



N2WS Backup & Recovery

Quick Start Guide

V4.2.0



Content

1	Introduction	3
2	Launching N2WS Backup & Recovery	4
2.1	Launching with CloudFormation	4
3	N2Ws Server Instance Configuration	5
3.1	N2WS Server Instance Connectivity	5
3.2	N2WS Server Instance Configuration	5
3.3	N2WS Server Configuration Wizard	5
4	Creating a Simple Backup Policy.....	12
4.1	Adding an AWS Account	12
4.2	Adding an Azure Account	13
4.3	Creating a Simple Backup Schedule.....	13
4.4	Creating a Simple AWS Backup Policy	14
5	Performing a Basic Recovery	18
6	How to Configure N2WS with CloudFormation	22
7	Using Azure with N2WS	27
7.1	Setting Up Your Azure Subscription	27
7.2	Adding an Azure Account to N2WS	29
7.3	Creating an Azure Policy	31
7.4	Backing Up an Azure Policy	32
7.5	Recovering from an Azure Backup	33
Appendix A – AWS Authentication.....		37
Appendix B – Adding Exception for Default Browser		44



1 Introduction

N2WS 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. N2WS 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 N2WS up and running.

A quick word about passwords before we get going. N2WS strongly recommends that you create a strong password for the server. Make sure no one can access it or guess it. Change passwords regularly. N2WS 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://www.youtube.com/watch?v=ohK5mvl8KPw&feature=emb_title

and you'll be set in ~19 minutes.



2 Launching N2WS Backup & Recovery

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

To launch N2WS as part of a 30-day free trial or as a BYOL edition:

1. Go to <https://aws.amazon.com/marketplace/>
2. Search for 'n2ws'.
3. Select **N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition**.
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**, select the relevant version in the **Software Version** list.
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 N2WS operations.

To configure N2WS using CloudFormation, see section 6.



3 N2WS Server Instance Configuration

3.1 N2WS Server Instance Connectivity

For the configuration process to work, as well as N2WS's normal operations, N2WS needs to be able to “talk” with AWS APIs. Thus, it needs to have outbound connectivity to the Internet. Verify that the N2WS 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 N2WS Server Instance Configuration

N2WS has a browser-based management console. N2WS supports Mozilla Firefox, Google Chrome, and Safari.

Note: For N2WS to work, Java Script needs to be enabled on your browser.

After launching the N2WS AWS instance, use AWS Management Console or any other management tool to obtain the address of the new instance:

Description	Status Checks	Monitoring	Tags
Instance ID	i-0b99675617115678f		
Instance state	running		
Instance type	t2.micro		
Elastic IPs			
Availability zone	us-east-1c		
Security groups	recover, view inbound rules		
			Public DNS (IPv4) ec2-54-147-118-77.compute-1.amazonaws.com
			IPv4 Public IP 54-147-118-77
			IPv6 IPs -
			Private DNS ip-172-31-37-18.ec2.internal
			Private IPs 172.31.37.18
			Secondary private IPs

Note: Use the address provided to you by N2WS to connect to the N2WS Server using the HTTPS protocol in your browser (`https://<server address>`).

When a new N2WS 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 44).

After adding the exception, you get the first screen of the N2WS configuration application.

3.3 N2WS Server Configuration Wizard

The N2WS Server Configuration wizard takes you through the process step by step. There are a few differences between configuring N2WS for the Free Trial and other paid editions.

For the Free Trial edition:

- A new volume must be defined for the N2WS server.
- You will need to enter a user name, a valid email address, and enter a strong password and verify it.

For other N2WS 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 N2WS instance. This step is required to verify that you are indeed the owner of this instance.



Select **Next**. In the next step the N2WS configuration procedure begins.


Step 2: Approve the N2WS license agreement

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





Step 3: Configure the license type, N2WS “root” account password, and user information

 Server Configuration
N2WS Backup & Recovery (CPM)

Instance Confirmation

End User License Agreement

License and Root User

Data Volume and Proxy

Server Configuration

Register Your Account

License:

I'm starting a free trial

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 N2WS Free Trial in the past on the same AWS account, you may receive an error message when trying to configure or connect to N2WS. Contact support@n2ws.com to resolve.

Note: If you are using one of the N2WS 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: N2WS does not enforce password rules. However, it is recommended 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

N2WS | Server Configuration
N2WS Backup & Recovery (CPM)

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

Choose Time:

Connect via web proxy:

Back Next

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 N2WS 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 N2WS data volumes.

N2WS | Server Configuration
N2WS Backup & Recovery (CPM)

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

Choose Time:

Choose new or existing:

Force Recovery Mode:

Connect via web proxy:

Important Notice:
Archived data to S3 from versions 2.4 to 2.6.x cannot be recovered with version 3.0
For additional information, please read [here](#).

Back Next

Note: The N2WS 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:

Server Configuration
N2WS Backup & Recovery (CPM)

Choose Time: Greenwich (GMT)

Connect via web proxy: Enabled

Proxy address:

Proxy port:

Proxy user:

Proxy password:

Back Next

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 N2WS 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.

Server Configuration
N2WS Backup & Recovery (CPM)

Capacity (GiB): 5

EBS Volume Type: General Purpose SSD (gp2)

Encrypt Volume: Not Encrypted

Web Server Port: 443

SSL Server Certificate File: No file chosen

SSL Server Private Key: No file chosen

Anonymous Usage Reports: Allow

Anonymous Usage Reports:
If allowed, anonymous usage reports will be sent from time to time, but will never include object names or ids, AWS credentials or user identification details. This data will be used by N2W Software for the sole purpose of product improvement. This setting may be altered at any time through the settings menu.

Leave empty for default self-signed certificate

Back Next

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



Existing CPM Data Volume: vol-0572ed603db0b2f08 (N2WS - Data Volume)

Web Server Port: 443

SSL Server Certificate File: No file chosen Leave empty for default self-signed certificate

SSL Server Private Key: No file chosen

Anonymous Usage Reports: Allow

If allowed, anonymous usage reports will be sent from time to time, but will never include: object names or ids, AWS credentials or user identification details. This data will be used by N2W Software for the sole purpose of product improvement. This setting may be altered at any time through the settings menu.

Back Next

3. Complete the Web Server settings. The default port 443 is used by the N2WS manager.
4. Allowing anonymous usage reports will enable N2WS to improve the product. The usage reports are sent to N2WS with no identifying details to maintain customer anonymity. You can disallow the anonymous reports at a later time in the N2WS **General Settings** menu.
5. Select **Next** when finished.

Step 6: Register the account with N2W Software

Full Name:

Email:

Company:

Country: Please choose your country

Zip Code:

Ref Code (optional):

Back Configure System

Registration is mandatory for free trials and optional for paid products. N2W Software 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:

[Sign In](#)

Or

[Sign in with Identity Provider](#)

[License Agreement](#)

You are now ready to log on with the credentials you created in the first screen and begin using N2WS. Selecting **Sign in with Identity Provider** will redirect you to the organization's IdP system using SAML.

Note: Logging on for the first time with a trial edition can take up to 5 minutes as N2WS 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.

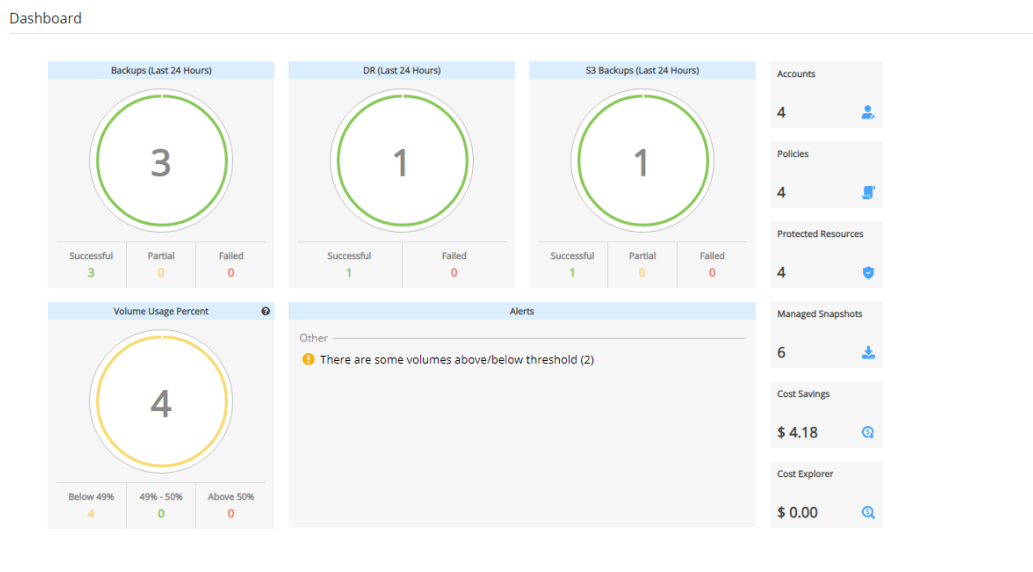


4 Creating a Simple Backup Policy

A backup policy requires an account from which to operate. While a backup schedule is geared toward a production environment, it is optional, as you can run a policy independently of a schedule.

4.1 Adding an AWS Account

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



It is currently empty. The first thing you will do is to associate an AWS account so you can start backing up EC2 instances. Depending on the edition of N2WS you registered to, you can associate one or more AWS accounts. In the left panel, select the **Accounts** tab and then + **New**. The **New Account** screen opens:

Accounts > New Account

Name User + New

Account Type

Authentication

☐ Scan Resources

☒ Capture VPCs



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 *N2WS Backup and Recovery (CPM) 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 N2WS 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 *N2WS Backup & Recovery (CPM) User Guide*.
4. Select **Scan Resources** to turn on the capability for this account to scan resources. Select the **Scan Regions** and **Resource Types** in their respective lists.
5. **Capture VPCs** is enabled by default. Clear **Capture VPCs** to turn off automatic capturing of VPCs for this account.
6. Select **Save**.

4.2 Adding an Azure Account

To associate an Azure account with an N2WS account, see section 7.

4.3 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**.

Schedules > New Schedule

Name: Daily_Sched User: demo + New

First Run: 10/22/2020 9:21 PM Expires: [toggle]


Time Zone: Italy (Europe/Rome)

Repeat Every: 1 Days

Enabled On: ☒ Sunday ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday

Description: [text area]

Save Cancel

1. Type a name for the schedule and an optional description.
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**.

4.4 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.



Policies > Create Policy

Policy Details

Backup Targets

More Options

DR

Lifecycle Management (Snapshot / S3 / Glacier)

Add Backup Targets

Instances

Volumes

RDS Databases

Aurora Clusters

Redshift Clusters

DynamoDB Tables

Elastic File Systems

FSx File Systems

S3 Bucket Sync

Previous

Next

Save

Cancel

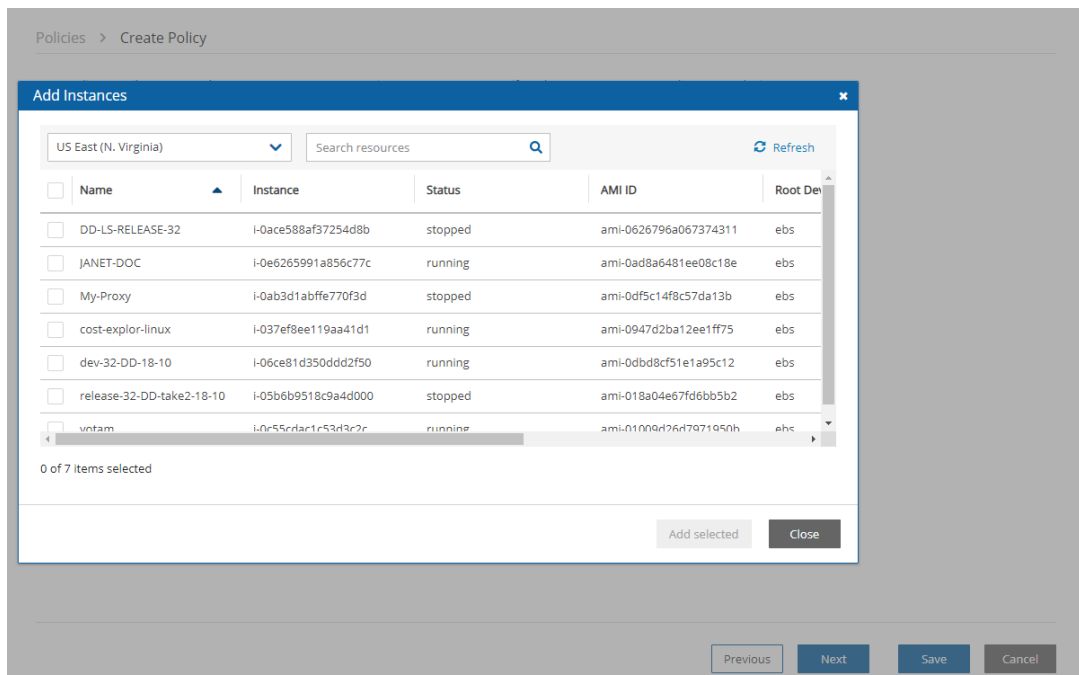
Following are the types of objects you can back up:

- **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 backup RDS databases using N2WS, 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.

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 a good practice to do so.



Select the instance that you want to back up and 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 an 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, N2WS 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

Search Policies		All Accounts	All Schedules	20 records/page	
+ New	Edit	Run ASAP	Backup Times	Delete Snapshots	Delete
Refresh					
<input type="checkbox"/>	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

N2WS 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

Search backups		by instance	All Policies	All Accounts	All Backup Statuses	
20 records/page		20 records/page	Show: [Grid] [List]			
Recover	Log	View Snapshots	Move to Freezer	Edit Frozen Item	Abort Copy to S3	Delete Frozen Item
Refresh						
<input type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status
<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 *N2WS Backup & Recovery (CPM) 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

Search backups by instance All Policies All Accounts All Backup Statuses

20 records/page

<input type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle
<input checked="" type="checkbox"/>	Oct 25, 2020 3:52 PM			ACCOUNT-3	Successful		
<input type="checkbox"/>	Oct 25, 2020 2:12 PM			ACCOUNT-1	Successful		
<input type="checkbox"/>	Oct 25, 2020 11:03 AM			ACCOUNT-3	Successful		Store
<input type="checkbox"/>	Oct 25, 2020 11:03 AM			ACCOUNT-1	Successful	Completed	
<input type="checkbox"/>	Oct 25, 2020 11:03 AM			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 1:37 PM	Oct 24, 2020 1:39 PM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/>	Oct 22, 2020 8:22 AM	Oct 22, 2020 8:24 AM	P2	ACCOUNT-1	Successful	Completed	

1 of 8 items selected

For each backup, you can see 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

Search backups by instance All Policies All Accounts All Backup Statuses

20 records/page Show:

<input type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status
<input checked="" type="checkbox"/>	Nov 14, 2020 1:44 AM	Nov 14, 2020 1:45 AM	vol-dr	aaa	Successful	Failed
<input type="checkbox"/>	Nov 14, 2020 12:22 AM	Nov 14, 2020 12:23 AM	vol-dr	aaa	Successful	Completed
<input type="checkbox"/>	Nov 14, 2020 12:07 AM	Nov 14, 2020 12:10 AM	23-RC	aaa	Successful	
<input type="checkbox"/>	Nov 8, 2020 12:24 PM	Nov 8, 2020 12:31 PM	ccc	ccc	Successful	
<input type="checkbox"/>	Nov 4, 2020 6:30 PM	Nov 5, 2020 11:11 AM	vol-dr	aaa	Successful	
<input type="checkbox"/>	Nov 4, 2020 6:14 PM	Nov 4, 2020 6:15 PM	vol-dr	aaa	Successful	Skipped
<input type="checkbox"/>	Nov 4, 2020 6:06 PM	Nov 4, 2020 6:07 PM	vol-dr	aaa	Successful	Completed
<input type="checkbox"/>	Nov 4, 2020 12:09 PM	Nov 4, 2020 12:10 PM	ins-s3	aaa	All Snapshots Deleted	
<input type="checkbox"/>	Nov 4, 2020 12:02 PM	Nov 4, 2020 12:03 PM	ins-s3	aaa	All Snapshots Deleted	

1 of 9 items selected

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

Resource ID or name

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
cost-explor-linux	i-037ef8ee119aa41d1	US East (N. Virginia)	ami-0947d2ba12ee1ff75	/dev/xvda	Unix / Linux
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 actually 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-profile

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 was 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 the *N2WS Backup & Recovery (CPM) User Guide* for details on “Recovering to a Cloned VPC”.

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.

Instance Recovery

AMI Assistant

Basic Options

Volumes

Advanced Options

<input checked="" type="checkbox"/>	Original Volume ID	Capacity (GiB)	Type	IOPS	Encrypted	Device	Preserve Tags	Delete on Term
<input checked="" type="checkbox"/>	vol-0642d2d3bbb11c...	8	General Purpose SSD	100	No	/dev/sda1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

AWS Credentials

Use account AWS Credentials

Recover Instance

Close



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

Instance Recovery

AMI Assistant

Basic Options

Volumes

Advanced Options

Architecture

x86_64

Tenancy

Shared

Shutdown Behaviour

Stop

API Termination

Enable

Auto-assign Public IP

Subnet Default

Kernel

RAM Disk

☒ Preserve Tags

AWS Credentials

Use account AWS Credentials

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 exactly the same as the original one, with all its EBS volumes.



6 How to Configure N2WS with CloudFormation

The process to configure N2WS to work with CloudFormation is a single stream that starts with subscribing to N2WS on the Amazon Marketplace and ends with configuring the N2WS server.

- N2WS provides a number of editions all of which support CloudFormation.
 - An IAM role will automatically be created with minimal permissions and assigned to the N2WS instance.
1. Go to <https://aws.amazon.com/marketplace>
 2. Search for N2WS.
 3. Select **Continue to Subscribe**.

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

By: [N2W Software](#) Latest Version: 3.0.0

N2WS Cloud Protection Manager is the AWS backup and disaster recovery solution of choice for thousands of customers worldwide. Combining the agility of the cloud with the robustness and

[Show more](#)

Linux/Unix **★★★★★** 22 AWS reviews | 2 external reviews ⓘ

BYOL

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price
\$0.042/hr
Total pricing per instance for services hosted on t3.medium in US East (N. Virginia). [View Details](#)

[Overview](#) [Pricing](#) [Usage](#) [Support](#) [Reviews](#)

Product Overview

TRY OUT This leading AWS backup, recovery and DR solution purpose-built for AWS workloads - N2WS Backup & Recovery 30-DAY FREE TRIAL & BYOL Edition. After trial ends, N2WS automatically converts into a FREE version that still protects you! (limited to protecting up to 5 instances)

By leveraging native snapshot technology N2WS provides an additional layer of security within your AWS environment and supports your EC2, NoSQL and serverless workloads. N2WS enables you to fully automate backup of EC2, EBS, RDS, Redshift, Aurora, EFS and DynamoDB - and leverage 1-click recovery to restore a single file or your entire environment in less than 30 seconds.

With support for different storage tiers: native AWS backups and archive to Amazon S3, N2WS enables cost reduction for data retained long term.

N2WS enables you to build effective disaster recovery plans and recover data across multiple AWS accounts and regions. In addition, flexible policies and schedules enables you to scale your AWS environment whilst ensuring it is fully protected.

Highlights

- Automate backup of EC2 instances, EBS volumes, RDS, DynamoDB, Aurora, EFS and Redshift using flexible policies and schedules. Clone your VPC settings and perform disaster recovery (DR) across AWS accounts or regions. Protect your environment from outages, failures and data loss
- Perform application consistent backups of your critical data, eliminating the need for maintenance windows and unnecessary downtime. Rapidly recover single files without having to restore the entire instance.
- Easy to use interface with real-time alerts, reporting and integration with other services via the N2WS CLI and RESTful API. N2WS is also designed for multi-tenancy allowing you to manage multiple accounts from one console

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


3.0.0 (Feb. 14, 2020) ▼

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
running on t3.medium
\$0/hr

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





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

[< 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	3.0.0
Region	US East (N. Virginia)

Usage Instructions

Choose Action

Launch CloudFormation

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

Launch

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

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template ☐ Create template in Designer

Specify template

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL, where it will be stored.

☒ Amazon S3 URL ☐ Upload a template file

Amazon S3 URL
`https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/14807ff7-6eb0-4030-9b61-8782f8e8e834.384bfe20-20ee-418c-37aa-63d707b17a06.template`
Amazon S3 template URL

S3 URL: `https://s3.amazonaws.com/awssmp-fulfillment-cf-templates-prod/14807ff7-6eb0-4030-9b61-8782f8e8e834.384bfe20-20ee-418c-37aa-63d707b17a06.template` [View in Designer](#)

Cancel **Next**

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



CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Create stack

Prerequisite - Prepare template

Prepare template
Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☒ Template is ready ☐ Use a sample template ☐ Create template in Designer

Specify template
A template is a JSON or YAML file that describes your stack's resources and properties.

Template source
Selecting a template generates an Amazon S3 URL where it will be stored.

☒ Amazon S3 URL ☐ Upload a template file

Amazon S3 URL

Amazon S3 template URL

S3 URL:

9. Under **Prepare template**, select **Template is ready**.

10. Under **Template source**, choose **Amazon S3 URL**. Select the default Amazon S3 URL and select **Next**. The **Specify stack details** page opens.

CloudFormation > Stacks > Create stack

Step 1
Specify template

Step 2
Specify stack details

Step 3
Configure stack options

Step 4
Review

Specify stack details

Stack name

Stack name

Stack name can include letters (A-Z and a-z), numbers (0-9), and dashes (-).

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

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

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 select **Launch Instance**. The **N2WS Server Configuration** page opens.

17. Continue from section 3.

This concludes the *Quick Start Guide*. See *N2WS Backup & Recovery (CPM) User Guide* for more details.



7 Using Azure with N2WS

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

1. Before starting, configure N2WS Backup and Recovery according to [Configuring N2WS](#).
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 N2WS, add an Azure account with the custom N2WS role. See section [7.2](#).
4. Create an Azure policy in N2WS 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

N2WS Backup and Recovery needs the following permissions to perform backup and recovery actions.

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"
        ]
      }
    ]
  }
}
```



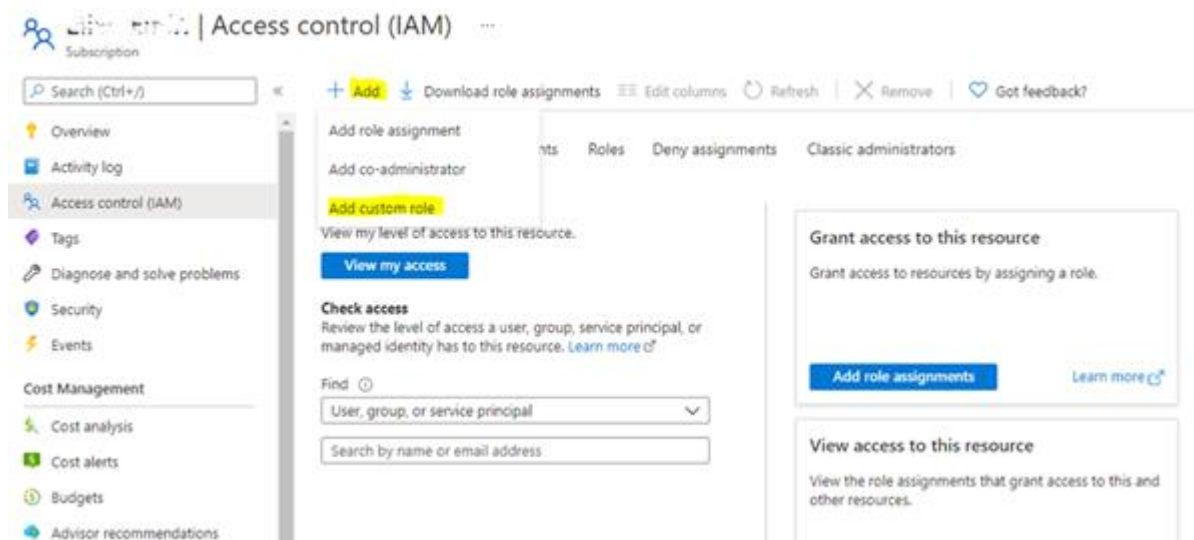
```
"notActions": [],  
"dataActions": [],  
"notDataActions": []  
}  
]  
}
```

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



with N2WS 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 ⓘ

N2WSBackupRecoveryRole 

Description

Role for N2WS Backup & Recovery

Baseline permissions ⓘ



Clone a role



Start from scratch



Start from JSON

Select a file



5. Create the role with the new JSON file.

7.2 Adding an Azure Account to N2WS

1. Log on to N2WS using the root username and password used during the N2WS configuration.
2. Select the **Accounts** tab.
3. If you have a license for Azure cloud, select **Azure account** in the **+ New** menu.

+ New 

AWS account

Azure account

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
<input type="text"/>	<input type="text" value="demo"/> ▼ ↻
Directory (tenant) ID	Application (client) ID
<input type="text"/>	<input type="text"/>
Client Secret	
<input type="text"/>	
<input type="checkbox"/> 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 *N2WS 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.

Accounts

Cloud: ↻ ⬆	<input type="text" value="Search Accounts"/> 🔍	20 records/page ▼
+ New ▼	Edit	Clone VPC
Check AWS Permissions	Generate Secured DR Report	Delete
Delete Account and Data	Refresh	
<input type="checkbox"/> Name	Cloud	Account Type
Authentication	Policy	
<input type="checkbox"/> azure-account	Azure	Backup
4e7e937e-1e69-4324-a435-376dab9ec1d0	p2-azu	

0 of 2 items selected



7.3 Creating an Azure Policy

To backup resources in Azure, create an N2WS policy.

1. In N2WS, 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 backup, Disks and/or Virtual Machines. The Add Virtual Machines / Disks screen opens.
6. When selecting Virtual Machines, it is *required* to filter by the **Location** of the target resources using the list in the upper left corner *before* selecting the individual targets. Filtering by Resource Group is optional.

Add Virtual Machines

Location:
(Europe) North Europe

Resource Group:
All Resource Groups

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

7. 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](#)

<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](#)


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

0 of 1 items selected

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

- To determine which disks for each Virtual Machines target to backup, 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 backup 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
5/1/2021 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	✓ Succ
<input type="checkbox"/>	Apr 6, 2021 7:05 PM	Apr 6, 2021 7:05 PM	p2-azure	azure-account	✓ Succ
<input type="checkbox"/>	Apr 6, 2021 6:54 PM	Apr 6, 2021 6:54 PM	p2-azure	azure-account	✓ Succ
<input checked="" type="checkbox"/>	Apr 6, 2021 4:07 PM	Apr 6, 2021 4:07 PM	p2-azure	azure-account	✓ Succ

1 of 4 items selected

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

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

Search by Resource

Resource ID or name

Virtual Machines

Recover Recover Disks Only

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

2. To recover a VM, with or without its attached disks, select the VM snapshot that you want to recover from and then select **Recover**.
 - 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


10.0.0.4

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 N2WS to perform its backup and restore management functions, it needs to have the correct permissions assigned.

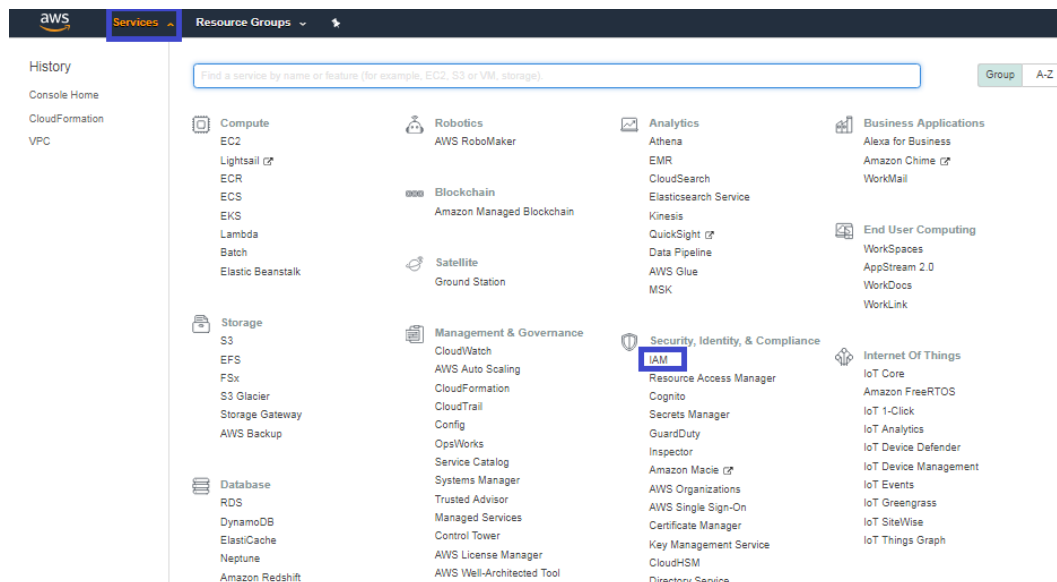
N2WS supports two different types of AWS authentication during setup:

- AccessKey / SecretKey
- Role based authentication (recommended)

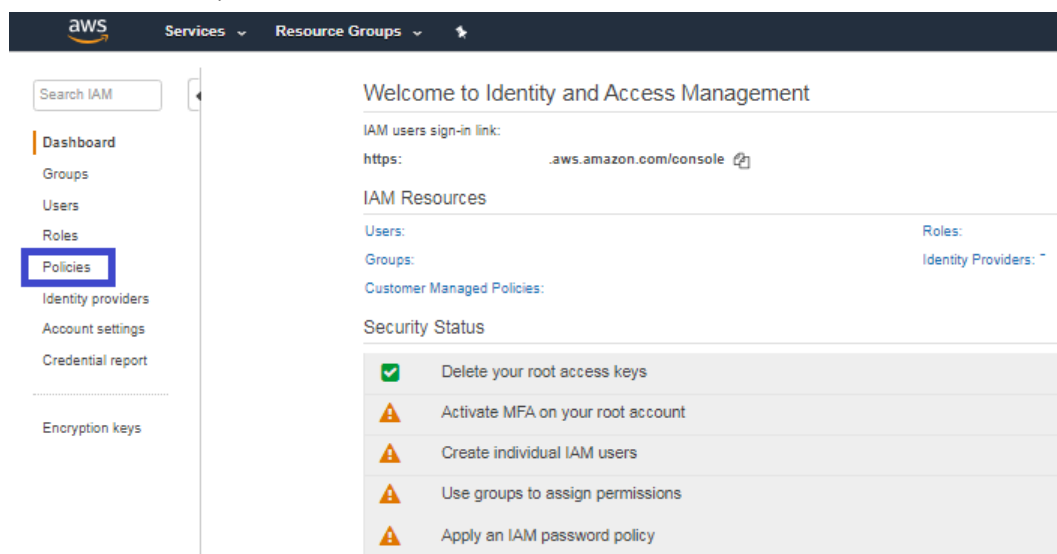
The permissions necessary have been combined into a JSON file for convenience and can be downloaded from the N2WS Knowledge Base:

<https://support.n2ws.com/portal/kb/articles/what-are-the-required-minimal-aws-permissions-roles-for-cpm-operation>

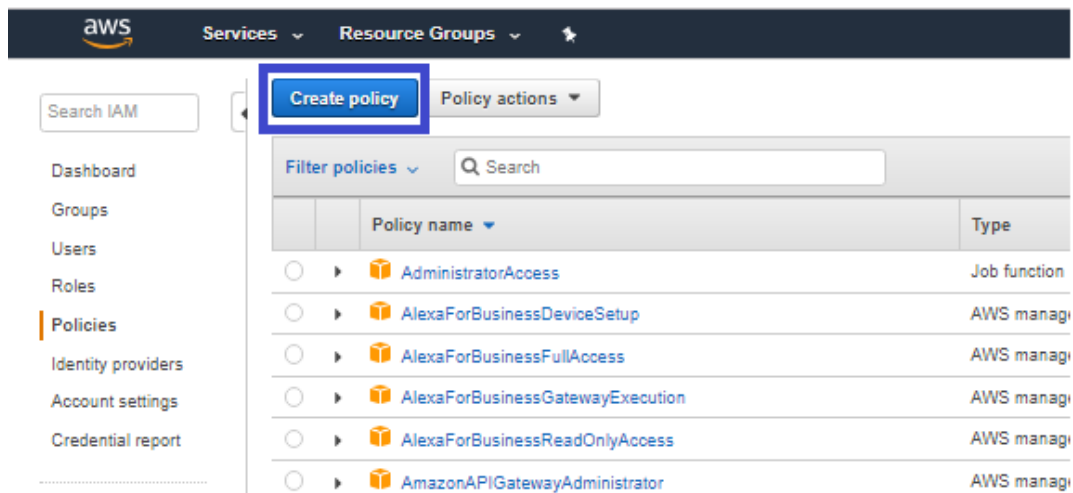
1. At the top of your AWS console, select the **Services** tab. In the **Security Identity & Compliance** section, select **IAM**.



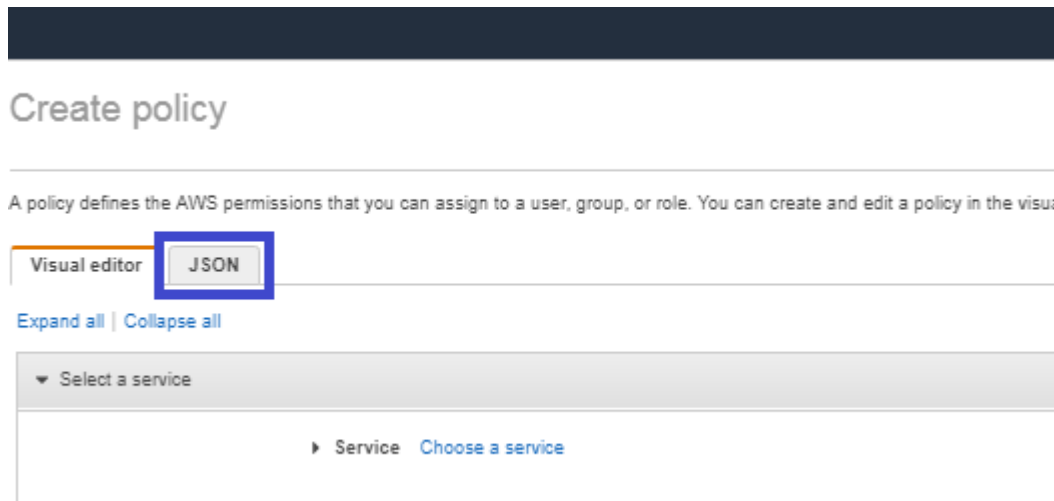
2. In the left menu, select **Policies**.



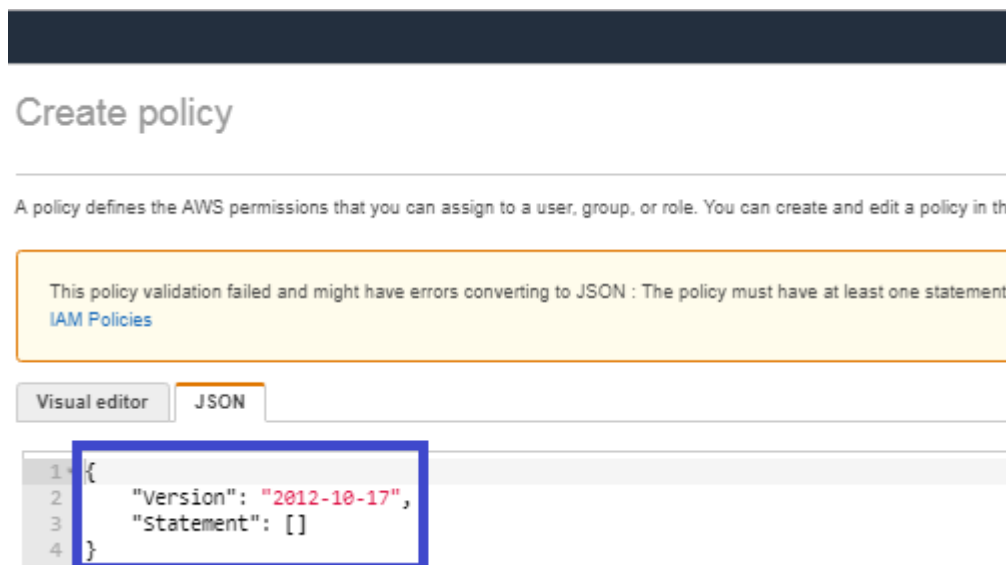
3. Select the **Create policy** button.



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 **Review Policy**.



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

Review policy

Name*

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

Description

Maximum 1000 characters. Use alphanumeric and '+-._@-' characters.

Summary

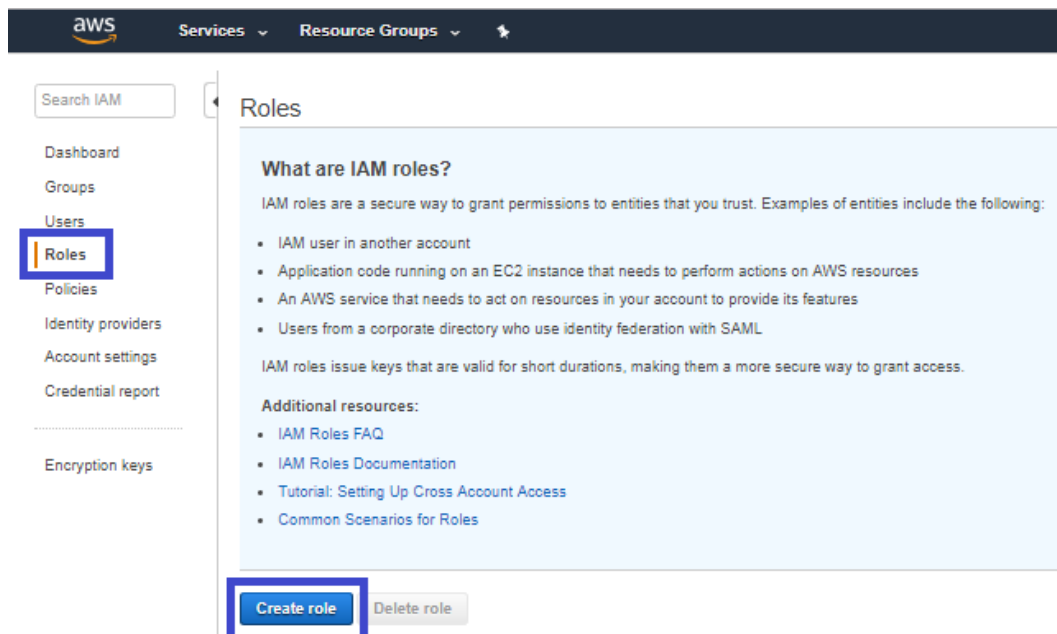
Filter

Service	Access level	Resource	Request condition
Allow (1 of 169 services) Show remaining 168			
Cloud Directory	Full: List, Read	All resources	None

* Required

[Cancel](#) [Previous](#) [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**.

Create role

1 2 3 4

Select type of trusted entity


AWS service
 EC2, Lambda and others


Another AWS account
 Belonging to you or 3rd party


Web identity
 Cognito or any OpenID provider


SAML 2.0 federation
 Your corporate directory

Allows AWS services to perform actions on your behalf. [Learn more](#)

Choose the service that will use this role

EC2

Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeBuild	EKS	Lambda	SMS
AWS Backup	CodeDeploy	EMR	Lex	SNS
AWS Support	Config	ElastiCache	License Manager	SWF
Amplify	Connect	Elastic Beanstalk	Machine Learning	SageMaker
AppSync	DMS	Elastic Container Service	Macie	Security Hub
Application Auto Scaling	Data Lifecycle Manager	Elastic Transcoder	MediaConvert	Service Catalog
Application Discovery Service	Data Pipeline	ElasticLoadBalancing	OpsWorks	Step Functions
Auto Scaling	DataSync	Glue	RAM	Storage Gateway
Batch	DeepLens	Greengrass	RDS	Transfer
CloudFormation	Directory Service	GuardDuty	Redshift	Trusted Advisor
CloudHSM	DynamoDB	Inspector	Rekognition	VPC
CloudTrail	EC2	IoT	S3	WorkLink
CloudWatch Events	EC2 - Fleet	Kinesis		

* Required

Cancel

Next: Permissions

11. In the **AWS services** list, select **EC2** again and select **Next: Permissions**.



Allows EC2 instances to call AWS services on your behalf.

Lambda

Allows Lambda functions to call AWS services on your behalf.

API Gateway	CodeBuild	EKS	Lambda	SMS
AWS Backup	CodeDeploy	EMR	Lex	SNS
AWS Support	Config	ElastiCache	License Manager	SWF
Amplify	Connect	Elastic Beanstalk	Machine Learning	SageMaker
AppSync	DMS	Elastic Container Service	Macie	Security Hub
Application Auto Scaling	Data Lifecycle Manager	Elastic Transcoder	MediaConvert	Service Catalog
Application Discovery Service	Data Pipeline	ElasticLoadBalancing	OpsWorks	Step Functions
Auto Scaling	DataSync	Glue	RAM	Storage Gateway
Batch	DeepLens	Greengrass	RDS	Transfer
CloudFormation	Directory Service	GuardDuty	Redshift	Trusted Advisor
CloudHSM	DynamoDB	Inspector	Rekognition	VPC
CloudTrail	EC2	IoT	S3	WorkLink
CloudWatch Events	EC2 - Fleet	Kinesis		

Select your use case

EC2

Allows EC2 instances to call AWS services on your behalf.

EC2 - Scheduled Instances

Allows EC2 Scheduled Instances to manage instances on your behalf.

EC2 - Spot Fleet

Allows EC2 Spot Fleet to launch and manage spot fleet 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 Role for Simple Systems Manager

Allows EC2 instances to call AWS services like CloudWatch and SSM on your behalf.

EC2 Spot Fleet Role

Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

* Required

Cancel

Next: Permissions

12. Search for the previously created policy, select its checkbox, and select **Next: Review**.



Create role

1234

▼ Attach permissions policies

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

Create policy

Filter policies Showing 1 result

	Policy name	Used as	Description
<input checked="" type="checkbox"/>	CD_RO	None	

► Set permissions boundary

* Required

Cancel

Previous

Next: Tags

13. Add optional tags for the role and select **Next: Review**.

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

Create role

1234

Review

Provide the required information below and review this role before you create it.

Role name* Use alphanumeric and '+-._@-' characters. Maximum 64 characters.

Role description Allows EC2 instances to call AWS services on your behalf. Maximum 1000 characters. Use alphanumeric and '+-._@-' characters.

Trusted entities AWS service: ec2.amazonaws.com

Policies [CD_RO](#)

Permissions boundary Permissions boundary is not set

No tags were added.

* Required

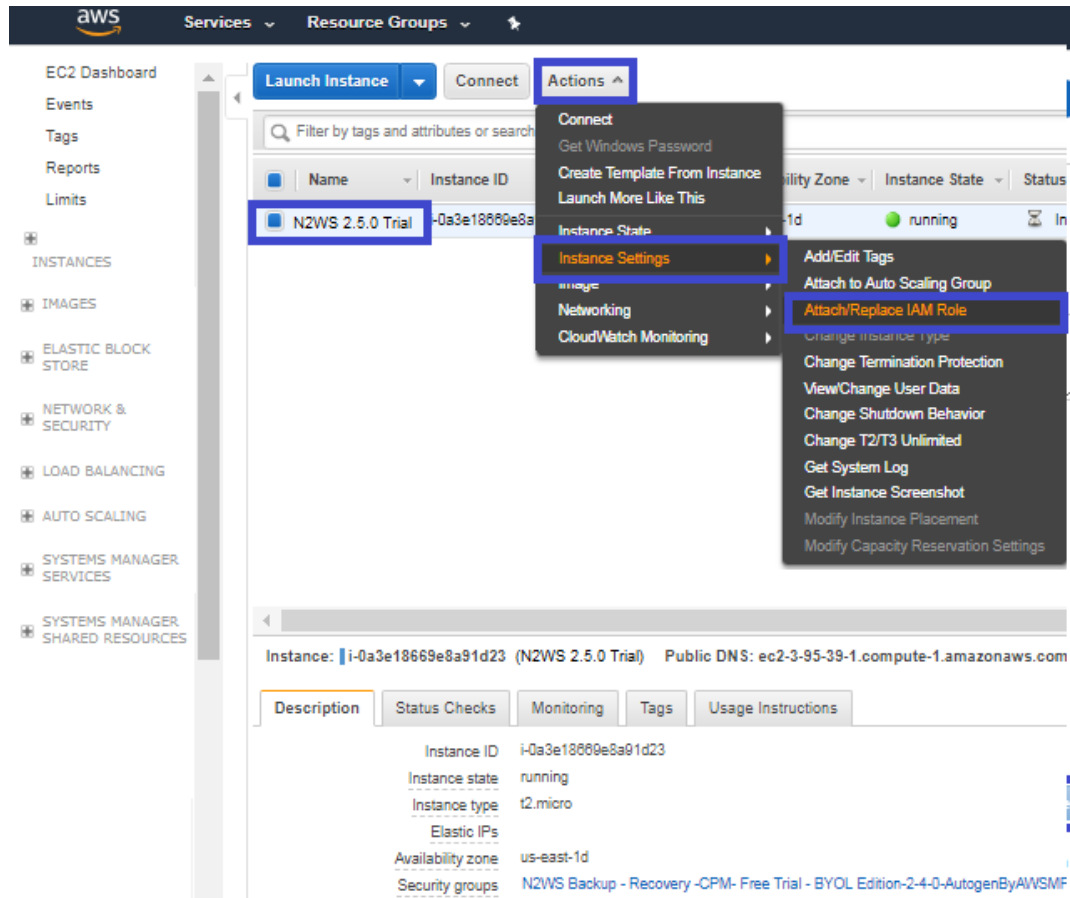
Cancel

Previous

Create role

15. Assign the resulting role to the N2WS trial instance:

- Select the N2WS instance name.
- In the **Actions** menu, select **Instance Settings** and then **Attach/Replace IAM Role**.



The screenshot shows the AWS Management Console interface. On the left is a navigation sidebar with categories like EC2 Dashboard, INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, AUTO SCALING, SYSTEMS MANAGER SERVICES, and SYSTEMS MANAGER SHARED RESOURCES. The main area displays a table of EC2 instances. One instance, 'N2WS 2.5.0 Trial' with ID 'i-0a3e18669e8a91d23', is highlighted. An 'Actions' dropdown menu is open for this instance, showing options like 'Connect', 'Create Template From Instance', 'Launch More Like This', 'Instance Settings', 'Networking', and 'CloudWatch Monitoring'. The 'Instance Settings' sub-menu is further expanded, showing options such as 'Add/Edit Tags', 'Attach to Auto Scaling Group', 'Attach/Replace IAM Role' (which is highlighted), 'Change Instance Type', 'Change Termination Protection', 'View/Change User Data', 'Change Shutdown Behavior', 'Change T2/T3 Unlimited', 'Get System Log', 'Get Instance Screenshot', 'Modify Instance Placement', and 'Modify Capacity Reservation Settings'. Below the instance list, the details for the selected instance are shown, including its ID, state (running), type (t2.micro), Elastic IPs, Availability zone (us-east-1d), and Security groups (N2WS Backup - Recovery -CPM- Free Trial - BYOL Edition-2-4-0-AutogenByAWSMF).

Name	Instance ID	Availability Zone	Instance State	Status
N2WS 2.5.0 Trial	i-0a3e18669e8a91d23	us-east-1d	running	In

Instance: **i-0a3e18669e8a91d23** (N2WS 2.5.0 Trial) Public DNS: ec2-3-95-39-1.compute-1.amazonaws.com

Description | Status Checks | Monitoring | Tags | Usage Instructions

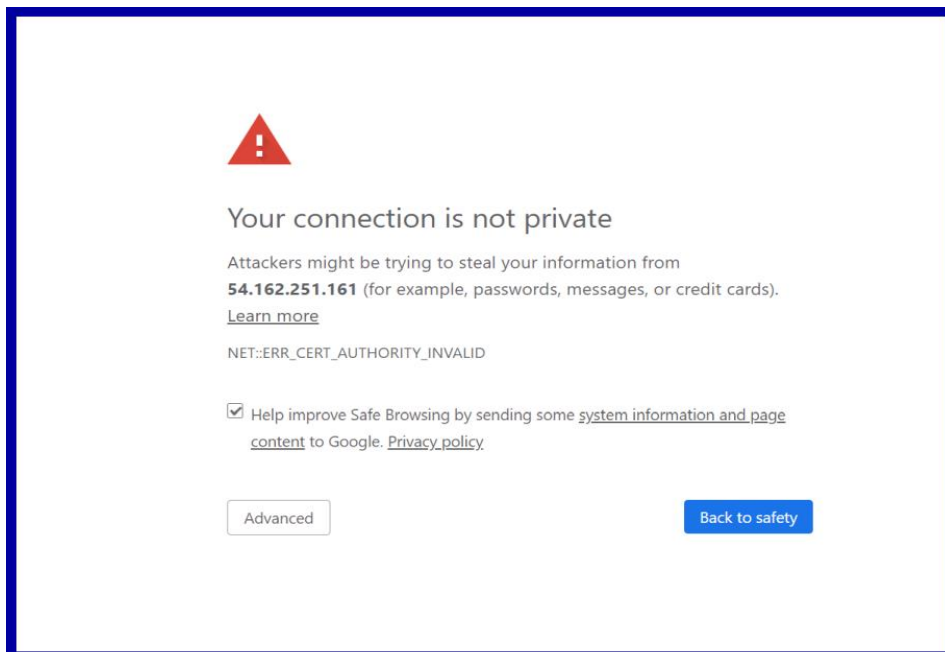
Instance ID	i-0a3e18669e8a91d23
Instance state	running
Instance type	t2.micro
Elastic IPs	
Availability zone	us-east-1d
Security groups	N2WS Backup - Recovery -CPM- Free Trial - BYOL Edition-2-4-0-AutogenByAWSMF




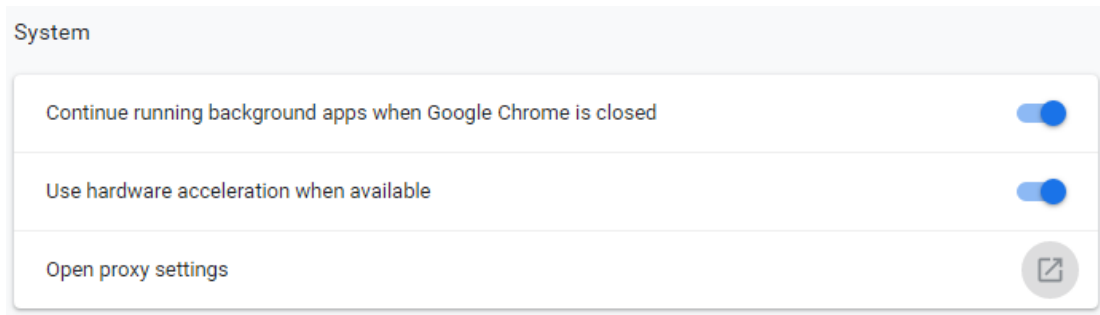
Appendix B – Adding Exception for Default Browser

For Chrome

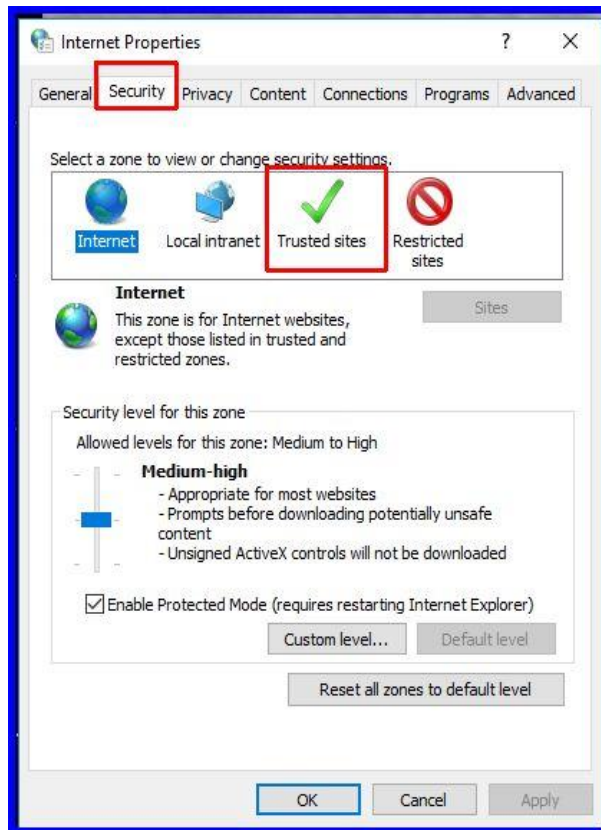
When you first navigate to your N2WS instance, you'll see a screen like this. It's nothing to worry about. We are SSL secured but because it is a self-signed certificate, you may want to add an exception to your browser following these steps.



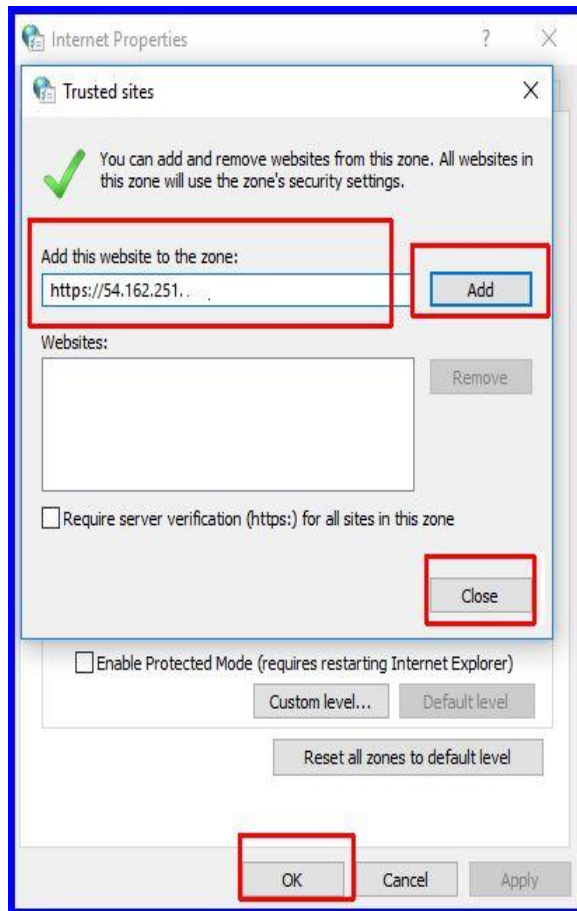
1. Open the Chrome browser. In the top right, select **More** .
2. Select **Settings**, **Advanced**, and then in the **System** section, select **Open proxy settings**.



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



4. Select the **Sites** button.
5. Type the N2WS 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).

