



N2WS Backup & Recovery (CPM)

Quick Start Guide

V3.0.0b



Content

1	Introduction	3
1.1	Launching the Instance	3
1.2	CloudFormation	3
1.3	N2WS Server Instance Connectivity	3
2	N2WS Server Instance Configuration	4
2.1	N2WS Server Configuration Wizard.....	4
3	Creating a Simple Backup Policy	11
3.1	Adding an AWS Account	11
3.2	Creating a Simple Backup Schedule.....	13
3.3	Creating a Simple Backup Policy	14
4	Performing a Basic Recovery	18
5	How to Configure N2WS with CloudFormation	24
	Appendix A – AWS Authentication.....	29
	Appendix B – Adding Exception for Default Browser	36



1 Introduction

1.1 Launching the Instance

You can quickly start using the N2WS Backup & Recovery (CPM) enterprise-class backup solution to fully protect your AWS cloud deployment.

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**.

1.2 CloudFormation

CloudFormation (CF) 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.

The IAM role will automatically contain the required permissions for N2WS operations.

See section 5 How to Configure N2WS with CloudFormation.

1.3 N2WS Server Instance Connectivity

In order 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.



2 N2WS Server Instance Configuration

N2WS has a browser-based management console. N2WS supports Mozilla Firefox, Google Chrome, Safari and IE (Version 9+).

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		
IP-4 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 36).

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

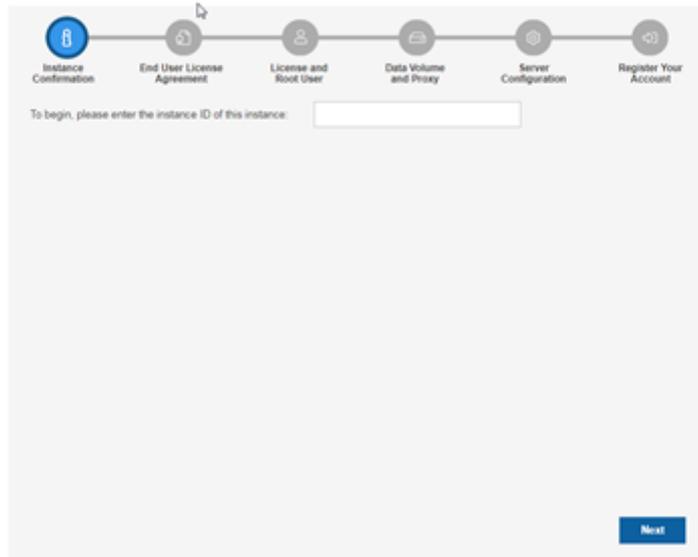
2.1 N2WS Server Configuration Wizard

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 password and verify it.

Step 1: Verify ownership of new instance

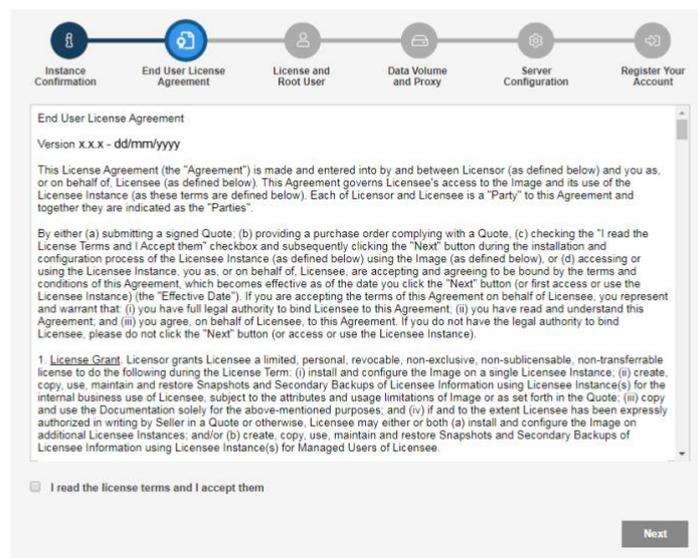
At the first screen you will be asked to type or paste the instance ID of this new N2WS instance. This step is required in order to verify that you are indeed the owner of this instance.



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 check box and select **Next**.





Step 3: Configure the license type, N2WS “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 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 prior to 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

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:

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.

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](#).

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:

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.

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-0572edf03db0b2f08 (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

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

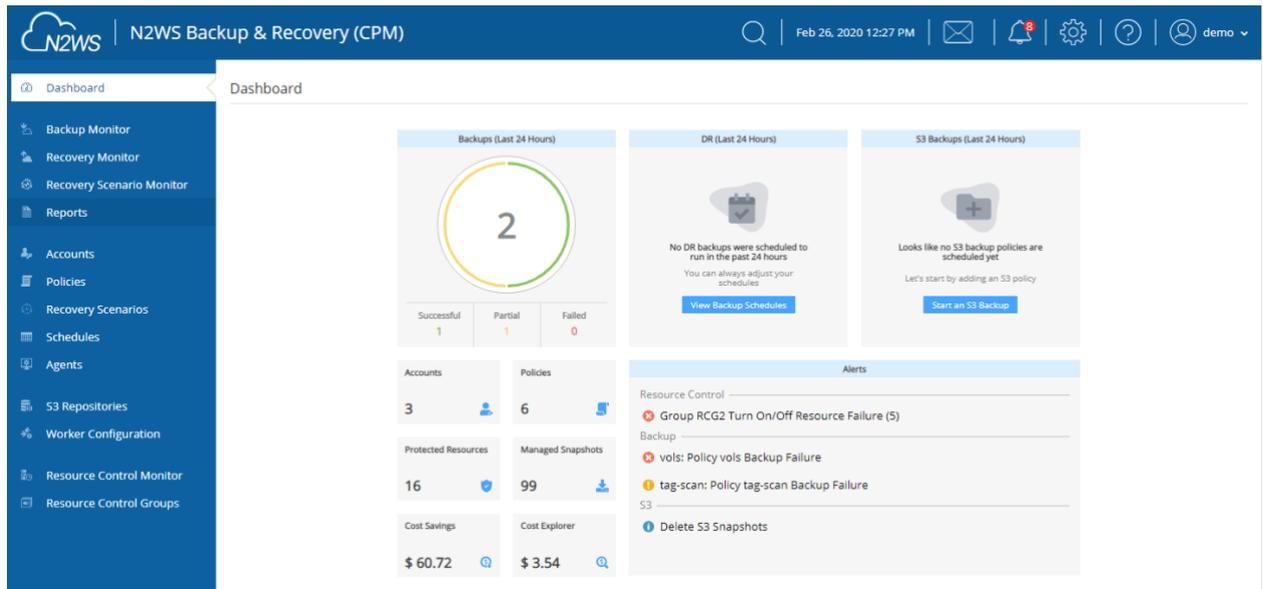


3 Creating a Simple Backup Policy

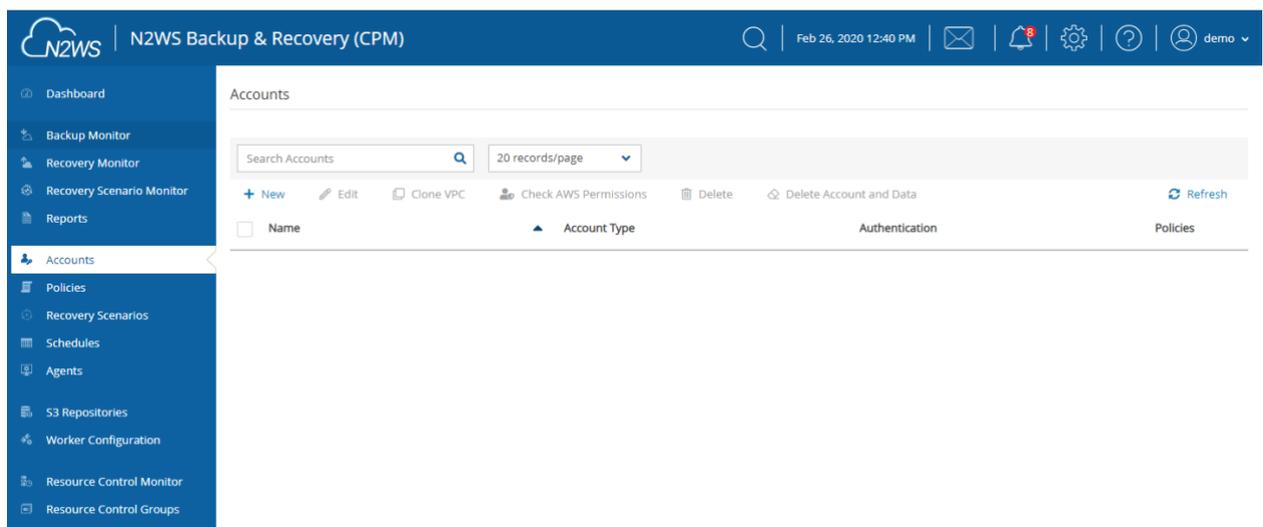
A backup policy requires an account from which to operate. While a backup schedule is geared toward a production environment, it is optional, as you can run a policy independently of a schedule.

3.1 Adding an AWS Account

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



It is currently empty. The first thing you will need to 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:

1. In the **Name** box, type the name you would like to associate to 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 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 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.

Capture VPCs is enabled by default. Clear **Capture VPCs** to turn off automatic capturing of VPCs for this account.



3.2 Creating a Simple Backup Schedule

In the left panel, select the **Schedules** tab. Currently, the list of schedules is empty.

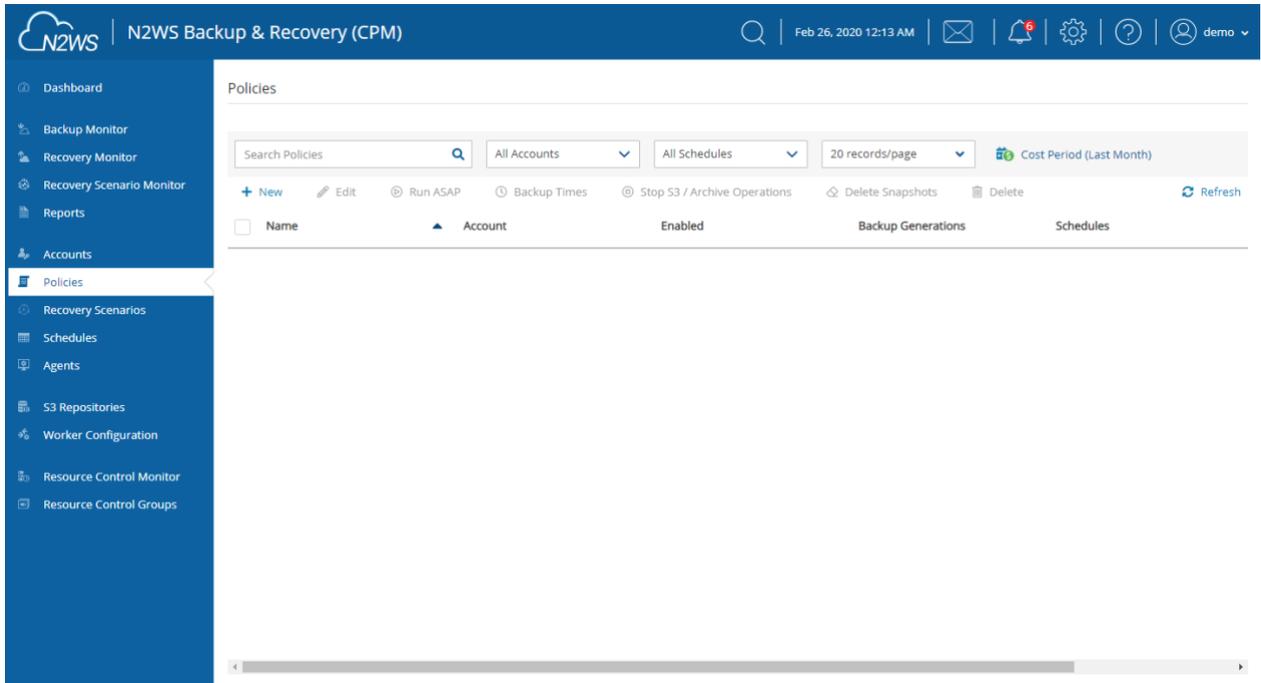
You will now create the first schedule. Select **+ New**.

1. Type a name 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** check boxes.



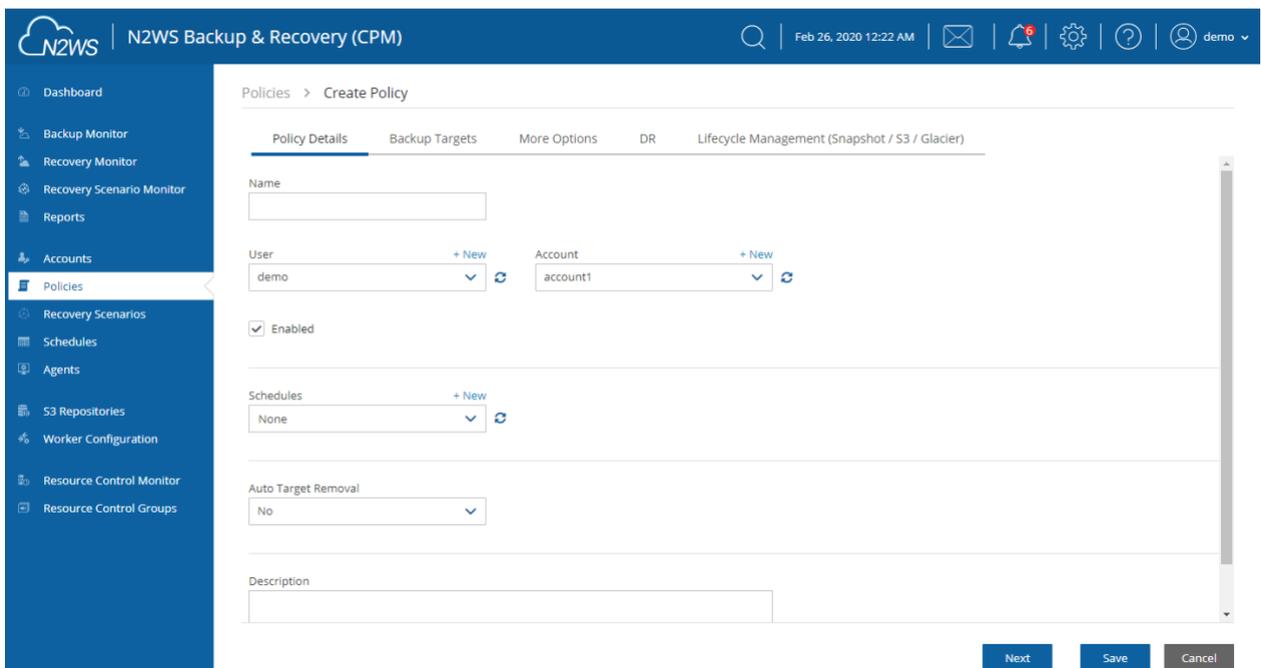
3.3 Creating a Simple Backup Policy

In the left panel, select the **Policies** tab. Currently, the list of policies is empty.



You will now create the first policy. Select **+ New**.

In the **Create Policy** page, enter a policy name and description:



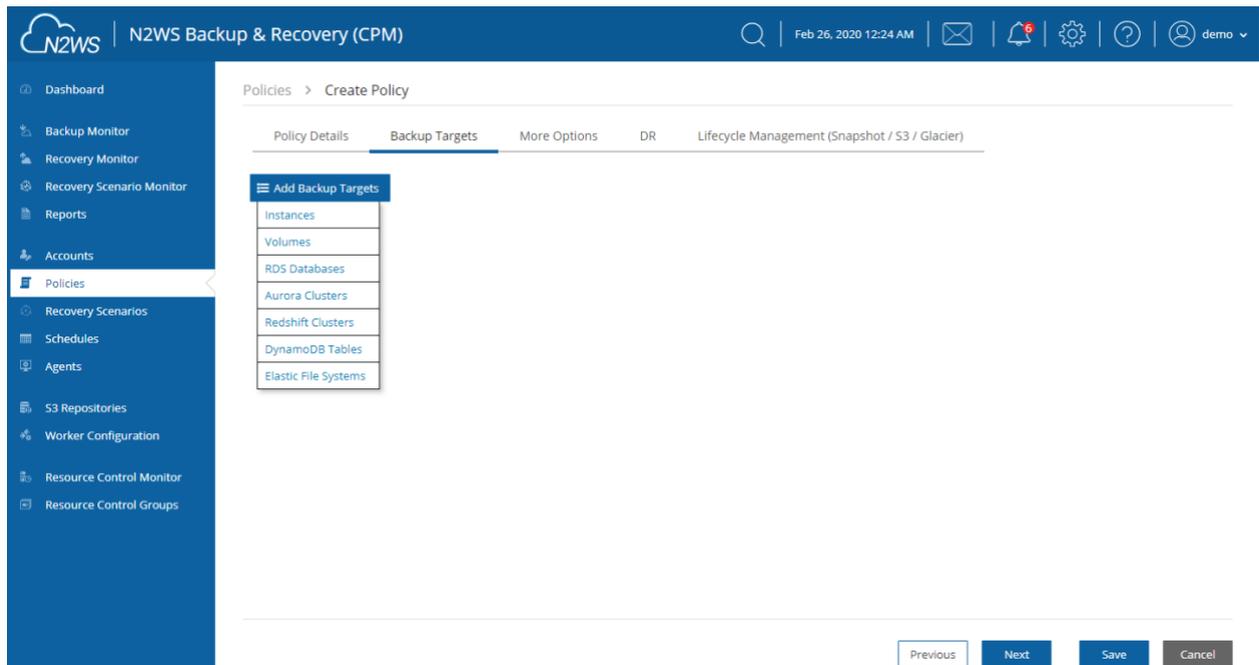
Other fields in this screen include:

- **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 list whether to automatically remove resources that no longer exist. If you enable this removal, if an instance is terminated, or an EBS volume deleted, the next backup will detect that and remove it from the policy. Choose **yes and alert** if you want the backup log to include a warning about such a removal.

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



Following are the types of objects you can back up:

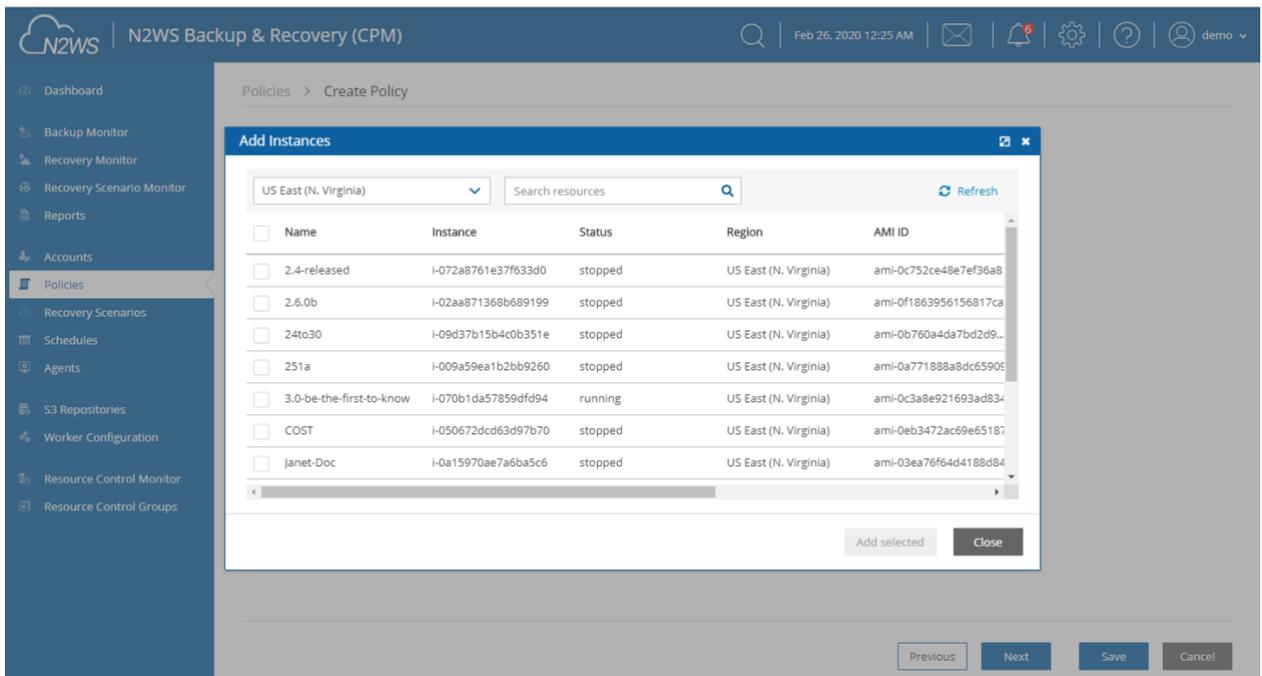
- **Instances** - Back up EC2 instances, including their metadata, and optionally some or all of their data volumes. This is the most common backup target.
- **Volumes** - Back up EBS volumes independently, whether or not they are attached to an instance, and regardless of which instance they are attached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



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**.



The screenshot shows the 'Policies' page in the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, Reports, Accounts, Policies (selected), Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, and Resource Control Groups. The main content area displays a table of policies with columns: Name, Account, Enabled, Backup Generations, and Schedules. The 'vols' policy is selected.

Name	Account	Enabled	Backup Generations	Schedules
AK-SK-P1	ACCOUNT-IAM-USER-edited	Yes	30	s1
cpmdata	account1	Yes	1	
p1	account1	Yes	5	s1
redShift	account1	Yes	1	
tag-scan	account1	Yes	30	
<input checked="" type="checkbox"/> vols	account1	Yes	30	

N2WS will report that the backup policy will now run. The process can be monitored by following the **Status** in the **Backup Monitor** tab.

The screenshot shows the 'Backup Monitor' page in the N2WS Backup & Recovery (CPM) interface. The left sidebar is the same as in the previous screenshot. The main content area displays a table of backup jobs with columns: Start Time, Finish Time, Policy / Frozen Item, Account, Status, and DR Status. The 'vols' backup is currently 'In Progress'.

Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status
Feb 26, 2020 11:01 AM		vols	account1	In Progress	
Feb 25, 2020 7:56 PM	Feb 25, 2020 7:58 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 25, 2020 2:11 AM	Feb 25, 2020 2:13 AM	tag-scan	account1	Partially Successful	
Feb 23, 2020 4:03 PM	Feb 23, 2020 4:05 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 23, 2020 2:59 PM	Feb 23, 2020 3:01 PM	tag-scan	account1	Successful	
Feb 23, 2020 2:53 PM	Feb 23, 2020 2:55 PM	tag-scan	account1	Successful	
Feb 22, 2020 8:18 PM	Feb 22, 2020 8:25 PM	p1	account1	Successful	Completed
Feb 22, 2020 7:56 PM	Feb 22, 2020 8:15 PM	p1	account1	Successful	Completed
Feb 22, 2020 12:53 AM	Feb 22, 2020 1:31 AM	p1	account1	Successful	Completed
Feb 20, 2020 5:40 PM	Feb 20, 2020 5:41 PM	redShift	account1	All Snapshots Deleted	

Consult the *N2WS Backup & Recovery (CPM) User Guide* to see how to create application consistency for Linux and Windows servers.



4 Performing a Basic Recovery

N2WS backs up the requested objects at the requested times. You can view the backups in the **Backup Monitor** tab:

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation options: Dashboard, Backup Monitor (selected), Recovery Monitor, Recovery Scenario Monitor, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, and Resource Control Groups. The main area is titled 'Backup Monitor' and features a search bar, filters for 'by resource', 'All Policies', 'All Accounts', and 'All Backup Statuses'. Below the filters are controls for '20 records/page', 'Show' (with icons for list, grid, and print), and a row of action buttons: Recover, Log, View Snapshots, Move to Freezer, Edit Frozen Item, Abort Copy to S3 Snapshots, Delete Frozen Item, and Refresh. A table displays backup records with columns: Start Time, Finish Time, Policy / Frozen Item, Account, Status, and DR Status. The table contains 10 rows of data, with the last row (Feb 22, 2020 12:53 AM) highlighted in blue. The bottom of the interface shows 'Page 1 of 2' and 'Displaying 1 - 20 of 23'.

Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status
Feb 26, 2020 11:12 AM	Feb 26, 2020 11:13 AM	vols	account1	Successful	
Feb 25, 2020 7:56 PM	Feb 25, 2020 7:58 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 25, 2020 2:11 AM	Feb 25, 2020 2:13 AM	tag-scan	account1	Partially Successful	
Feb 23, 2020 4:03 PM	Feb 23, 2020 4:05 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 23, 2020 2:59 PM	Feb 23, 2020 3:01 PM	tag-scan	account1	Successful	
Feb 23, 2020 2:53 PM	Feb 23, 2020 2:55 PM	tag-scan	account1	Successful	
Feb 22, 2020 8:18 PM	Feb 22, 2020 8:25 PM	p1	account1	Successful	Completed
Feb 22, 2020 7:56 PM	Feb 22, 2020 8:15 PM	p1	account1	Successful	Completed
Feb 22, 2020 12:53 AM	Feb 22, 2020 1:31 AM	p1	account1	Successful	Completed
Feb 20, 2020 5:40 PM	Feb 20, 2020 5:41 PM	redShift	account1	All Snapshots Deleted	

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. In order to recover from a particular backup (typically the most recent successful backup), select the backup and then select **Recover**:

This screenshot is similar to the previous one, but the backup record for 'Feb 22, 2020 8:18 PM' is selected, indicated by a checkmark in the left column. The table now shows '1 of 20 items selected' at the top. The selected row is highlighted in blue.

Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status
Feb 25, 2020 7:56 PM	Feb 25, 2020 7:58 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 25, 2020 2:11 AM	Feb 25, 2020 2:13 AM	tag-scan	account1	Partially Successful	
Feb 23, 2020 4:03 PM	Feb 23, 2020 4:05 PM	AK-SK-P1	ACCOUNT-IAM-USER-edited	Successful	
Feb 23, 2020 2:59 PM	Feb 23, 2020 3:01 PM	tag-scan	account1	Successful	
Feb 23, 2020 2:53 PM	Feb 23, 2020 2:55 PM	tag-scan	account1	Successful	
<input checked="" type="checkbox"/> Feb 22, 2020 8:18 PM	Feb 22, 2020 8:25 PM	p1	account1	Successful	Completed
Feb 22, 2020 7:56 PM	Feb 22, 2020 8:15 PM	p1	account1	Successful	Completed

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.



N2WS Backup & Recovery (CPM) | Feb 26, 2020 11:10 AM | demo

Backup Monitor > p1 - 02/22/2020 8:18 PM > Recover

Search by Resource: Resource ID or name [Q]

Restore From: Original Account (account1)

Restore to Account: Same as Snapshot (account1)

Restore to Region: Origin

Instances

Recover Recover Volumes Only Explore

<input type="checkbox"/>	Name	ID	Region	Image ID	Root Device	Platform
<input type="checkbox"/>	proxy	i-077441dd85a72e6d5	us-east-1	ami-07ebfd5b3428b6f4d	/dev/sda1	Unix / Linux
<input type="checkbox"/>	windows	i-0d6abf533c3049e61	us-east-1	ami-09f2114fecbe506e2	/dev/sda1	windows

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-04b9e92b5572fa0d1

Instance Type: t3a.medium

Instance Profile ARN: arn:aws:iam::726541571499:instance-profile

Instances to Launch: 1

Key Pair: my-key-pair

Networking

Placement: By VPC

VPC: vpc-1a4e8062 () **Clone VPC**

VPC Subnet: subnet-a4239bc0 (default for us-east-)

Security Group: My-Proxy

VPC Assign IP: 172.31.3.33

Additional NICs:

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.

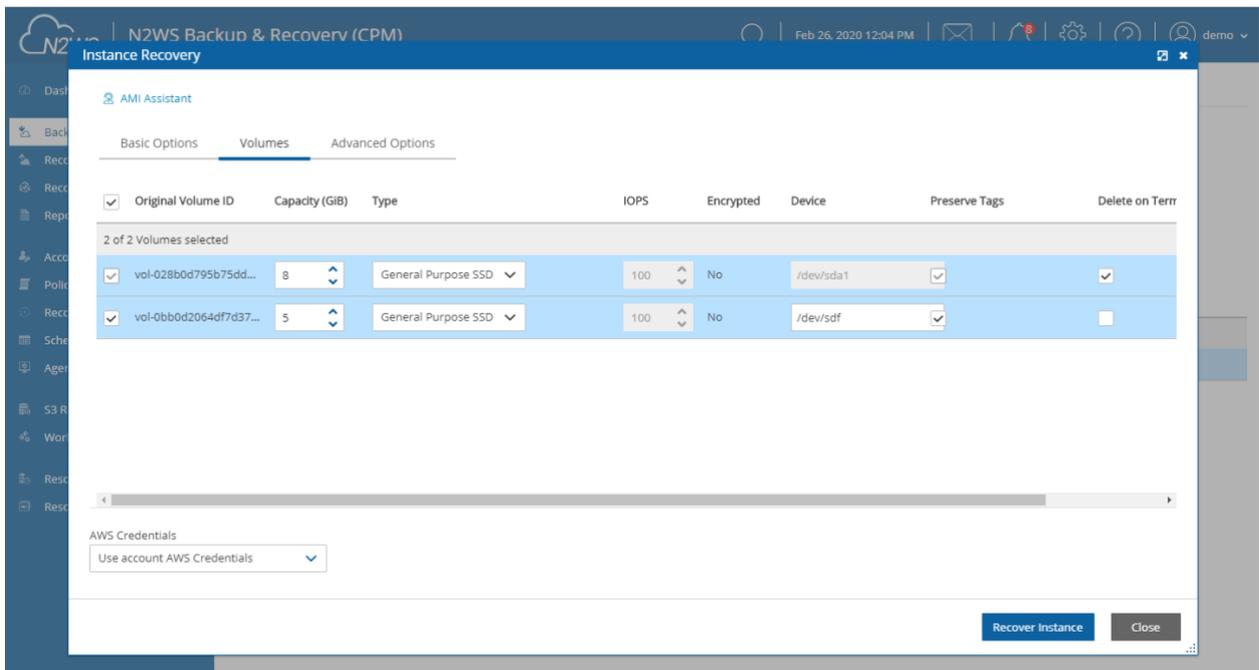


VPC
vpc-1a4e8062 () ▼ Clone VPC

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 originally backed up instance, you will need to change the IP in order to avoid an IP conflict. This can be mitigated by leaving the **VPC Assign IP** box blank:

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





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

Instance Recovery

AMI Assistant

Basic Options Volumes **Advanced Options**

Architecture: x86_64 Tenancy: Shared

Shutdown Behaviour: Stop API Termination: Disable

Auto-assign Public IP: Subnet Default

Kernel: RAM Disk:

Preserve Tags

Allow Monitoring

ENA

EBS Optimized

Enable User Data

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**.



N2WS Backup & Recovery (CPM) | Feb 26, 2020 12:09 PM

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

Recovery Time	Backup Time	Recovery Type	Policy	Account	Status	
<input type="checkbox"/>	Feb 23, 2020 4:23 PM	Feb 23, 2020 4:03 PM	Instance	AK-SK-P1	ACCOUNT-IAM-USER-edited	Recovery in progress
<input type="checkbox"/>	Feb 23, 2020 4:23 PM	Feb 23, 2020 4:03 PM	Instance	AK-SK-P1	ACCOUNT-IAM-USER-edited	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 6:15 PM	Feb 20, 2020 5:40 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 6:14 PM	Feb 20, 2020 5:40 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 6:13 PM	Feb 20, 2020 5:40 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 5:43 PM	Feb 20, 2020 5:40 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 5:43 PM	Feb 20, 2020 5:40 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 4:40 PM	Feb 20, 2020 4:31 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 4:39 PM	Feb 20, 2020 4:23 PM	Redshift Cluster	redShift	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 3:26 PM	Feb 20, 2020 3:20 PM	Volume	vols	account1	Recovery succeeded
<input type="checkbox"/>	Feb 20, 2020 3:26 PM	Feb 20, 2020 3:20 PM	Volume	vols	account1	Recovery succeeded

Page 1 of 2 | Displaying 1 - 20 of 26

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.



5 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

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

BYOL

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

< 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

< 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	\$0/hr
--	--------

BYOL
running on t3.medium

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

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
 Amazon S3 template URL

S3 URL: [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 N2WS

Networking and Security Configuration

Key Pair
Name of an existing EC2 KeyPair

VPC
The VPC in which you want to Launch N2WS

Subnet
Subnetid in VPC

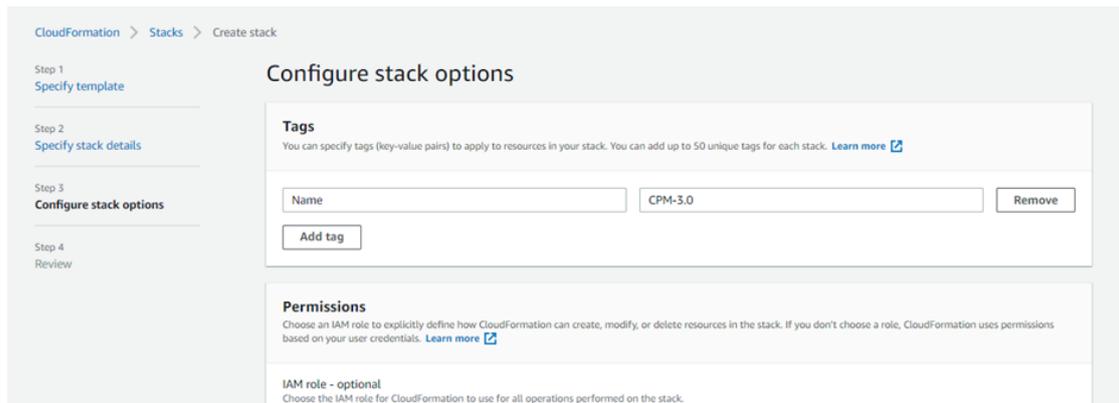
Inbound Access CIDR
CIDR for Security Groups source IP

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:

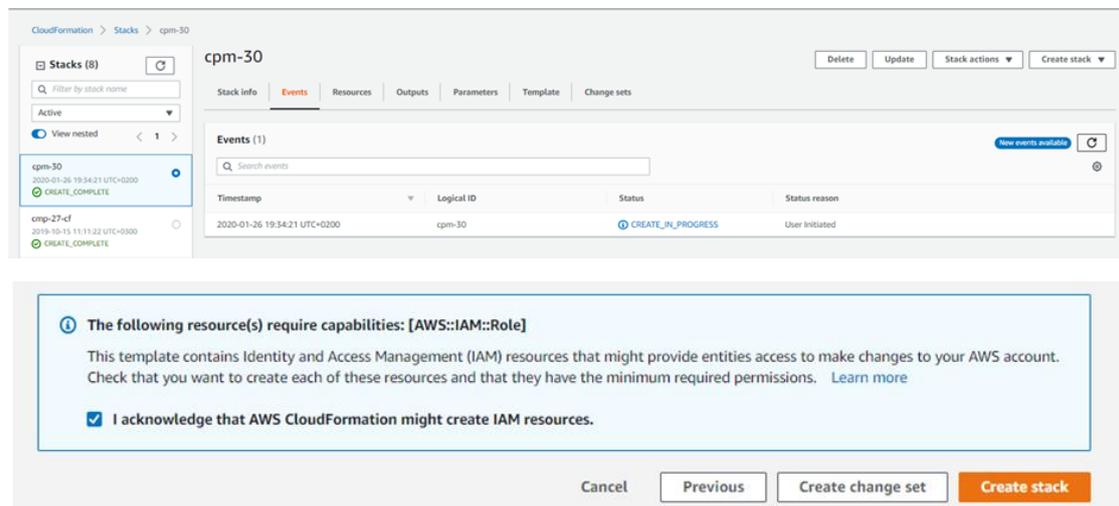


- If your IPv4 address is 203.0.113.25, specify 203.0.113.25/32 to list this single IPv4 address in CIDR notation. If your company allocates addresses within a range, specify the entire range, such as 203.0.113.0/24.
- If you specify 0.0.0.0/0, it will enable all IPv4 addresses to access your instance 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 as from section 2.1.

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



Appendix A – AWS Authentication

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

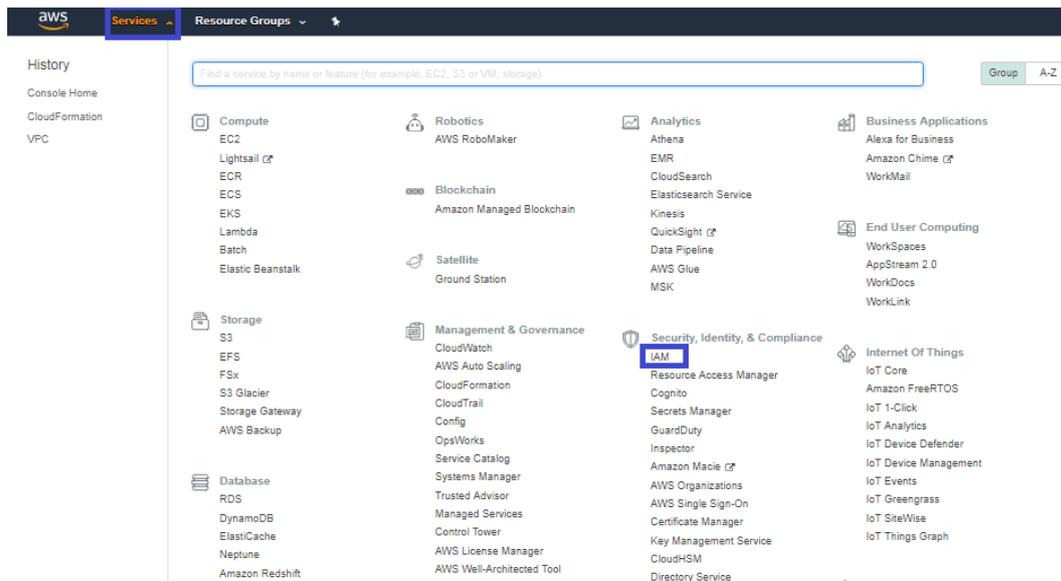
N2WS supports two different types of AWS authentication during setup:

- AccessKey / SecretKey
- Role based authentication (recommended)

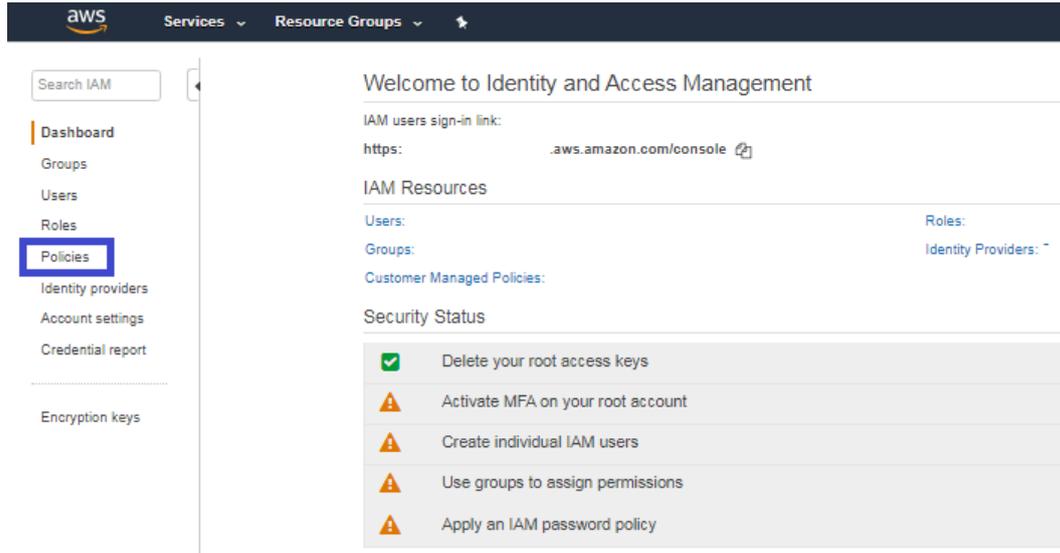
The permissions necessary have been combined into a JSON file for convenience and can be downloaded from the N2WS Knowledge Base:

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

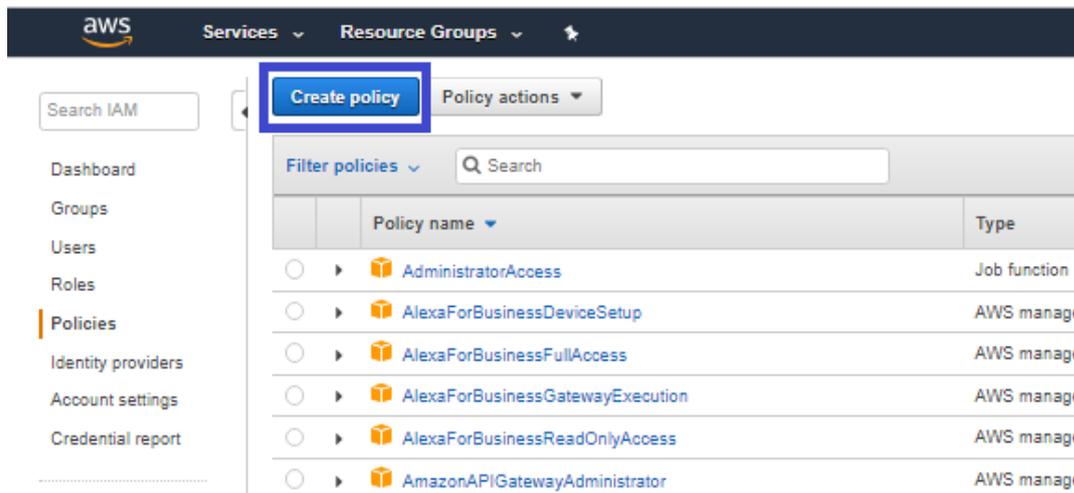
1. At the top of your AWS console, select the **Services** tab. In the **Security Identity & Compliance** section, select **IAM**.



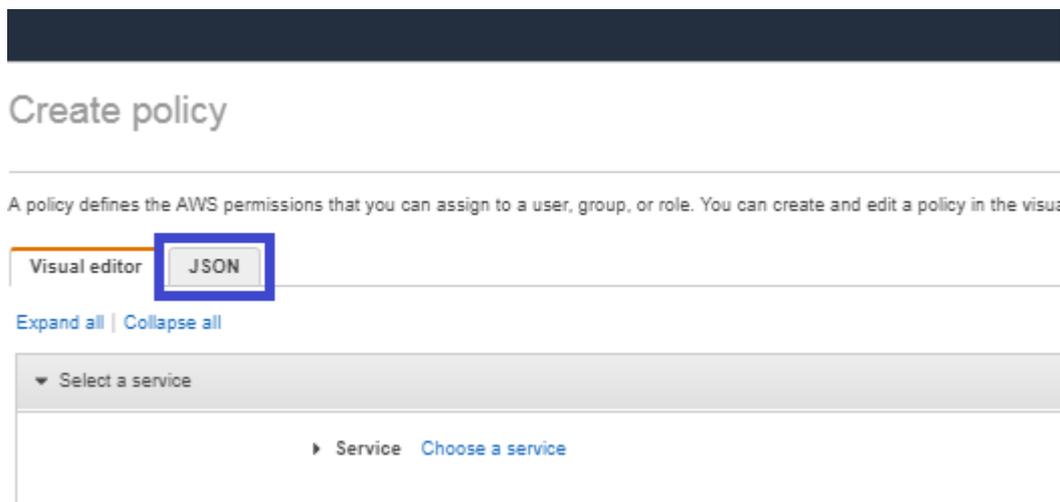
2. In the left menu, select **Policies**.



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).

Create policy

A policy defines the AWS permissions that you can assign to a user, group, or role. You can create and edit a policy in the

This policy validation failed and might have errors converting to JSON : The policy must have at least one statement.
[IAM Policies](#)

Visual editor

JSON

```
1 {
2   "Version": "2012-10-17",
3   "Statement": []
4 }
```

- At the bottom of the screen, select **Review Policy**.

Cancel

Review policy

- 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

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

Next, 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**. 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.

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**



10. 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**

11. Search for the previously created policy, select its check box, and select **Next: Review**.



Create role

1 2 3 4

Attach permissions policies

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

Create policy



Filter policies	Search	Showing 1 result
Policy name	Used as	Description
<input checked="" type="checkbox"/> CD_RO	None	

Set permissions boundary

* Required

Cancel

Previous

Next: Tags

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

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

Create role

1 2 3 4

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

14. Assign the resulting role to the N2WS trial instance by:

b. Select the N2WS instance name.



c. 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 INSTANCES, IMAGES, ELASTIC BLOCK STORE, NETWORK & SECURITY, LOAD BALANCING, AUTO SCALING, SYSTEMS MANAGER SERVICES, and SYSTEMS MANAGER SHARED RESOURCES. The main content area displays a table of EC2 instances. One instance, named 'N2WS 2.5.0 Trial' with ID 'i-0a3e18669e8a91d23', is selected. An 'Actions' dropdown menu is open over this instance, showing options like 'Connect', 'Instance Settings', and 'Attach/Replace IAM Role'. The 'Attach/Replace IAM Role' option is highlighted in blue. Below the table, the instance details for 'i-0a3e18669e8a91d23' are shown, including its state (running), type (t2.micro), and security groups.

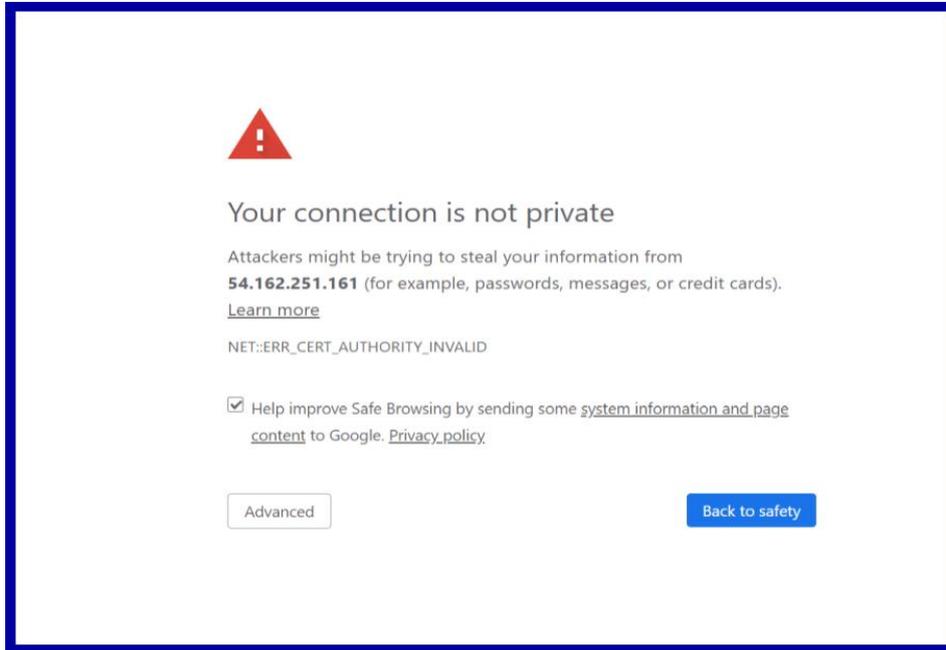
Name	Instance ID	Availability Zone	Instance State	Status
N2WS 2.5.0 Trial	i-0a3e18669e8a91d23	us-east-1d	running	In

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

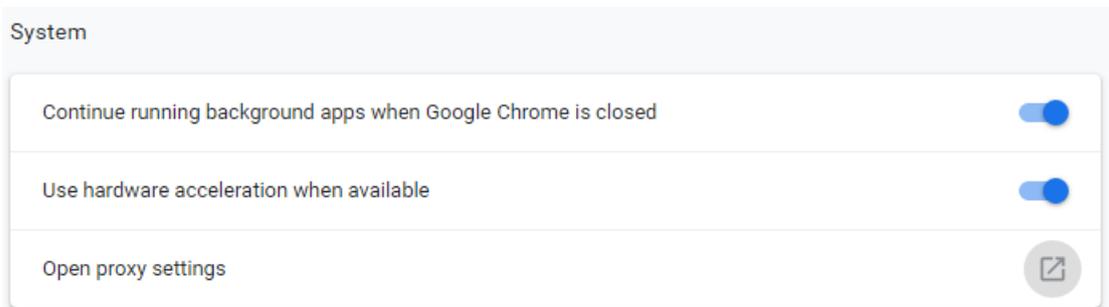
Description	Status Checks	Monitoring	Tags	Usage Instructions
Instance ID	i-0a3e18669e8a91d23			
Instance state	running			
Instance type	t2.micro			
Elastic IPs				
Availability zone	us-east-1d			
Security groups	N2WS Backup - Recovery -CPM- Free Trial - BYOL Edition-2-4-0-AutogenByAWSMF			

Appendix B – Adding Exception for Default Browser

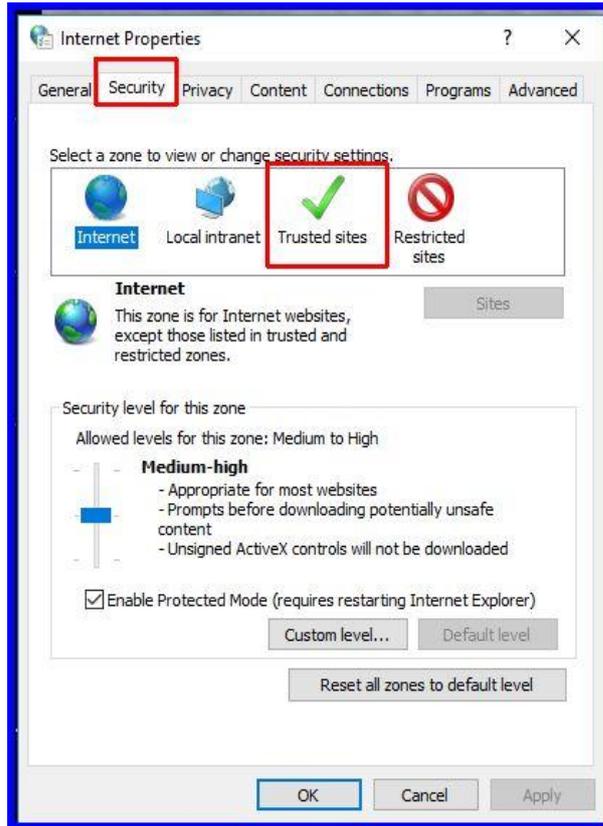
For Chrome



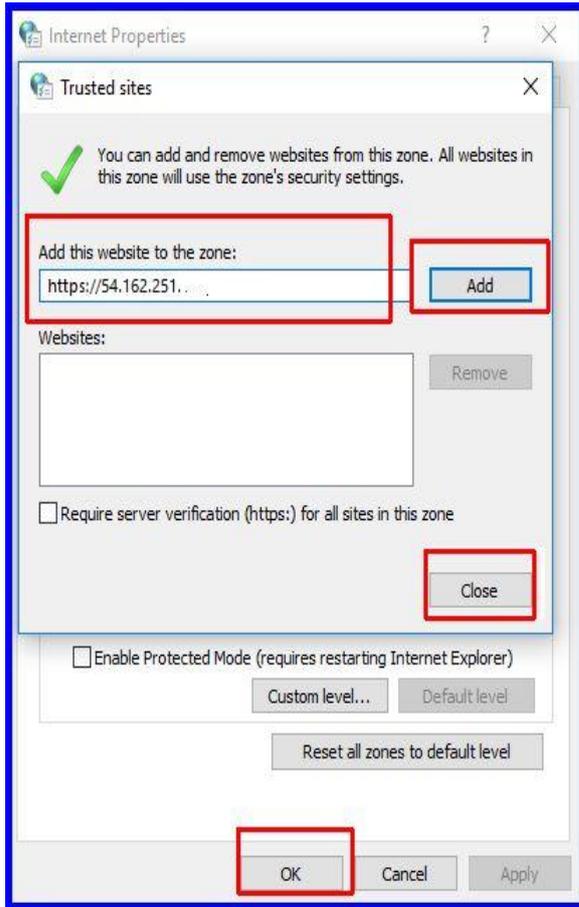
1. Open the Chrome browser. In top right, select **More** .
2. Select **Settings, Advanced**, and then in the **System** section, select **Open proxy settings**.



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

