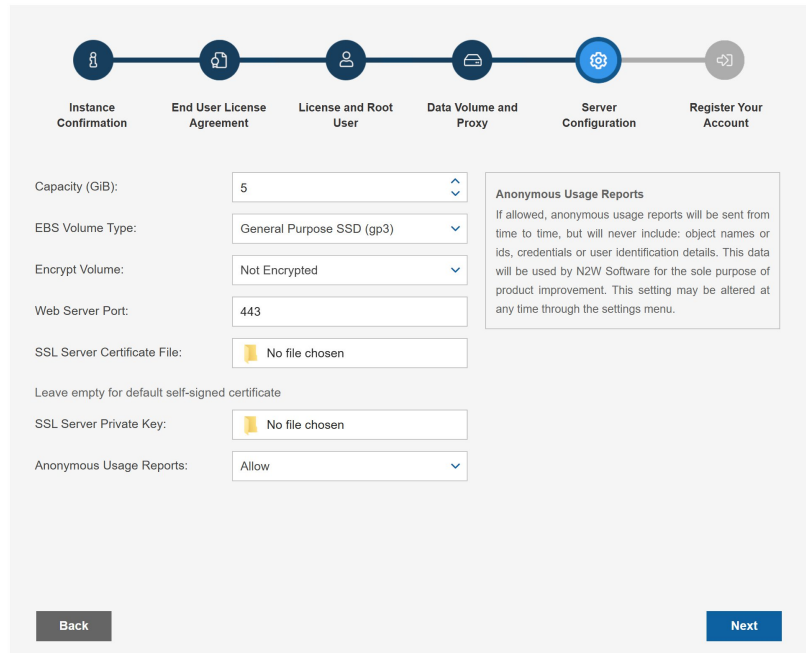
- Choose Time: Greenwich (GMT) (dropdown menu)
- Choose new or existing volume: Create New Data Volume (dropdown menu)
- Auto Backup Data Volume: Yes (dropdown menu)
- Connect via web proxy: Enabled (dropdown menu)
- Proxy address: (text input field)
- Proxy port: (text input field)
- Proxy user: (text input field)
- Proxy password: (text input field)

At the bottom, there are two buttons: 'Back' on the left and 'Next (Connect Proxy)' on the right.

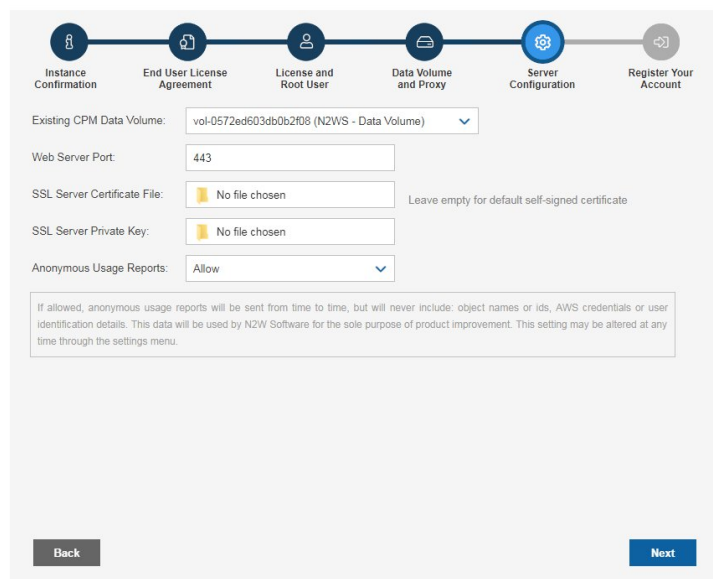
4. Select **Next**.

Step 5: Data volume type and encryption, security settings, and anonymous usage reports

1. If you are configuring a new data volume, you have an option to encrypt N2W user data. Select **Encrypted** in the **Encrypt Volume** drop-down list and choose a key in the **Encryption Key** list. You have the option to use a custom ARN.
 - Volume capacity should be at least 10 GB, which is large enough to manage roughly 50 instances and about 3 times as many EBS volumes.
 - If your environment is larger than 50 instances, increase the volume at about the ratio of 1 GB per 10 backed up instances.
 - Volume type should be at least GP3.

2. If you choose to use an existing volume or selected **Force Recovery Mode** in Step 4, you will see a drop-down volume selection box.

3. Complete the Web Server settings. The default port 443 is used by the N2W manager.

4. Allowing anonymous usage reports will enable N2W to improve the product. The usage reports are sent to N2W with no identifying details to maintain customer anonymity. You can disallow the anonymous reports at a later time in the N2W **General Settings** menu.
5. Select **Next** when finished.

Step 6: Register the account with N2W Software



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

Instance Confirmation End User License Agreement License and Root User Data Volume and Proxy Server Configuration Register Your Account

Full Name:

Email:

Company:

Country:

Zip Code:

Ref Code (optional):

I will register later

Registration is mandatory for free trials and optional for paid products. N2W recommends that all customers register, as it will enable us to provide faster support. N2W Software guarantees not to share your contact information with anyone.

If you have a Reference Code, enter it in the **Ref Code** box.

WARNING: Use English characters only in registration. Non-English characters (e.g. German, French) will cause the operation to fail.

Select **Configure System** when finished. The Configuring Server message appears.



Configuring Server. It may take a while ...

The registration and configuration process may take a while, after which a 'Configuration Successful – Starting Server ...' message appears. It will take a few seconds for the application to start.

Note: If, for any reason, you are not directed automatically to the application logon screen, reboot the instance from the management console.



Username:

Password:

You are now ready to log on with the credentials you created in the first screen and begin using N2W.

Note: Logging on for the first time with a trial edition can take up to 5 minutes as N2W must connect and get approved by our licensing service.

The “Please wait ...” message should go away in a few minutes. Allow 4-5 minutes and then refresh the screen.

4 Creating a Simple Backup Policy

Note: For instructions on how to quickly start using Azure with N2W, see section 7.

N2W automatically creates your first AWS account and policy. The required `cpmdata` policy is used to back up the N2W data volume.

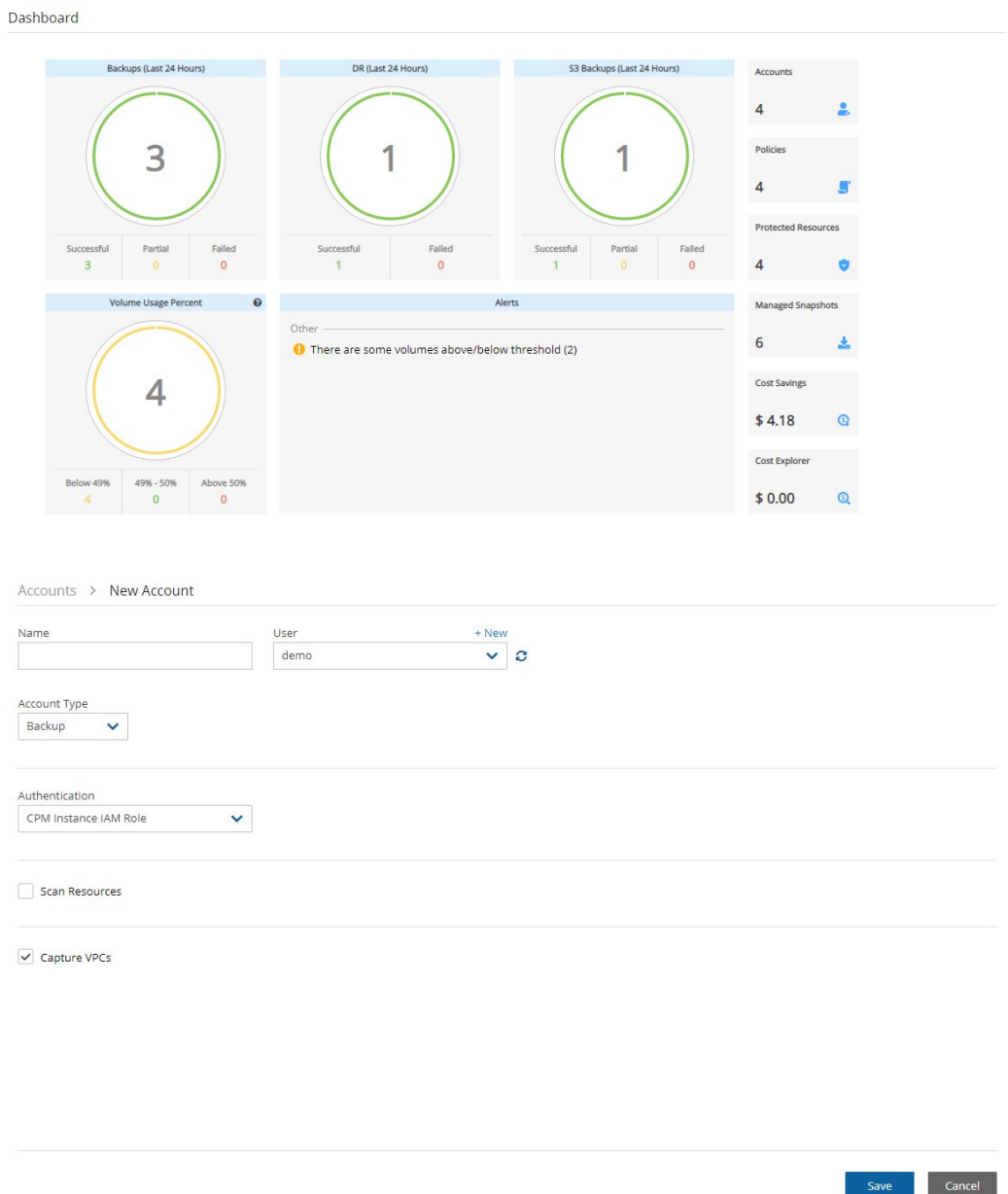
You can create additional accounts by following the instructions in section 4.1, or see <https://n2ws.zendesk.com/hc/en-us/articles/28829961679901-How-to-add-an-additional-AWS-account-to-N2W-for-Backup-or-DR>

For creating a simple AWS backup policy, see section 4.3. While a backup schedule is geared toward a production environment, it is optional, as you can run a policy independently of a schedule. To set a backup schedule, see section 4.2.

4.1 Adding an AWS Account

After logging on to the system for the first time, you will see the main screen, the Dashboard:

Dashboard



The dashboard displays several key metrics:

- Backups (Last 24 Hours):** 3 Successful, 0 Partial, 0 Failed.
- DR (Last 24 Hours):** 1 Successful, 0 Failed.
- S3 Backups (Last 24 Hours):** 1 Successful, 0 Partial, 0 Failed.
- Volume Usage Percent:** 4 Below 49%, 0 49% - 50%, 0 Above 50%.
- Alerts:** Other - There are some volumes above/below threshold (2).
- Accounts:** 4
- Policies:** 4
- Protected Resources:** 4
- Managed Snapshots:** 6
- Cost Savings:** \$ 4.18
- Cost Explorer:** \$ 0.00

Accounts > New Account

Name:

User: [+ New](#)

Account Type:

Authentication:

Scan Resources

Capture VPCs

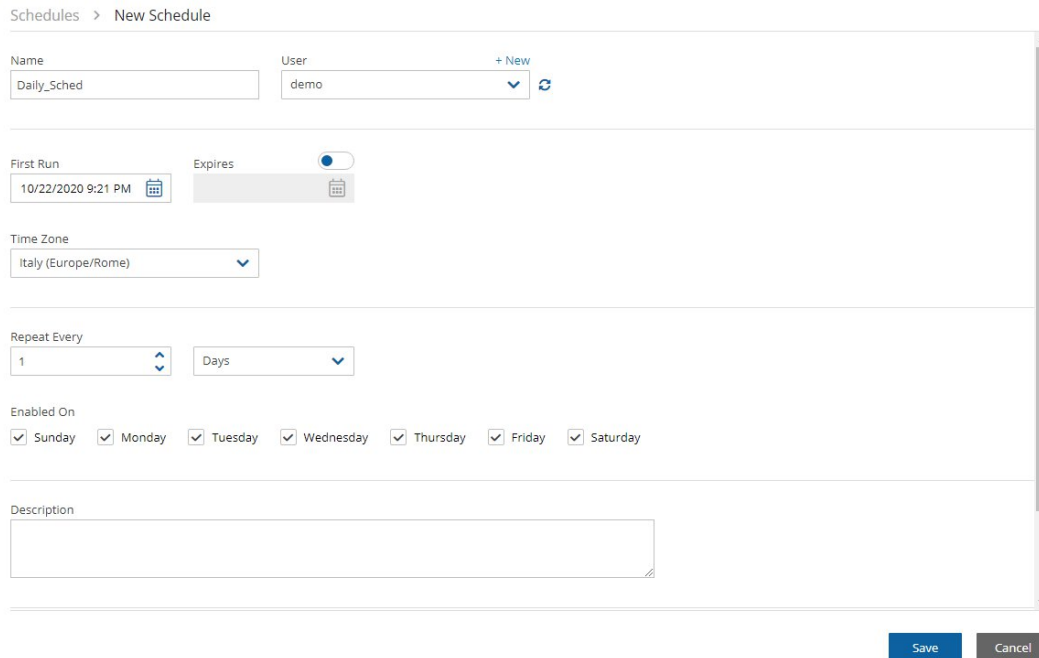
[Save](#) [Cancel](#)


6. Go to **Accounts** and click **New**
1. In the **Name** box, type the name you would like to associate with your primary AWS account.
2. In the **Account Type** list, select **Backup**. A **DR** account is for cross-account backup and recovery and is out of the scope of this guide. See “Account Type” in the *N2W Backup and Recovery User Guide*.
3. In the **Authentication** list, select your desired type of authentication. You can either choose to use your AWS access key and secret key or **CPM Instance IAM Role**, which is recommended. These credentials are saved in the N2W database. However, the secret key is kept in an encrypted form. There is no way these credentials will ever appear in a clear text format anywhere. See “Security Concerns and Best Practices” in the *N2W Backup & Recovery User Guide*.
4. Select **Scan Resources** to turn on the capability for this account to scan resources based on tags. Select the **Scan Regions** and **Scan Resource Types** in their respective lists.

5. **Capture Network Environments** is enabled by default.
6. Select **Save**.

4.2 Creating a Simple Backup Schedule

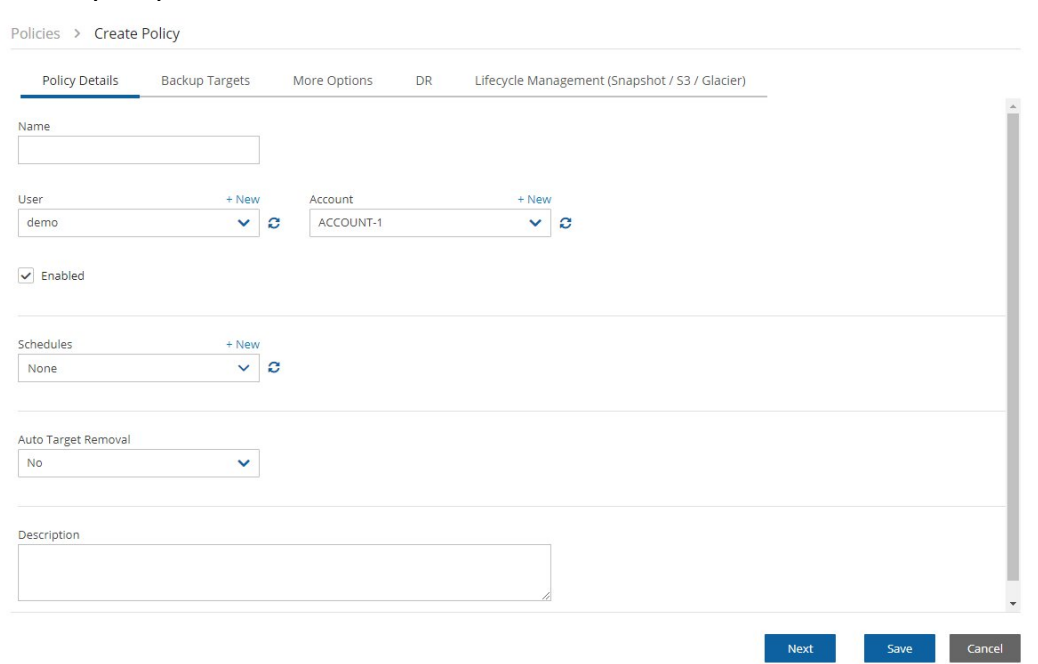
In the left panel, select the **Schedules** tab. Currently, the list of schedules is empty. You will now create the first schedule. Select **+ New**.



1. Type a name and optional description for the schedule.
2. In the **First Run** box, if the First Run is other than immediately, select **Calendar**  to choose the date and time to first run this schedule. The time set in **First Run** becomes the regular start time for the defined schedule. The default schedule expiration is never.
3. Set the schedule frequency in the **Repeat Every** list. Available units are minutes, hours, days, weeks, and months. Set the days of the week on which the schedule runs in the **Enabled-On** checkboxes.
4. Select **Save**.

4.3 Creating a Simple AWS Backup Policy

In the left panel, select the **Policies** tab. Currently, the list of policies is empty. You will now create the first policy. Select **+ New**.



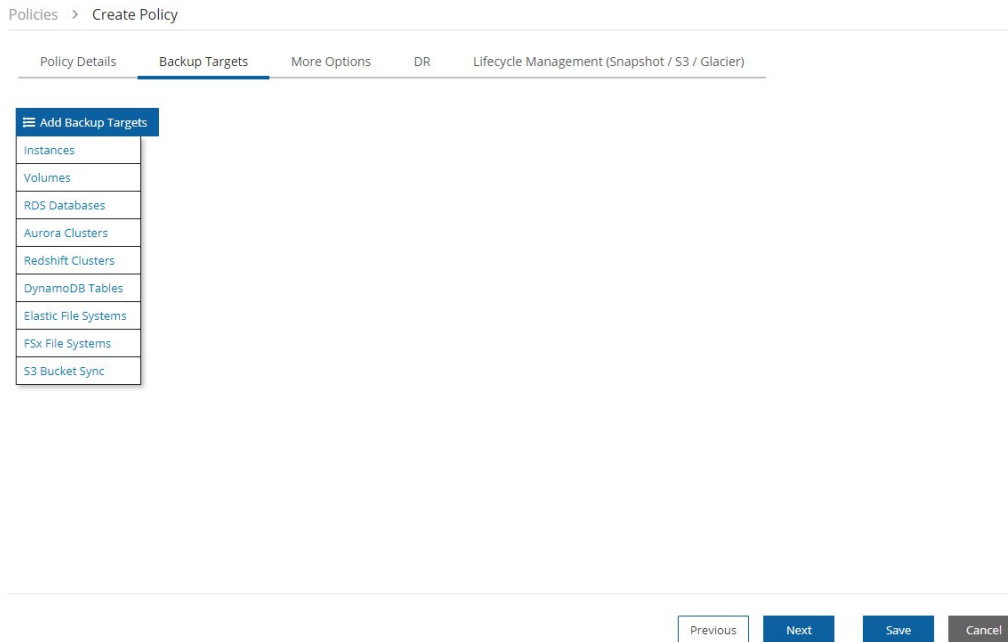
The screenshot shows the 'Create Policy' page in the AWS Backup console. The page is titled 'Policies > Create Policy' and has several tabs: 'Policy Details' (selected), 'Backup Targets', 'More Options', 'DR', and 'Lifecycle Management (Snapshot / S3 / Glacier)'. The form includes the following fields:

- Name:** An empty text input field.
- User:** A dropdown menu with 'demo' selected and a '+ New' link.
- Account:** A dropdown menu with 'ACCOUNT-1' selected and a '+ New' link.
- Enabled:** A checked checkbox.
- Schedules:** A dropdown menu with 'None' selected and a '+ New' link.
- Auto Target Removal:** A dropdown menu with 'No' selected.
- Description:** A large text area for entering a description.

At the bottom right, there are three buttons: 'Next' (blue), 'Save' (blue), and 'Cancel' (grey).

1. In the **Create Policy** page, enter a policy name and description. Other fields in this screen include:
 - **Account** – Each policy can be associated with one AWS account.
 - **Auto Target Removal** – Whether to auto-remove resources that no longer exist.
 - **Enabled** – By default, a policy is enabled.
 - **Schedules** – Select the schedule just created.
 - **Auto Target Removal** – Select from the list whether to automatically remove resources that no longer exist. If you enable this removal, if an instance is terminated, or an EBS volume deleted, the next backup will detect that and remove it from the policy. Choose **yes and alert** if you want the backup log to include a warning about such a removal.

- When finished, select **Save** and select the **Backup Targets** tab. Backup targets define what a policy is going to back up.



Following are the types of objects you can back up:

- **Instances** - Back up EC2 instances, including their metadata, and optionally some or all of their data volumes. This is the most common backup target.
- **Volumes** - Back up EBS volumes independently, whether or not they are attached to an instance, and regardless of which instance they are attached to. This can be useful to back up volumes that are not always attached to an instance, or volumes that move between instances, like cluster volumes.
- **RDS Databases** - Back up RDS DB instances. This will use RDS snapshots and can be useful for backing up RDS databases together with other types of objects, or for anyone who wishes to back up RDS databases using N2W, in addition to or instead of using AWS automatic backup.
- **Aurora Clusters** - Aurora is similar to RDS but handles Aurora clusters.
- **Redshift Clusters** - Manage Redshift Cluster snapshots.
- **DynamoDB Tables** - Back up DynamoDB Tables.

Elastic File Systems - Back up EFSs.

FSx File Systems - Back up FSx File Systems.

S3 Bucket Sync - Copy objects between S3 buckets.

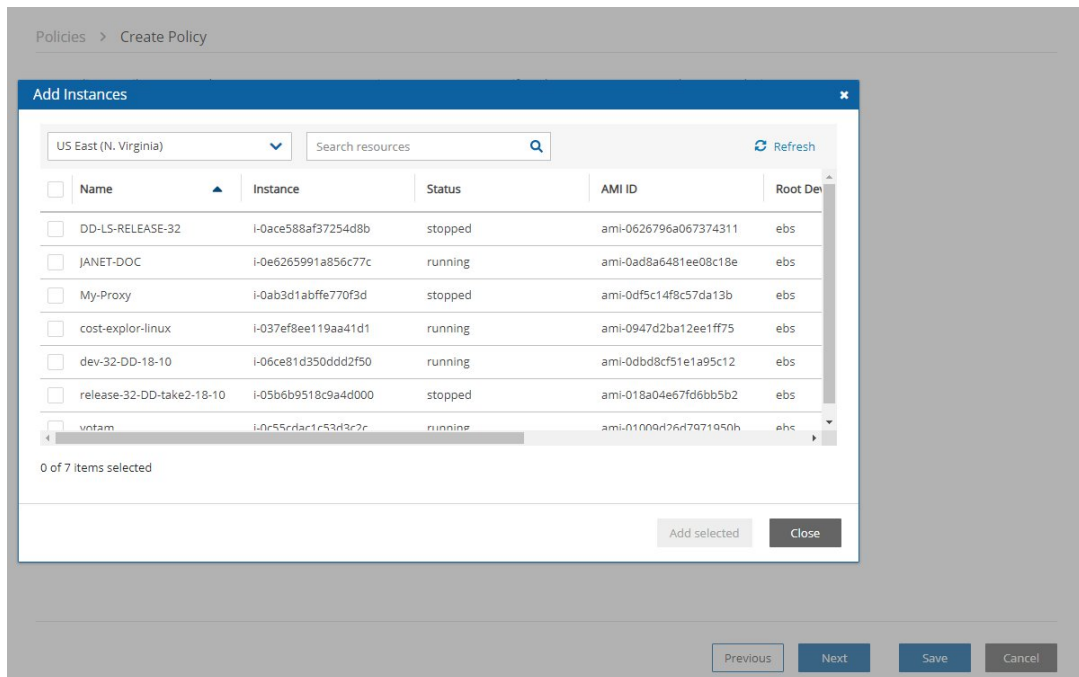
S3 Bucket - Backup S3 buckets to vault.

EKS - Backup EKS Clusters and Namespaces

To add an instance, for example, to the policy:

In the **Add Backup Targets** menu, select **Instances**. The list of instances you have in the region for the policy's account appears. The **Region** list allows you to switch between different regions. You can use the free text search, column-based sorting, or pagination if there are a lot of instances and you are seeking a specific one.

Note: Although you can add backup objects from different regions in the same policy, in many cases it is not good practice to do so.



Select the instance that you want to back up, and then select **Add Selected**. This will add the requested instance to the screen in the background and remove it from the popup window, although it does not close the popup. You can add as many instances as you want up to the limit of your licence. Select **Close** when finished.

Back in the **Backup Targets** screen, you can see the instance in the list of instances. You have the option to remove it from the policy and a **Configure** button. Select the instance, and then select **Configure** to review which volumes to back up and other options.

By default, all EBS volumes which are attached to this instance will be backed up. If a volume gets detached from or attached to the instance, it will not interfere with the normal operations of the policy. In every backup, N2W will check which volumes are attached to the instance and take snapshots of them.

To view the planned backups for this policy, select **Backup Times** in the Policies list. The backups will start automatically at the time configured previously in the schedule. If you want to initiate an immediate backup, select a policy, and then select **Run ASAP**.

Policies

Name	Account	Enabled	Backup Generations	Sched
<input type="checkbox"/> 23-RC	aaa	Yes	30	
<input type="checkbox"/> ccc	ccc	Yes	30	
<input type="checkbox"/> cpmdata	aaa	Yes	30	
<input type="checkbox"/> ins-s3	aaa	Yes	1	
<input type="checkbox"/> vol-dr	aaa	Yes	2	s1

0 of 5 items selected

N2W will report that the backup policy will now run. The process can be monitored by following the **Status** in the **Backup Monitor** tab.

Backup Monitor

Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle:
<input type="checkbox"/> Oct 25, 2020 2:12 PM		P1	ACCOUNT-1	In Progress		
<input type="checkbox"/> Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P3	ACCOUNT-3	Successful		Store
<input type="checkbox"/> Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/> Oct 25, 2020 11:03 AM	Oct 25, 2020 11:13 AM	P1	ACCOUNT-1	Successful		
<input type="checkbox"/> Oct 25, 2020 11:03 AM	Oct 25, 2020 11:04 AM	CPMDATA	ACCOUNT-1	Successful		
<input type="checkbox"/> Oct 24, 2020 2:43 PM	Oct 24, 2020 2:44 PM	P3	ACCOUNT-3	Successful		Delete
<input type="checkbox"/> Oct 24, 2020 1:37 PM	Oct 24, 2020 1:39 PM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/> Oct 24, 2020 1:37 PM	Oct 24, 2020 1:49 PM	P1	ACCOUNT-1	Successful		
<input type="checkbox"/> Oct 24, 2020 1:37 PM	Oct 24, 2020 1:37 PM	CPMDATA	ACCOUNT-1	Successful		
<input type="checkbox"/> Oct 22, 2020 8:22 AM	Oct 22, 2020 8:24 AM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/> Oct 22, 2020 8:21 AM	Oct 22, 2020 8:22 AM	P1	ACCOUNT-1	Successful		

0 of 11 items selected

Consult the *N2W Backup & Recovery User Guide* to see how to create application consistency for Linux and Windows servers.

5 Performing a Basic Recovery

You can view the backups in the **Backup Monitor** tab. You can search for snapshots based on the Backup Target type, Policy, Account, and backup status.

Backup Monitor

Recover
Log

Start Time
by instance
by volume
by RDS database
by Aurora cluster
by Redshift cluster
by DynamoDB table
by Elastic File System
by FSx File System
by S3 bucket sync
by policy/frozen item

Move to Freezer
Edit Frozen Item
Abort Copy to S3
Delete Frozen Item
Refresh

Policy / Frozen Item	Account	Status	DR Status	Lifecycle
ACCOUNT-3	ACCOUNT-3	Successful		
ACCOUNT-1	ACCOUNT-1	Successful		
ACCOUNT-3	ACCOUNT-3	Successful		Store
ACCOUNT-1	ACCOUNT-1	Successful	Completed	
ACCOUNT-1	ACCOUNT-1	Successful		
CPMDATA	ACCOUNT-1	Successful		
P2	ACCOUNT-1	Successful	Completed	
P2	ACCOUNT-1	Successful	Completed	

1 of 8 items selected

For each backup, you can see the exact start and finish times, and status. Select **View Snapshots** to see the individual EBS snapshots of all the volumes. Select **Log** to view the log of this backup with all the details. To recover from a particular backup (typically the most recent successful backup), select the backup, and then select **Recover**:

Backup Monitor

Recover
Log
View Snapshots
Move to Freezer
Edit Frozen Item
Delete Frozen Item
Abort Copy to Storage Repository

Show: 10
Clear Filters

Start Time	Finish Time	Policy / Frozen Item	User	Account	Cloud	Status	DR Status	Lifecycle Status
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:01 AM	ZeroEBS	admin	AWS_Account1	AWS	All Snapshots Dele...	Completed	Stored in Storage Repository
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:01 AM	Linux_Servers	admin	AWS_Account1	AWS	Successful	Completed	
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:01 AM	Windows_Servers	admin	AWS_Account1	AWS	Successful	Completed	Stored in Storage Repository
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:00 AM	EFS	admin	AWS_Account1	AWS	Successful		
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:04 AM	MySQL_RDS	admin	AWS_Account1	AWS	Successful	Completed	
Jun 3, 2024 12:00 AM	Jun 3, 2024 12:00 AM	Azure_VM	admin	AzureDemoAccount	Azure	Successful		
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:01 AM	Linux_Servers	admin	AWS_Account1	AWS	Successful	Completed	
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:01 AM	Windows_Servers	admin	AWS_Account1	AWS	Successful	Completed	Stored in Storage Repository
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:02 AM	ZeroEBS	admin	AWS_Account1	AWS	All Snapshots Dele...	Completed	Stored in Storage Repository
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:00 AM	EFS	admin	AWS_Account1	AWS	Successful		
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:00 AM	Azure_VM	admin	AzureDemoAccount	Azure	Successful		
Jun 2, 2024 12:00 AM	Jun 2, 2024 12:02 AM	MySQL_RDS	admin	AWS_Account1	AWS	Successful	Completed	
Jun 1, 2024 12:00 AM	Jun 1, 2024 12:01 AM	ZeroEBS	admin	AWS_Account1	AWS	All Snapshots Dele...	Completed	Stored in Storage Repository
Jun 1, 2024 12:00 AM	Jun 1, 2024 12:01 AM	Linux_Servers	admin	AWS_Account1	AWS	Successful	Completed	
Jun 1, 2024 12:00 AM	Jun 1, 2024 12:01 AM	Windows_Servers	admin	AWS_Account1	AWS	Successful	Completed	Stored in Storage Repository
Jun 1, 2024 12:00 AM	Jun 1, 2024 12:02 AM	MySQL_RDS	admin	AWS_Account1	AWS	Successful	Completed	

0 of 98 items selected

Page 1 of 5

Displaying 1 - 20 of 98

In the **Recover** screen, you can see all the instances that this backup contains. Should this policy include also EBS volumes, RDS databases, Redshift Clusters, or DynamoDB Tables, you will have a tab to recover them as well. In order to recover an instance, select the **Instances** tab.

Backup Monitor > P1 - 10/25/2020 2:12 PM > Recover

Search by Resource: Restore From: Original Account (ACCOUNT-1) Restore to Account: Same as Snapshot (ACCOUNT-1) Restore to Region: Origin

Instances

Recover Recover Volumes Only Explore

Name	ID	Region	Image ID	Root Device	Platform
<input checked="" type="radio"/> cost-explor-linux	i-037ef8ee119aa41d1	US East (N. Virginia)	ami-0947d2ba12ee1ff75	/dev/xvda	Unix / Linux
<input type="radio"/> 310-milan-CPM	i-0d93e780248d9f1c4	EU (Milan)	ami-03d09fd20a7752f5c	/dev/sda1	Unix / Linux

Note: **Recover Volumes Only** is for recovering only the EBS volumes of the instance without creating a new instance.

Select the instance to recover and select **Recover** again. The **Basic Options** tab of the **Instance Recovery** page opens. You can enlarge the page by selecting in the upper right corner.

Instance Recovery

AMI Assistant

Basic Options Volumes Advanced Options

Launch from: Snapshot AMI Handling: Deregister after Recovery Image ID: ami-0df5c14f8c57da13b

Instance Type: t2.micro Instance Profile ARN: arn:aws:iam::774583829984:instance-profil Instances to Launch: 1

Key Pair: No Key Pair

Networking

Placement: By VPC

VPC: vpc-5d093327 (default) **Clone VPC**

AWS Credentials: Use account AWS Credentials

Recover Instance Close

Most of the options when launching EC2 instances are available here and may be modified. The currently selected defaults are exactly the options the original backed-up instance had at the time of the backup, including the tags associated with it.

A further option worth mentioning here is **Launch from**. This sets the option for the image the new instance will be launched from. In case of an instance-store-based instance, the only option would be to launch from an image. The default will be the original image, although it can be changed. In case it is a Linux EBS-based instance, as in this example, and the backup includes the snapshot of the boot device, you can choose between launching from an image (the original image or another), and launching from the snapshot, which is the default.

If you choose to launch from a snapshot, a new image (AMI) will be created, and you can choose whether you want to keep the image after the recovery is complete or deregister it. You can even choose not to perform the recovery now, and only create the image, to recover from it later.

Select **Recover Instance** to recover an instance exactly like the original one.

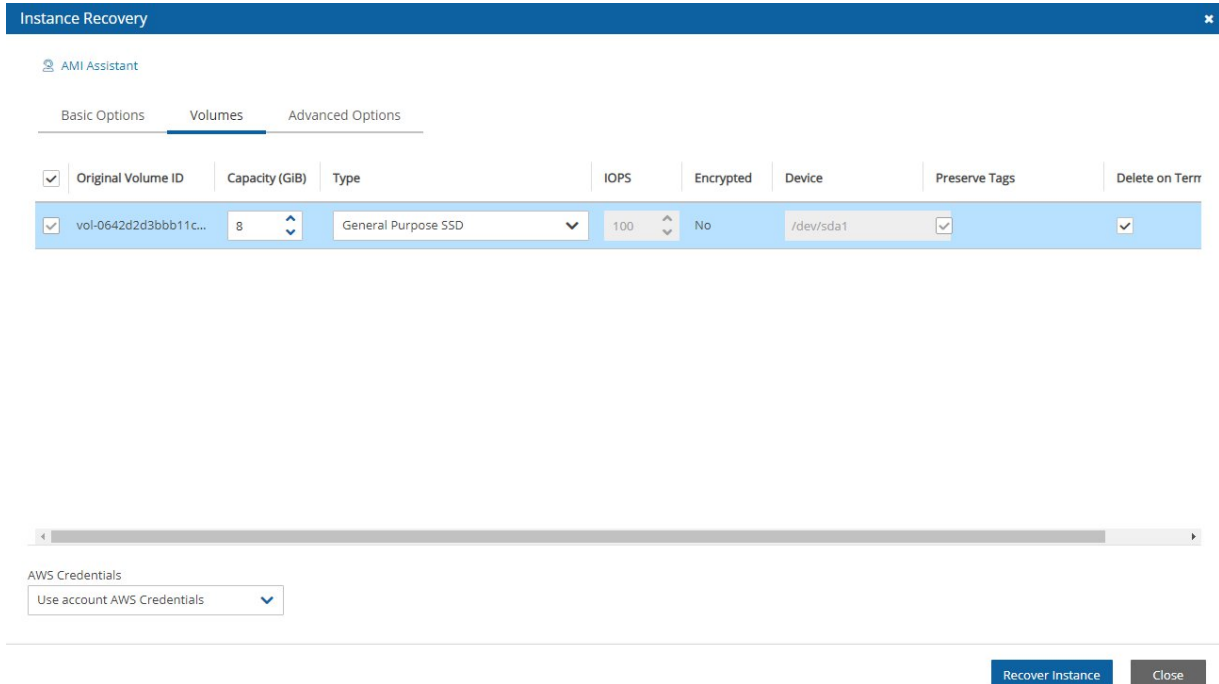
For paid editions, if Capture VPCs were enabled in the **Account** settings, the **Basic Options** tab will also contain a **Clone VPC** button next to the **VPC** box.



The **Clone VPC** option allows you to recover the instance to a clone of a selected VPC environment. See <https://docs.n2ws.com/user-guide/10-performing-recovery>

Important: If you intend to test the recovery of an instance in the same region as the instance that was originally backed up, you will need to change the IP to avoid an IP conflict. This can be mitigated by leaving the **VPC Assign IP** box blank.

Select the **Volumes** tab to choose which volumes to recover and how.



Select the **Advanced Options** tab for additional recovery parameters.

Instance Recovery ✕

AMI Assistant

Basic Options Volumes **Advanced Options**

Architecture:

Shutdown Behaviour:

Auto-assign Public IP:

Kernel:

Preserve Tags

AWS Credentials:

Tenancy:

API Termination:

RAM Disk:

Recover Instance
Close

After you select **Recover Instance** and confirm, you will be directed to the Recovery Monitor page where you can follow progress in the **Status** column. You can view recovery details by selecting **Log**.

Recovery Monitor ✔ Recovery Started
[\(Open Recovery Monitor\)](#)

All Policies
All Accounts
All Recovery Statuses
Not Filtered by Scenario Run
20 records/page

↻ Recover Again
📄 Log
🗑️ Abort Recover from S3
🗑️ Delete Record
🔄 Refresh

<input type="checkbox"/>	Recovery Time	Backup Time	Recovery Type	Original Resource ID	Policy	Account	Status
<input type="checkbox"/>	Oct 26, 2020 11:24 PM	Oct 26, 2020 10:12 PM	Volume	vol-0d62e0cc15dfd5...	P3	ACCOUNT-3	🔄 Initializing recovery
<input type="checkbox"/>	Oct 25, 2020 10:54 PM	Oct 25, 2020 3:52 PM	FSx	fs-083362023b7894f...	fsx	ACCOUNT-3	✔ Recovery succeeded

0 of 2 items selected

The log message will include the instance ID of the new instance, and now you can go and verify the successful recovery in the AWS Management Console. The recovered instance is the same as the original one, with all its EBS volumes.

6 How to Configure N2W with CloudFormation

The process of configuring N2W to work with CloudFormation is a single stream that starts with subscribing to N2W on the Amazon Marketplace and ends with configuring the N2W server.

Note:

- N2W provides several editions, all of which support CloudFormation.
- An IAM role will automatically be created with minimal permissions and assigned to the N2W instance.

1. Go to <https://aws.amazon.com/marketplace>
2. Search for N2W.
3. Select **Continue to Subscribe**.

N2WS Backup & Recovery for AWS Free Trial/BYOL

Continue to Launch

< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option
CloudFormation Template
CloudFormation Template
Deploy a complete solution configuration using a CloudFormation template

N2WS Backup & Recovery Free Trial & BYOL (CFT)

Software version
4.3.0 (Jun 03, 2024)
Whats in This Version
N2WS Backup & Recovery for AWS Free Trial/BYOL running on t2.small
Learn more

Region
US East (N. Virginia)

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Product Code: 17p1fh23ueq6b2b9xg6d8jwok
Release notes (updated June 3, 2024)

Pricing information
This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing
N2WS Backup & Recovery for AWS Free Trial/BYOL running on t2.small \$0 /hr

4. Log in and select **Accept Terms**.

N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition

Continue to Configuration

< Product Detail Subscribe

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

N2W Software Offer

5. Select **Configure to Configuration**.

N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition

Continue to Launch
You must first configure the software.

< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option

Select a fulfillment option ▼

- Amazon Machine Image**
Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2
- CloudFormation Template**
Deploy a complete solution configuration using a CloudFormation template

Pricing information

Choose and configure a delivery method to see an estimate of typical software and infrastructure costs.

6. In the **Fulfillment Option** drop-down list, select **CloudFormation Template**.

N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition

Continue to Launch

< Product Detail Subscribe Configure

Configure this software

Choose a fulfillment option below to select how you wish to deploy the software, then enter the information required to configure the deployment.

Fulfillment Option

CloudFormation Template ▼

Cloud Protection Manager Free Trial & BYOL (CFT) ▼

CloudFormation Template
Deploy a complete solution configuration using a CloudFormation template

Software Version

4.3.0 Jun 03, 2024 ▼

Whats in This Version
N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition
running on t3.medium
[Learn more](#)

Pricing information

This is an estimate of typical software and infrastructure costs based on your configuration. Your actual charges for each statement period may differ from this estimate.

Software Pricing

N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition	\$0/hr
--	--------

BYOL
running on t3.medium

7. Select the relevant **Software Version** and then select **Continue to Launch**.



[< Product Detail](#) [Subscribe](#) [Configure](#) [Launch](#)

Launch this software

Review your configuration and choose how you wish to launch the software.

Configuration Details

Fulfillment Option	Cloud Protection Manager Free Trial & BYOL (CFT) N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition <i>running on t3.medium</i>
Software Version	4.3.0
Region	US East (N. Virginia)

Usage Instructions

Choose Action

Launch CloudFormation ▼

Choose this action to launch your configuration through the AWS CloudFormation console.

Launch

- In the **Launch this software** page, select **Launch CloudFormation** in the **Choose Action** list, and then select **Launch**.

The **Create stack/Select Template** page opens.

- Under **Prepare template**, select **Choose an existing template**.
- Under **Specify template**, choose **Amazon S3 URL**. Select the default Amazon S3 URL, and then select **Next**. The **Specify stack details** page opens.

Step 1
● Create stack

Step 2
○ Configure stack options

**Step 3
● Specify stack details**

Step 4
○ Review and create

Specify stack details

Provide a stack name

Stack name

Stack name must contain only letters (a-z, A-Z), numbers (0-9) and hyphens (-) and start with a letter. Max 128 characters. Character count: 0/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

Instance Configuration

Instance Type

Instance type for NZWS

AMI ID

This is the alias of the Marketplace AMI that will be deployed as part of this stack. Ensure this parameter is set to the following value: /aws/service/marketplace/prod-4cylolqzfg/4.4.1.

Networking and Security Configuration

Key Pair

Name of an existing EC2 KeyPair

VPC

The VPC in which you want to Launch NZWS

Subnet

SubnetId in VPC

Inbound Access CIDR

CIDR for Security Groups source IP

Cancel Previous Next

11. Complete the **Stack Details** and **Parameters**. For **Inbound Access CIDR**, security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. Configuring **Inbound Access CIDR** allows you to add rules to a security group that enable you to connect to your Linux instance from your IP address using SSH:

- If your IPv4 address is 203.0.113.25, specify 203.0.113.25/32 to list this single IPv4 address in CIDR notation. If your company allocates addresses within a range, specify the entire range, such as 203.0.113.0/24.
- If you specify 0.0.0.0/0, it will enable all IPv4 addresses to access your instance using SSH.
- For further details, refer to “Adding a Rule for Inbound SSH Traffic to a Linux Instance” at <https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/authorizing-access-to-an-instance.html>

12. Select Next. The Options page opens.

Step 1 Create stack
Step 2 Specify stack details
Step 3 **Configure stack options**
Step 4 Review and create

Configure stack options

Tags - optional
Tags (key-value pairs) are used to apply metadata to AWS resources, which can help in organising, identifying and categorising those resources. You can add up to 50 unique tags for each stack.
No tags associated with the stack.
[Add new tag](#)
You can add 50 more tag(s)

Permissions - optional
Specify an existing AWS Identity and Access Management (IAM) service role that CloudFormation can assume.
IAM role - optional
Choose the IAM role for CloudFormation to use for all operations performed on the stack.
IAM role name [Remove](#) [+](#)

Stack failure options
Behaviour on provisioning failure
Specify the roll-back behaviour for a stack failure. [Learn more](#)
 Roll back all stack resources
Roll back the stack to the last known stable state.
 Preserve successfully provisioned resources
Preserves the state of successfully provisioned resources, while rolling back failed resources to the last known stable state. Resources without a last known stable state will be deleted upon the next stack operation.
Delete newly created resources during a rollback
Specify whether resources that were created during a failed operation should be deleted regardless of their deletion policy. [Learn more](#)
 Use deletion policy
Retains or deletes created resources according to their attached deletion policy.
 Delete all newly created resources
Deletes created resources during a rollback regardless of their attached deletion policy.

Additional settings
You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

▶ **Stack policy - optional**
Defines the resources that you want to protect from unintentional updates during a stack update.

▶ **Rollback configuration - optional**
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

▶ **Notification options - optional**
Specify a new or existing Amazon Simple Notification Service topic where notifications about stack events are sent.

13. Complete the stack options and select Next. The Review page opens.

Additional settings
You can set additional options for your stack, like notification options and a stack policy. [Learn more](#)

▶ **Stack policy - optional**
Defines the resources that you want to protect from unintentional updates during a stack update.

▶ **Rollback configuration - optional**
Specify alarms for CloudFormation to monitor when creating and updating the stack. If the operation breaches an alarm threshold, CloudFormation rolls it back.

▶ **Notification options - optional**
Specify a new or existing Amazon Simple Notification Service topic where notifications about stack events are sent.

▶ **Stack creation options - optional**
Specify the timeout and termination protection options for stack creation.

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources.

[Cancel](#) [Previous](#) [Next](#)

The following resource(s) require capabilities: [AWS::IAM::Role]
This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. [Learn more](#)

I acknowledge that AWS CloudFormation might create IAM resources.

[Cancel](#) [Previous](#) [Create change set](#) [Create stack](#)

14. Select the I acknowledge that AWS CloudFormation might create IAM resources check box, and then select Create stack. The CloudFormation Stacks page opens.

15. Select the new stack. The Instances page opens.

16. Select the instance. Copy the **Instance ID** value shown in the **Description** tab, and then select **Launch Instance**. The **N2W Server Configuration** page opens.
17. Now, you can continue from section 3.

7 Using Azure with N2W

Following are the steps for setup, backup, and recovery of Azure VMs, SQL Servers, and Disks:

1. Before starting, configure N2W Backup and Recovery according to [Configuring N2W](#).
2. After the final configuration screen, prepare your Azure Subscription by adding the required permissions and custom IAM role in AWS. See section [7.1](#).
3. In N2W, add an Azure account with the custom N2W role. See section [7.2](#).
4. Create an Azure policy in N2W with Azure backup targets. See section [7.3](#).
5. Back up the policy. See section [7.4](#).
6. Recover from a backup. See section [7.5](#).

7.1 Setting Up Your Azure Subscription

N2W Backup and Recovery need the following permissions to perform backup and recovery actions. In addition, see <https://n2ws.zendesk.com/hc/en-us/articles/28833036917021-Required-Minimum-Azure-permissions-for-N2W-operations>

1. Save the following text in a JSON file, adding your Subscription ID value to the “subscriptions” attribute:

```
{
  "properties": {
    "roleName": "CPM",
    "description": "",
    "assignableScopes": [
      "/subscriptions/<subscriptionID>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/virtualMachines/read",
          "Microsoft.Compute/disks/read",
          "Microsoft.Compute/snapshots/write",
          "Microsoft.Network/networkInterfaces/read",
          "Microsoft.Compute/snapshots/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Compute/disks/write",
          "Microsoft.Compute/snapshots/delete",
          "Microsoft.Resources/subscriptions/resourceGroups/delete",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/read",
          "Microsoft.Network/networkInterfaces/write",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Network/networkInterfaces/join/action",
          "Microsoft.Compute/virtualMachines/write",
          "Microsoft.Compute/diskEncryptionSets/read",
          "Microsoft.Compute/virtualMachines/powerOff/action",
          "Microsoft.Compute/virtualMachines/start/action",
          "Microsoft.Compute/availabilitySets/read",
          "Microsoft.Compute/availabilitySets/vmSizes/read"
        ],
        "notActions": [],
        "dataActions": []
      }
    ]
  }
}
```

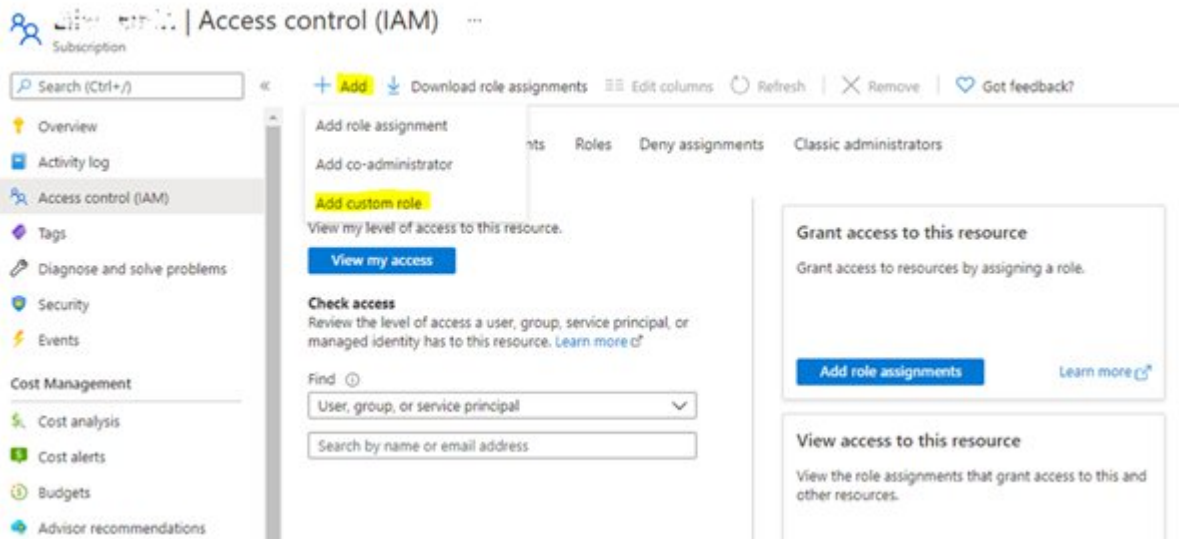
```
"notDataActions": []  
  }  
] }  
}
```

2. In the Azure Portal, go to your subscription and select a subscription that you want to use




with N2W Backup & Recovery. [Subscriptions](#)

3. Select **Access control (IAM)**, select **+Add**, and then select **Add custom role**.



4. Complete the form as follows using **N2WSBackupRecoveryRole** as the **Custom role name**, and then select the JSON file saved in step 1.

Create a custom role ...

 Got feedback?


[Basics](#) [Permissions](#) [Assignable scopes](#) [JSON](#) [Review + create](#)

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

* Custom role name ✓

Description

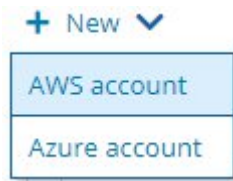
Baseline permissions Clone a role Start from scratch Start from JSON



5. Create the role with the new JSON file.

7.2 Adding an Azure Account to N2W

1. Log on to N2W using the root username and password used during the N2W configuration.
2. Select the **Accounts** tab.
3. If you have a license for Azure cloud, select **Azure account** in the **+ New** menu.



4. Complete the New Azure Account screen using the App Registration view information in the Azure portal as needed.

Accounts > New Azure Account

Name

User + New ▼ ↻

Directory (tenant) ID

Application (client) ID

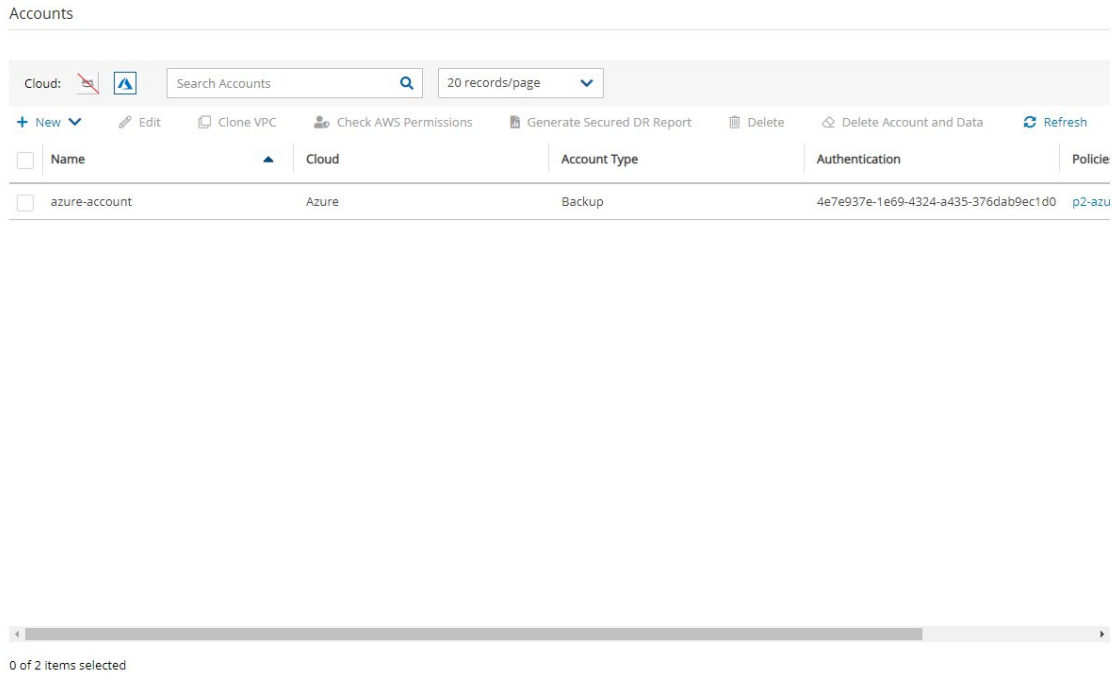
Client Secret

Scan Resources

Save Cancel

- **Name** - Copy from your App Registration name.
- In the **User** list, select your username. Or select **+ New** to add a new user. See section 18 in the *N2W Backup & Recovery User Guide*.
- **Directory (tenant) ID** - Copy from your App Registration.
- **Application (client) ID** - Copy from your App Registration.
- **Client Secret** - Copy from your App registration Certificates & Secrets in the App Registration view, or set a new secret.

5. Select **Save**. The new account appears in the Accounts list as an Azure Cloud account.



7.3 Creating an Azure 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.

- 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 ▼

Search resources 🔍

↻ Refresh

<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

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	Disk
<input type="checkbox"/>	linux-ubuntu-europe_disk1...	Reserved	northeurope	first-rg	30 GIB	St...

0 of 1 items selected

Previous
Save
Cancel

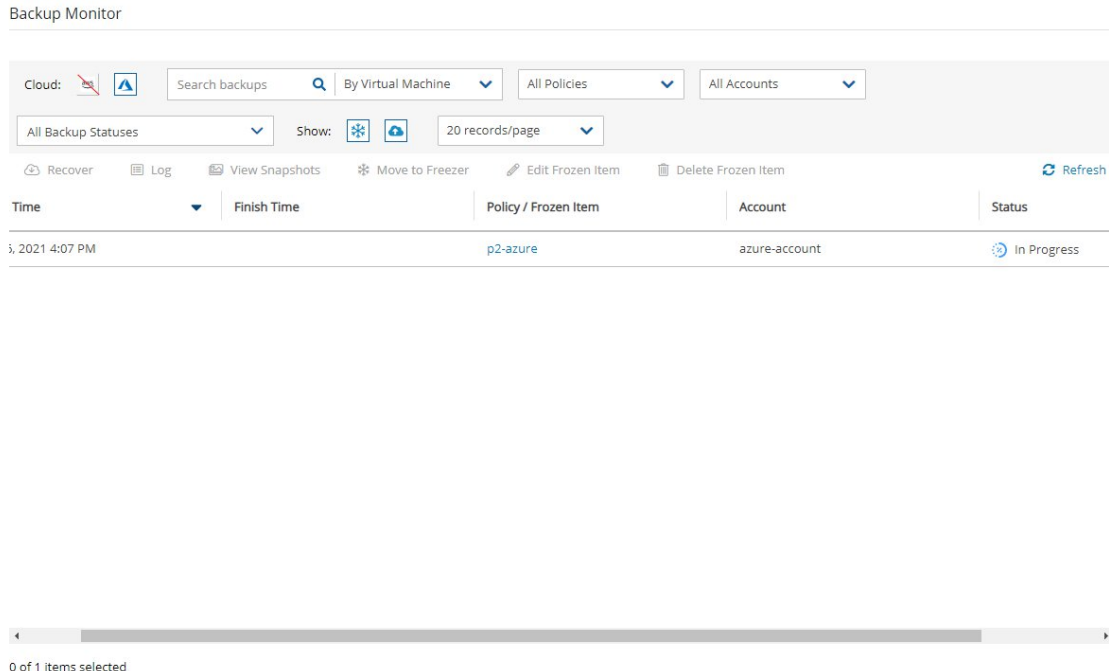
- To determine which disks for each Virtual Machines target to back up, select **Configure**. In the **Which Disks** list of the Policy Virtual Machine and Disk Configuration screen, select the disks to include or exclude in the backup.
- When finished, in the **Backup Targets** tab, select **Save**.



7.4 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
3/21/2021 4:07 PM		p2-azure	azure-account	 In Progress

0 of 1 items selected

7.5 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 in order 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.

7.5.1 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	Succes
<input type="checkbox"/>	Apr 6, 2021 7:05 PM	Apr 6, 2021 7:05 PM	p2-azure	azure-account	Succes
<input type="checkbox"/>	Apr 6, 2021 6:54 PM	Apr 6, 2021 6:54 PM	p2-azure	azure-account	Succes
<input checked="" type="checkbox"/>	Apr 6, 2021 4:07 PM	Apr 6, 2021 4:07 PM	p2-azure	azure-account	Succes

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

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**.
 - a. 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
 No Infrastructure Redundancy Required
 Availability Zone
 Availability Set


Virtual Network
FIRST-RG-vnet

Subnet
default

Private IP Address
 Auto assigned

Preserve Tags

Recover Virtual Machine Close

- b. 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.
 - c. In the **Private IP Address** box, assign an available IP address or switch the **Custom** toggle key to **Auto assigned**.
 - d. In the **Disks** tab, enter a new **Name** for each disk. Similar names will cause the recovery to fail.
 - e. 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.

7.5.2 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:
 - a. Enter a new **Name** for each disk to recover as similar names will cause failure.

- b. See Note in section 7 about changing the **Encryption Set** for certain disks.
- c. 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"/>

[Recover Disk](#) [Close](#)

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

Appendix A – AWS Authentication

For N2W to perform its backup and restore management functions, it needs to have the correct permissions assigned.

N2W supports two different types of AWS authentication during setup:

- AccessKey / SecretKey
- Role based authentication (recommended)

The permissions necessary have been combined into a JSON file for convenience and can be downloaded from the N2W Knowledge Base:

1. <https://n2ws.zendesk.com/hc/en-us/articles/28832964188573-Required-Minimum-AWS-IAM-permissions-for-N2W-operations>

At the top of your AWS console, select the **Services** tab. In the **Security Identity & Compliance** section, select **IAM**.

2. In the left menu, select **Policies**.

3. Select the **Create policy** button.

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	↻
AdministratorAccess	AWS managed - job function	Permissions policy (4)	↻
AdministratorAccess-Amplify	AWS managed	None	↻
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	↻
AIQOpsAssistantPolicy	AWS managed	None	↻

4. Select the **JSON** tab.

5. Delete the default contents and copy and paste the contents of the JSON file downloaded from our Knowledge Base (see above).

Step 1
Specify permissions
Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Visual | **JSON** | Actions

```

1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Sid": "Statement1",
6       "Effect": "Allow",
7       "Action": [],
8       "Resource": []
9     }
10  ]
11 }

```

+ Add new statement

JSON Ln 11, Col 1

6042 of 6144 characters remaining

6. At the bottom of the screen, select **Next**.

7. Type a **Name** for the policy and select **Create policy**.

Step 1
Specify permissions
Step 2
Review and create

Review and create Info

Review the permissions, specify details, and tags.

Policy details

Policy name
Enter a meaningful name to identify this policy.

Maximum 128 characters. Use alphanumeric and '+*=@_-' characters.

Description - optional
Add a short explanation for this policy.

Maximum 1,000 characters. Use alphanumeric and '+*=@_-' characters.

8. Create a role, and then assign the policy you just created to that role. In the left menu, select **Roles** and then select **Create role**.

Identity and Access Management (IAM)

Roles (36) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Search IAM

Dashboard

<input type="checkbox"/>	Role name	Trusted entities	Last activity
<input type="checkbox"/>	AmazonSSMRoleForInstancesQuickSetup	AWS Service: ec2	18 days ago

Delete Create role

9. In the list of **type of trusted entity**, select **AWS service** and then select **EC2**.

10. Select **Next: Permissions**.

Trusted entity type

- AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

- EC2**
Allows EC2 instances to call AWS services on your behalf.
- EC2 Role for AWS Systems Manager**
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
- EC2 Spot Fleet Role**
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
- EC2 - Spot Fleet Auto Scaling**
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
- EC2 - Spot Fleet Tagging**
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
- EC2 - Spot Instances**
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
- EC2 - Spot Fleet**
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
- EC2 - Scheduled Instances**
Allows EC2 Scheduled Instances to manage instances on your behalf.

11. On the **Add Permissions** page, search for the 3 previously created polices and then select **Next**

Step 1: Select trusted entity
Step 2: **Add permissions**
Step 3: Name, review, and create

Add permissions

Permissions policies (1078)

Choose one or more policies to attach to your new role.

Filter by Type: All types (3 matches)

Policy name	Type	Description
N2WS_Policy1	Customer managed	-
N2WS_Policy2	Customer managed	-
N2WS_Policy3	Customer managed	-

Set permissions boundary - optional

Cancel Previous **Next**

12. Name the **Role** and select **Create Role**.

Step 1: Select trusted entities
Step 2: Add permissions
Step 3: **Name, review, and create**

Name, review, and create

Role details

Role name
Enter a meaningful name to identify this role.
Maximum 64 characters. Use alphanumeric and "+, @, -" characters.

Description
Add a short explanation for this role.
Allows EC2 instances to call AWS services on your behalf.
Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: "_", "+", "@", ":", "!", "#", "\$", "%", "&";

Step 1: Select trusted entities Edit

13. Assign the resulting role to the N2W trial instance:

- e. Select the N2W instance name.
- f. In the **Actions** menu, select **Instance Settings** and then **Attach/Replace IAM Role**.

Instances (1/1) Info Last updated less than a minute ago [Refresh](#) [Connect](#) [Instance state](#) [Actions](#) [Launch instances](#)

Running

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS	Public IPv4
<input checked="" type="checkbox"/> N2W_4.4.1	i-06dce863eef142c8b	Running	t3.medium	3/3 checks passed	View alarms	eu-west-2a		

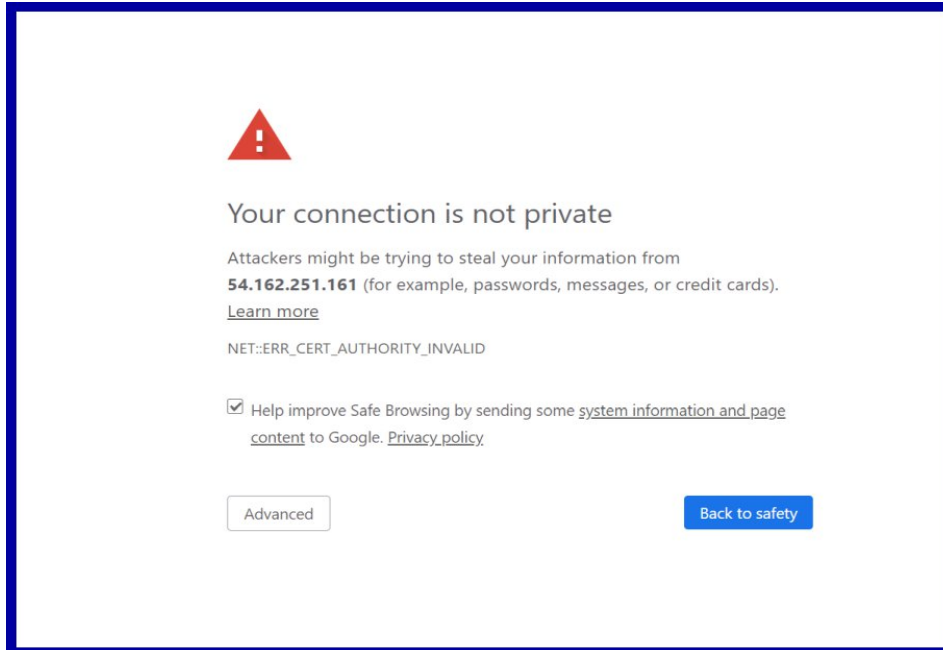
- Change security groups
- Get Windows password
- Modify IAM role


- Instance diagnostics
- Instance settings
- Networking
- Security
- Image and templates
- Monitor and troubleshoot

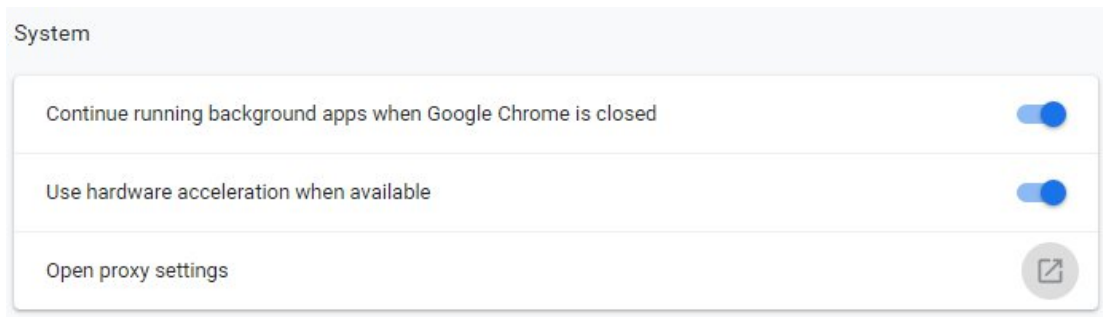
Appendix B – Adding Exception for Default Browser

For Chrome

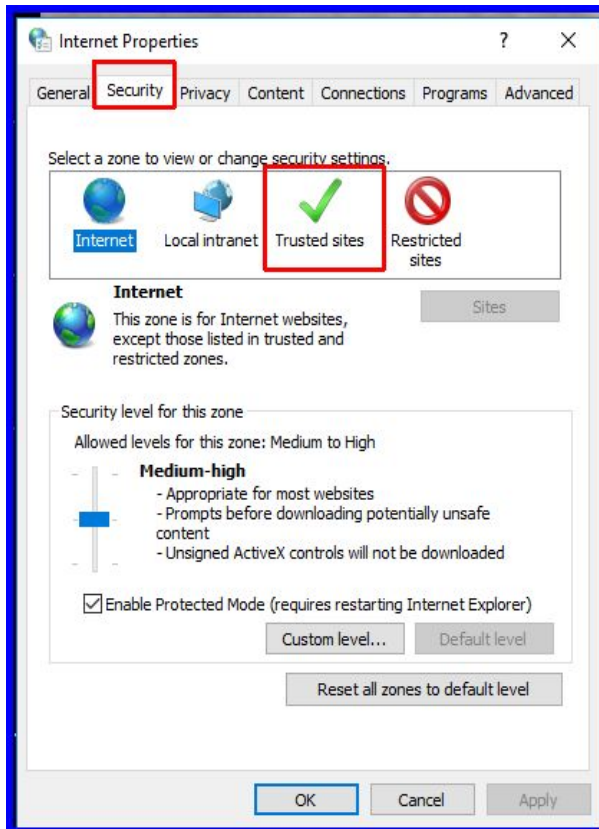
When you first navigate to your N2W instance, you'll see a screen like this. It's nothing to worry about. We are SSL secure but because it is a self-signed certificate, you may want to add an exception to your browser following these steps.



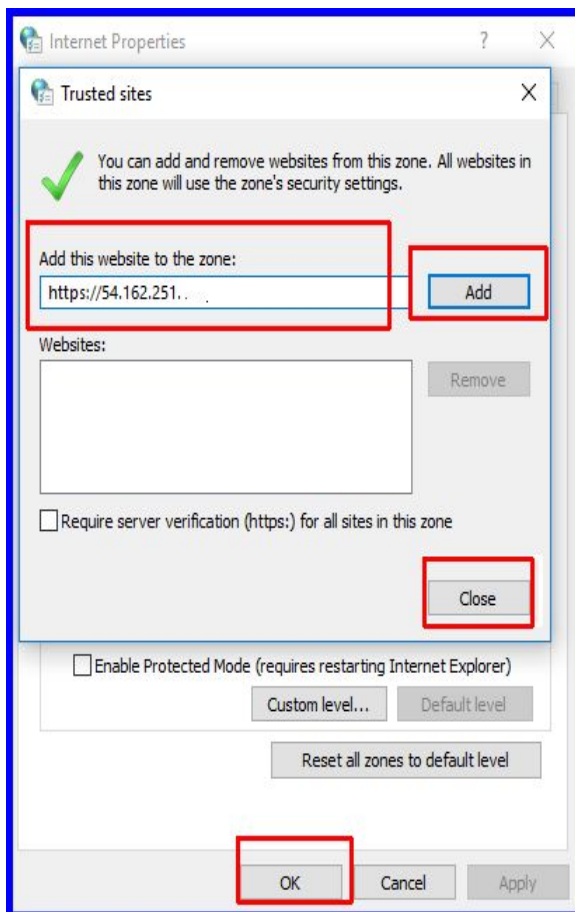
1. Open the Chrome browser. In the top right, select **More** .
2. Select **Settings, Advanced**, and then in the **System** section, select **Open proxy settings**.



3. Choose the **Security** tab and then select **Trusted Sites**.



4. Select the **Sites** button.
5. Type the N2W server's IP address in the **Add this website to the zone** box and then select **Add**, **Close**, and **OK**.



You should not get the warning on the certificate again.

For Firefox

The example is from Firefox Quantum.

1. Select **Advanced** (1)
2. Select **Add Exception** for this server (2).

