N2W Backup & Recovery

Quick Start Guide for AWS

Version 5.0.2

docs.n2ws.com

Contents

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 Connecting to the N2W Server 7

3.4 N2W Server Configuration Wizard 7

4. Creating a Simple Backup Policy 16

4.1 Adding an AWS Account 16

4.2 Creating a Simple Backup Schedule 17

4.3 Creating a Simple AWS Backup Policy 19

5. Performing a Basic Recovery 23

6. How to Configure N2W with CloudFormation 27

Appendix A – AWS Authentication 31

Appendix B – Adding an Exception for the Default Browser 35

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 to make backup and recovery worry-free. This Quick Start Guide walks you through the core steps to get N2W up and running.

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

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

2 Launching N2W Backup & Recovery

You have two options to launch: the 8 steps below, or CloudFormation.

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

1. Go to aws.amazon.com/marketplace.
2. Search for **n2w**.
3. Select your edition of **N2W Backup & Recovery (CPM)**.
4. Select **Continue to Subscribe**.
5. On 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**, and continue with 3.2 Creating an Instance When Launching through EC2.

2.1 Launching with CloudFormation

CloudFormation is an AWS service that lets you treat a collection of AWS resources as one logical unit. It provides a common language 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 automatically contains the required permissions for N2W operations.

To configure N2W using CloudFormation, see section 6.

3 N2W Server Instance Configuration

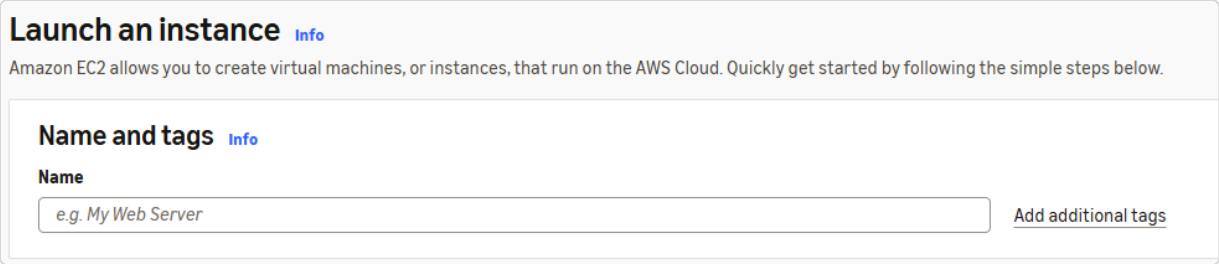
3.1 N2W Server Instance Connectivity

For the configuration process and N2W's normal operations to work, N2W must be able to talk to AWS APIs, so it needs outbound connectivity to the internet. Verify that the N2W instance has internet connectivity. You can achieve this by placing the instance in a public subnet with a public IP address, assigning an Elastic IP to the instance, using a NAT instance, or using an Internet Gateway.

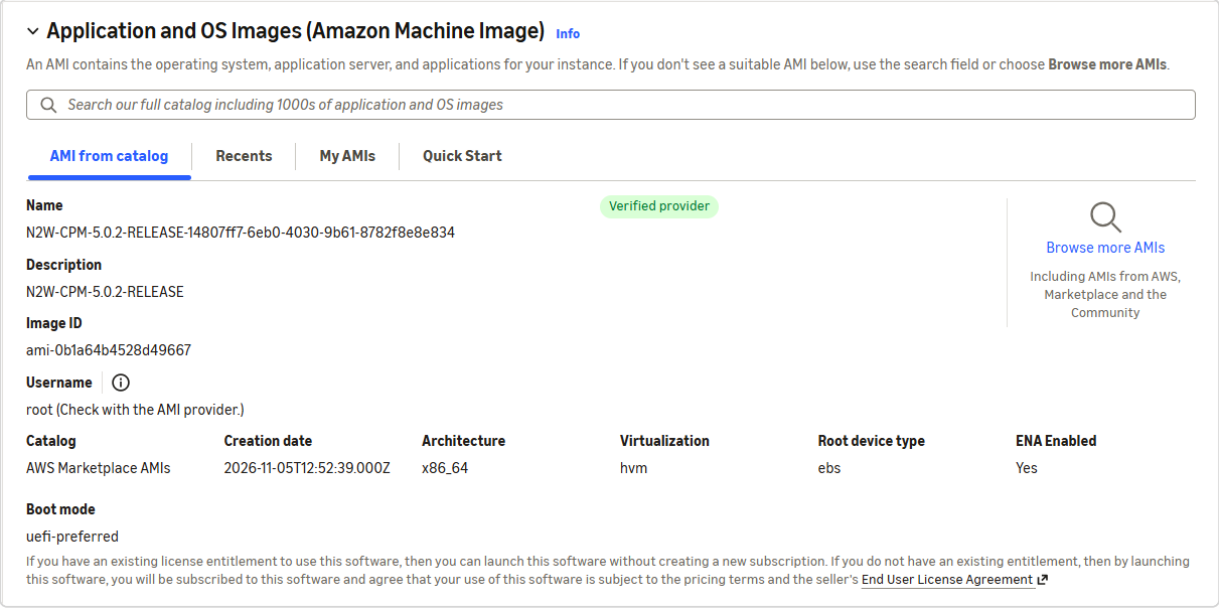
Also make sure DNS is configured properly, and that HTTPS is open for outbound traffic in the VPC security group settings (it is by default).

3.2 Creating an Instance When Launching through EC2

1. Under **Name and tags**, enter a name for your instance in the **Name** box. If required, select **Add additional tags**.

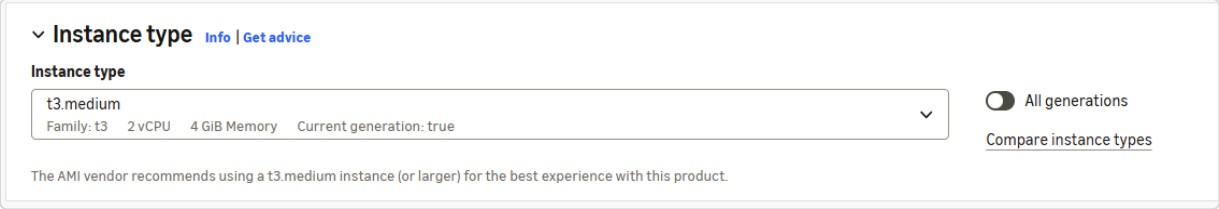


2. Under **Application and OS images (Amazon Machine Image)**, leave all default values. This section shows the AMI used for the EC2 instance image.

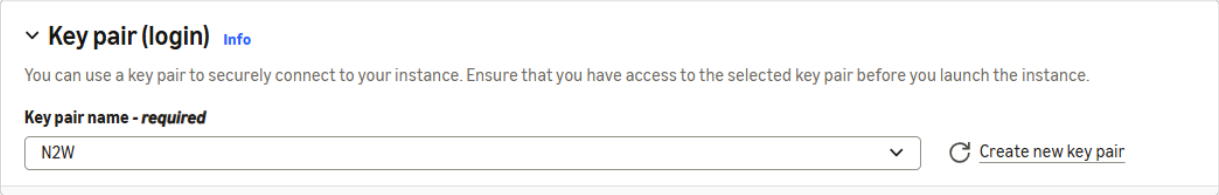


3. Under **Instance type**, the recommended minimum size is **t3.medium**. Larger environments may need a larger type.

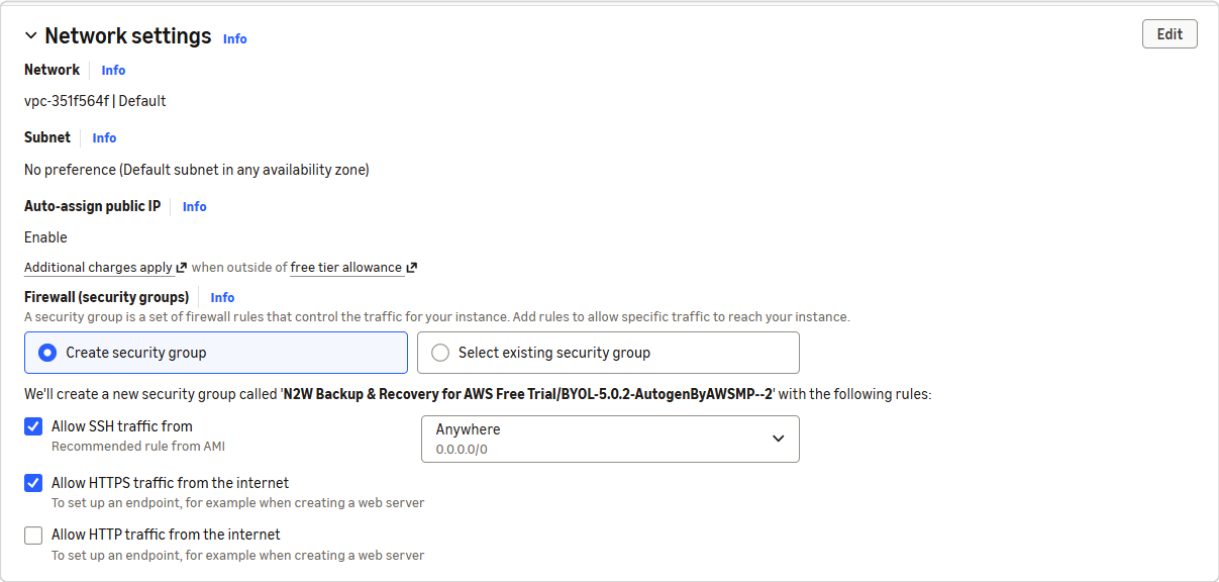
> **Note.** To choose the right size, see the KB article Recommended instance sizes and volume types for N2W Servers.



4. Under **Key pair**, create a new key pair or use an existing one. The key pair is used to connect to the instance's CLI.



5. Under **Network settings**, select a **VPC**, **Subnet**, and **Security group** for the instance. N2W needs outbound HTTPS connectivity to the internet, through one of:
   - A public IP
   - An Elastic IP attached to the instance
   - A NAT setup, Internet Gateway, or HTTP proxy



6. Under **Advanced details**, the only mandatory field to change is **IAM instance profile**. Create a new role that gives the EC2 instance the minimum permissions it needs. See 5.0.2 Required Minimum AWS Permissions for N2W Operations and Appendix A.

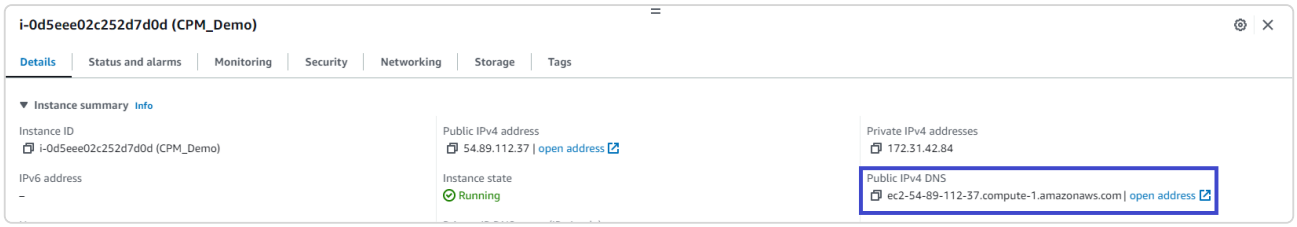
7. Select **Launch instance**.

3.3 Connecting to the N2W Server

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

> **Note.** JavaScript must be enabled in your browser for N2W to work.

After launching the N2W AWS instance, use the AWS Management Console or another management tool to get the IP address of the new instance:



Use the IP address to connect to the N2W Server over HTTPS in your browser: `https://<server address>`.

When a new N2W Server boots for the first time, it automatically creates a self-signed SSL certificate. You can upload a different certificate after initial configuration. Because the certificate is unique to this server, it is safe to use. However, because it is self-signed, you need to approve it as an exception in your browser. For Chrome and Firefox, see Appendix B – Adding an Exception for the Default Browser.

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

3.4 N2W Server Configuration Wizard

The N2W Server Configuration wizard takes you through the process step by step. Configuring the Free Trial differs slightly from paid editions.

For the N2W Free Trial edition

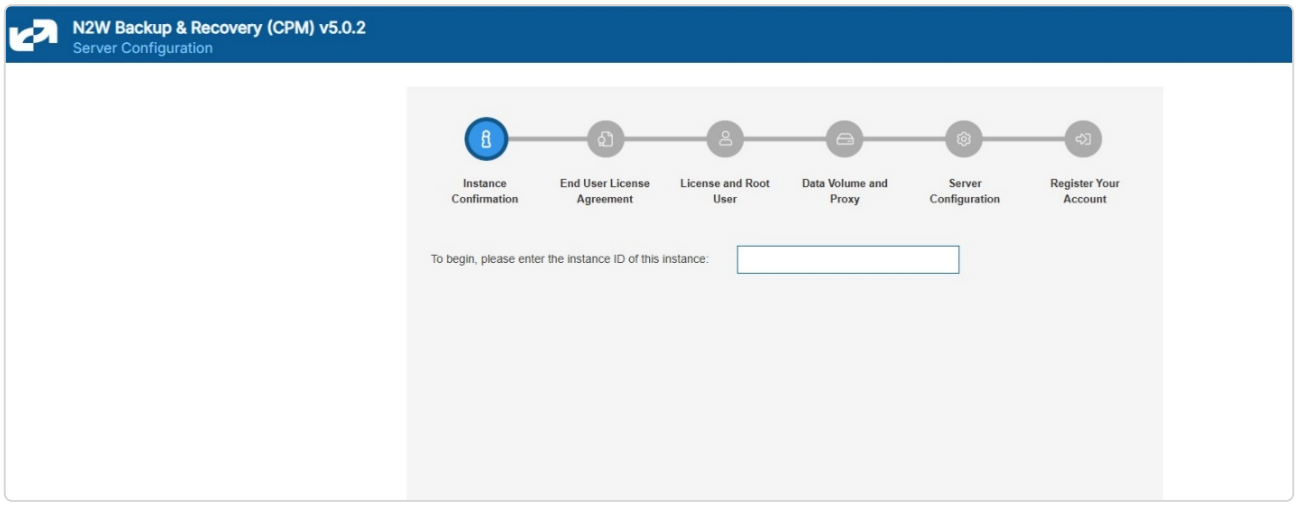
- A new volume must be defined for the N2W server.
- You need to enter a user name, a valid email address, and a strong password, and verify the password.

For other N2W editions

Follow Steps 1–6 below.

Step 1: Verify ownership of the new instance

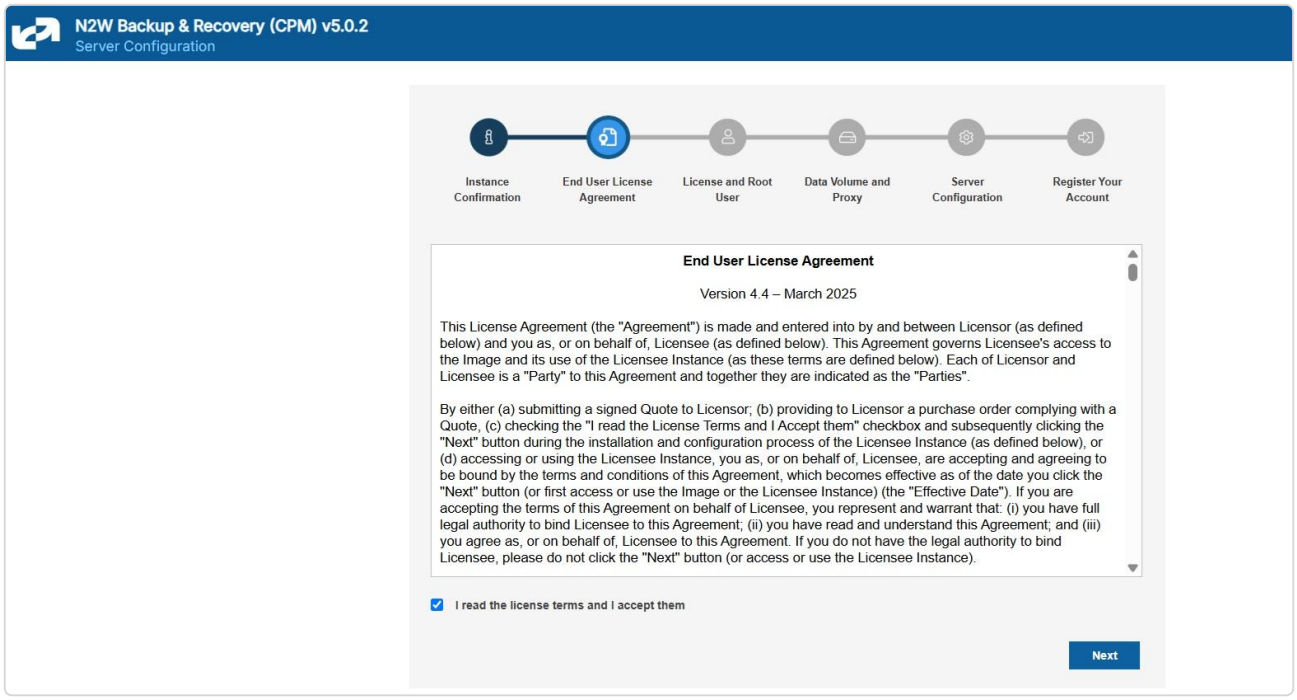
On the first screen, type or paste the instance ID of the new N2W instance. This verifies that you own the instance.



Select **Next**. The N2W configuration procedure begins.

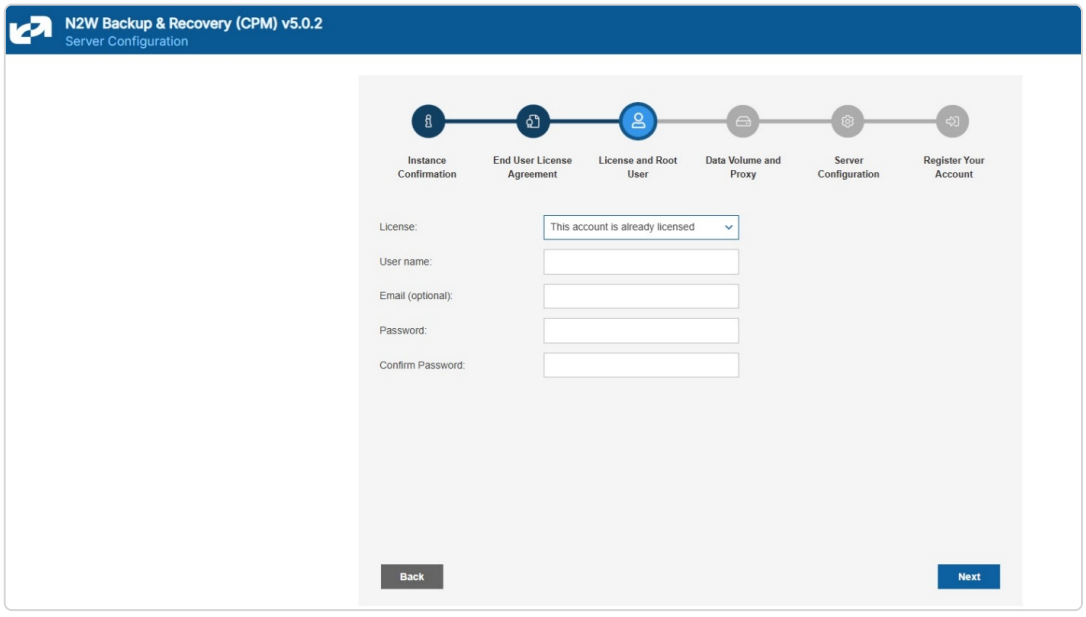
Step 2: Approve the N2W license agreement

Review the end user license terms, select the acceptance checkbox, and then select **Next**.



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

For the Free Trial, in the **License** list, select **I'm starting a free trial**. If you purchased a license directly from N2W Software, choose one of the **License** options according to the instructions you received.



Notes.

- If anyone in your organization installed an N2W Free Trial on the same AWS account before, you may get an error when configuring or connecting to N2W. Contact support@n2ws.com to resolve it.
- If you use one of the N2W paid products on AWS Marketplace, you won't see the **License** field.
- If this is an upgrade, the username must stay the same as before the upgrade, but the password can be changed.

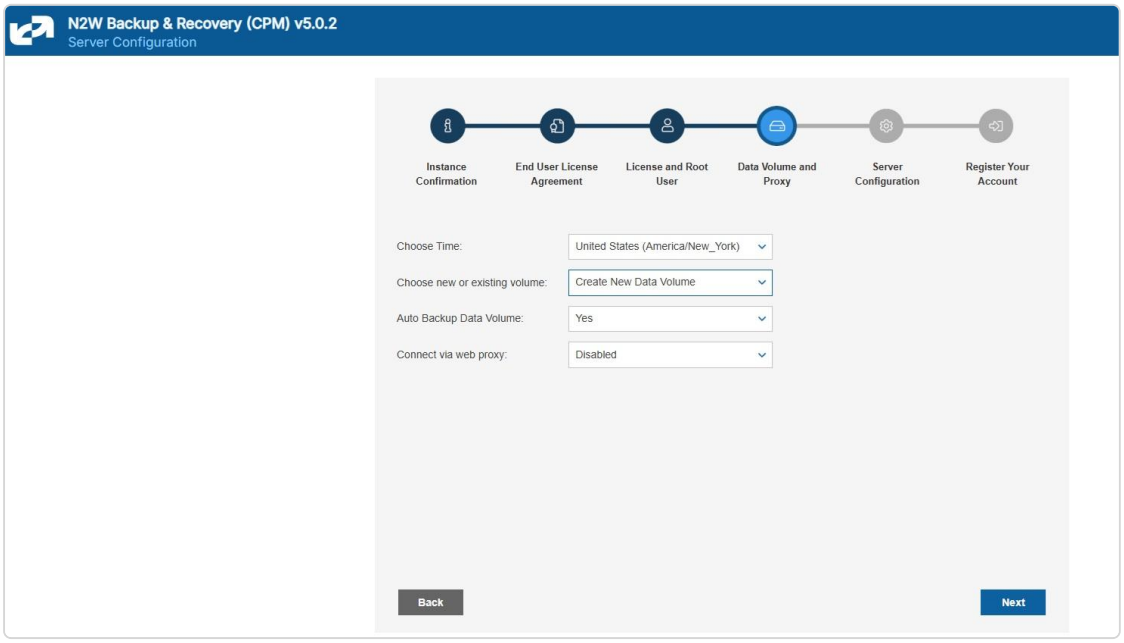
When you have completed Step 3, select **Next**.

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

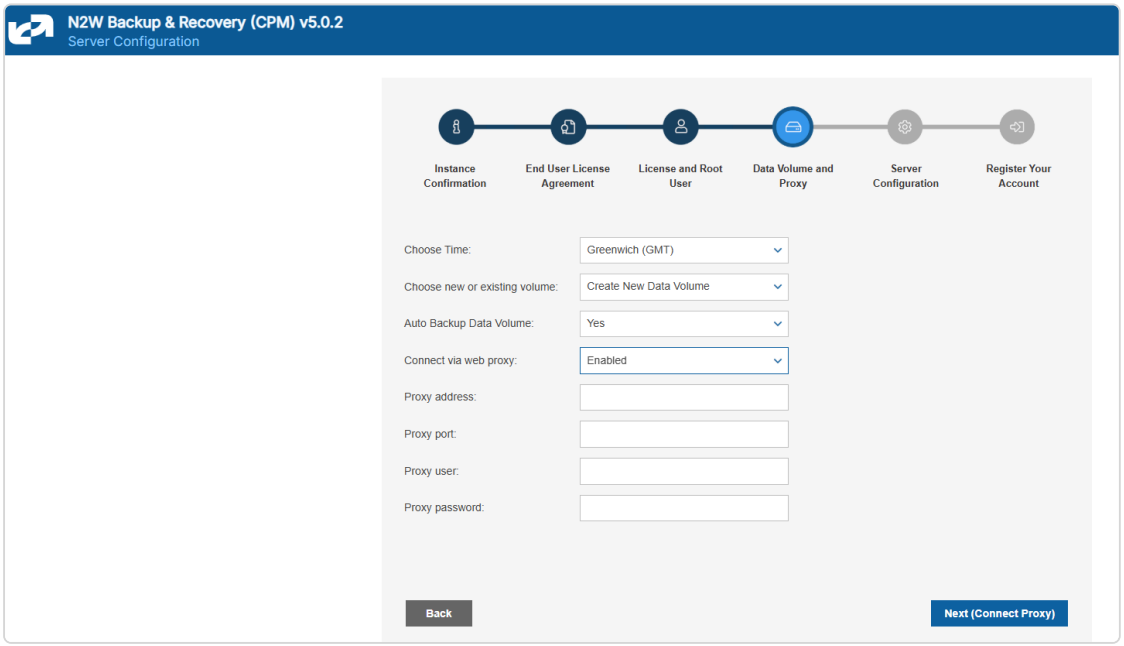
1. Choose your time zone.
2. If configuring a paid edition, choose whether to create a new data volume or use an existing one. To configure an additional N2W server in recovery mode only, choose an existing data volume and select **Force Recovery Mode**. In Step 5, you will see a list of existing N2W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

   Note. An N2W server configured for recovery mode will NOT:

   - Perform backups.
   - Perform data Lifecycle Management operations.
   - Have Resource Control management.
   - Perform any scheduled operations.



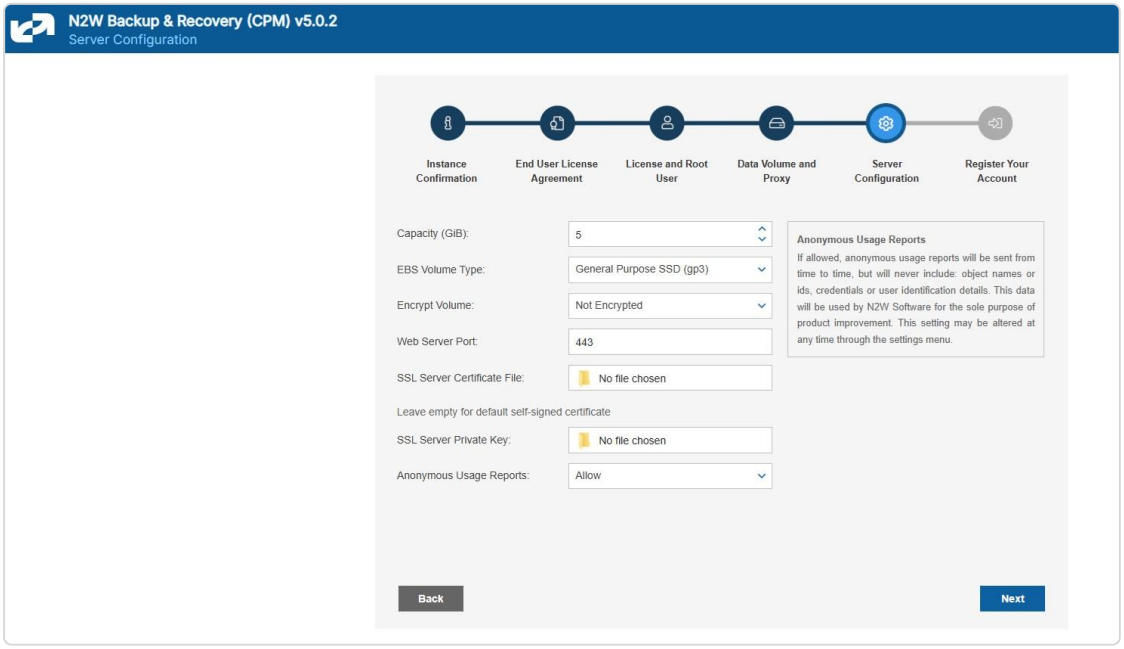
3 If you select **Enabled** for **Connect via Web proxy**, additional boxes appear for defining the proxy:



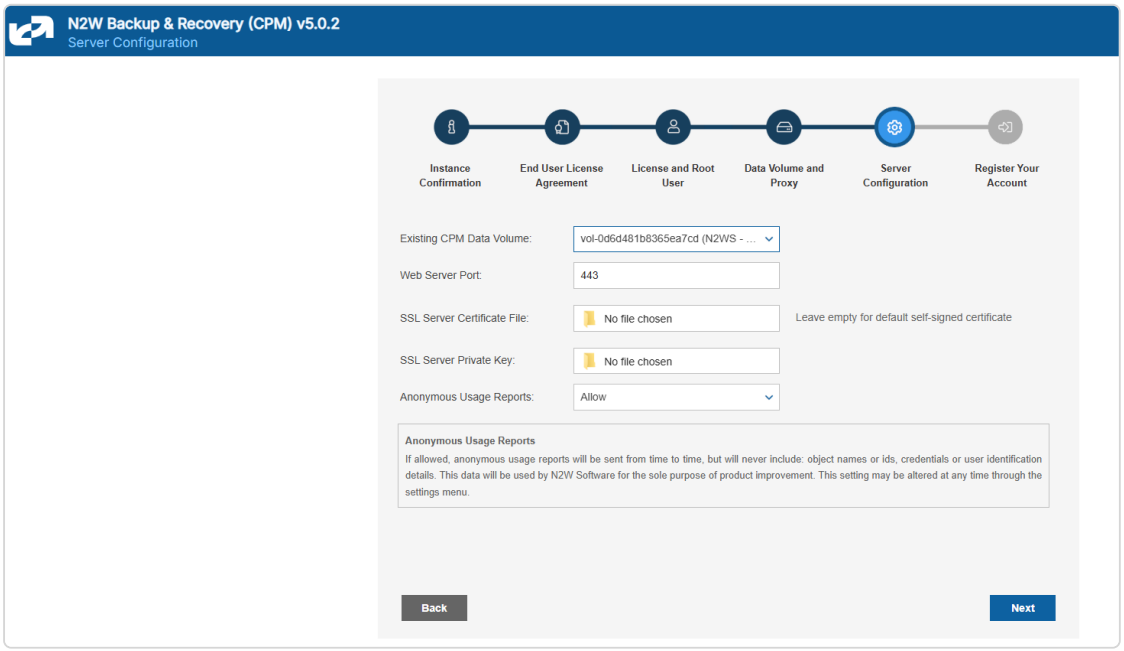
4 Select **Next**.

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

1. If you are configuring a new data volume, you can encrypt N2W user data. Select **Encrypted** in the **Encrypt Volume** list and choose a key in the **Encryption Key** list. You can also use a custom ARN.
   - Volume capacity should be at least 10 GB, enough to manage roughly 50 instances and about 3 times as many EBS volumes.
   - If your environment has more than 50 instances, increase the volume by about 1 GB per 10 backed-up instances.
   - Volume type should be at least GP3.



2. If you chose to use an existing volume, or selected **Force Recovery Mode** in Step 4, a volume selection list appears.



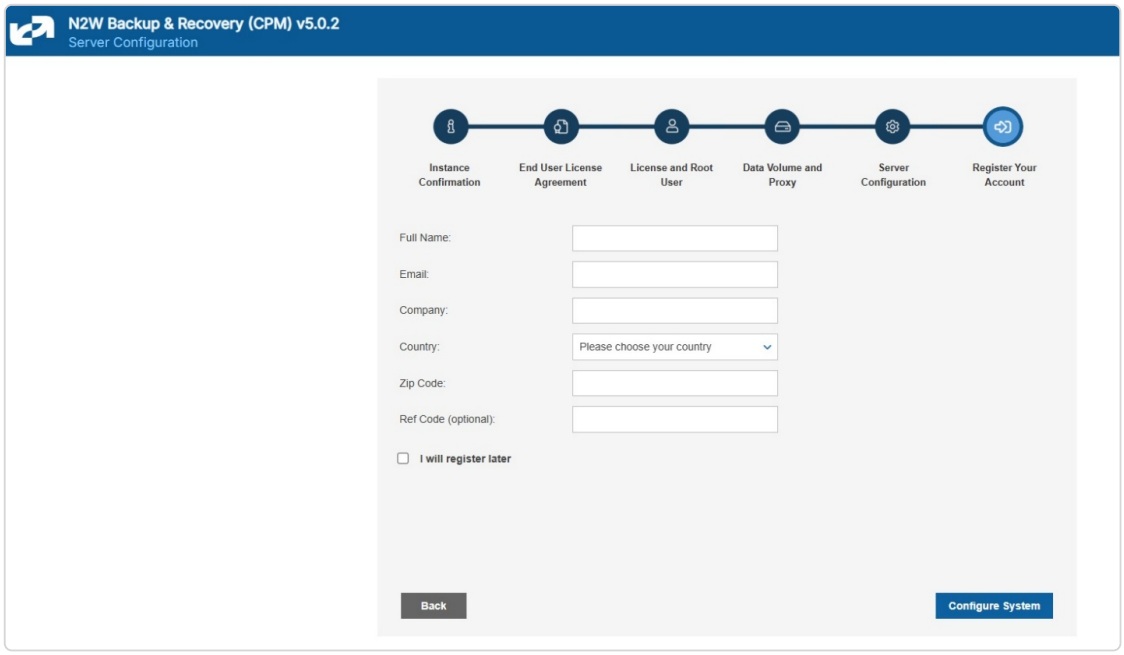
3. Complete the Web Server settings. The N2W manager uses the default port 443.
4. Allowing anonymous usage reports helps N2W improve the product. Reports are sent with no identifying details. You can disallow them later in the N2W **General Settings** menu.
5. Select **Next** when finished.

Step 6: Register the account with N2W Software

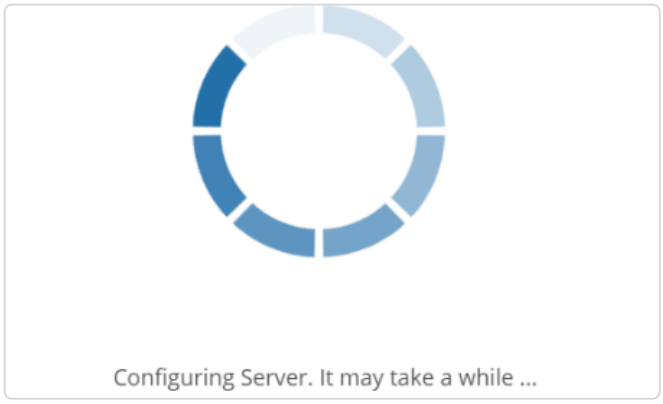
Registration is mandatory for free trials and optional for paid products. N2W recommends that all customers register, as it enables faster support. N2W Software guarantees not to share your contact information with anyone.

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.

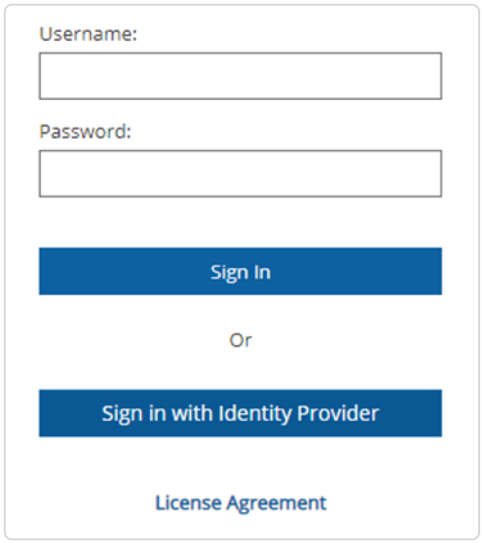


Select **Configure System** when finished. The Configuring Server message appears.



Registration and configuration can take a while, after which a **Configuration Successful – Starting Server...** message appears. The application takes a few seconds to start.

> **Note.** If you are not directed automatically to the application logon screen, reboot the instance from the management console.



You can now log on with the credentials you created in Step 3 and start using N2W.

> **Note.** Logging on for the first time with a trial edition can take up to 5 minutes, as N2W must connect to and be 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.** To get started with Azure, see the *N2W Backup & Recovery Quick Start Guide for Azure*.

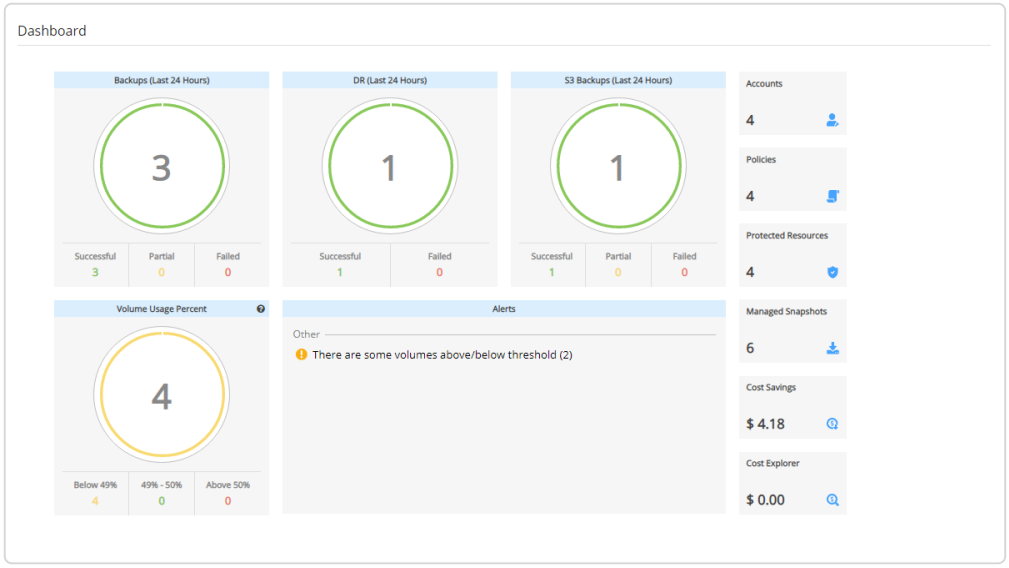
N2W automatically creates your first AWS account and policy. The required **cpmdata** policy backs up the N2W data volume.

To create additional accounts, follow 4.1 Adding an AWS Account, or see the KB article How to add an additional AWS account to N2W for Backup or DR.

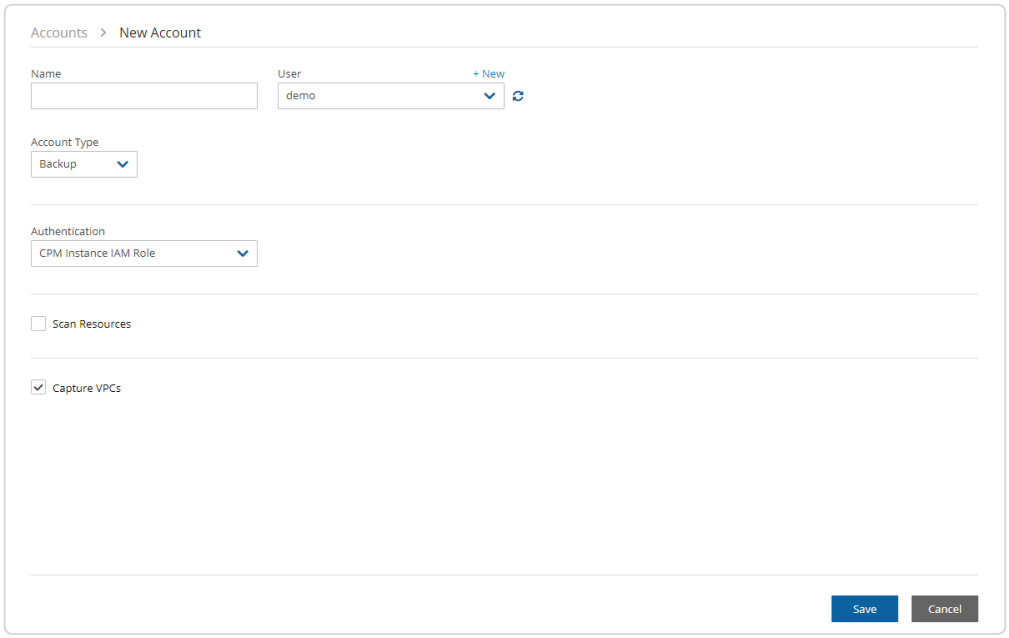
To create a simple AWS backup policy, see 4.3. A backup schedule suits production environments but is optional, since you can run a policy without one. To set a schedule, see 4.2.

4.1 Adding an AWS Account

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



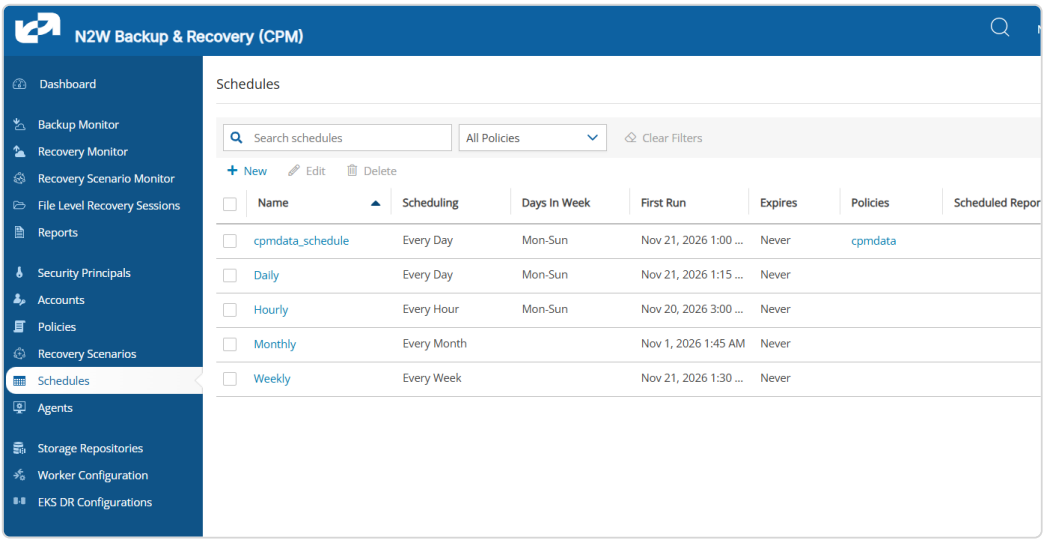
Go to **Accounts** and select **AWS Account**.

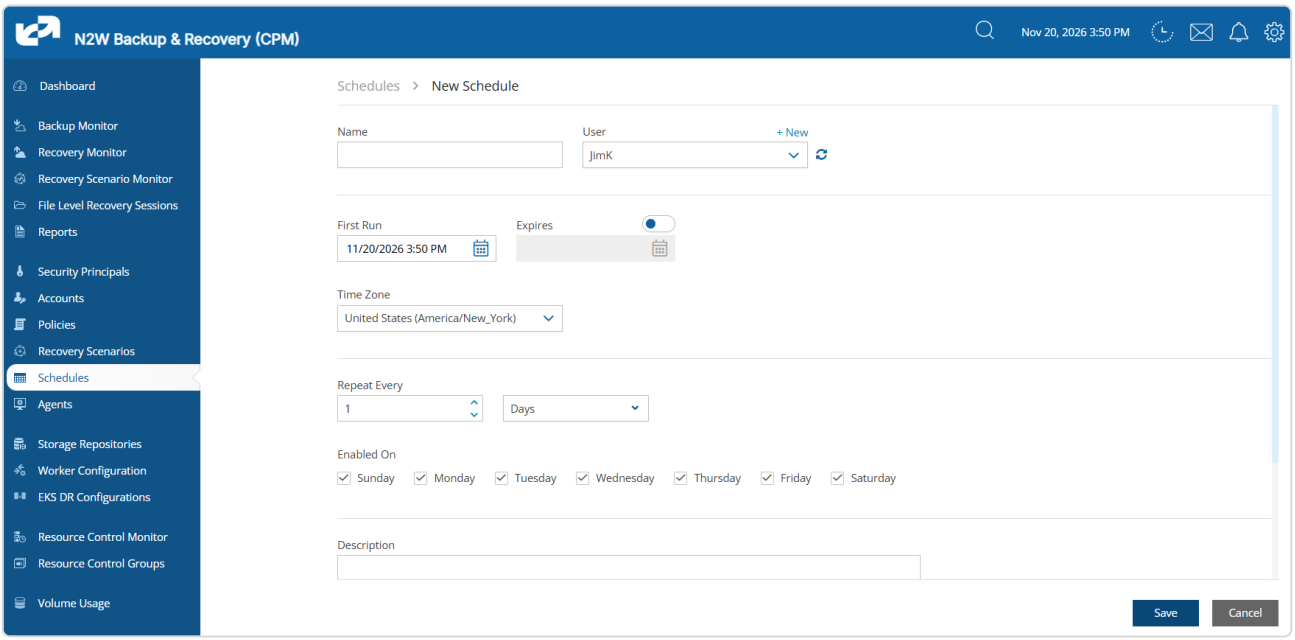


1. In the **Name** box, type the name you want to associate with your AWS account.
2. In the **Account Type** list, select **Backup**. A **DR** account is for cross-account backup and recovery and is outside the scope of this guide. See “Account Type” in the *N2W Backup & Recovery User Guide*.
3. In the **Authentication** list, select the authentication type: your AWS access key and secret key, or **CPM Instance IAM Role** (recommended). These credentials are saved in the N2W database, with the secret key encrypted. They never appear in clear text anywhere. See “Security Concerns and Best Practices” in the *N2W Backup & Recovery User Guide*.
4. Select **Scan Resources** to let this account scan resources based on tags. Select the **Scan Regions** and **Scan Resource Types** in their 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, and then select **+ New**.

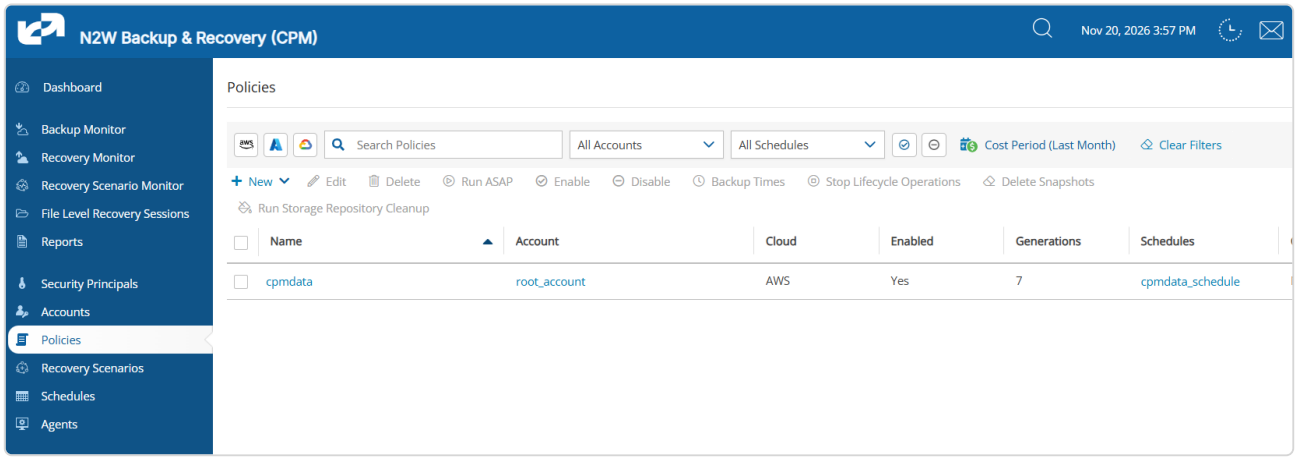


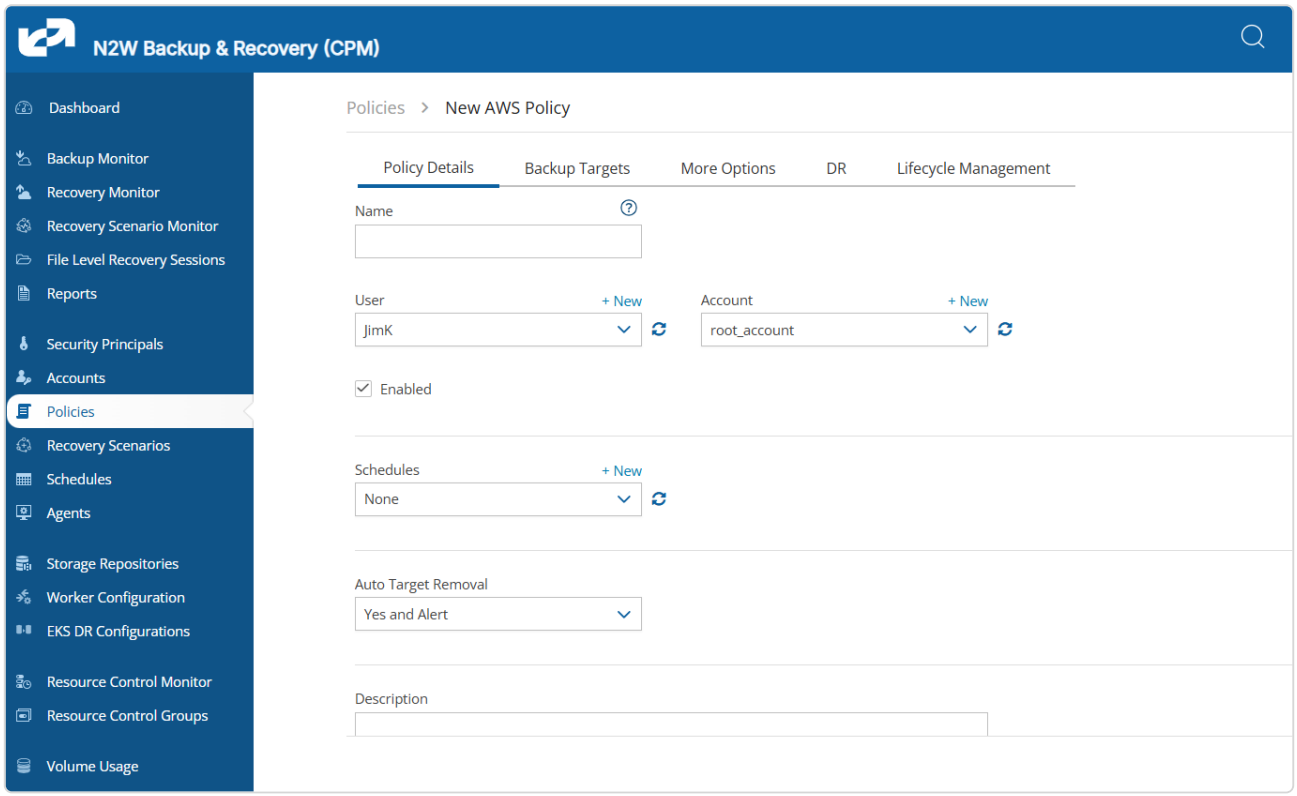


1. Type a name and optional description for the schedule.
2. In the **First Run** box, if the first run is other than immediately, select **Calendar** to choose the date and time of the first run. The **First Run** time becomes the regular start time for the schedule. By default, the schedule never expires.
3. Set the frequency in the **Repeat Every** list. Available units are minutes, hours, days, weeks, and months. Set the days 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, and then select **+ New**.

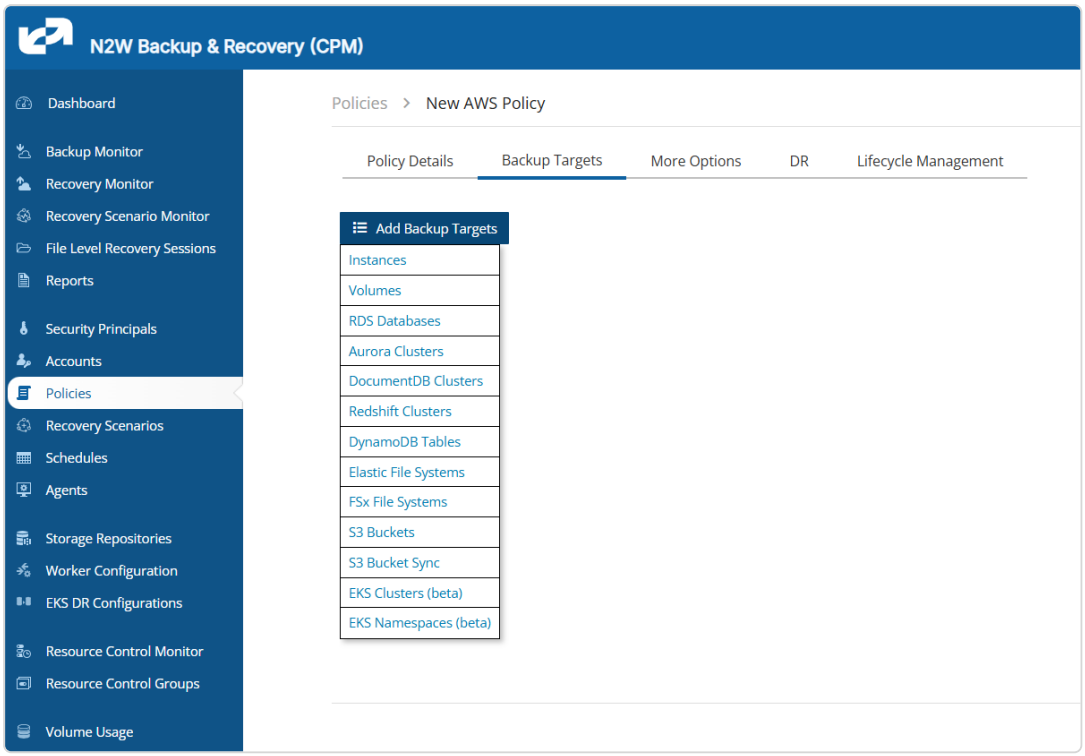




1. On the **Create Policy** page, enter a policy name and description. Other fields include:
   - **Account** – Each policy can be associated with one AWS account.
   - **Enabled** – Policies are enabled by default.
   - **Schedules** – Select the schedule you just created.
   - **Auto Target Removal** – Choose whether to automatically remove resources that no longer exist. If enabled, when an instance is terminated or an EBS volume deleted, the next backup

detects it and removes it from the policy. Choose **Yes and alert** to also log a warning about the removal.

2. When finished, select **Save**, and then select the **Backup Targets** tab. Backup targets define what a policy backs up.



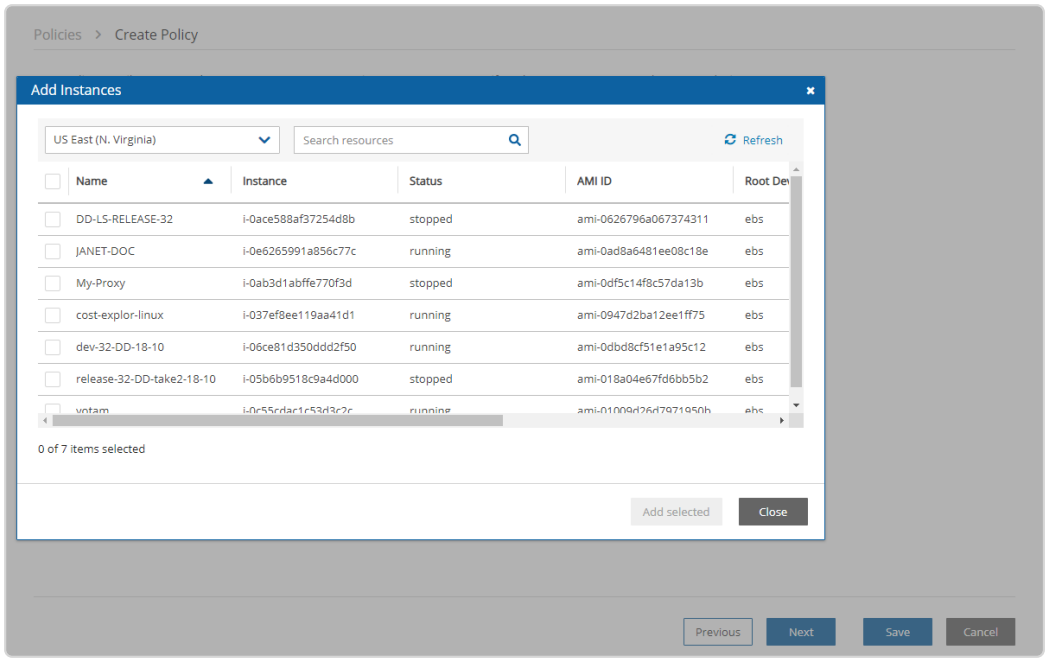
You can back up these types of objects:

- **Instances** – EC2 instances, including their metadata, and optionally some or all of their data volumes. This is the most common backup target.
- **Volumes** – EBS volumes independently, whether or not they are attached to an instance and regardless of which instance. Useful for volumes that aren't always attached or that move between instances, like cluster volumes.
- **RDS Databases** – RDS DB instances, using RDS snapshots. Useful for backing up RDS databases together with other object types, or in addition to or instead of AWS automatic backup.
- **Aurora Clusters** – Like RDS, but for 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** – Back up S3 buckets to a vault.
- **EKS** – Back up EKS clusters and namespaces.

Example: add an instance to the policy

1. In the **Add Backup Targets** menu, select **Instances**. The instances in the policy account's region appear. Use the **Region** list to switch regions. Free-text search, column sorting, and pagination help you find a specific instance.

   > **Note.** You can add backup objects from different regions to the same policy, but in many cases this is not good practice.



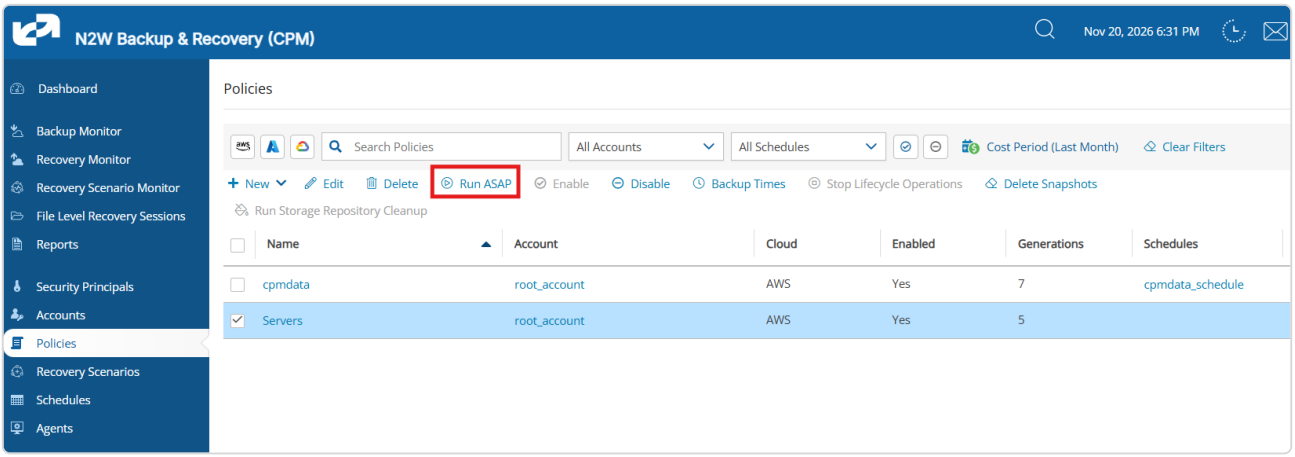
2. Select the instance you want to back up, and then select **Add Selected**. The instance is added in the background and removed from the popup, which stays open. You can add as many instances as your license allows. Select **Close** when finished.

3. Back in **Backup Targets**, the instance appears in the list, with the option to remove it from the policy. Select the instance and select **Configure** to review which volumes to back up and other options.

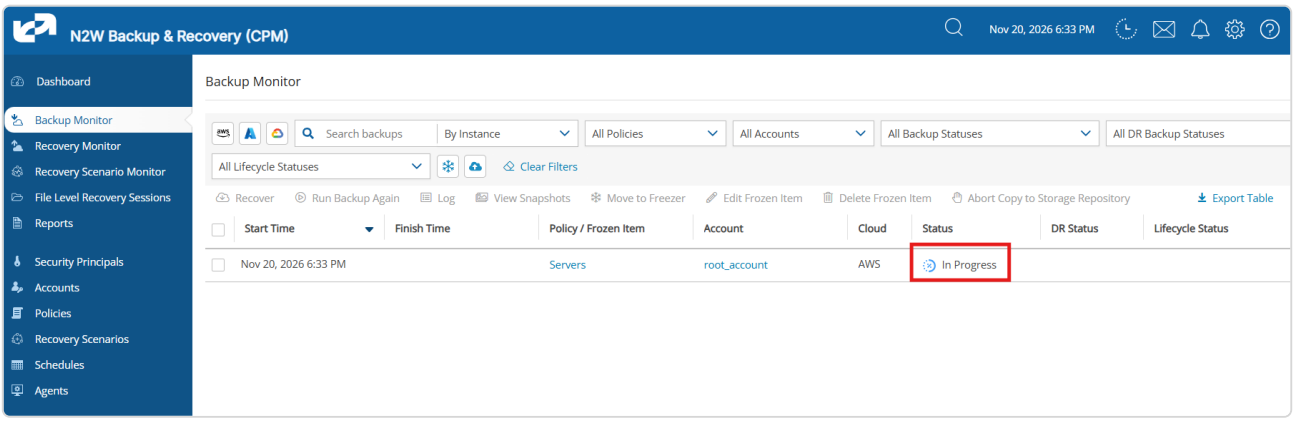
   By default, all EBS volumes attached to the instance are backed up. Attaching or detaching a volume doesn't interfere with the policy: on every backup, N2W checks which volumes are attached and snapshots them.

To view the planned backups for this policy, select **Backup Times** in the Policies list. Backups start automatically at the time set in the schedule.

To start a backup immediately, select a policy, and then select **Run ASAP**.



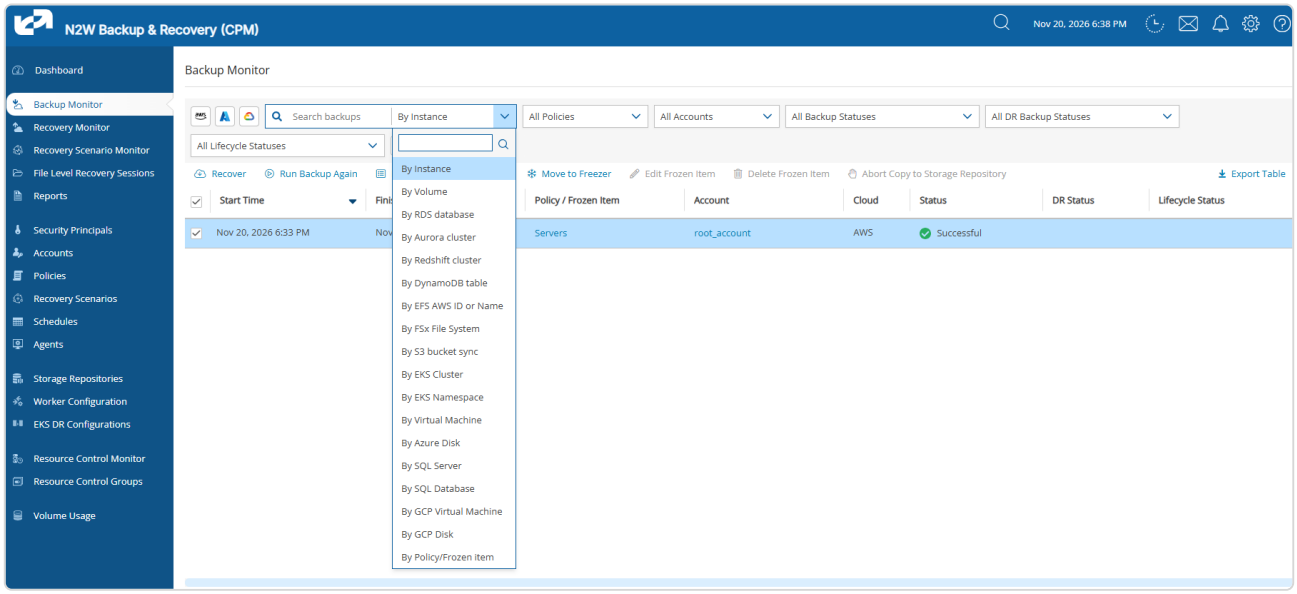
N2W reports that the backup policy will now run. Follow progress in the **Status** column of the **Backup Monitor** tab.



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

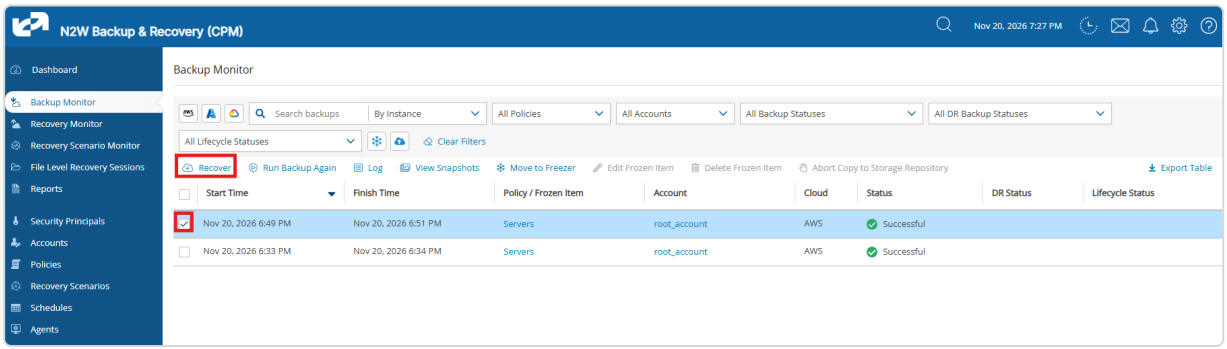
5 Performing a Basic Recovery

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

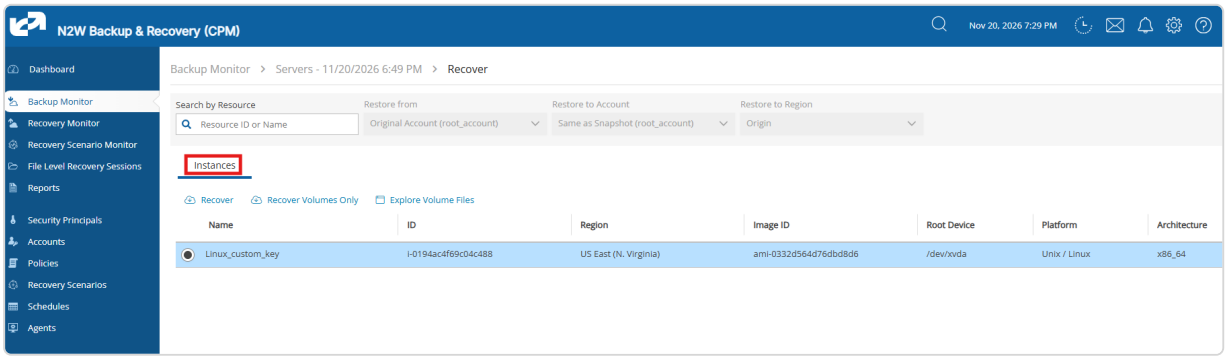


For each backup, you can see the exact start and finish times and the status. Select **View Snapshots** to see the individual EBS snapshots of all volumes. Select **Log** to view the backup's full log.

1. To recover from a backup (typically the most recent successful one), select the backup, and then select **Recover**.

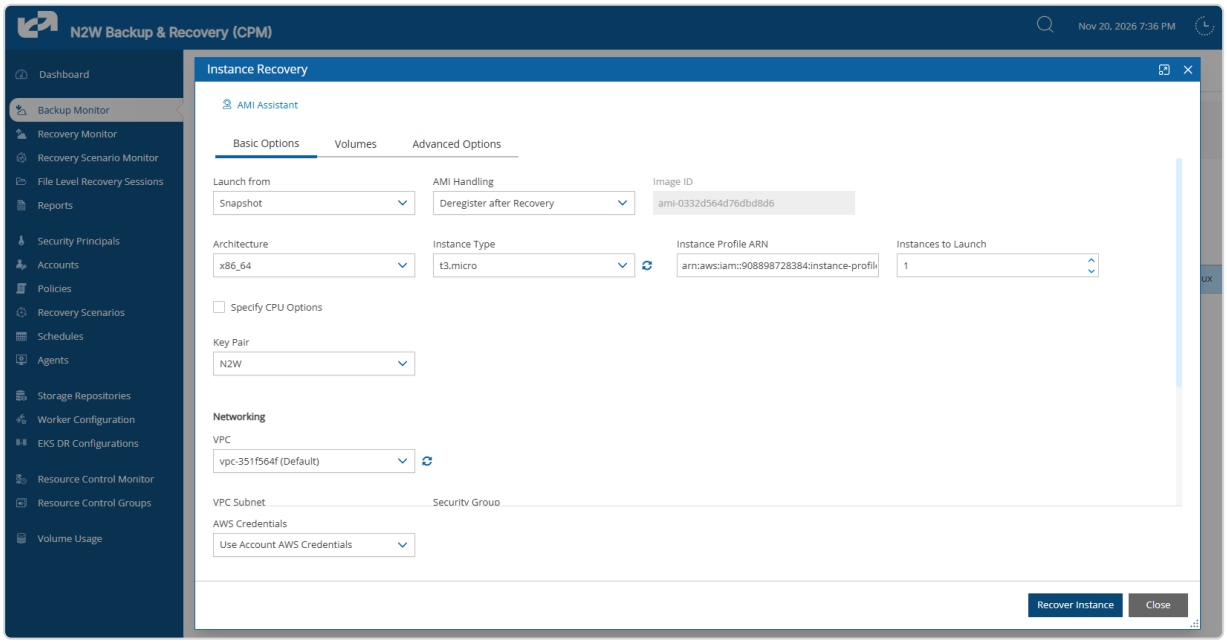


2. The **Recover** screen shows all instances in the backup. If the policy also includes EBS volumes, RDS databases, Redshift clusters, or DynamoDB tables, each has its own tab. To recover an instance, select the **Instances** tab.



> **Note.** **Recover Volumes Only** recovers only the instance's EBS volumes, without creating a new instance.

3. Select the instance to recover and select **Recover** again. The **Basic Options** tab of the **Instance Recovery** page opens. To enlarge the page, select ⛶ in the upper-right corner.



Most EC2 launch options are available here and can be changed. The defaults are exactly the options the original instance had at backup time, including its tags.

Launch from sets the image the new instance launches from. An instance-store-based instance can only launch from an image; the default is the original image, which you can change. For a Linux EBS-based instance, as in this example, where the backup includes a snapshot of the boot device, you can launch from an image (the original or another) or from the snapshot, which is the default.

If you launch from a snapshot, N2W creates a new image (AMI). You can keep the image after recovery or deregister it, or only create the image now and recover from it later.

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

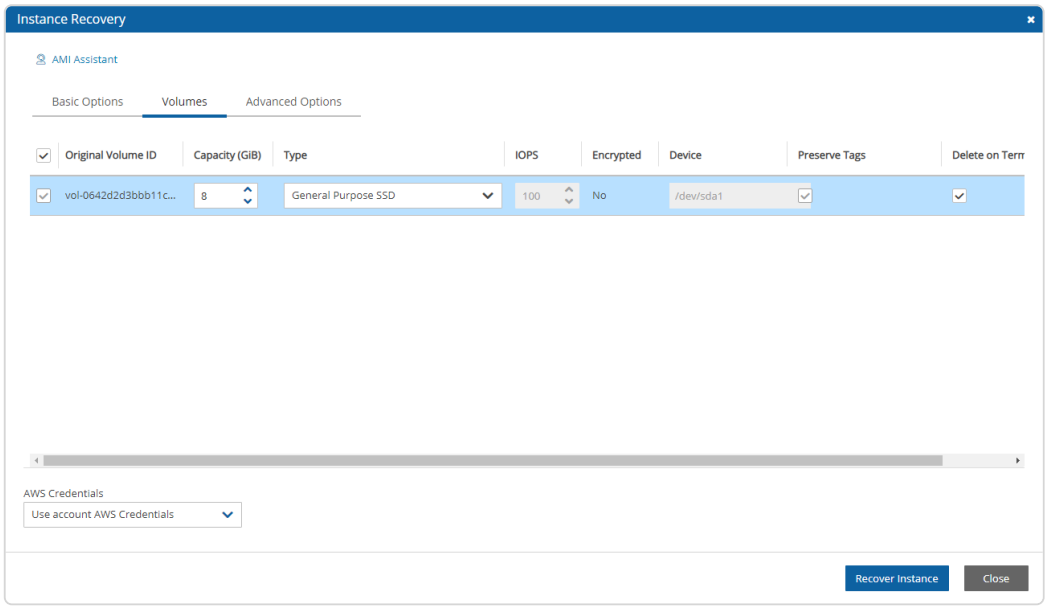
For paid editions, if **Capture Network Environments** was enabled in the **Account** settings, the **Basic Options** tab also has a **Clone VPC** button next to the **VPC** box.



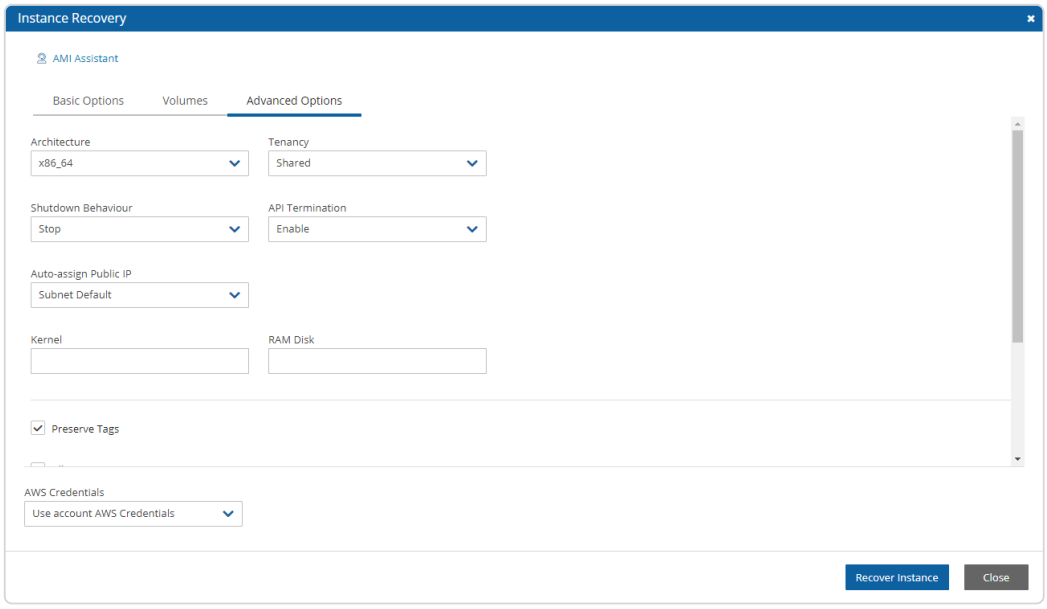
Clone VPC recovers the instance to a clone of a selected VPC environment. See Performing Recovery in the N2W User Guide.

> **Important.** If you test recovery of an instance in the same region as the original, change the IP to avoid an IP conflict. You can avoid this by leaving the **VPC Assign IP** box blank.

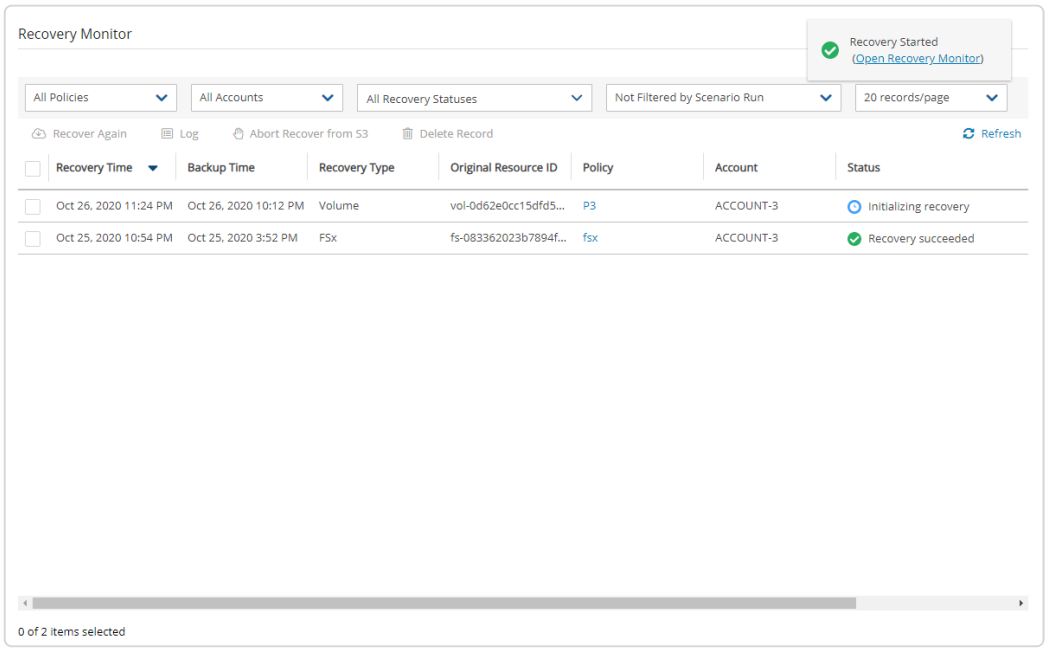
Select the **Volumes** tab to choose which volumes to recover and how.



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



After you select **Recover Instance** and confirm, you are taken to the Recovery Monitor, where you can follow progress in the **Status** column. Select **Log** for recovery details.



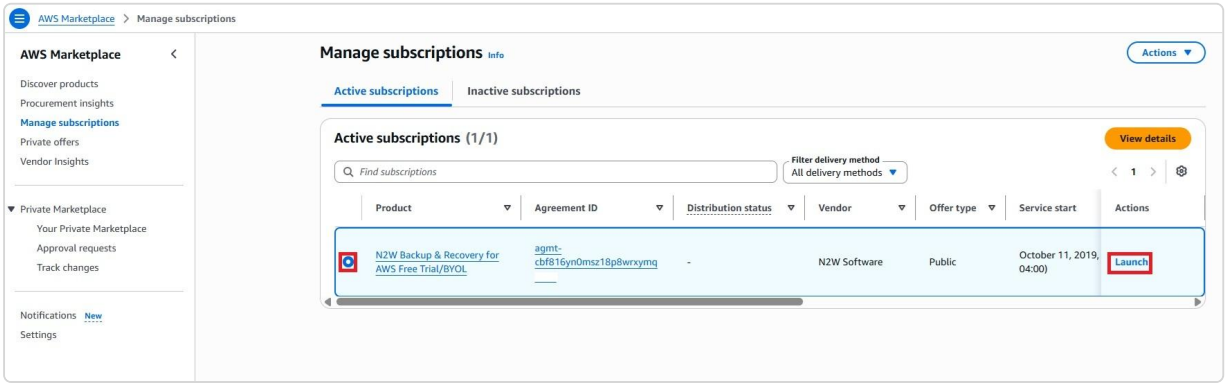
The log includes the new instance's ID, so you can verify the recovery in the AWS Management Console. The recovered instance is the same as the original, with all its EBS volumes.

6 How to Configure N2W with CloudFormation

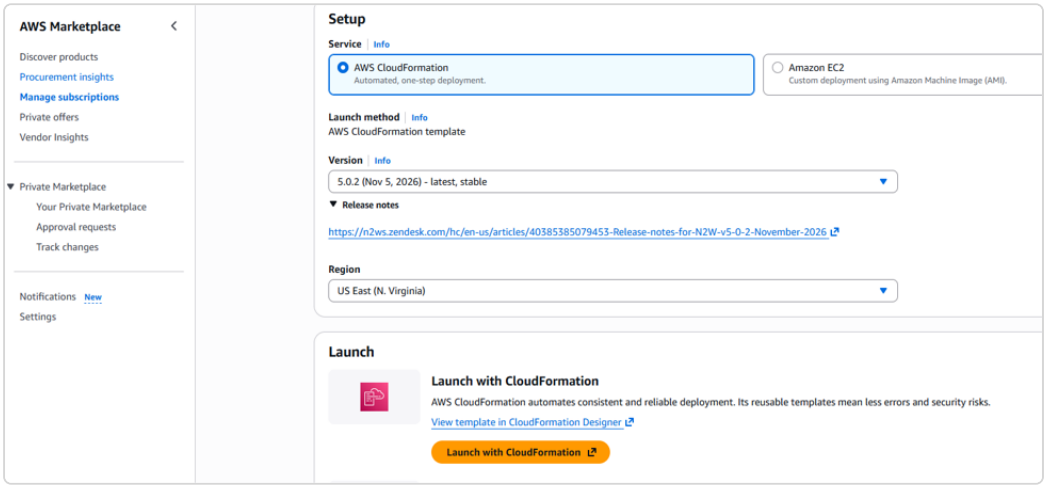
Configuring N2W with CloudFormation is a single flow, from subscribing to N2W on AWS Marketplace to configuring the N2W server.

> **Notes.**
>
> - All N2W editions support CloudFormation.
> - An IAM role with minimal permissions is created automatically and assigned to the N2W instance.

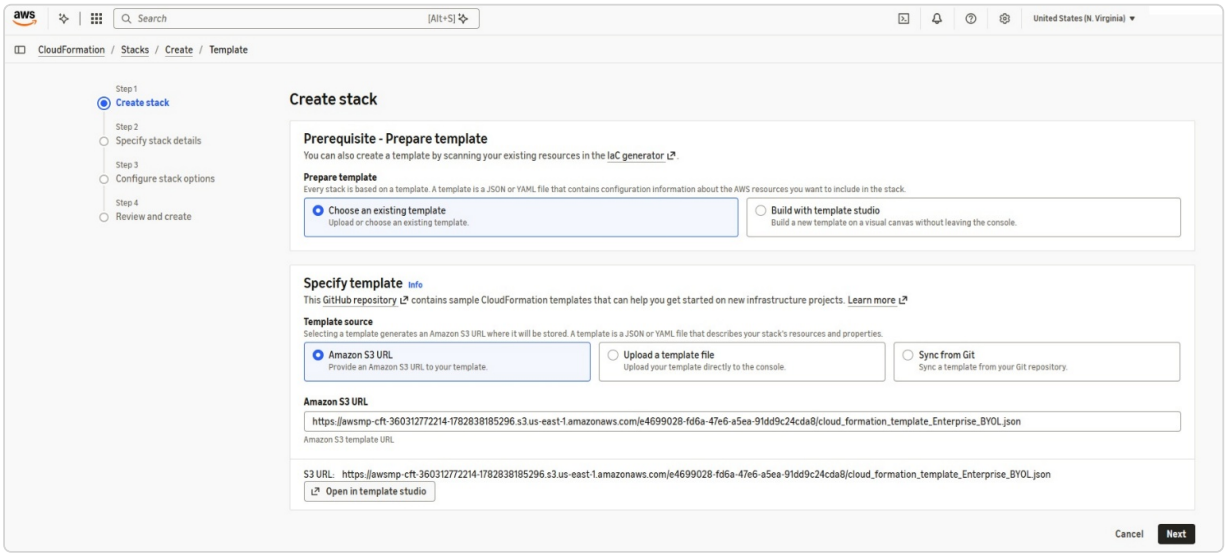
1. Go to aws.amazon.com/marketplace.
2. Select **Manage Subscriptions**.
3. Select your active N2W subscription and select **Launch**.



4. On the Setup page, select **AWS CloudFormation** and the version, and then select **Launch with CloudFormation**.

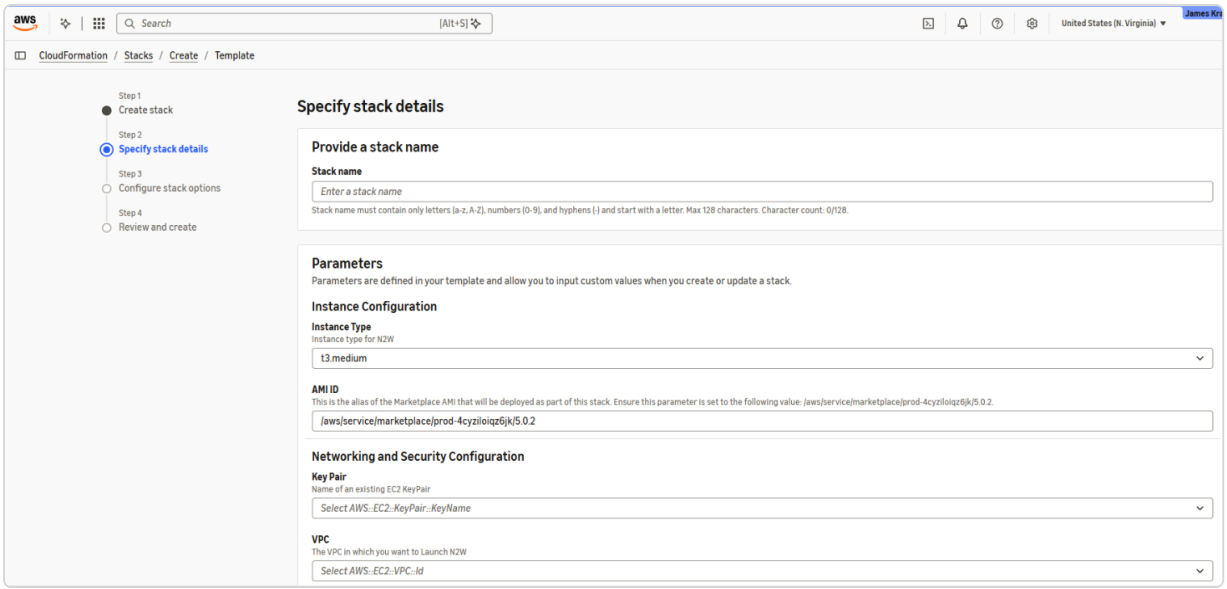


5. The **Create stack / Select Template** page opens.



6. Under **Prepare template**, select **Choose an existing template**.

7. Under **Specify template**, choose **Amazon S3 URL**. Select the default Amazon S3 URL, and then select **Next**. The **Specify stack details** page opens.

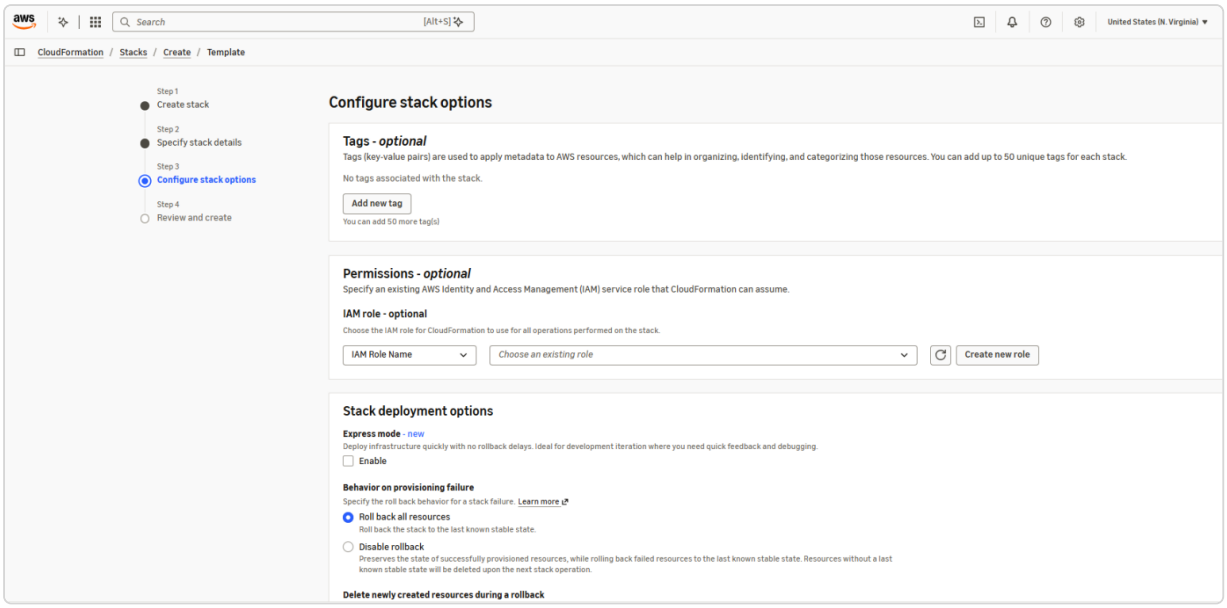


8. Complete the **Stack Details** and **Parameters**. Security groups act as a firewall for associated instances, controlling inbound and outbound traffic at the instance level. **Inbound Access CIDR** adds security group rules that let you connect to your Linux instance from your IP address over SSH:

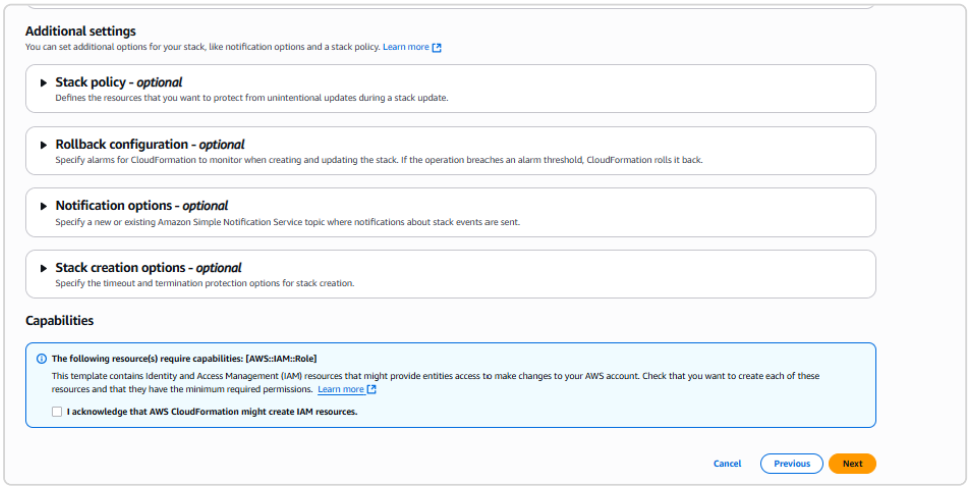
   - If your IPv4 address is 203.0.113.25, specify `203.0.113.25/32` to list this single address in CIDR notation. If your company allocates addresses within a range, specify the whole range, such as `203.0.113.0/24`.
   - Specifying `0.0.0.0/0` lets all IPv4 addresses access your instance over SSH.

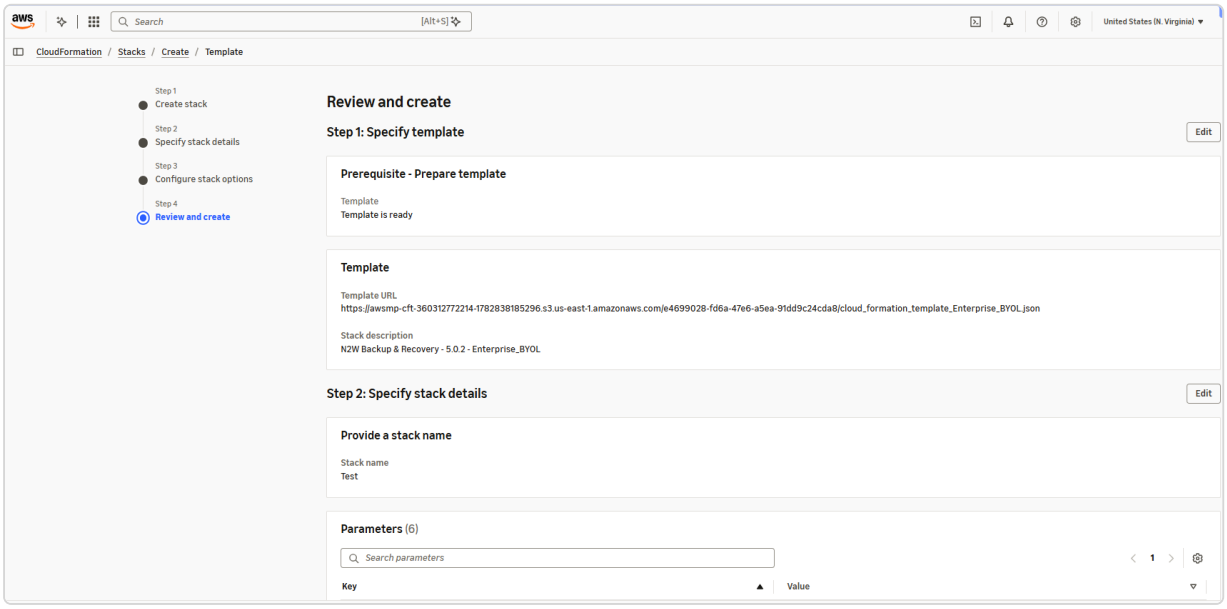
- For more, see AWS's Adding a Rule for Inbound SSH Traffic to a Linux Instance.

9. Select **Next**. The **Options** page opens.



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





11. Select the **I acknowledge that AWS CloudFormation might create IAM resources** checkbox, and then select **Create stack**. The **CloudFormation Stacks** page opens.
12. Select the new stack. The **Instances** page opens.
13. Select the instance. Copy the **Instance ID** value in the **Description** tab, and then select **Launch Instance**. The **N2W Server Configuration** page opens.
14. Continue from 3.4 N2W Server Configuration Wizard.

Appendix A – AWS Authentication

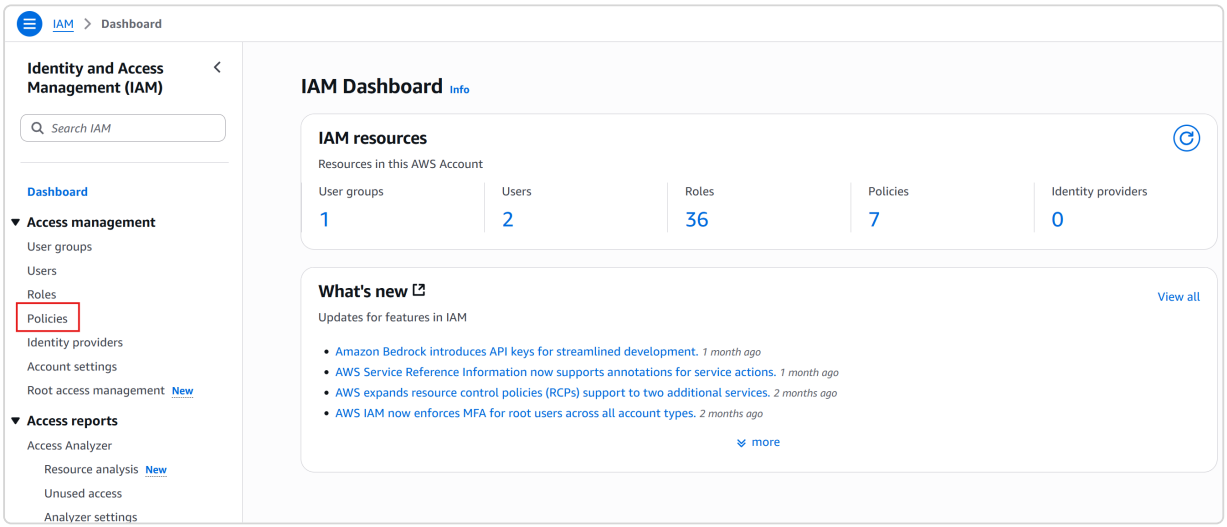
To perform its backup and restore management functions, N2W needs the correct permissions. N2W supports two types of AWS authentication during setup:

- AccessKey / SecretKey
- Role-based authentication (recommended)

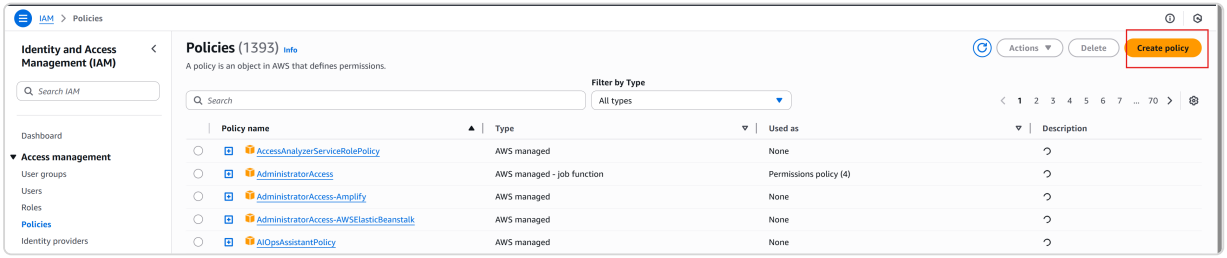
The required permissions are combined into a JSON file you can download from the N2W Knowledge Base: 5.0.2 Required Minimum AWS Permissions for N2W Operations.

> **New in 5.0.0.** You can generate permission updates for existing AWS accounts: in **Accounts**, select the accounts, and then select **Generate Permissions Template**. This produces a CloudFormation template. The first time creates a stack; later updates use the same stack.

1. Download the JSON permissions file from the KB article above.
2. In the AWS console, use the search bar to find and open **IAM**.
3. In the left menu, select **Policies**.

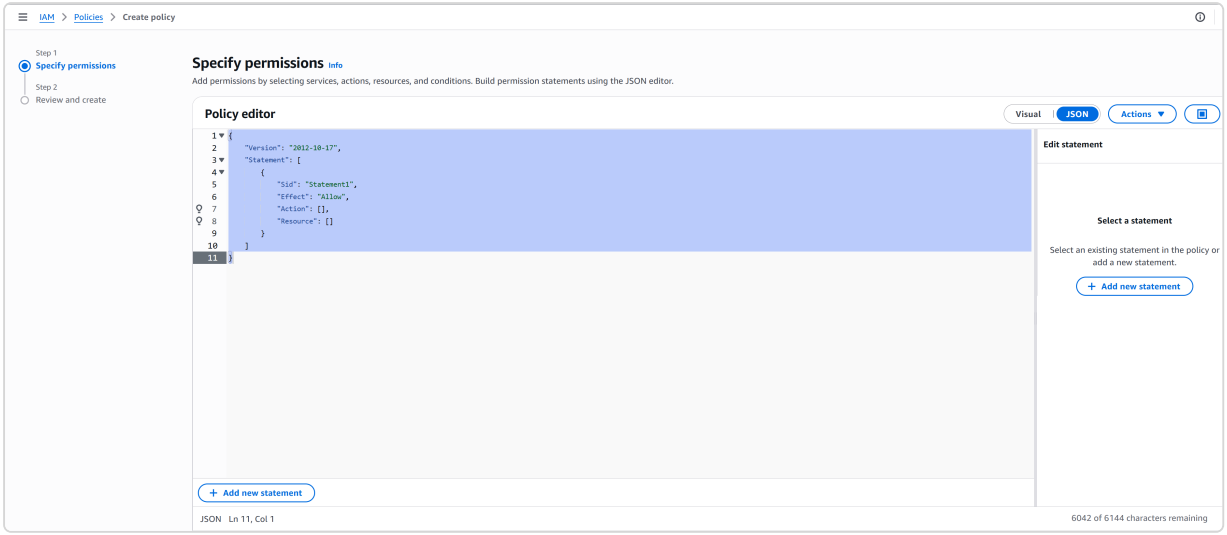


4. Select **Create policy**.



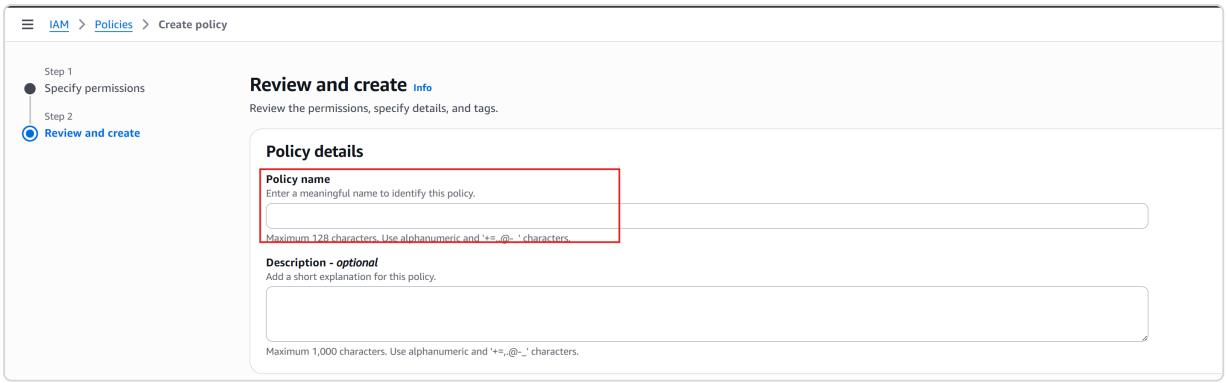
5. Select the **JSON** editor.

6. Delete the default contents and paste the contents of the downloaded JSON file.

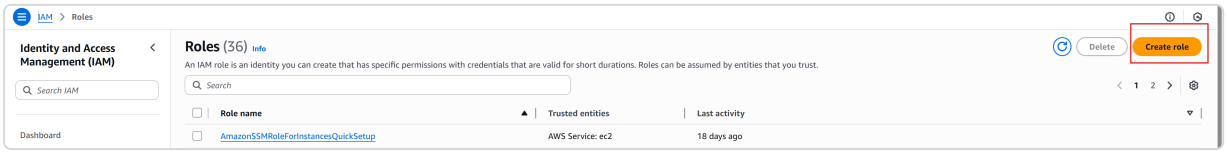


7. At the bottom of the screen, select **Next**.

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

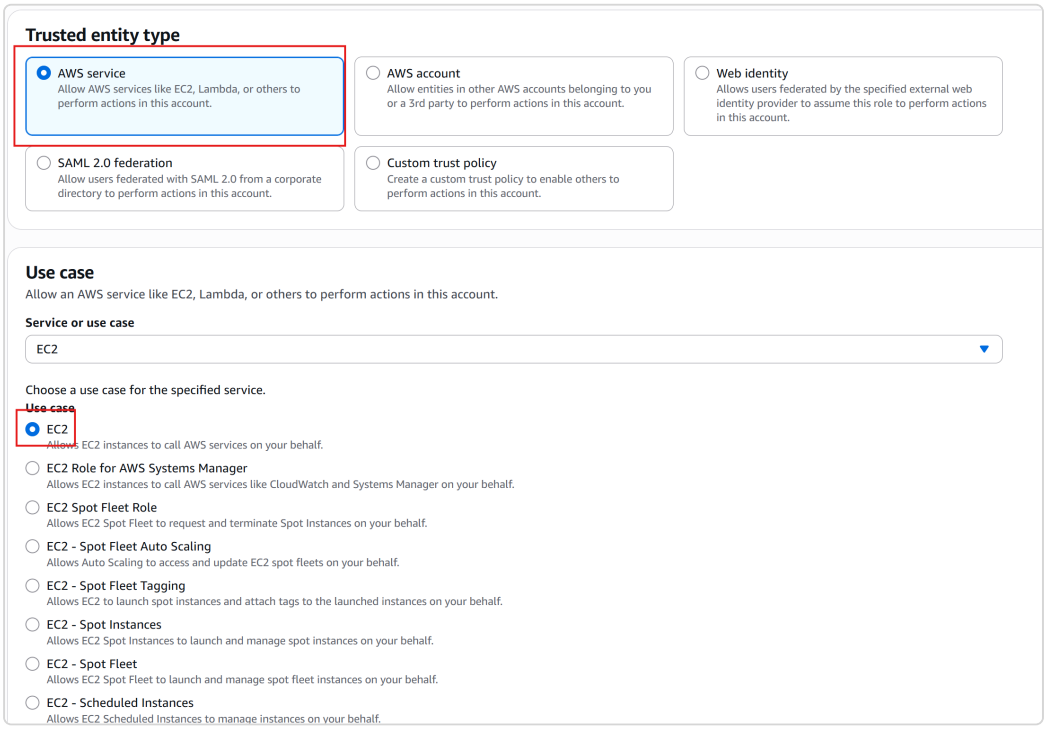


9. Create a role and assign the new policy to it. In the left menu, select **Roles**, and then select **Create role**.

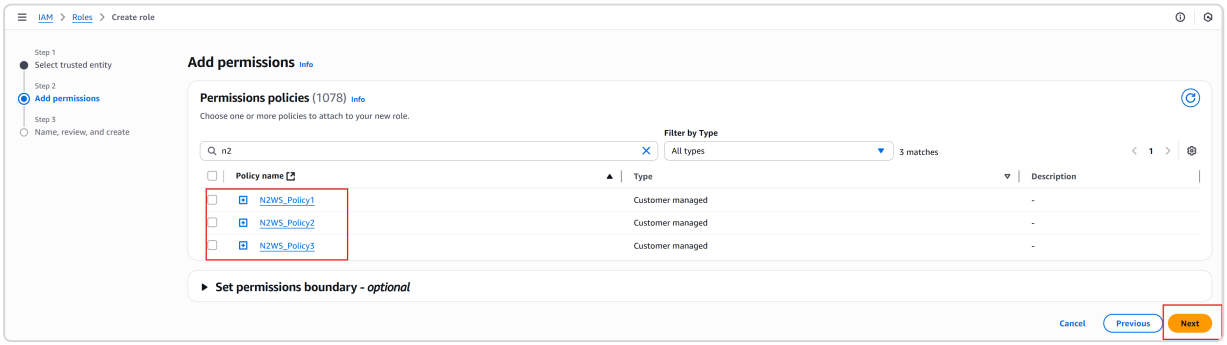


10. Under **Trusted entity type**, select **AWS service**, and under **Use case**, select **EC2**.

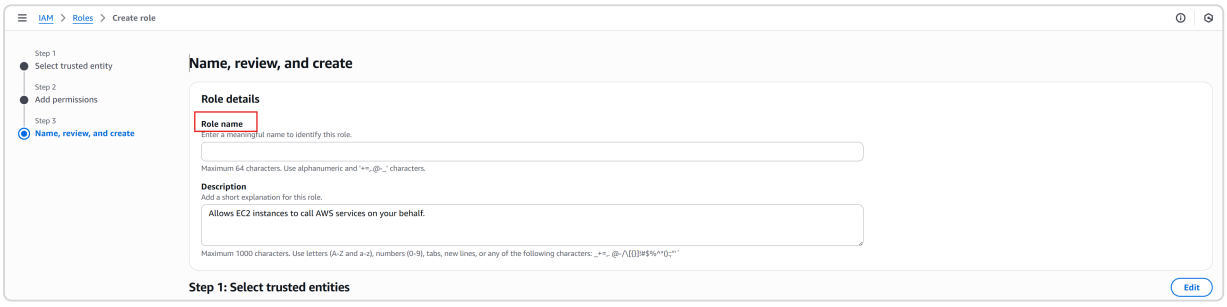
11. Select **Next**.



12 On the **Add Permissions** page, search for the previously created policy or policies, and then select **Next**.



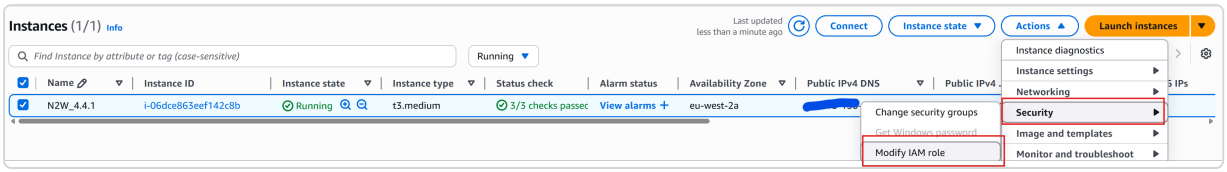
13 Name the **Role** and select **Create Role**.



14 Assign the role to the N2W trial instance:

a. Select the N2W instance name.

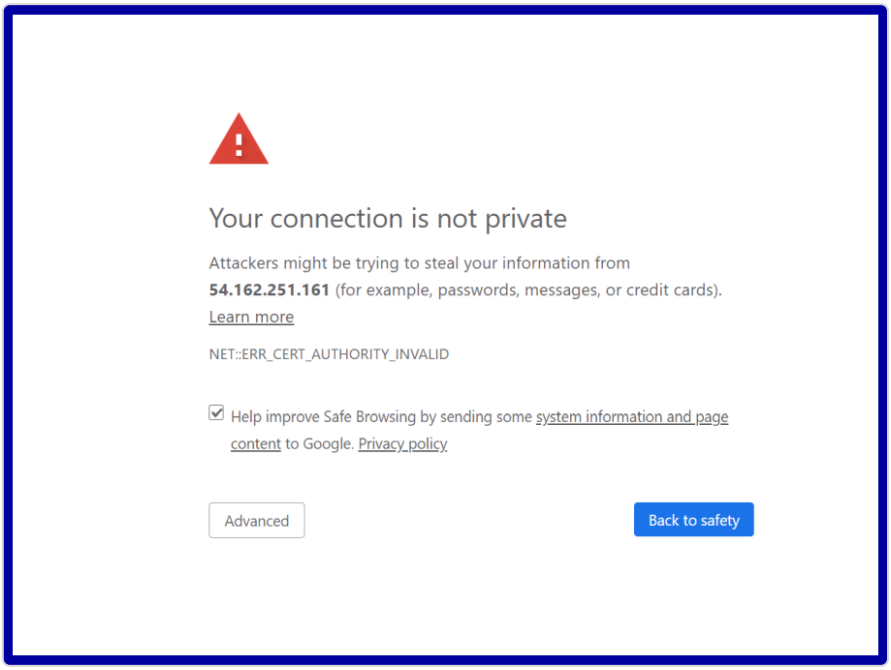
b. In the **Actions** menu, select **Security**, and then **Modify IAM role**.



Appendix B – Adding an Exception for the Default Browser

When you first go to your N2W instance, you'll see a warning like the one below. It's nothing to worry about: the connection is SSL-secured, but because the certificate is self-signed, you may want to add a browser exception.

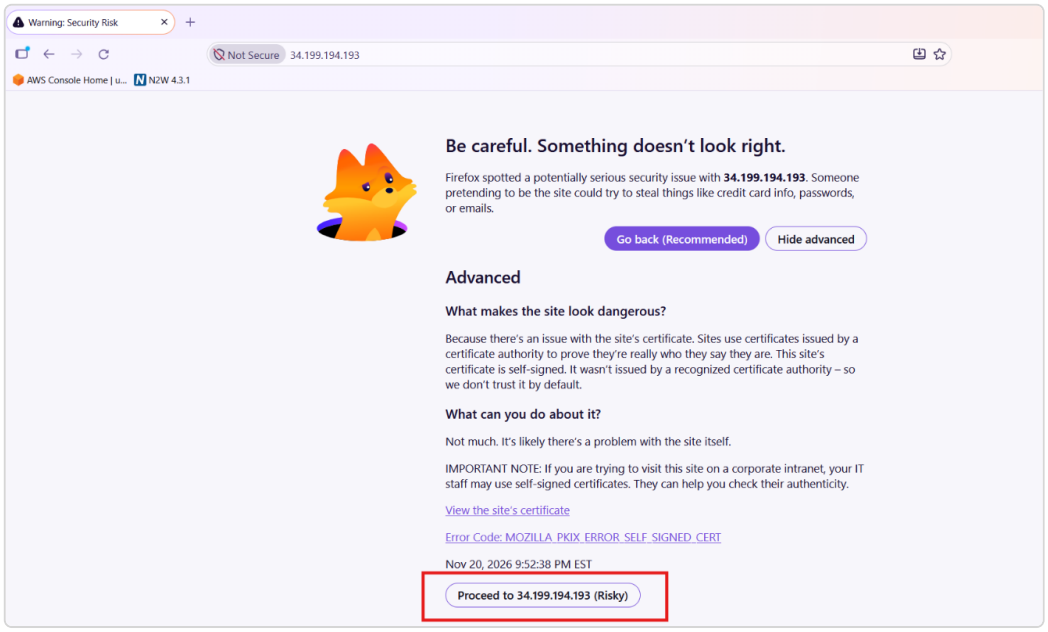
For Chrome



1. On the warning page, select **Advanced**.
2. Select **Proceed to <server address> (unsafe)**.

For Firefox

1. Select **Advanced**.
2. Select **Proceed to <server address>**.


Warning: Security Risk
Not Secure
34.199.194.193
AWS Console Home | u...
N2W 4.3.1
Be careful. Something doesn't look right.
Firefox spotted a potentially serious security issue with 34.199.194.193. Someone pretending to be the site could try to steal things like credit card info, passwords, or emails.
Go back (Recommended)
Hide advanced
Advanced
What makes the site look dangerous?
Because there's an issue with the site's certificate. Sites use certificates issued by a certificate authority to prove they're really who they say they are. This site's certificate is self-signed. It wasn't issued by a recognized certificate authority – so we don't trust it by default.
What can you do about it?
Not much. It's likely there's a problem with the site itself.
IMPORTANT NOTE: If you are trying to visit this site on a corporate intranet, your IT staff may use self-signed certificates. They can help you check their authenticity.
View the site's certificate
Error Code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT
Nov 20, 2026 9:52:38 PM EST
Proceed to 34.199.194.193 (Risky)