N2W Backup & Recovery

AWS Quick Start Guide

V4.5.1

Content

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

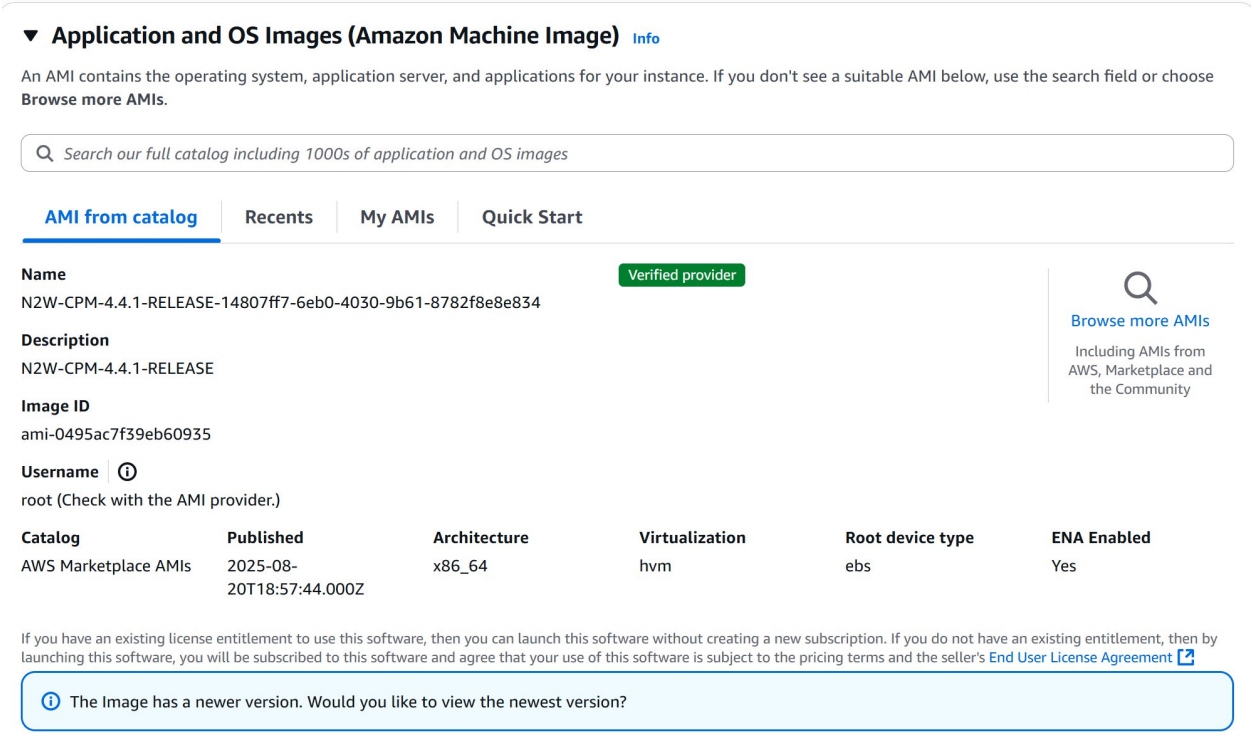
3.1 N2W Server Instance Connectivity

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.

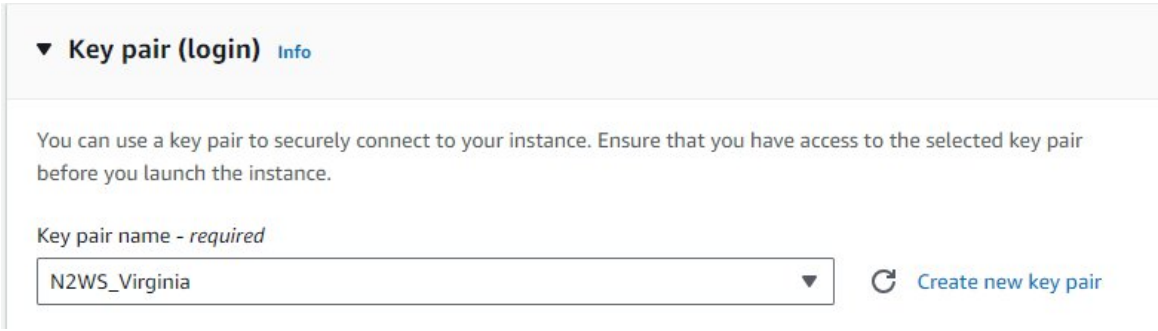
   If required, select **Add additional tags.**
2. Under **Application and OS images (Amazon Machine Image)**, leave all default values, as this section shows what AMI we are using for the EC2 instance image.



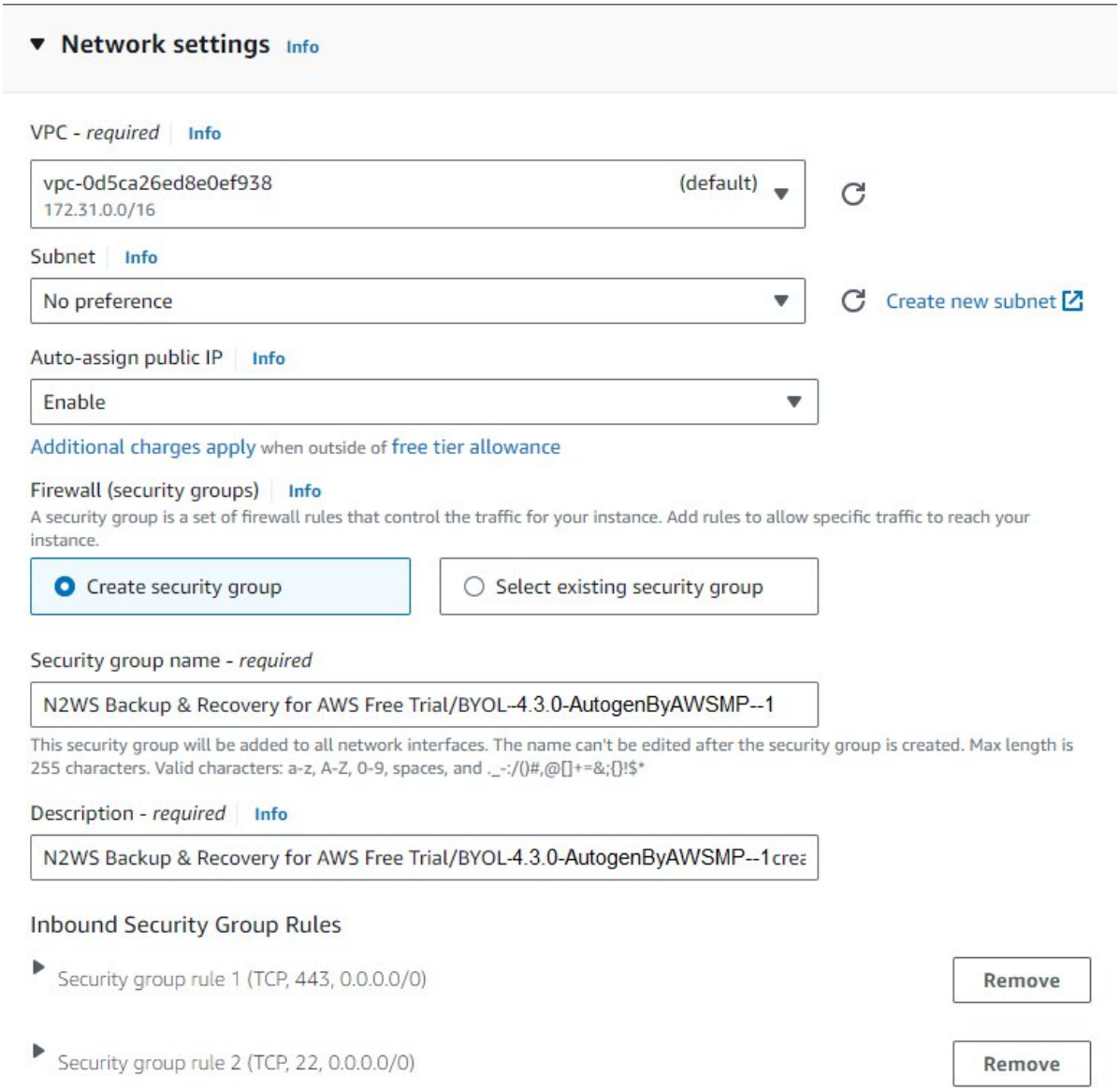
3. Under **Instance type**, the recommended minimum size is **t3.medium**. However, for bigger environments, the type may need to be larger.

   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

4. 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.



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,



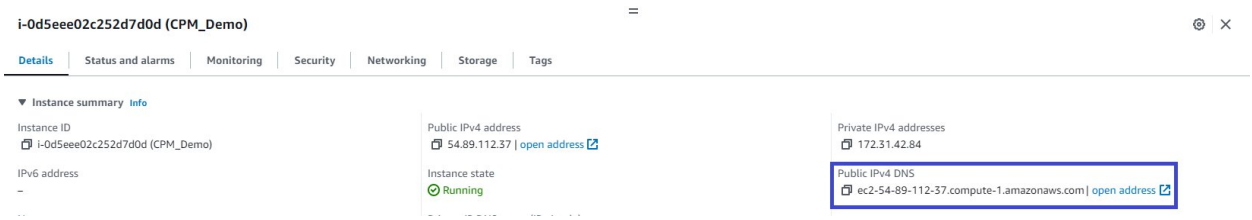
6. Under **Advanced details**, the only mandatory field to change is the IAM instance profile. Create a new role to give the EC2 instance the minimum permissions needed to perform its functions. See https://n2ws.zendesk.com/hc/en-us/articles/33252616725533--4-5-0-Required-Minimum-AWS-permissions-for-N2W-operations
7. 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

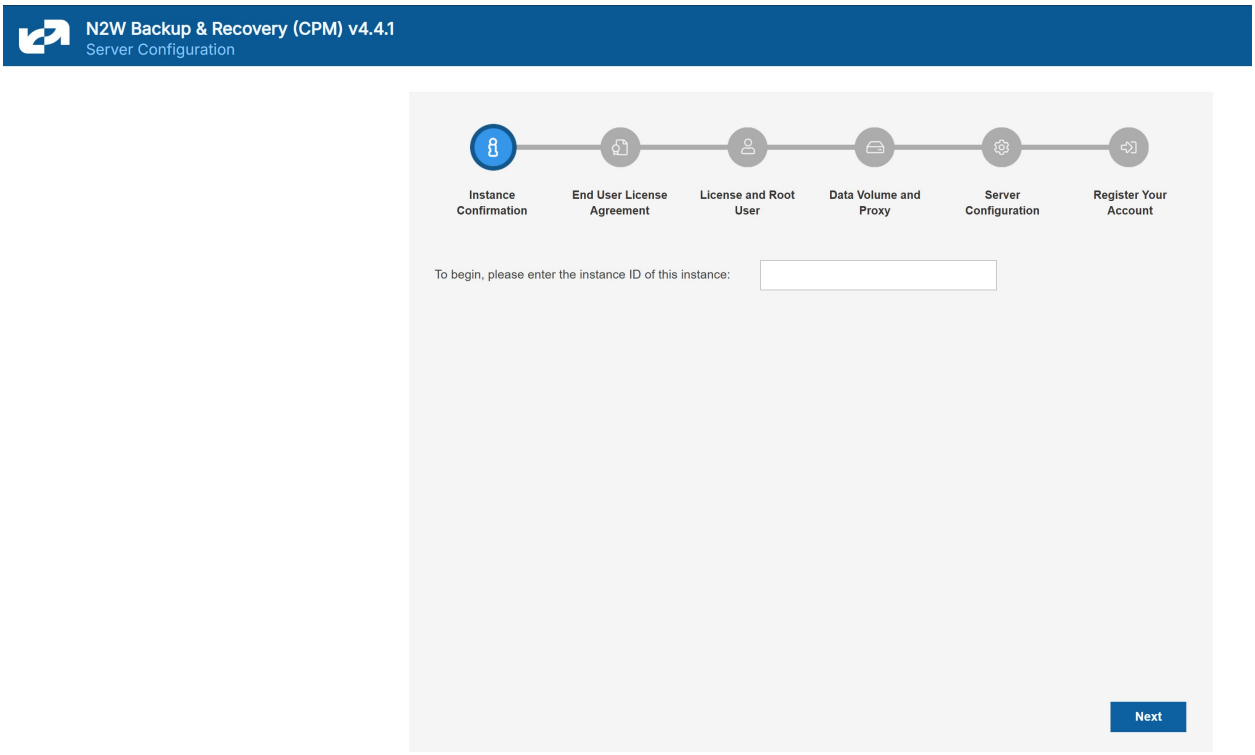
The N2W Server Configuration wizard takes you through the process step by step. There are a few differences between configuring N2W for the Free Trial and other paid editions.
For the Free Trial edition:

- 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

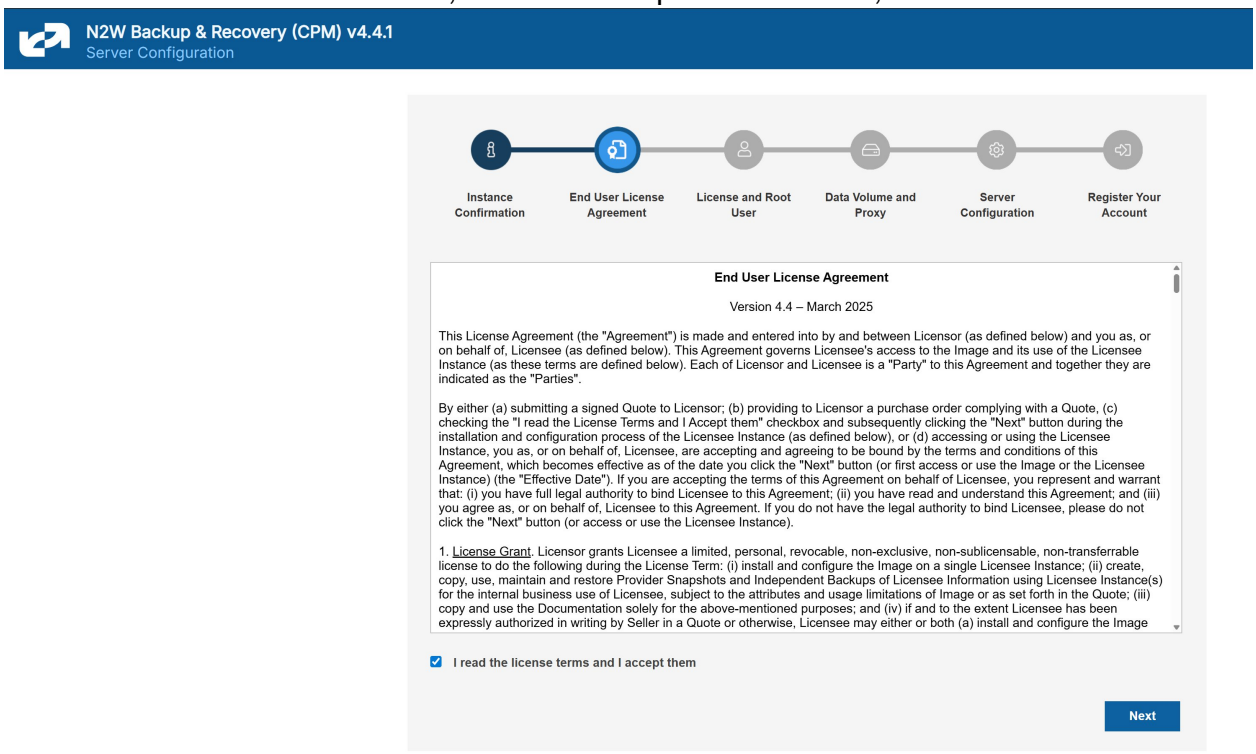
On the first screen you will be asked to type or paste the instance ID of this new N2W instance. This step is required to verify that you are indeed the owner of this instance.



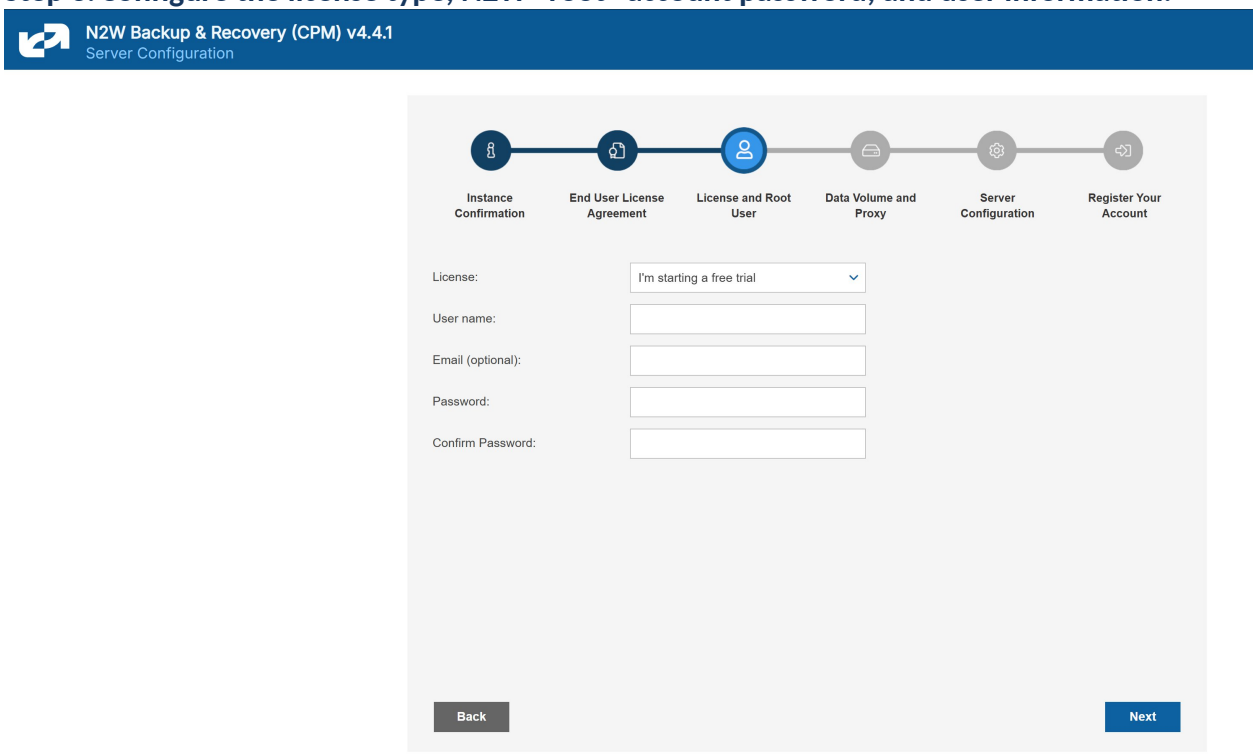
Select **Next**. In the next step the N2W configuration procedure begins.

Step 2: Approve the N2W license agreement.

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



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



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.

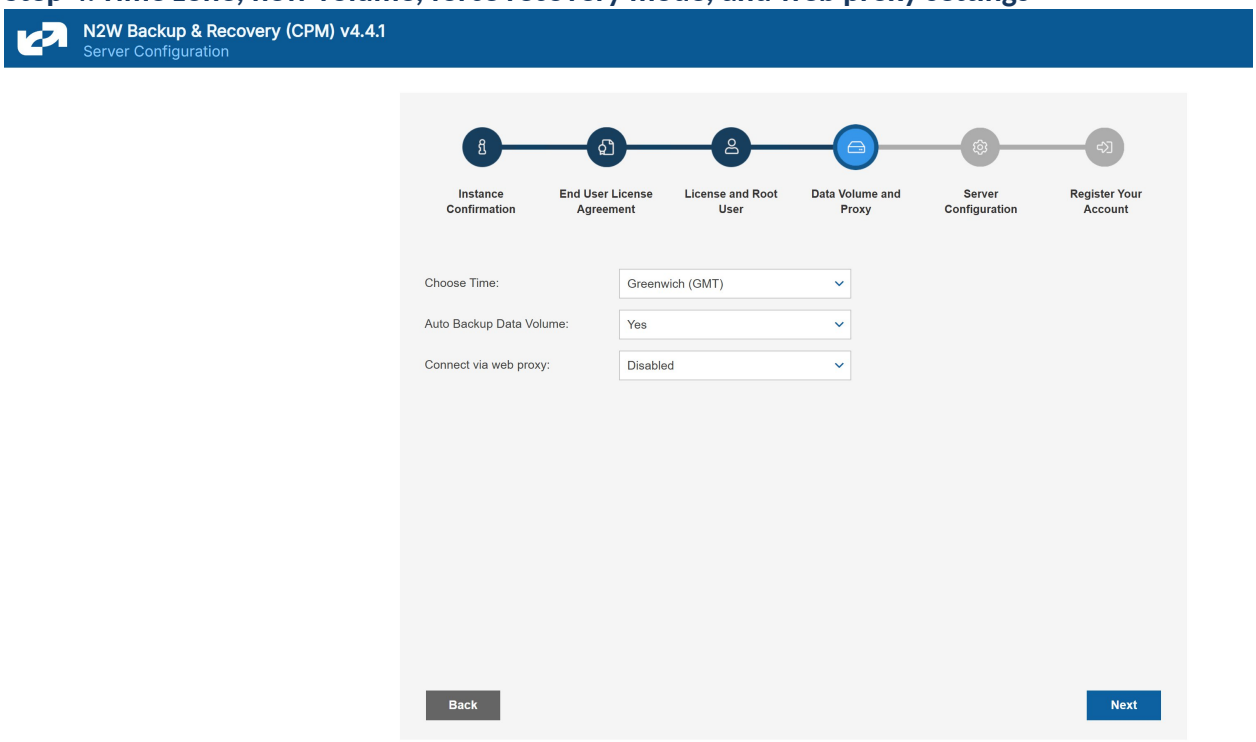
Note: If you are using one of the N2W paid products on AWS Marketplace, you will not see the License field.

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.

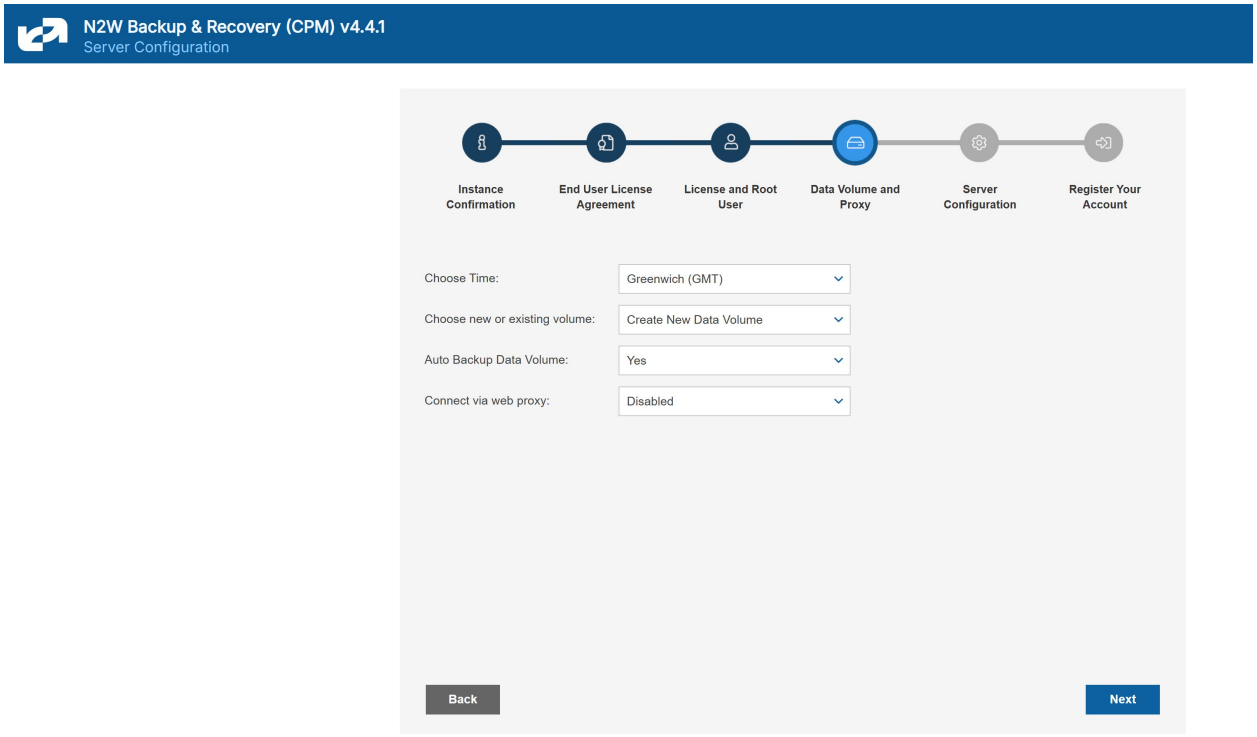
When you have completed entering the details for Step 3, select **Next**.

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



1. Choose your time zone.

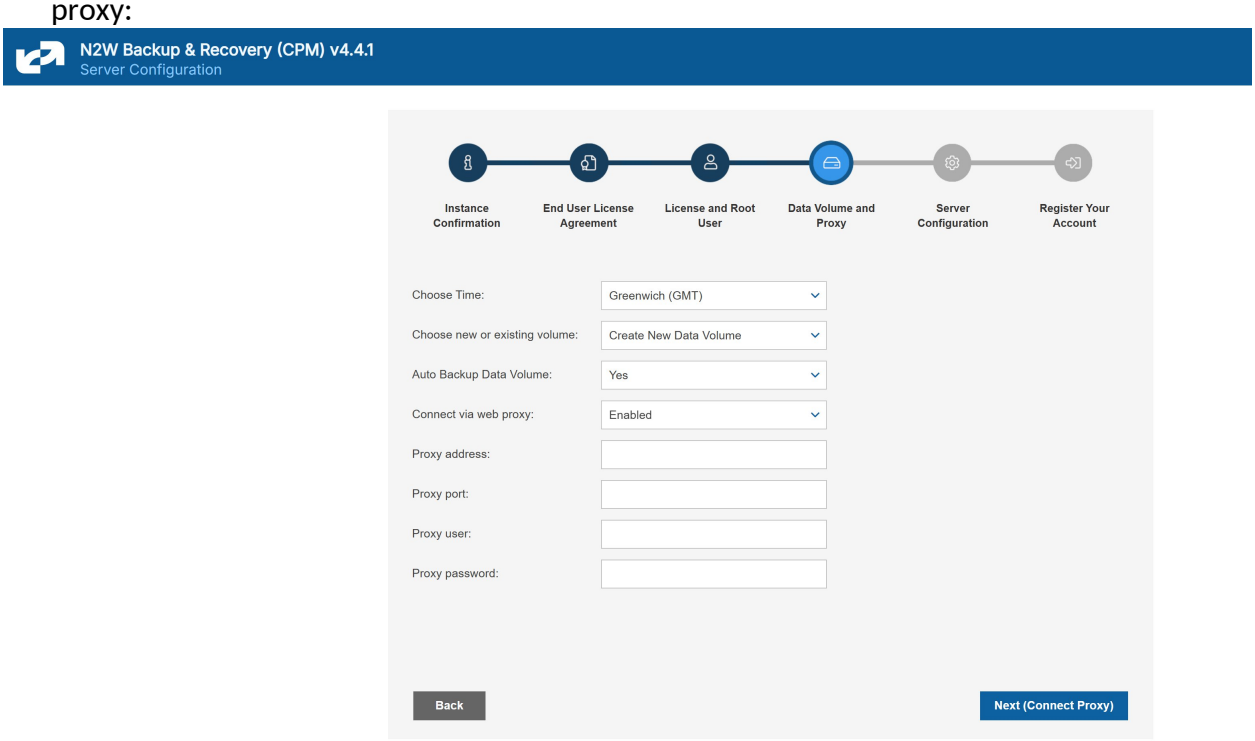
2. If configuring a paid edition, choose whether to create a new data volume or use an existing one. To configure an additional N2W server, in recovery mode only, choose an existing data volume and select **Force Recovery Mode**. In Step 5, you will be presented with a list of existing N2W data volumes.



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

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

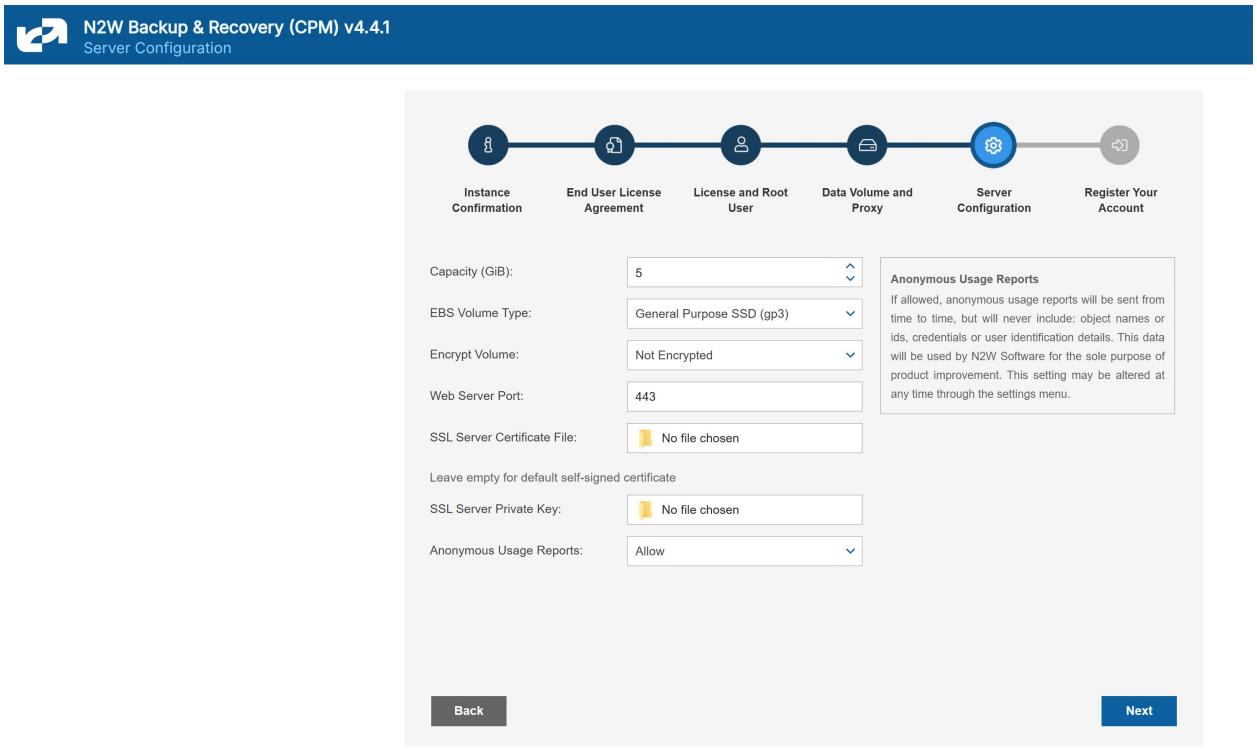
3. If you select **Enabled** for **Connect via Web proxy**, additional boxes appear for defining the proxy:



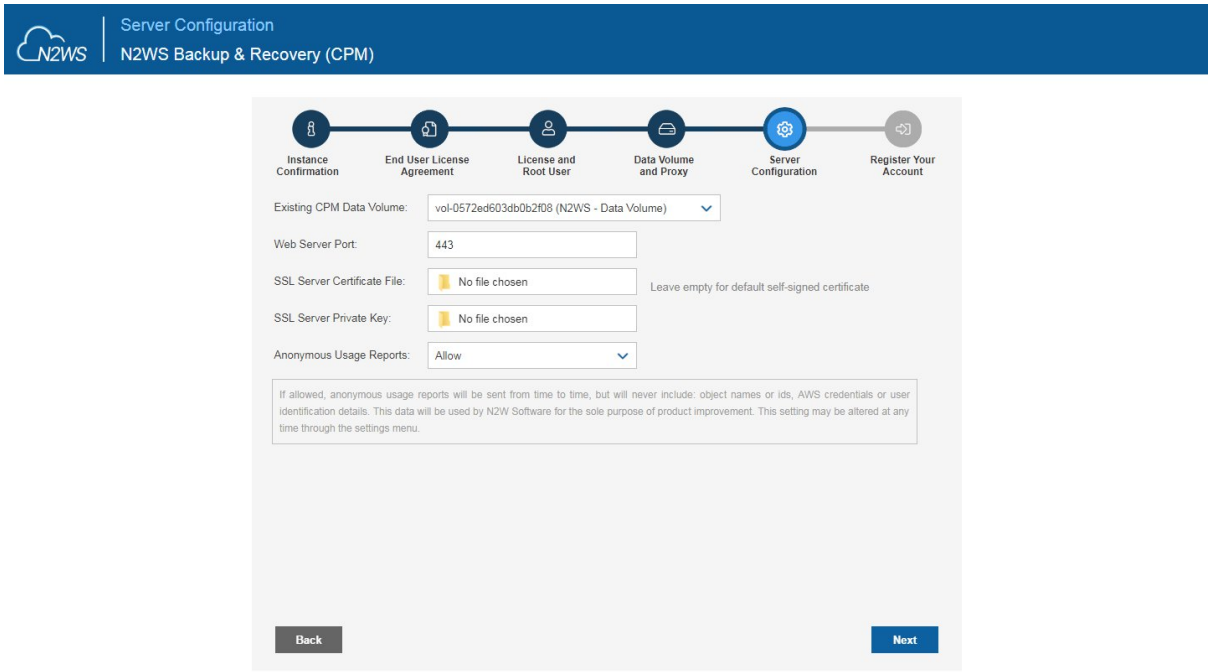
4. Select **Next**.

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.



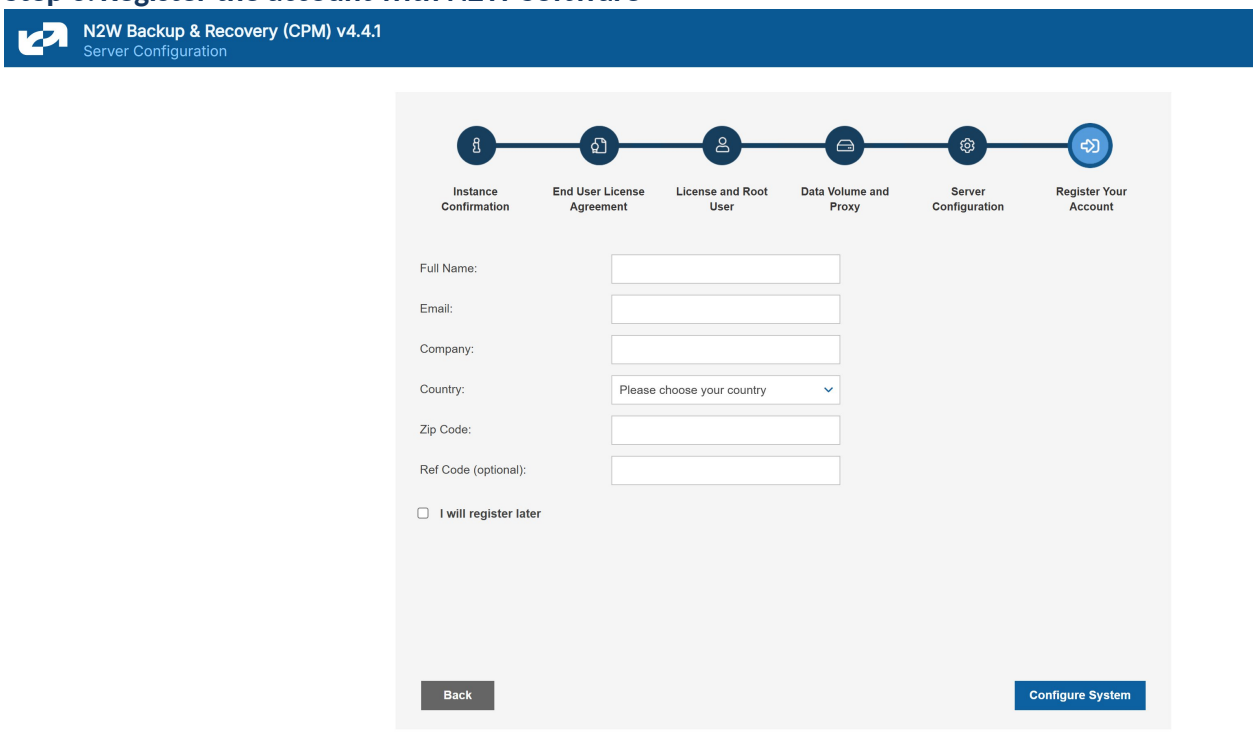
2. If you choose to use an existing volume or selected **Force Recovery Mode** in Step 4, you will see a drop-down volume selection box.



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



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.

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.

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.

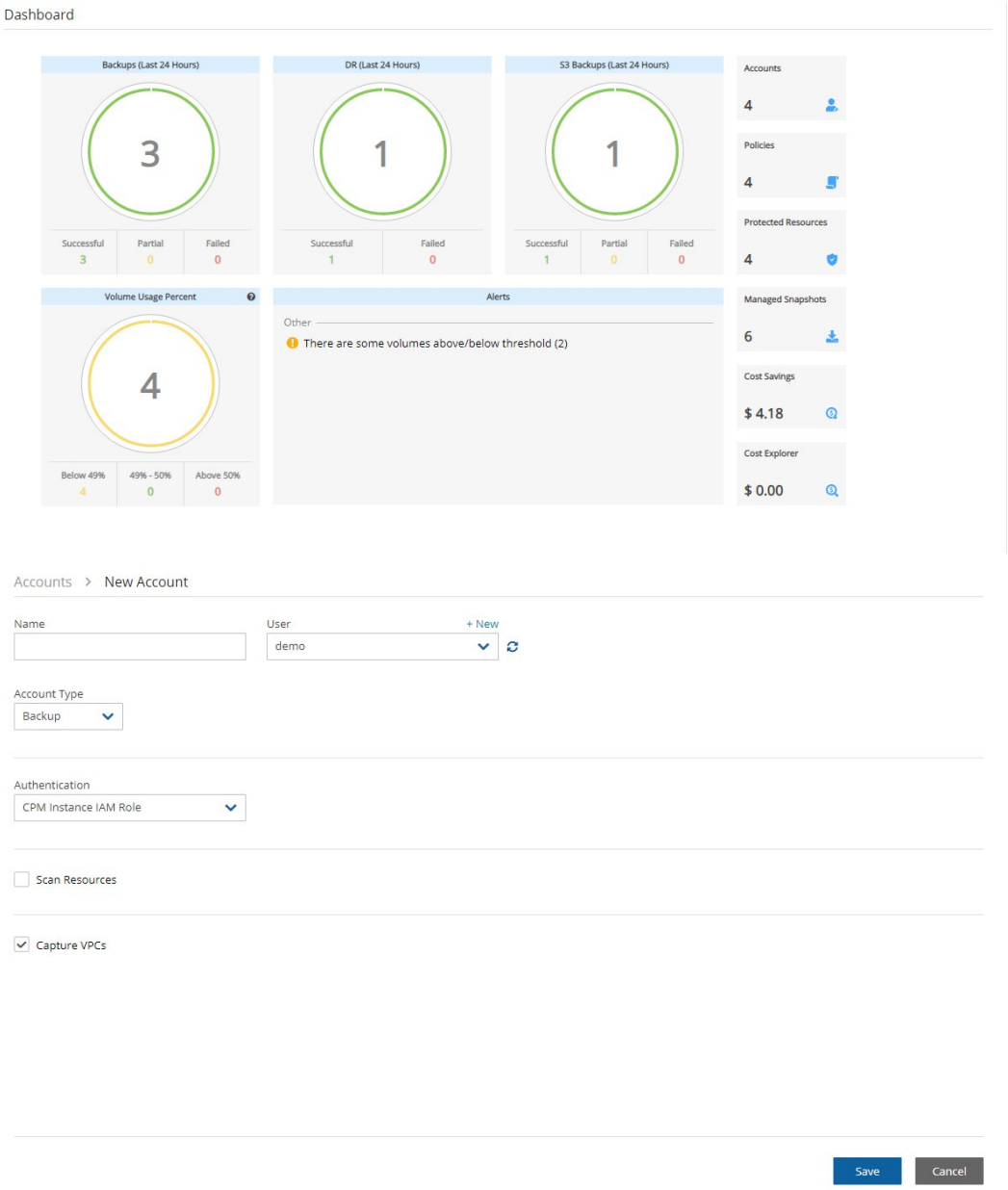
N2W automatically creates your first AWS account and policy. The required **cpmdata** policy is used to back up the N2W data volume.

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:

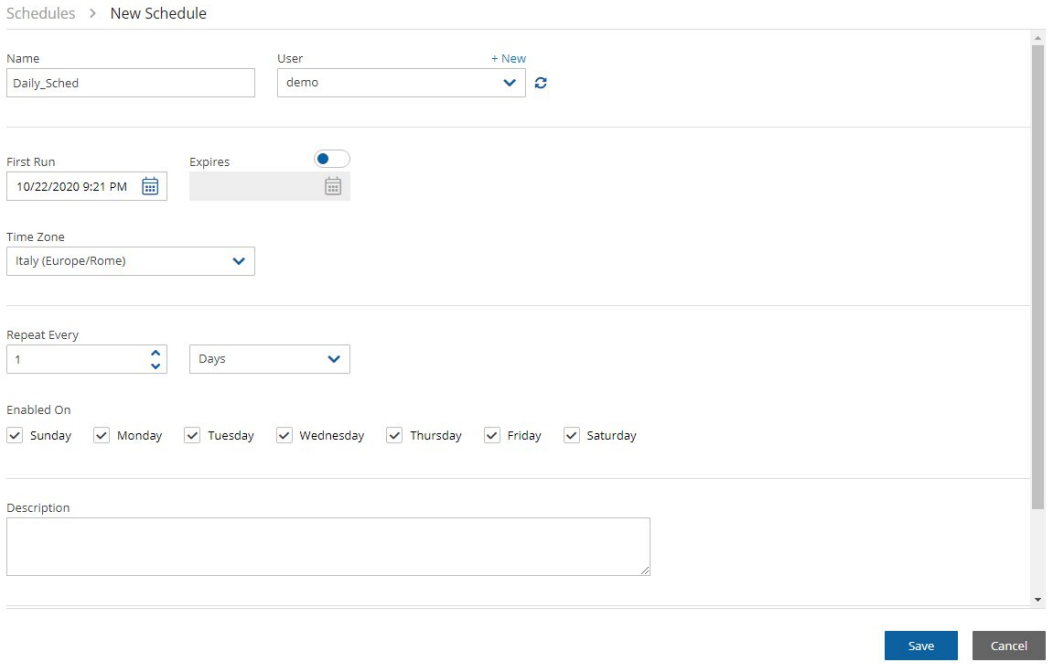


6. Go to **Accounts** and click **New**
1. In the **Name** box, type the name you would like to associate with your primary AWS account.
2. In the **Account Type** list, select **Backup**. A **DR** account is for cross-account backup and recovery and is out of the scope of this guide. See “Account Type” 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

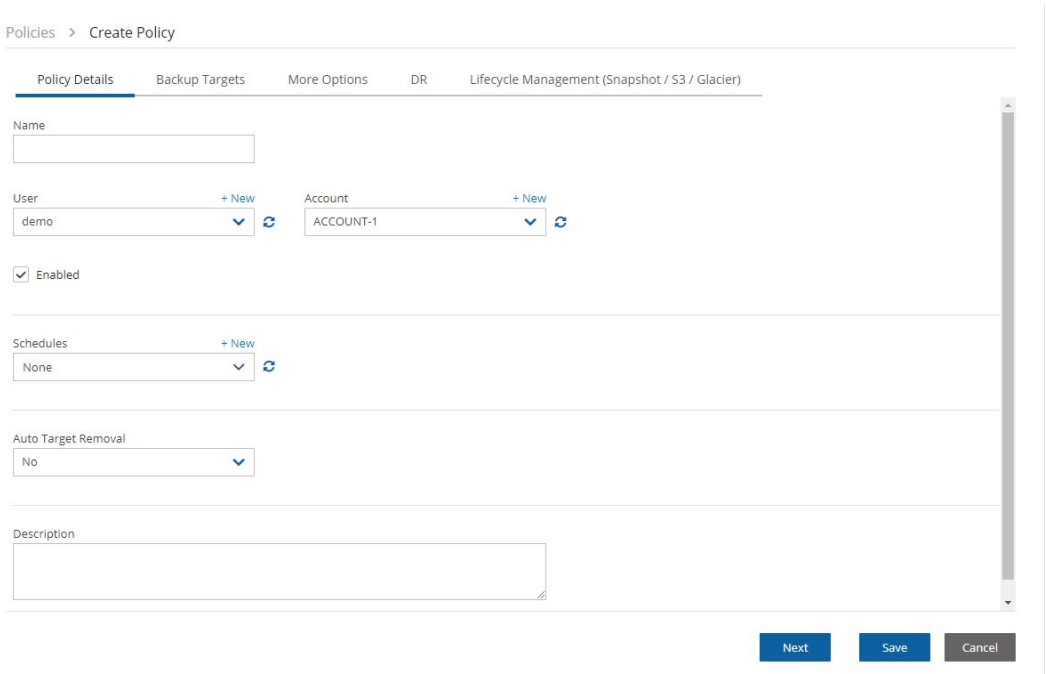
In the left panel, select the **Schedules** tab. Currently, the list of schedules is empty. You will now create the first schedule. Select + **New**.



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**.

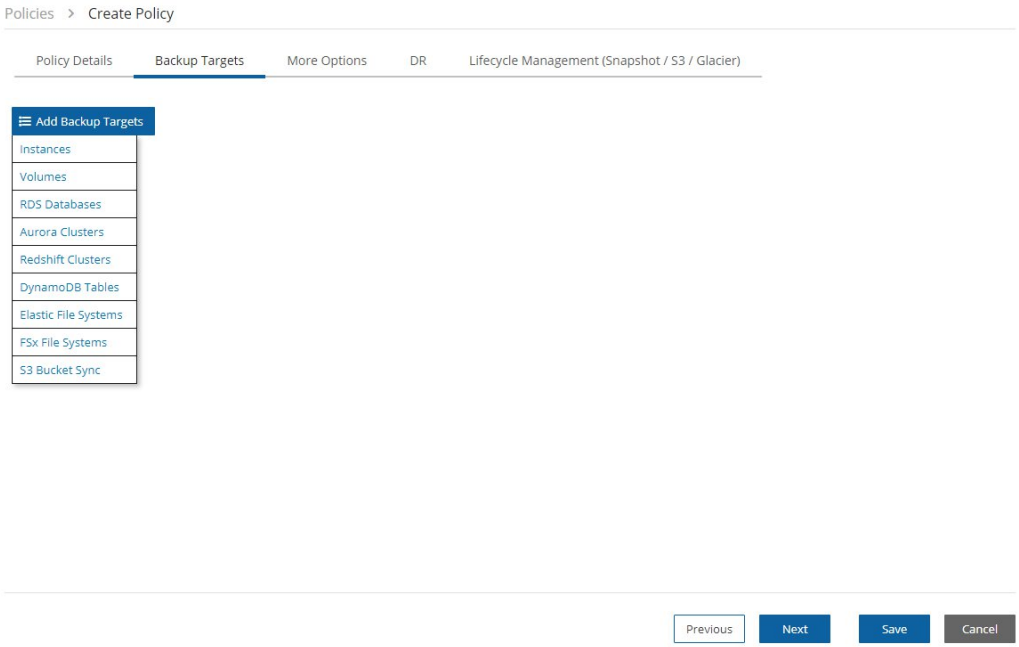
4.3 Creating a Simple AWS Backup Policy

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



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.

2. 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:

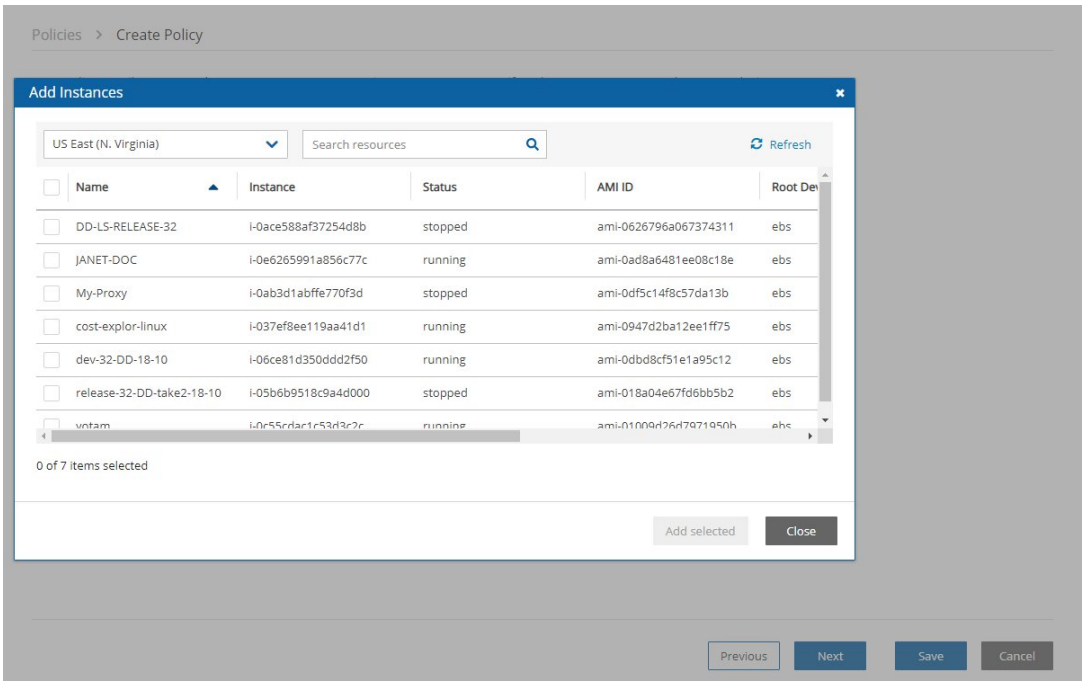
- **Instances** - Back up EC2 instances, including their metadata, and optionally some or all of their data volumes. This is the most common backup target.
- **Volumes** - Back up EBS volumes independently, whether or not they are attached to an instance, and regardless of which instance they are attached 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.

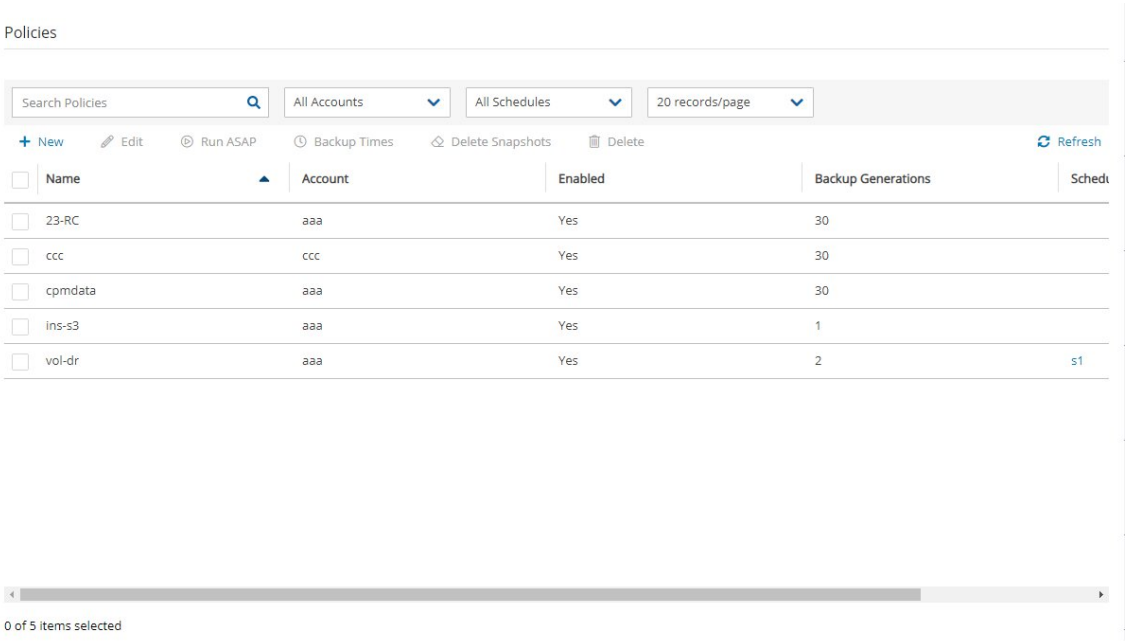


Select the instance that you want to back up, and then select **Add Selected**. This will add the requested instance to the screen in the background and remove it from the popup window, although it does not close the popup. You can add as many instances as you want up to the limit of your licence. Select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

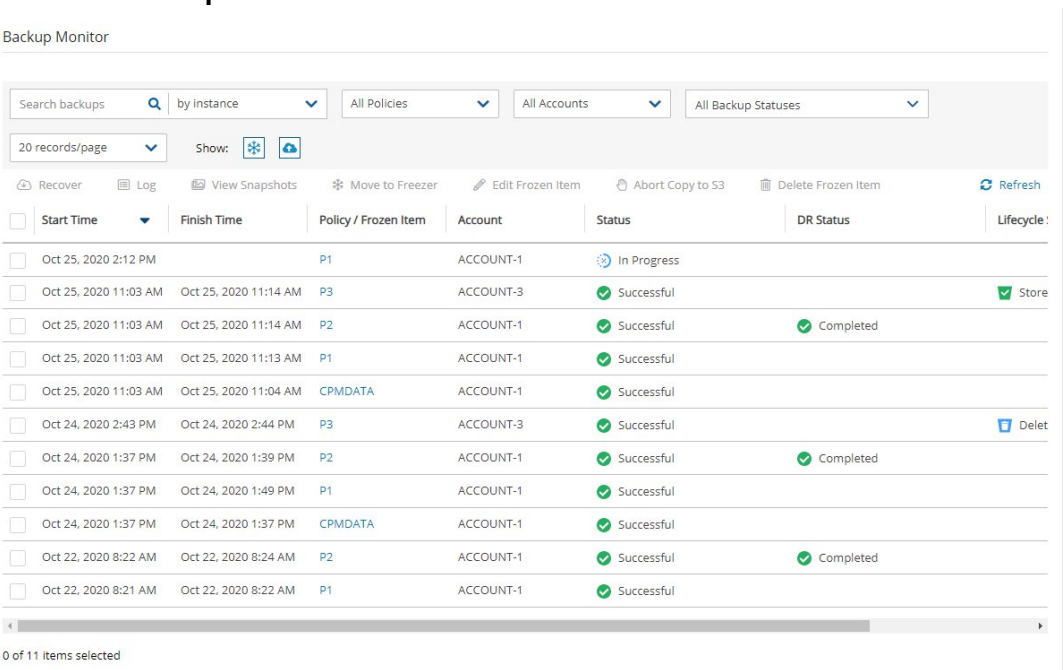
Back in the **Backup Targets** screen, you can see the instance in the list of instances. You have the option to remove it from the policy and a **Configure** button. Select the instance, and then select **Configure** to review which volumes to back up and other options.

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.**



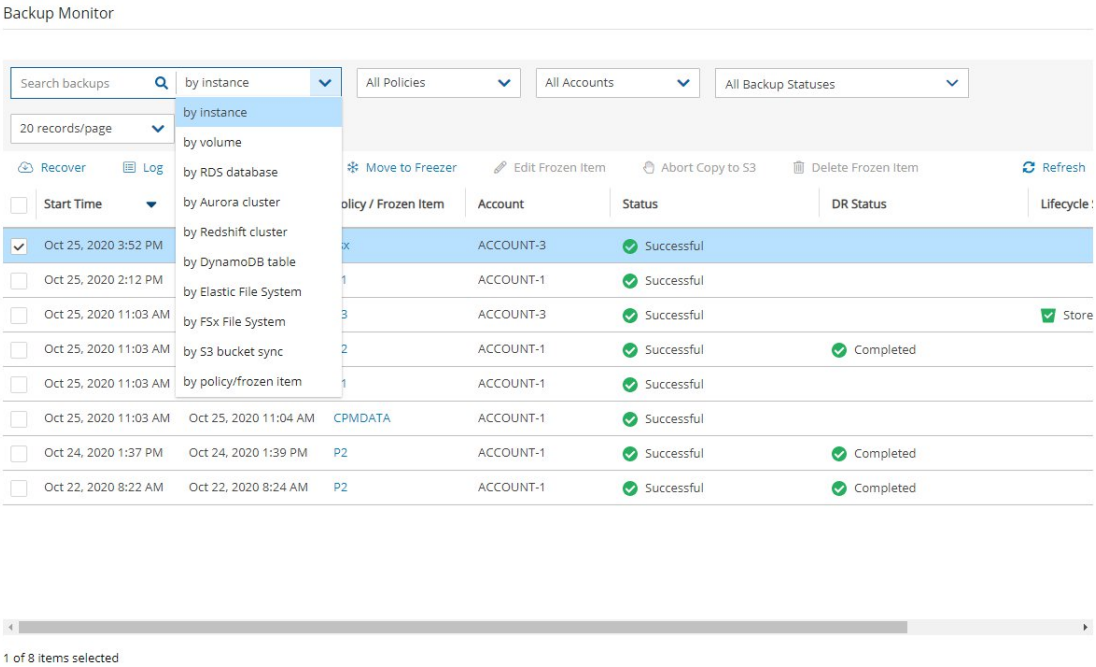
N2W will report that the backup policy will now run. The process can be monitored by following the **Status** in the **Backup Monitor** tab.



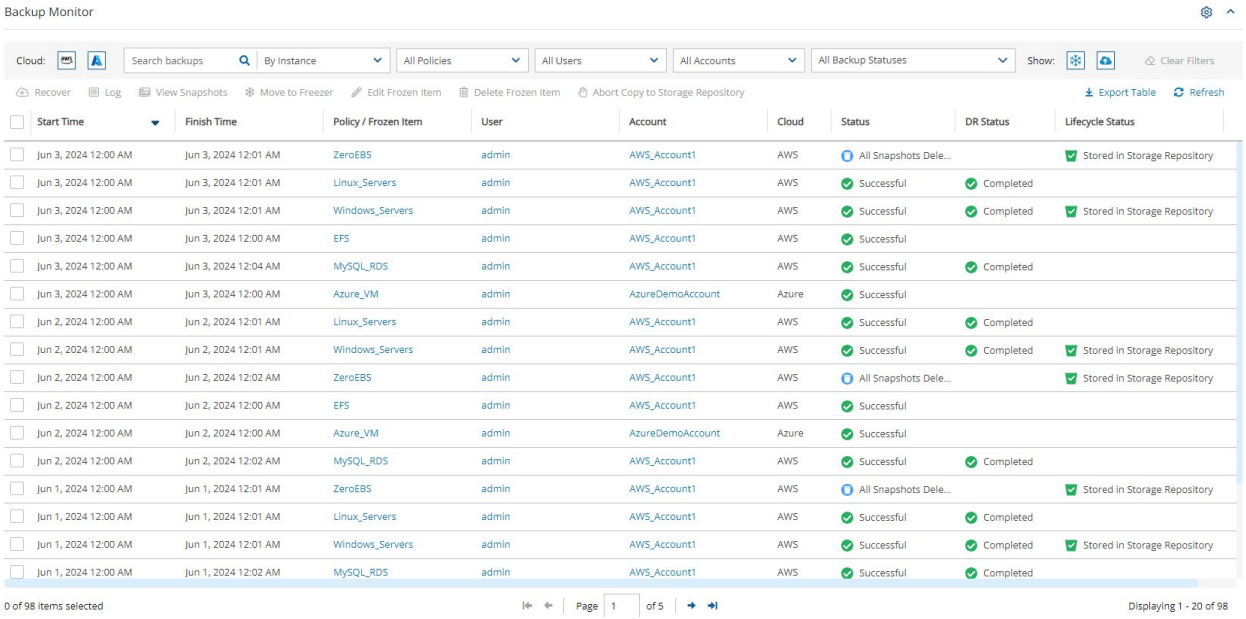
Consult the *N2W Backup & Recovery User Guide* to see how to create application consistency for Linux and Windows servers.

5 Performing a Basic Recovery

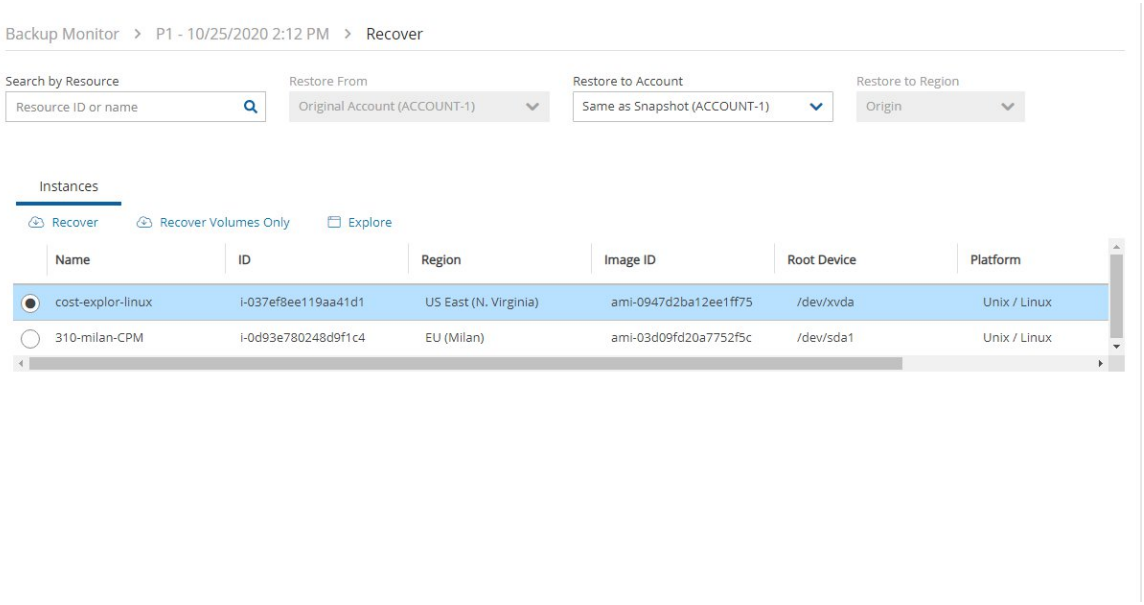
You can view the backups in the **Backup Monitor** tab. You can search for snapshots based on the Backup Target type, Policy, Account, and backup status.



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**:

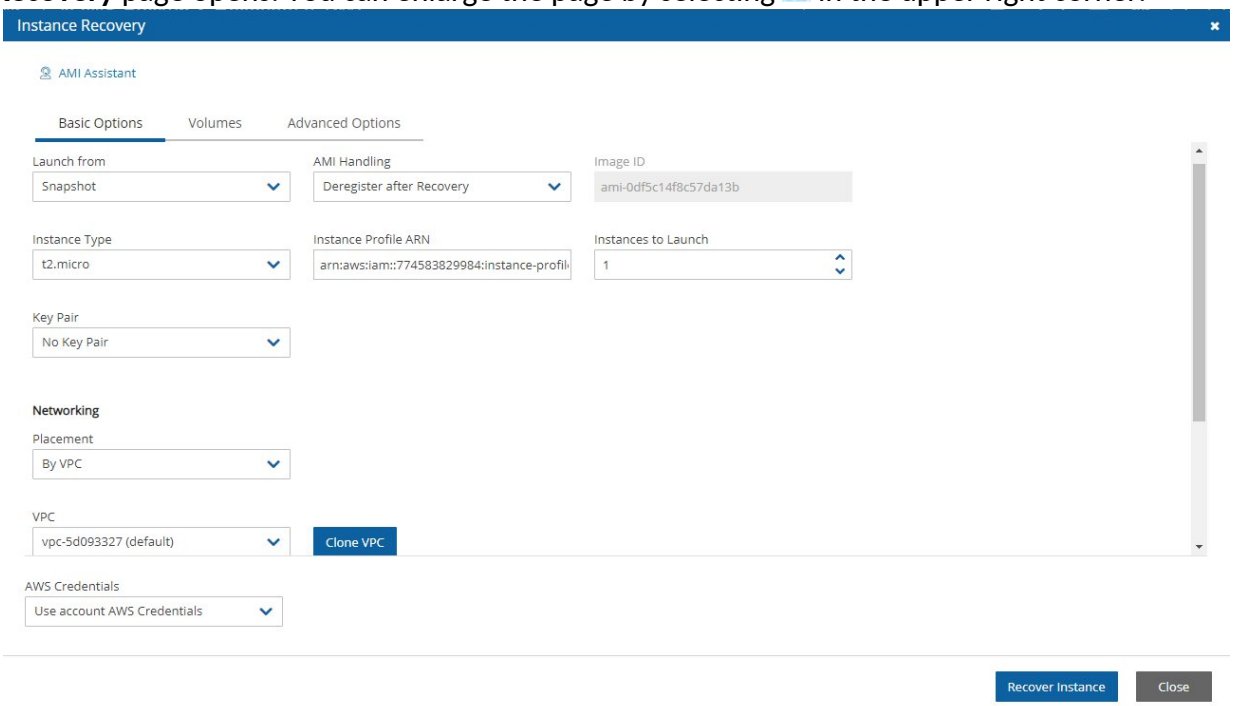


In the **Recover** screen, you can see all the instances that this backup contains. Should this policy include also EBS volumes, RDS databases, Redshift Clusters, or DynamoDB Tables, you will have a tab to recover them as well. In order to recover an instance, select the **Instances** tab.



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.



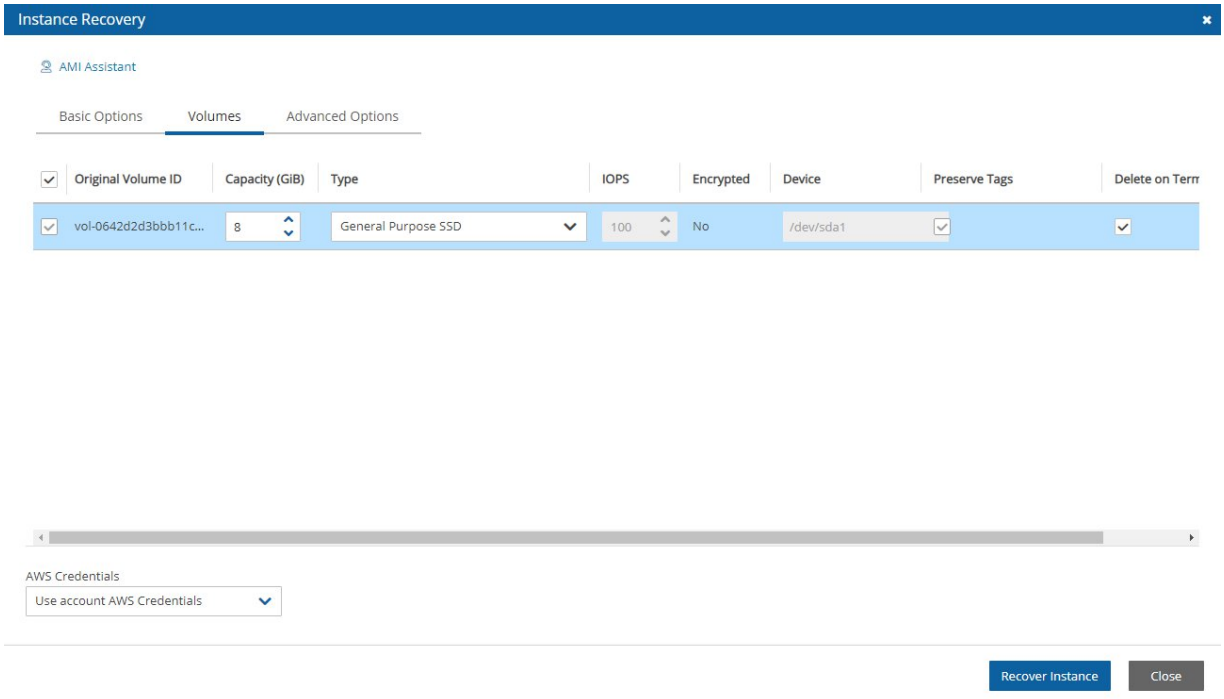
Most of the options when launching EC2 instances are available here and may be modified. The currently selected defaults are exactly the options the original backed-up instance had at the time of the backup, including the tags associated with it.

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.

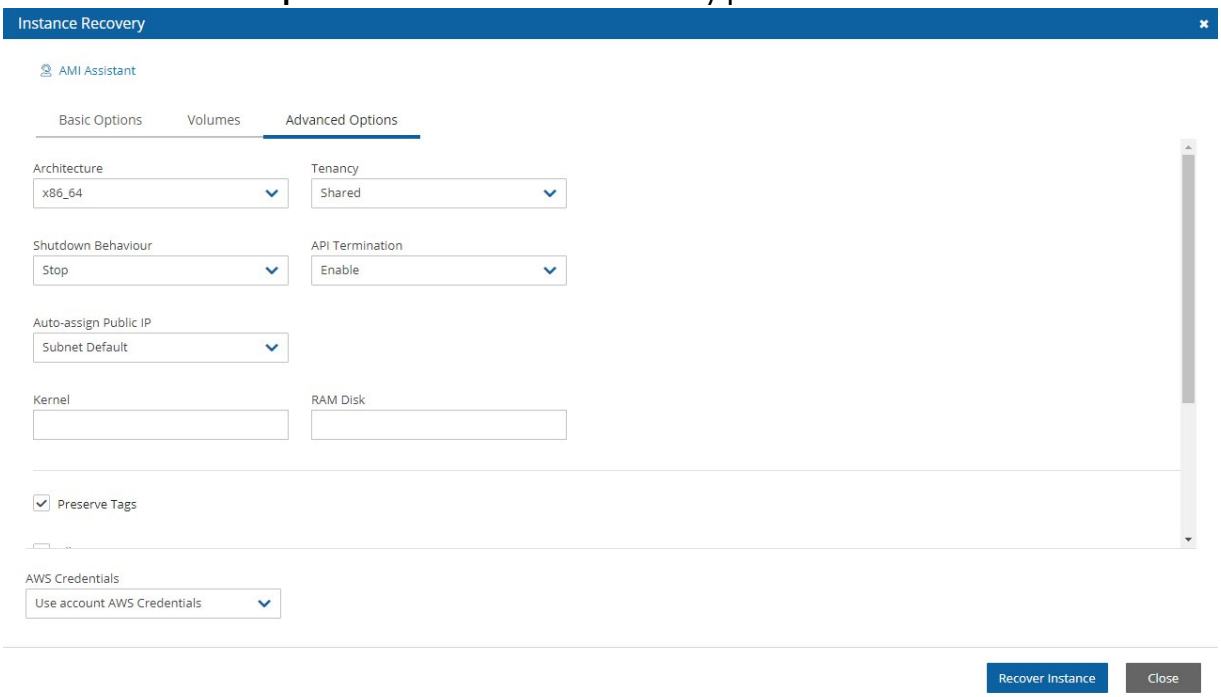
The **Clone VPC** option allows you to recover the instance to a clone of a selected VPC environment. See https://docs.n2ws.com/user-guide/10-performing-recovery

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.

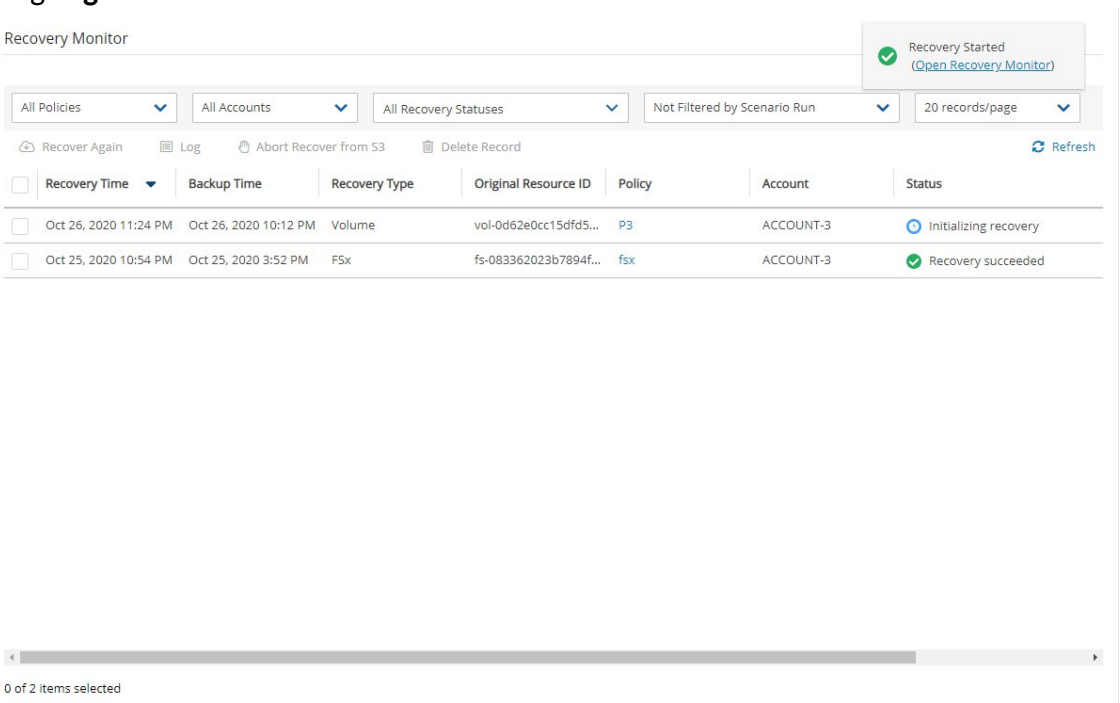
Select the **Volumes** tab to choose which volumes to recover and how.



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



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**.



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.

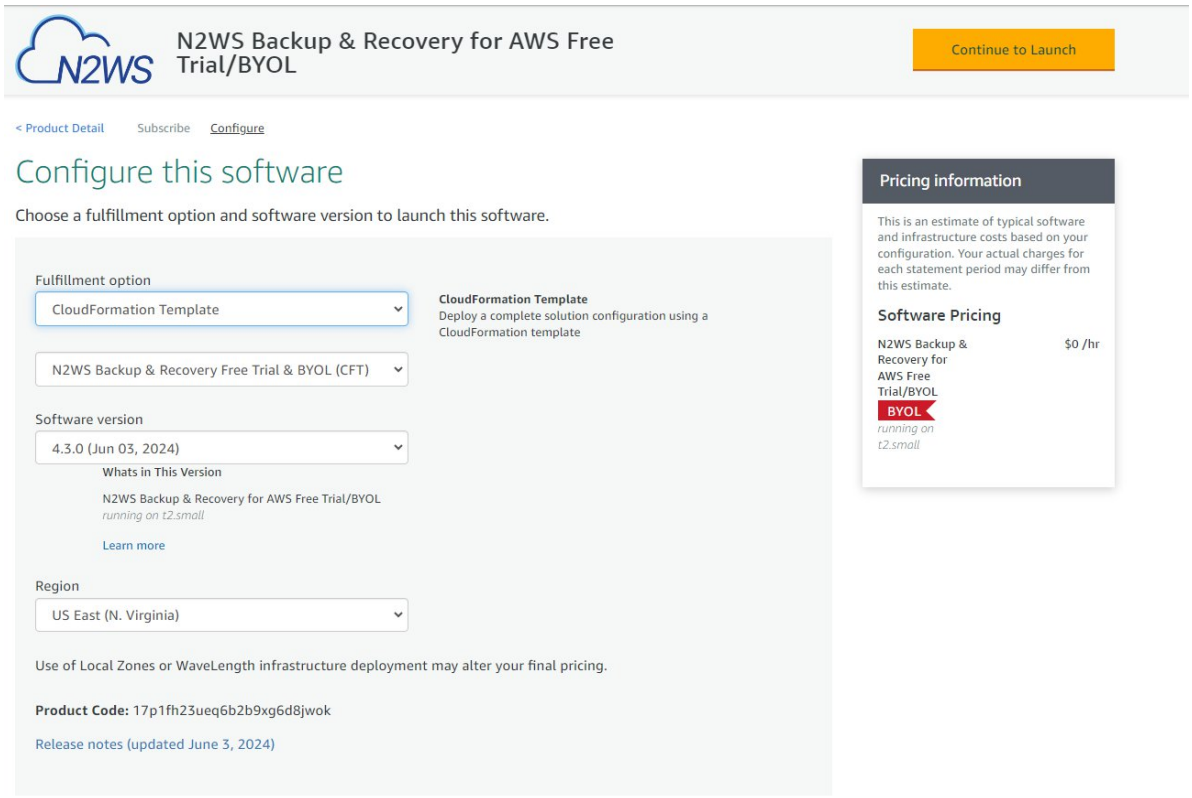
6 How to Configure N2W with CloudFormation

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.

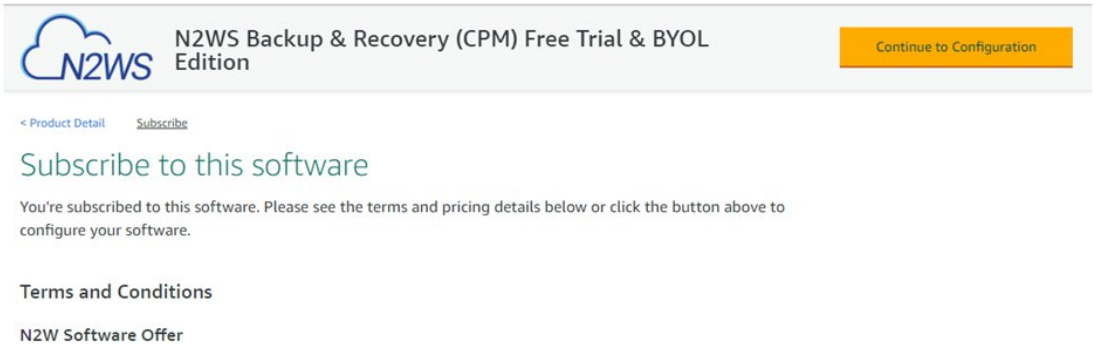
Note:

- 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.

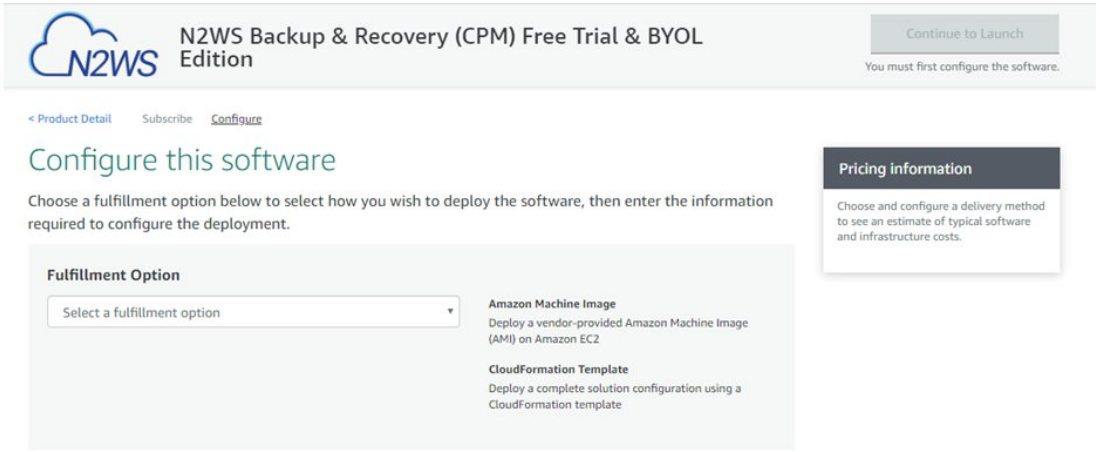
1. Go to https://aws.amazon.com/marketplace
2. Search for N2W.
3. Select **Continue to Subscribe**.



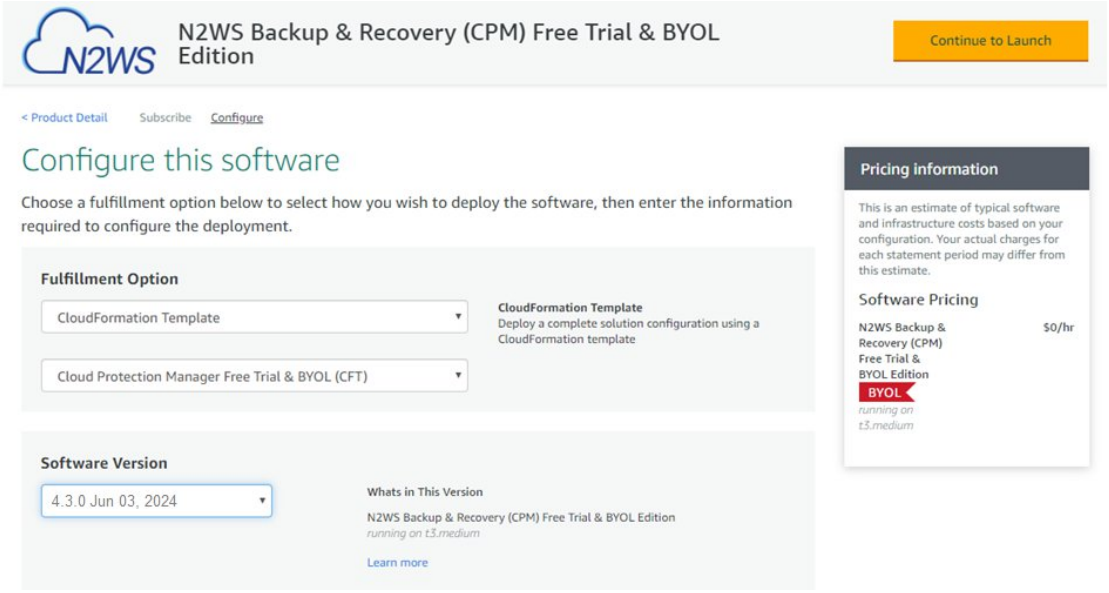
4. Log in and select **Accept Terms**.



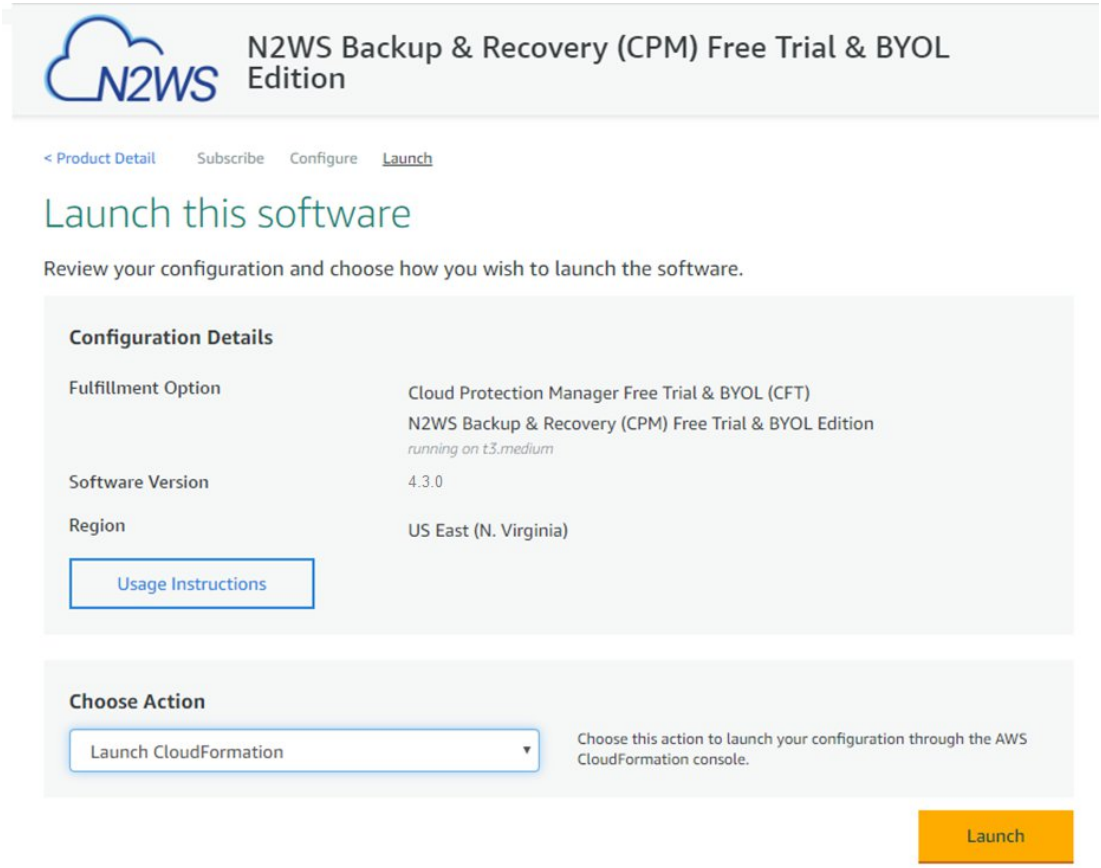
5. Select **Configure to Configuration**.



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

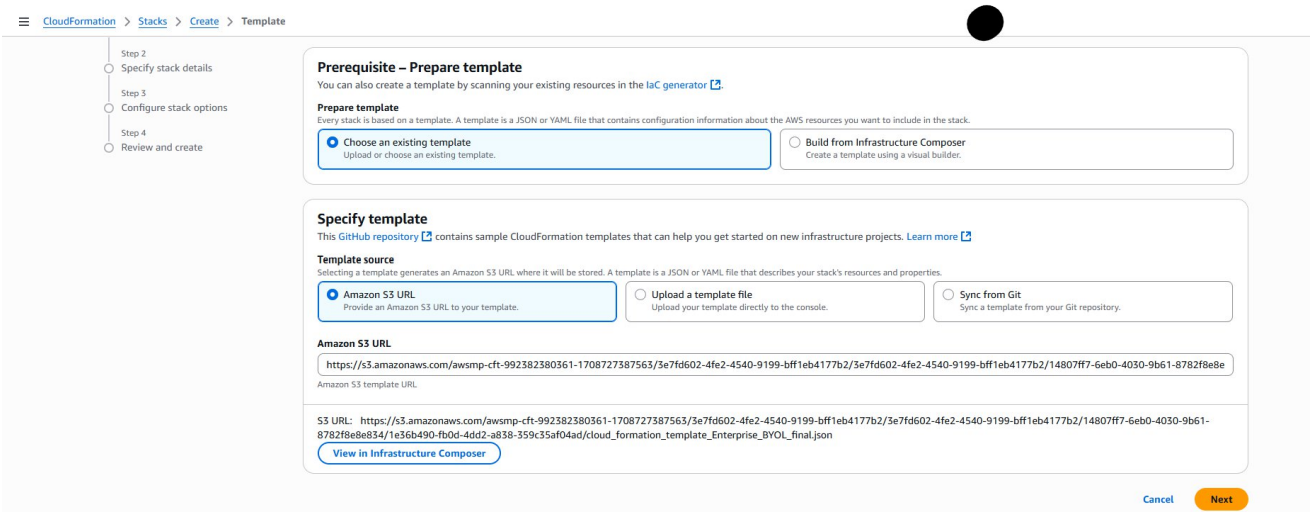


7. Select the relevant **Software Version** and then select **Continue to Launch**.

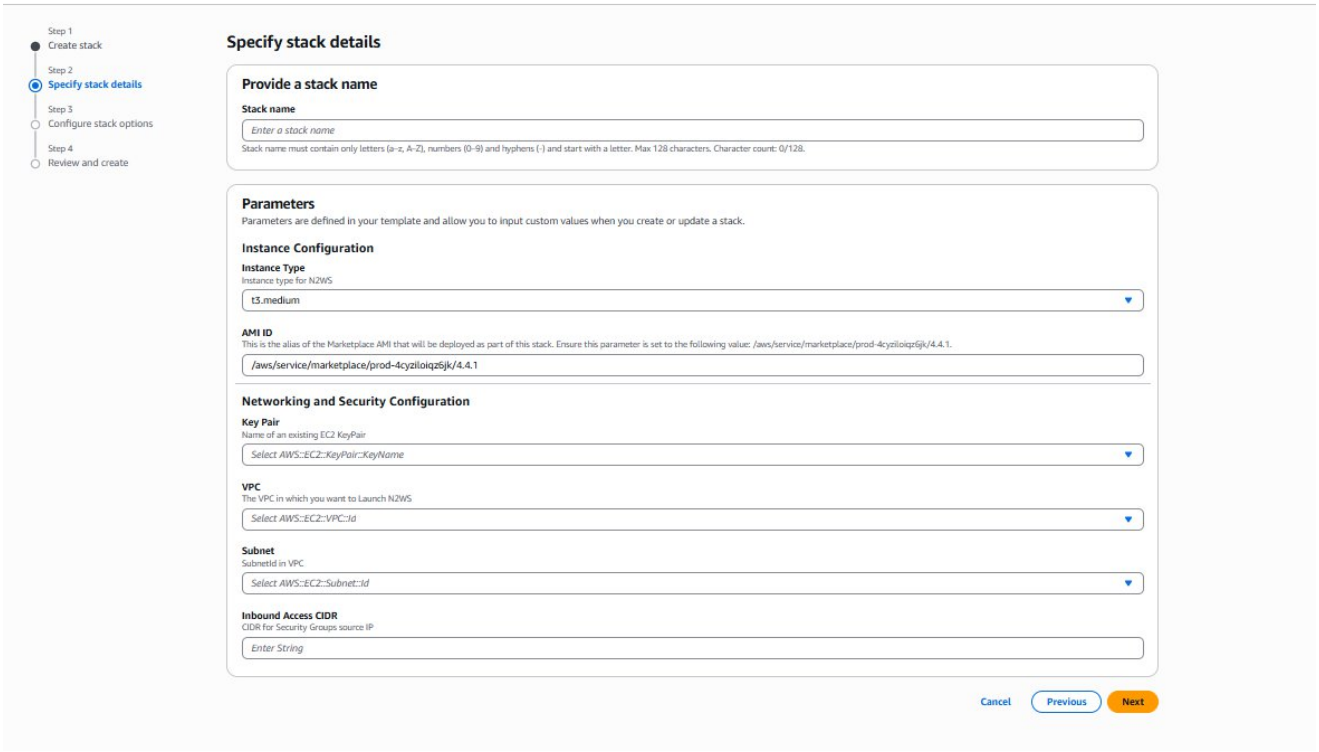


8. In the **Launch this software** page, select **Launch CloudFormation** in the **Choose Action** list, and then select **Launch**.

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

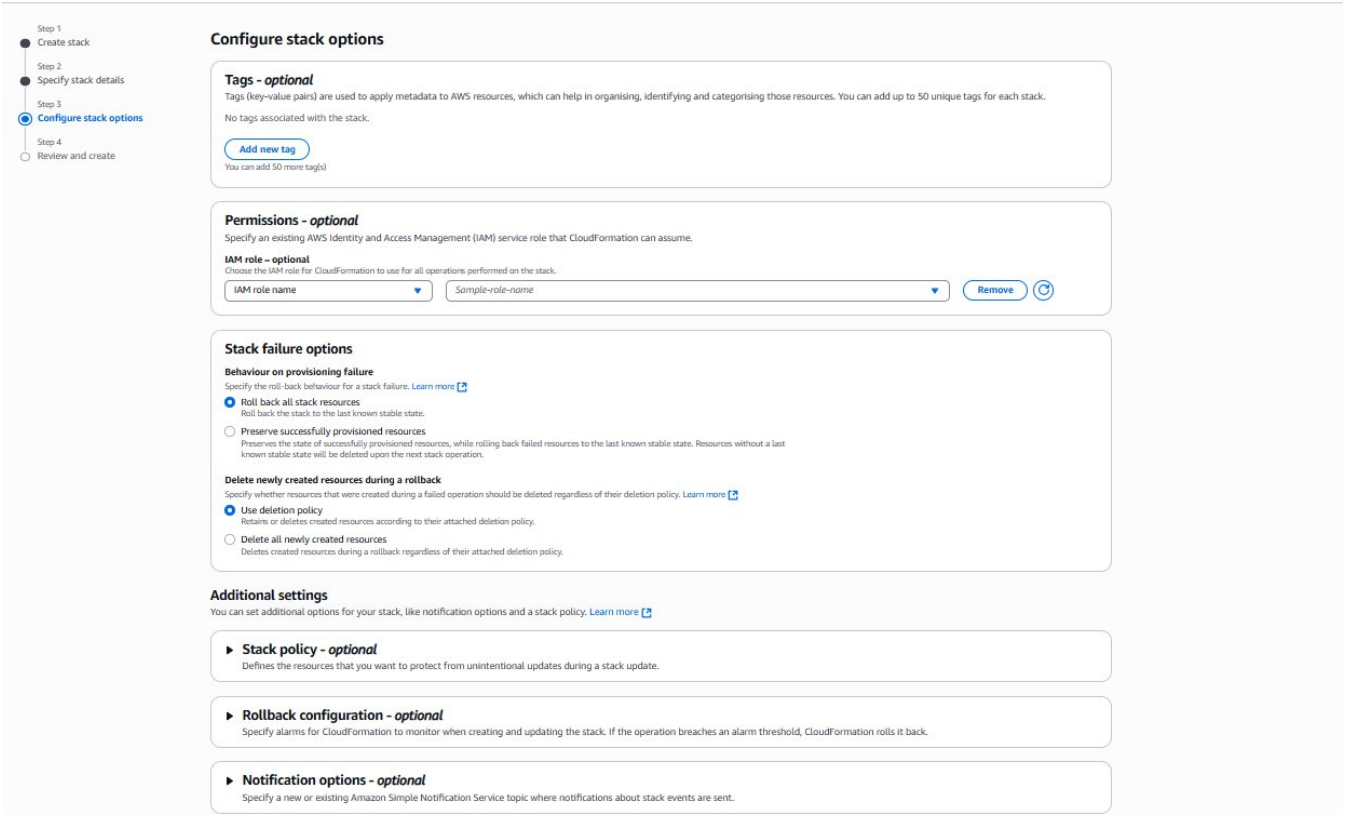


9. Under **Prepare template**, select **Choose an existing template**.
10. Under **Specify template**, choose **Amazon S3 URL**. Select the default Amazon S3 URL, and then select **Next**. The **Specify stack details** page opens.

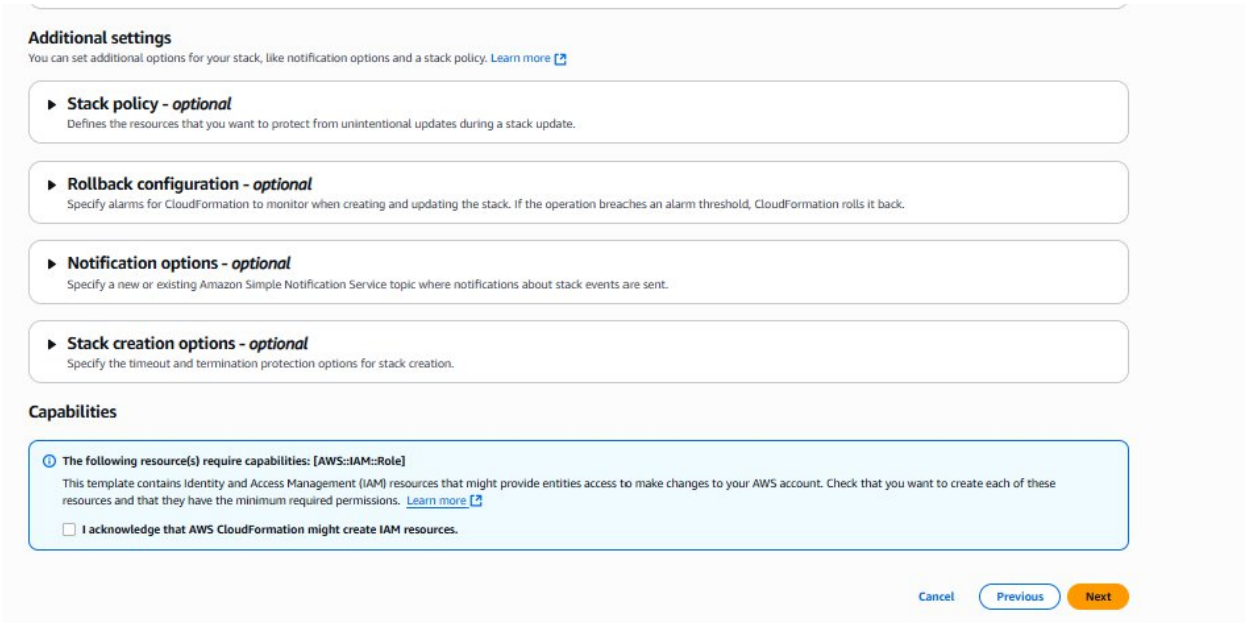


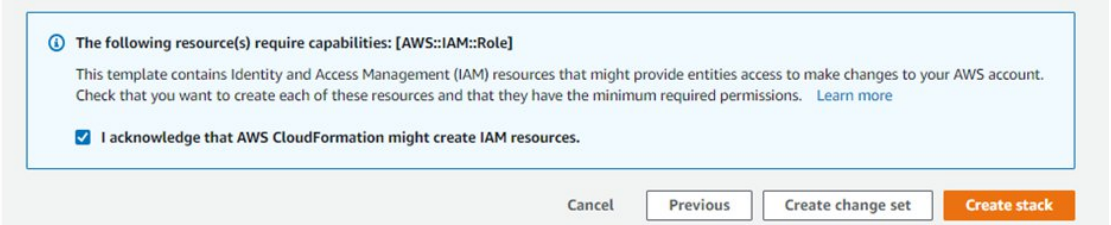
11. Complete the **Stack Details** and **Parameters**. For **Inbound Access CIDR**, security groups act as a firewall for associated instances, controlling both inbound and outbound traffic at the instance level. Configuring **Inbound Access CIDR** allows you to add rules to a security group that enable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



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





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

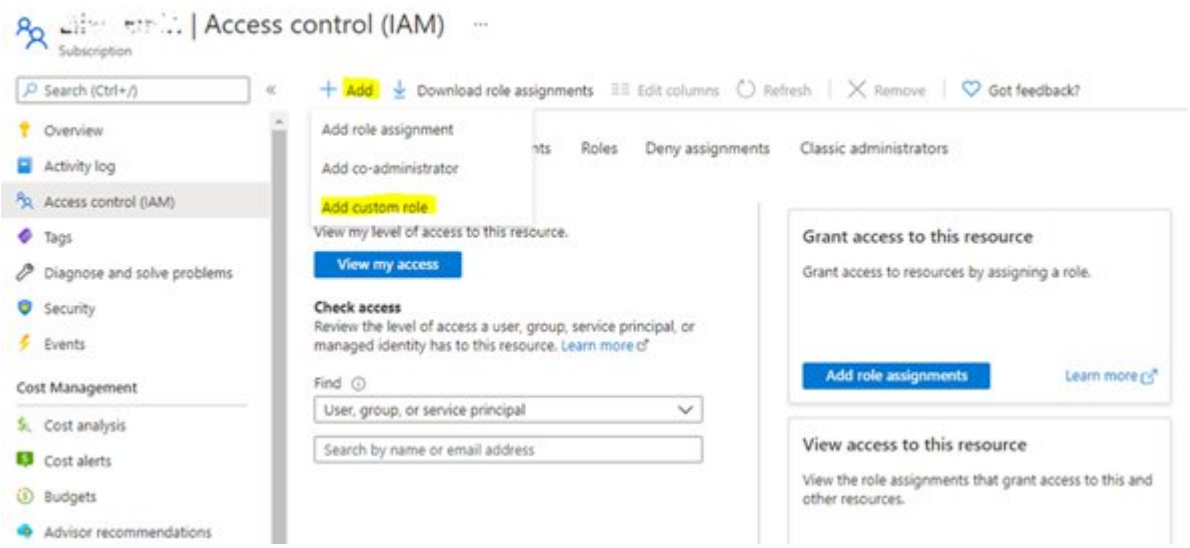
1. Save the following text in a JSON file, adding your Subscription ID value to the "subscriptions" attribute:

```
{
  "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": [],
```

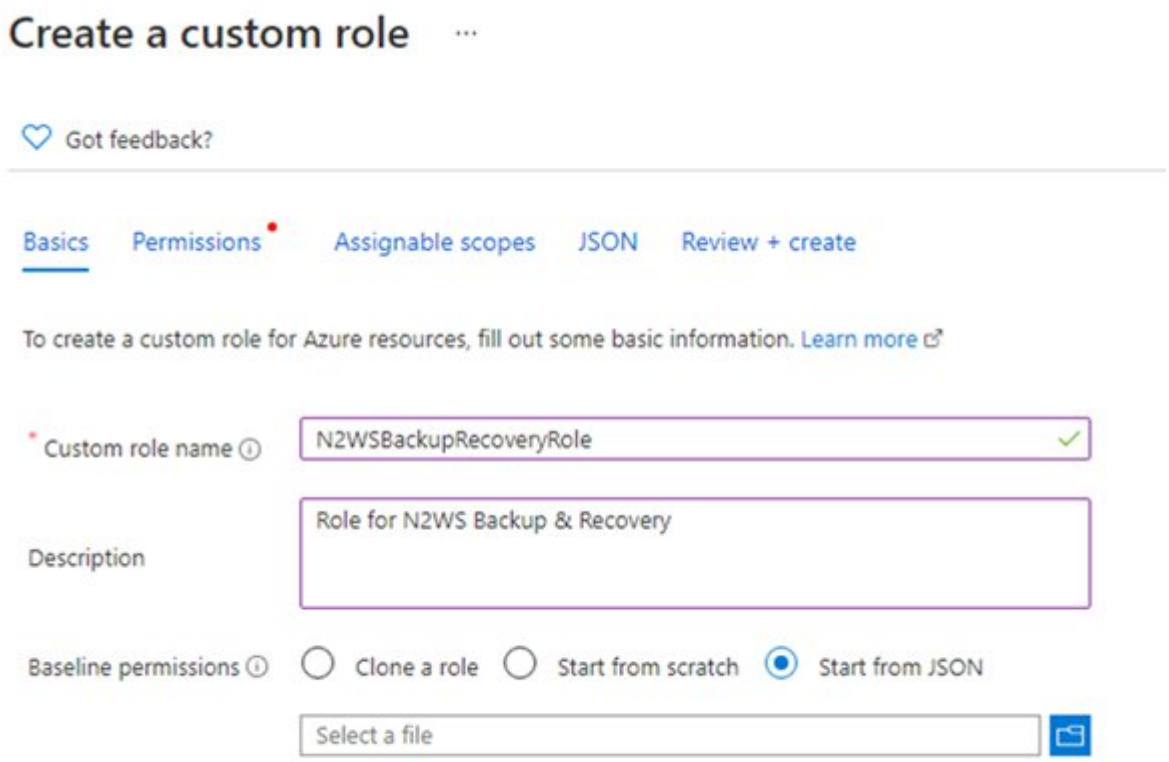
```
            "notDataActions": []
        }
      ]
    }
  }
```

2. In the Azure Portal, go to your subscription and select a subscription that you want to use with N2W Backup & Recovery. 

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



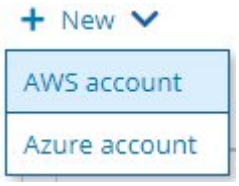
4. Complete the form as follows using **N2WSBackupRecoveryRole** as the **Custom role name**, and then select the JSON file saved in step 1.



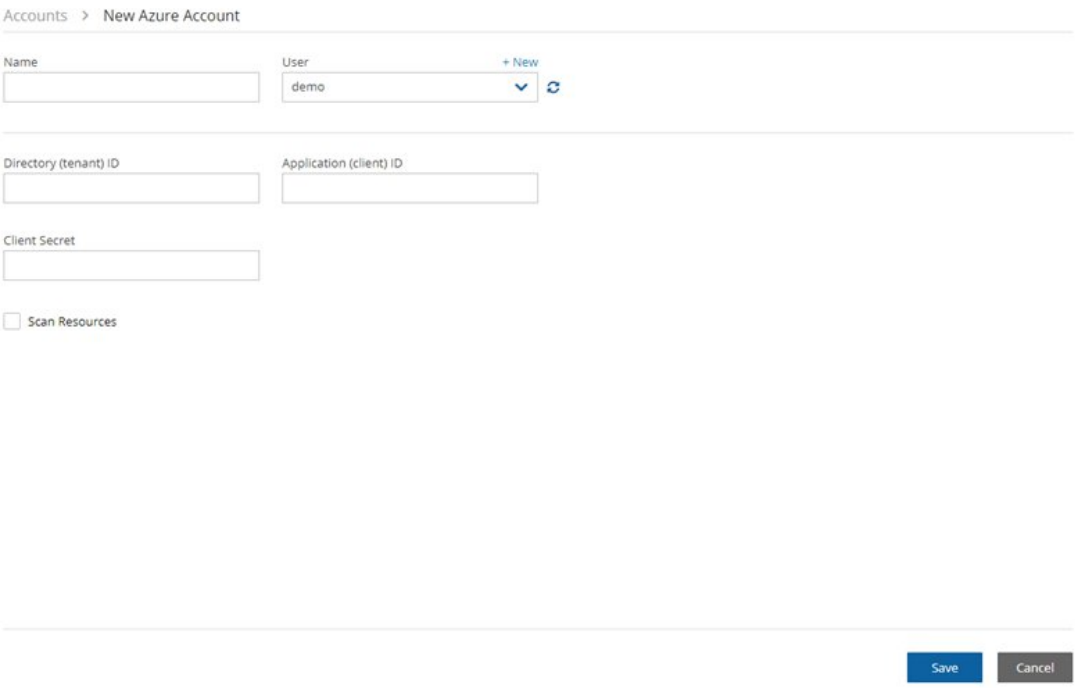
5. Create the role with the new JSON file.

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.

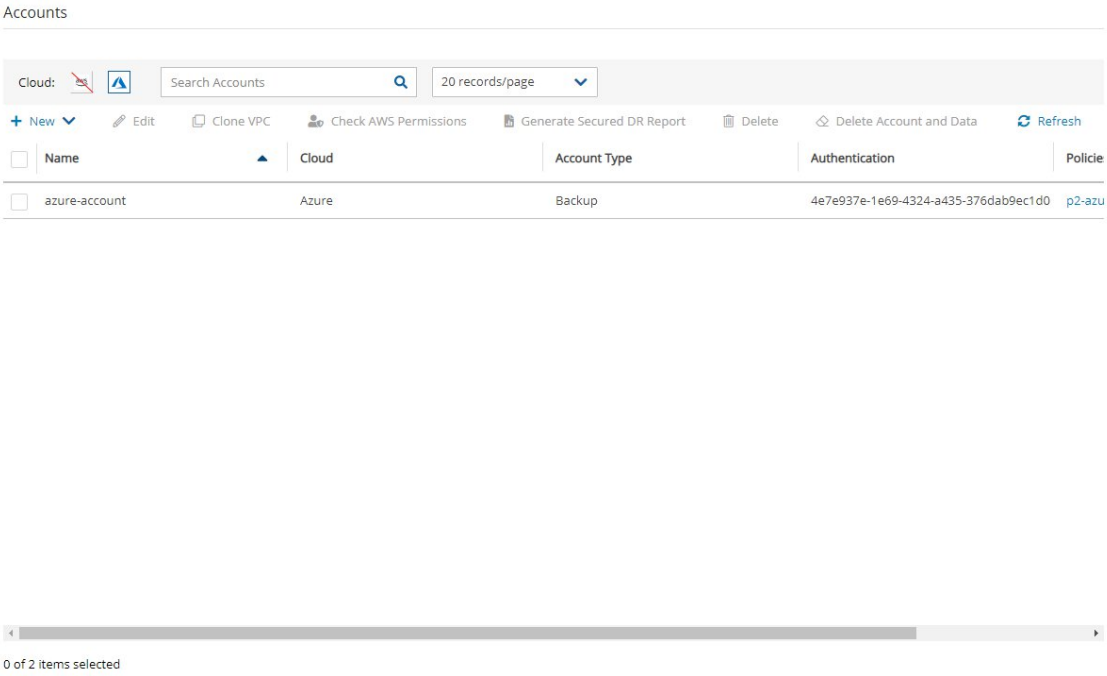


4. Complete the New Azure Account screen using the App Registration view information in the Azure portal as needed.



- **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.

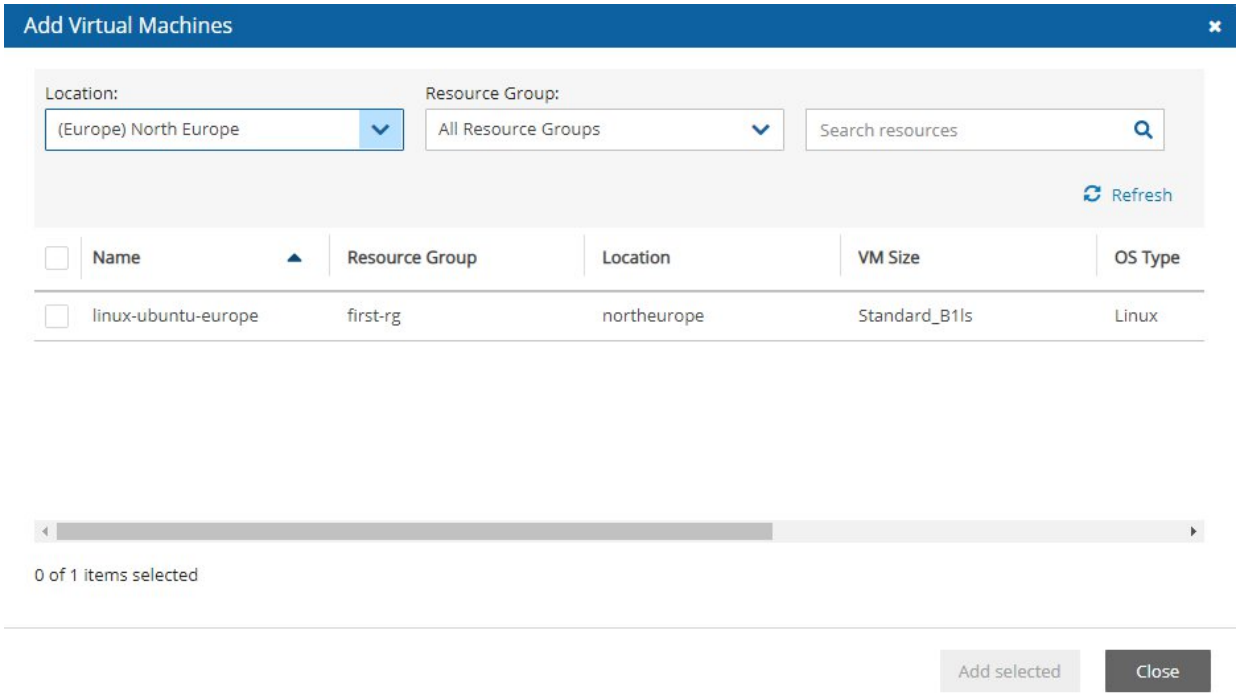


7.3 Creating an Azure Policy

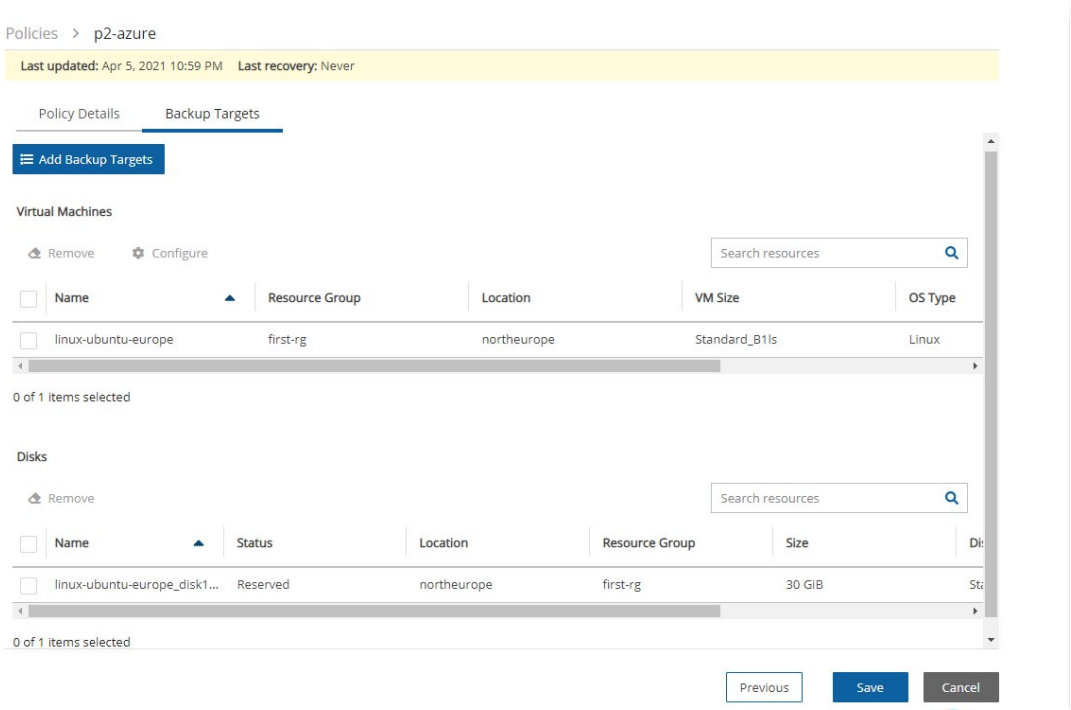
To back up resources in Azure, create an N2W policy.

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.

6. When selecting Virtual Machines, it is *required* to filter by the **Location** of the target resources using the list in the upper left corner *before* selecting the individual targets. Filtering by Resource Group is optional.



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

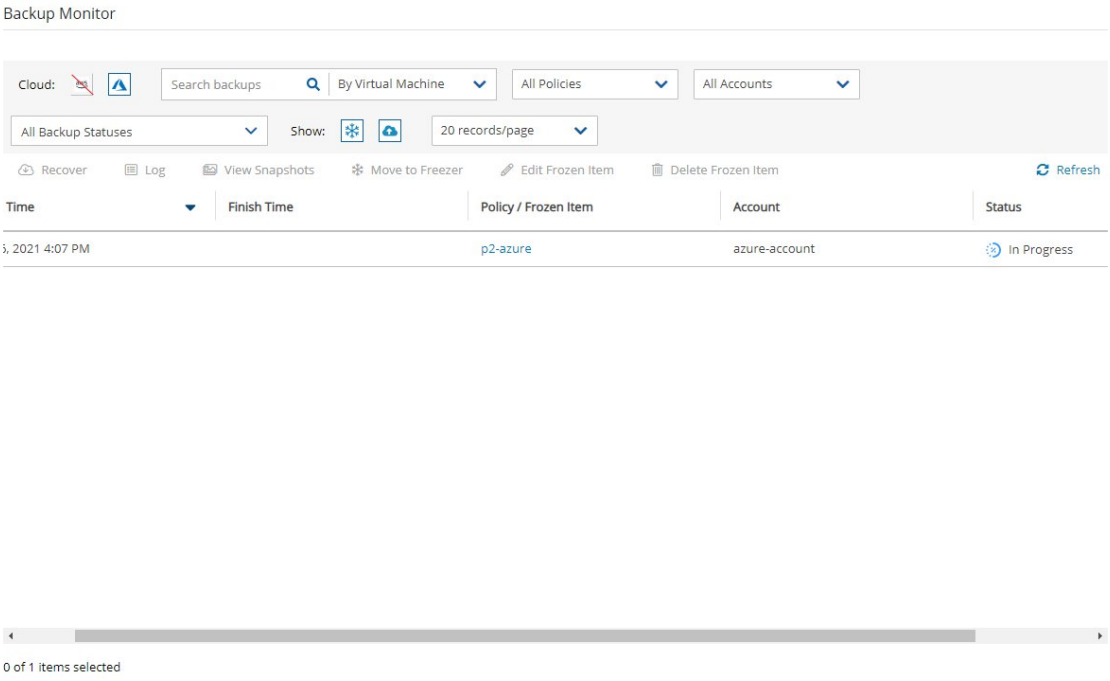


8. To determine which disks for each Virtual Machines target to back up, select **Configure**. In the **Which Disks** list of the Policy Virtual Machine and Disk Configuration screen, select the disks to include or exclude in the backup.
9. When finished, in the **Backup Targets** tab, select **Save**.

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.



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.

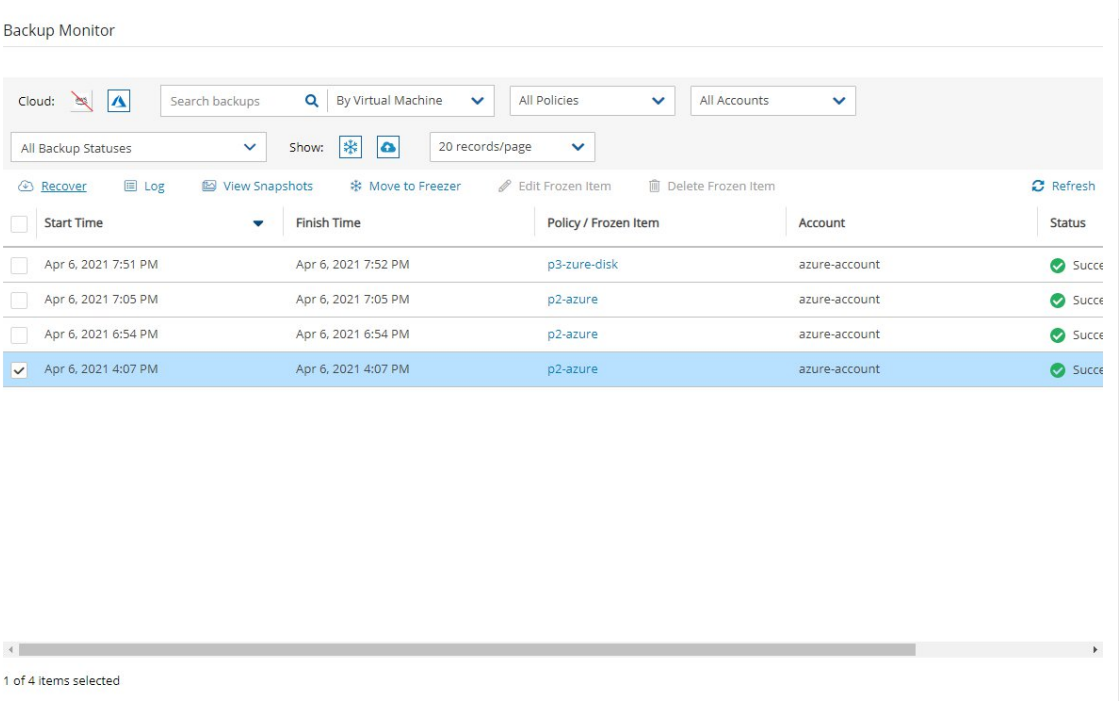
In the Disk Recovery screen, you may be presented with an option to change the encryption when recovering certain disks.

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.

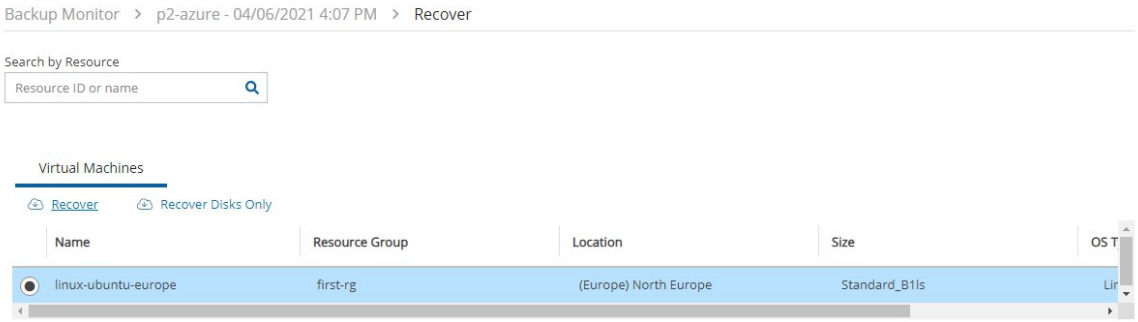
Disk encryption settings can be changed only when the disk is unattached or the owner VM is deallocated.

7.5.1 Recovering a VM and Disks

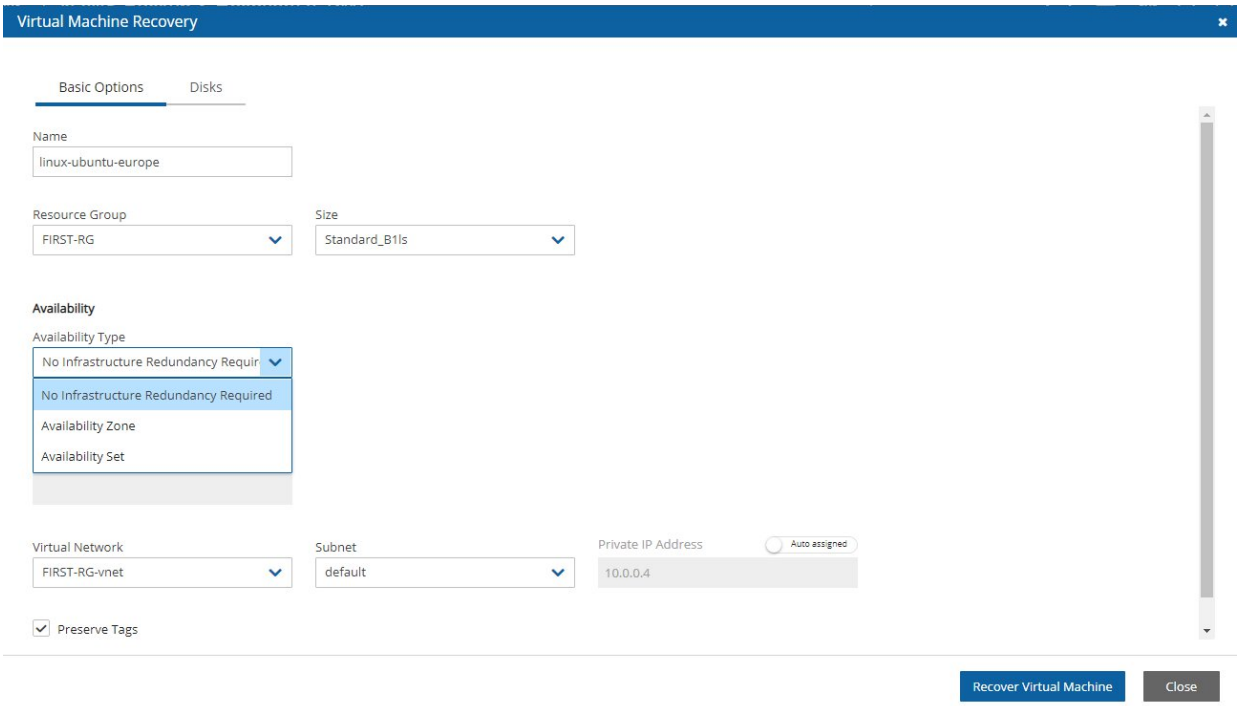
To recover a VM and/or attached disks:



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



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.



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.

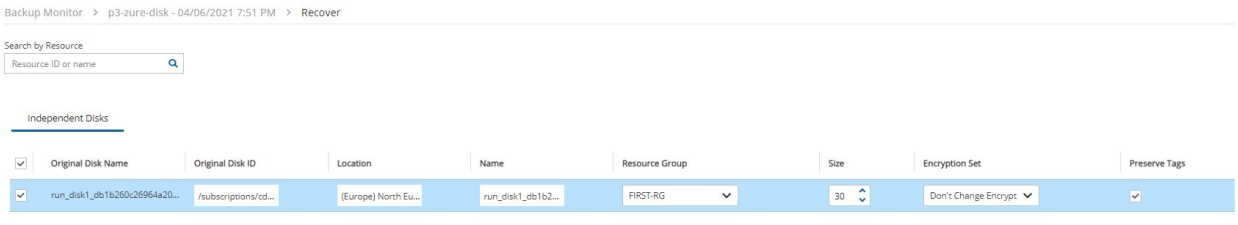
e. Select **Recover Virtual Machine**.

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

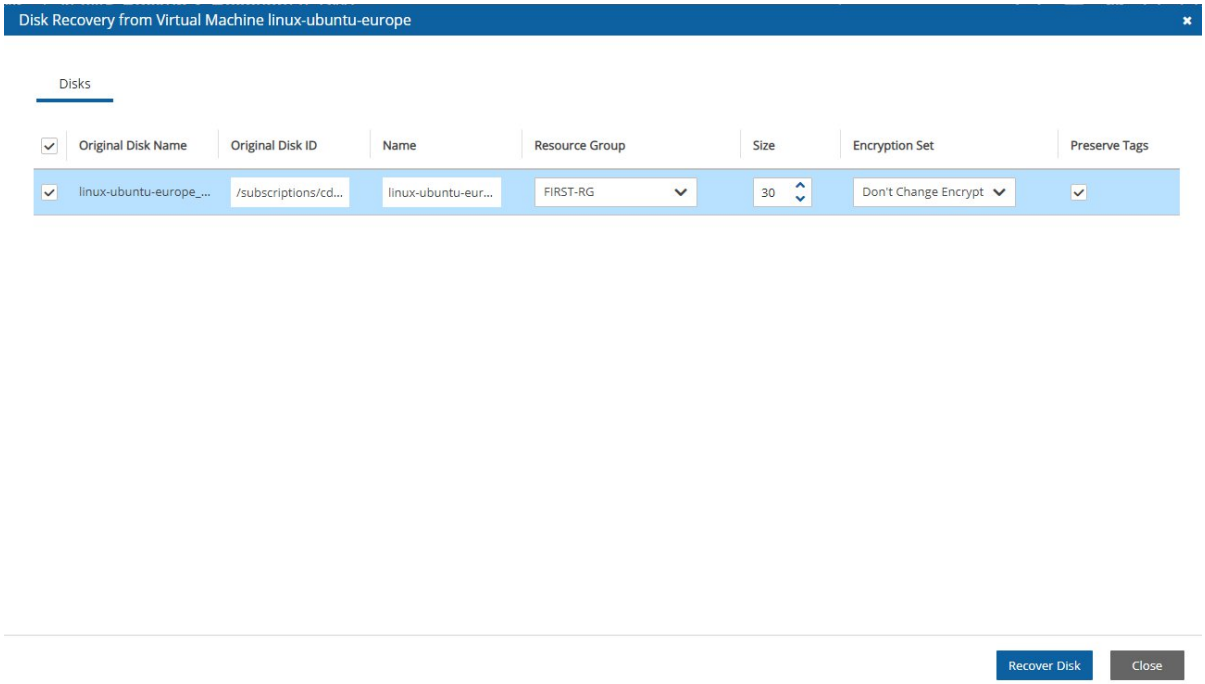
To recover from backups with independent disks:

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



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.



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

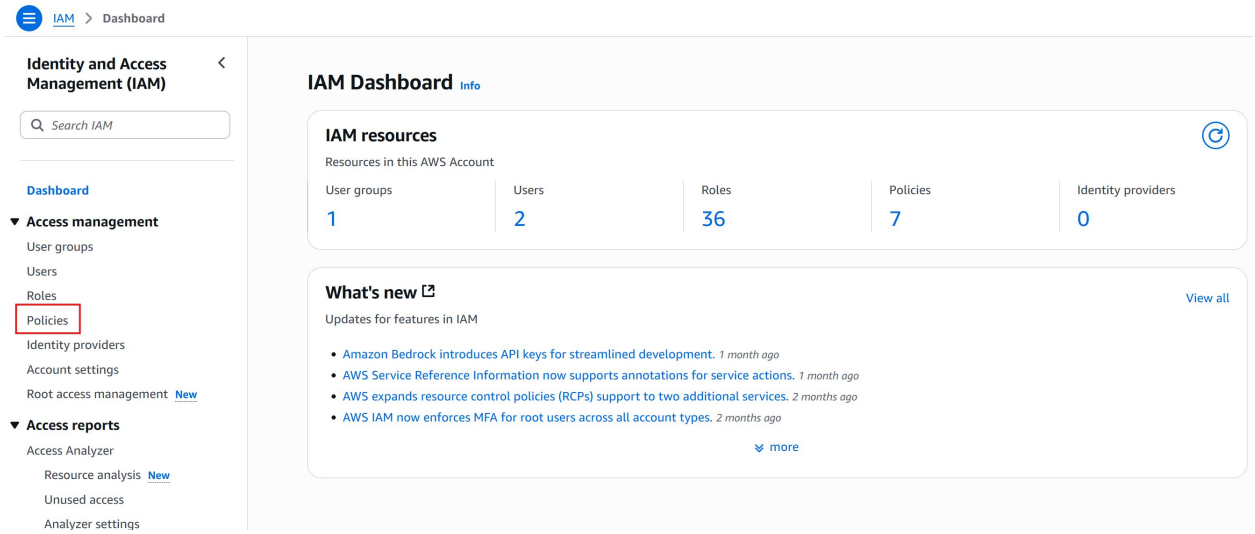
For N2W to perform its backup and restore management functions, it needs to have the correct permissions assigned.
N2W supports two different types of AWS authentication during setup:

- AccessKey / SecretKey
- Role based authentication (recommended)

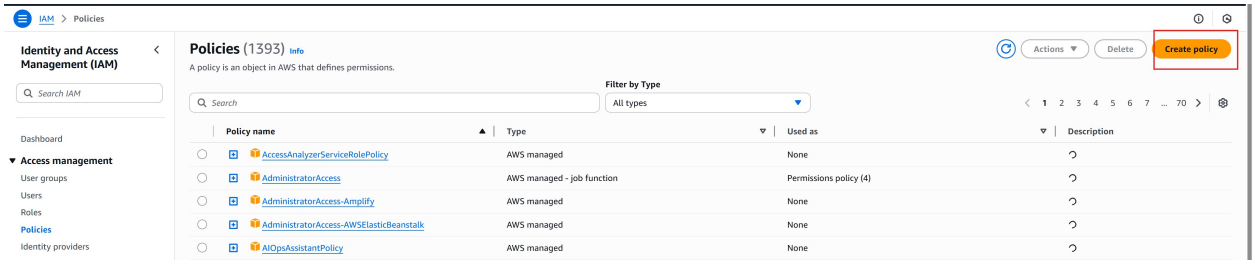
The permissions necessary have been combined into a JSON file for convenience and can be downloaded from the N2W Knowledge Base:

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**.

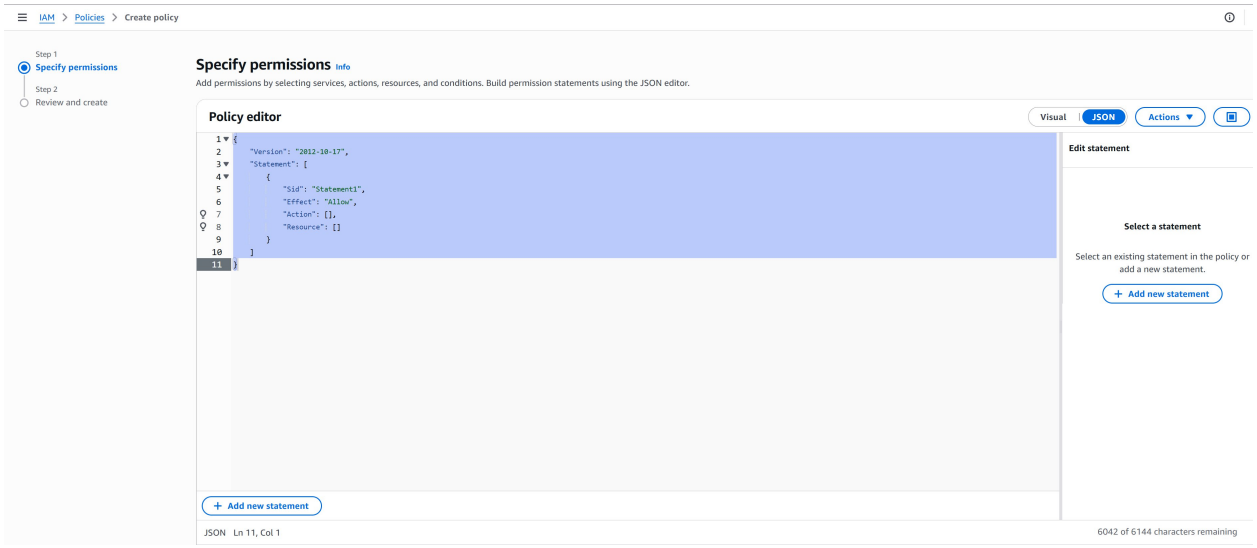


3. Select the **Create policy** button.



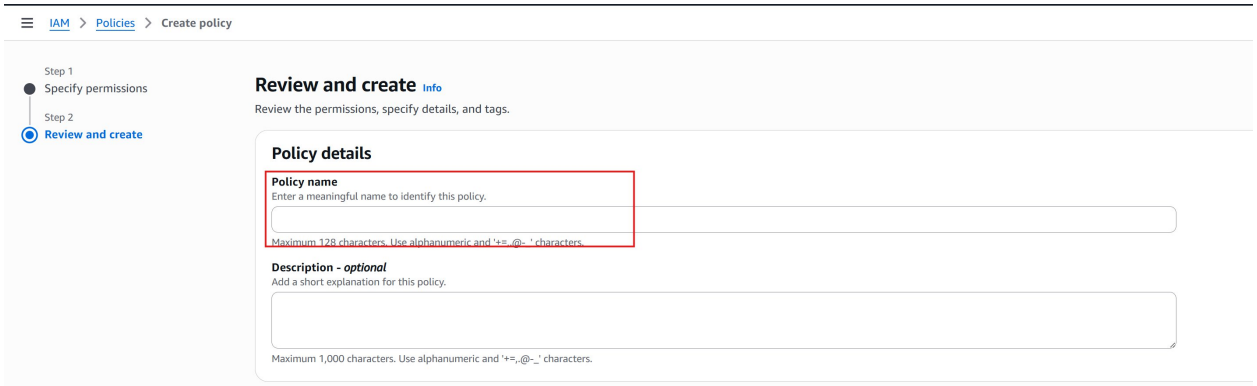
4. Select the **JSON** tab.

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

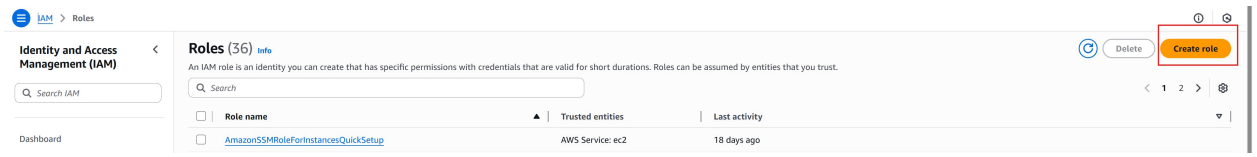


6. At the bottom of the screen, select **Next**.

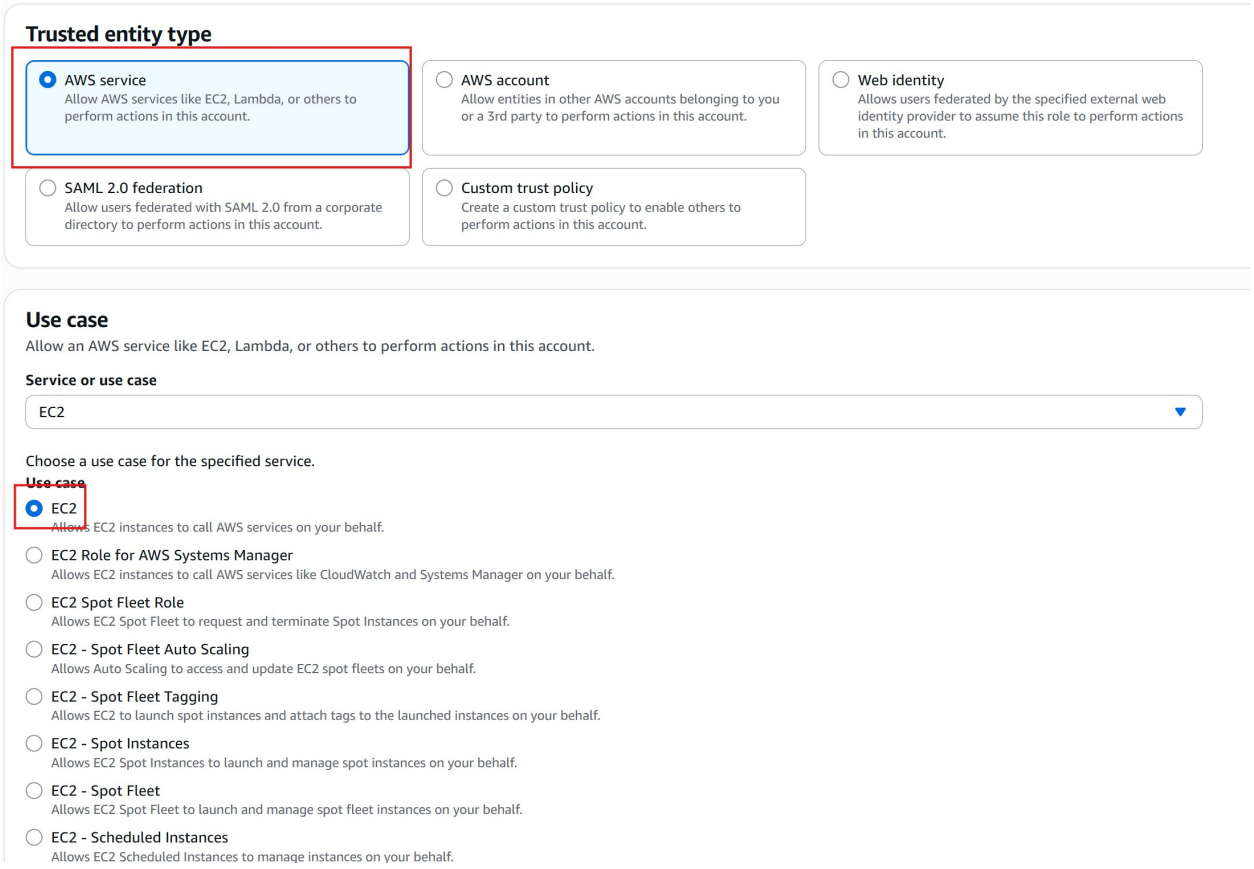
7. Type a **Name** for the policy and select **Create policy**.



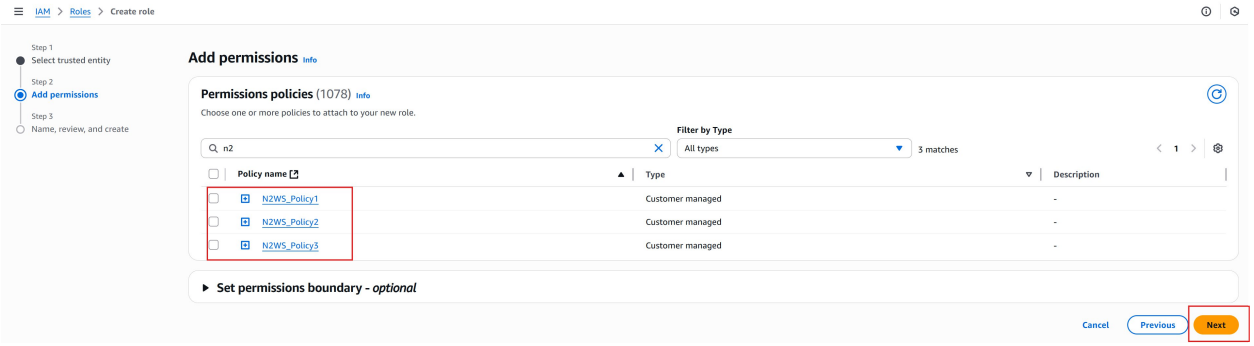
8. Create a role, and then assign the policy you just created to that role. In the left menu, select **Roles** and then select **Create role**.



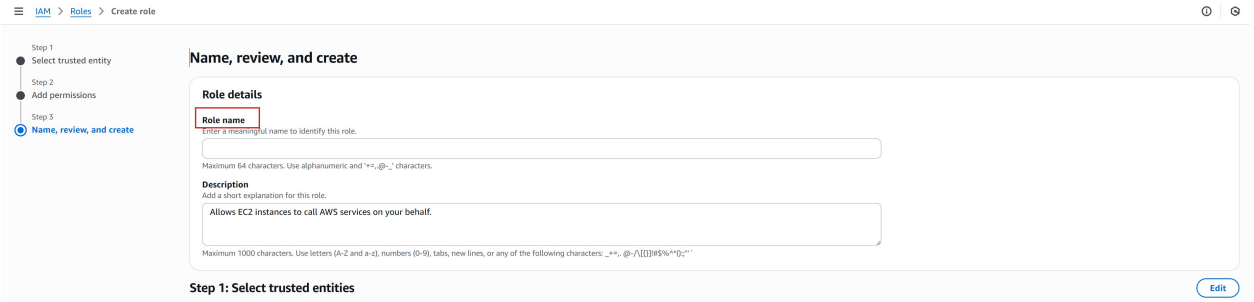
9. In the list of **type of trusted entity**, select **AWS service** and then select **EC2**.
10. Select **Next: Permissions**.



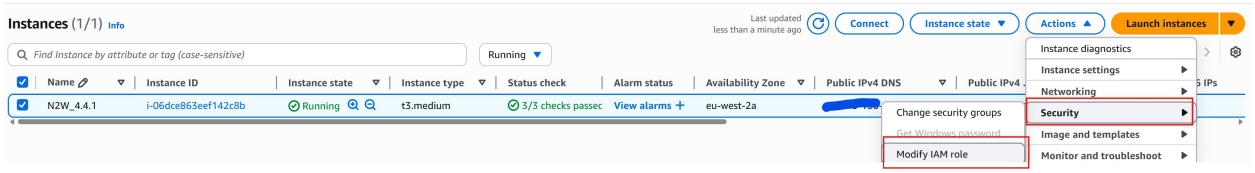
11. On the **Add Permissions** page, search for the 3 previously created polices and then select **Next**



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



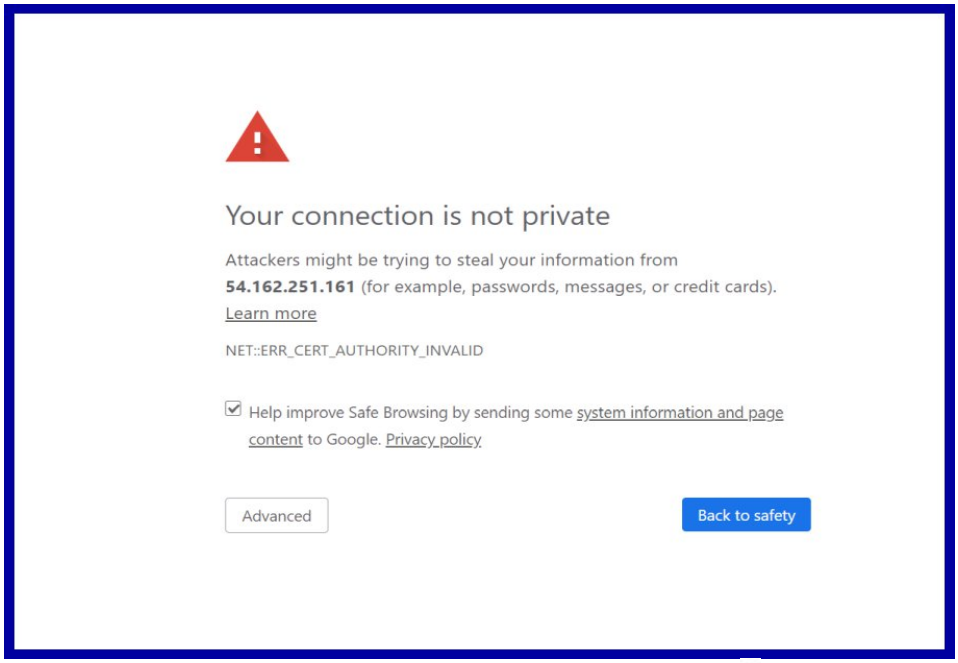
13. Assign the resulting role to the N2W trial instance:
    e. Select the N2W instance name.
    f. In the **Actions** menu, select **Instance Settings** and then **Attach/Replace IAM Role**.


Instances (1/1) Info
Last updated less than a minute ago
Connect
Instance state
Actions
Launch instances
Find Instance by attribute or tag (case-sensitive)
Running
Name
Instance ID
Instance state
Instance type
Status check
Alarm status
Availability Zone
Public IPv4 DNS
N2W_4.4.1
i-06dce863eef142c8b
Running
t3.medium
3/3 checks passed
View alarms
eu-west-2a
Instance diagnostics
Instance settings
Networking
Security
Image and templates
Monitor and troubleshoot
Change security groups
Get Windows password
Modify IAM role

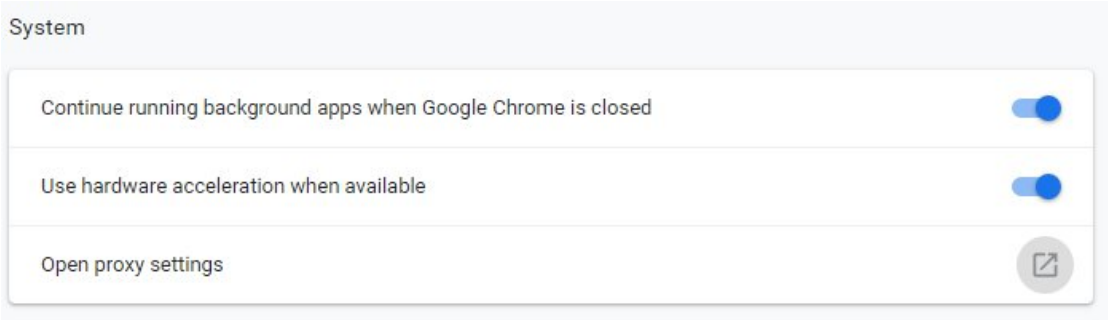
Appendix B – Adding Exception for Default Browser

For Chrome

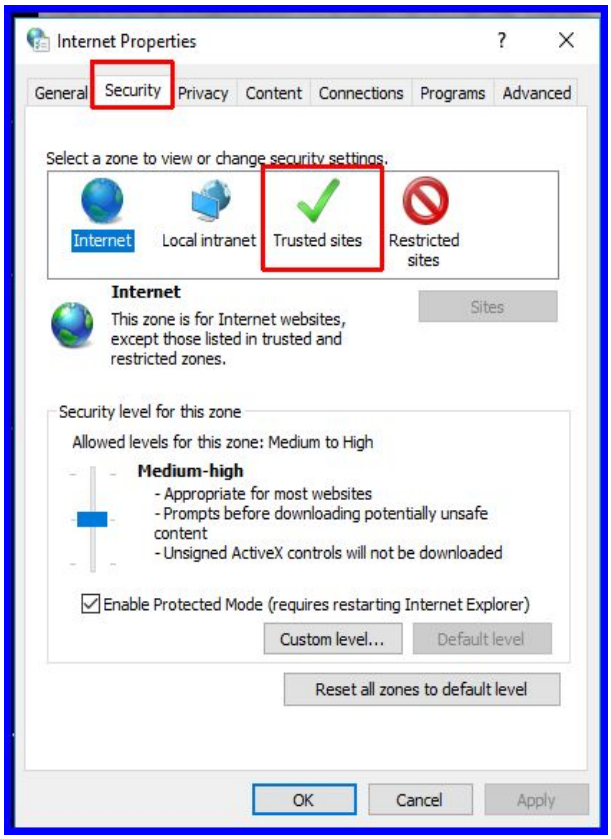
When you first navigate to your N2W instance, you'll see a screen like this. It's nothing to worry about. We are SSL secure but because it is a self-signed certificate, you may want to add an exception to your browser following these steps.



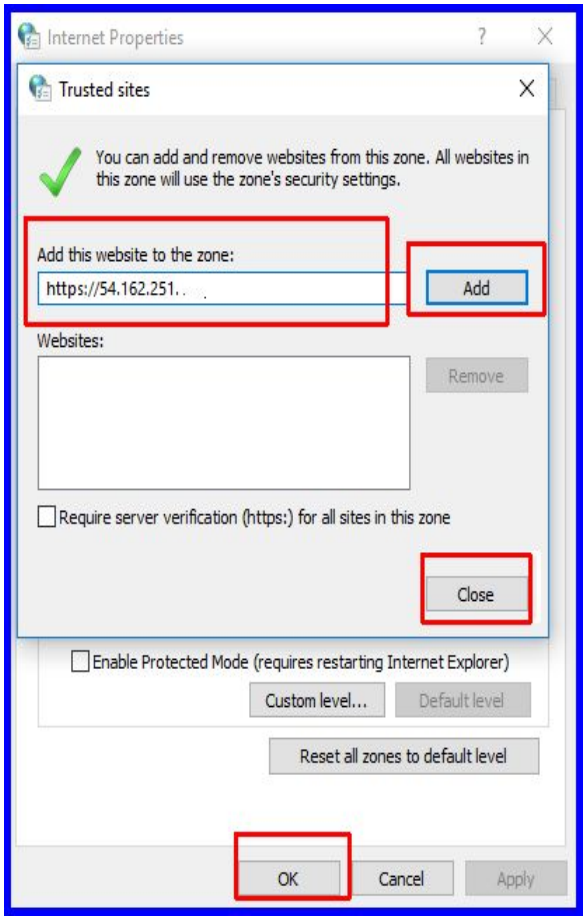
1. Open the Chrome browser. In the top right, select **More** ⋮.
2. Select **Settings**, **Advanced**, and then in the **System** section, select **Open proxy settings.**



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).