N2WS Backup & Recovery (CPM)

Quick Start Guide

V2.5.0

Content

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. Click **Continue to Subscribe**.
5. In the AWS logon page, enter your AWS account information, and click **Continue to Configuration**.
6. Under **Configure this software**, select the relevant version in the **Software Version** list.
7. Click **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

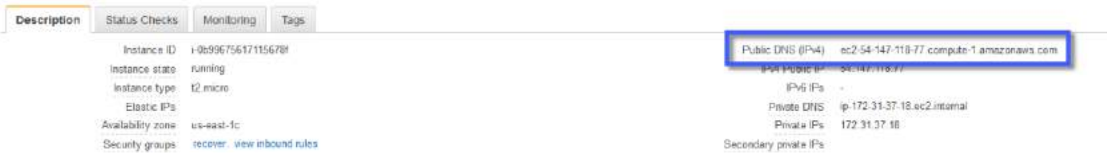
In order for the configuration process to work, as well as N2WS’s normal operations, N2WS needs to be able to “talk” with AWS APIs. Thus, it needs to have outbound connectivity to the Internet. Verify that the N2WS instance has Internet connectivity; this can be achieved by placing the instance in a 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:



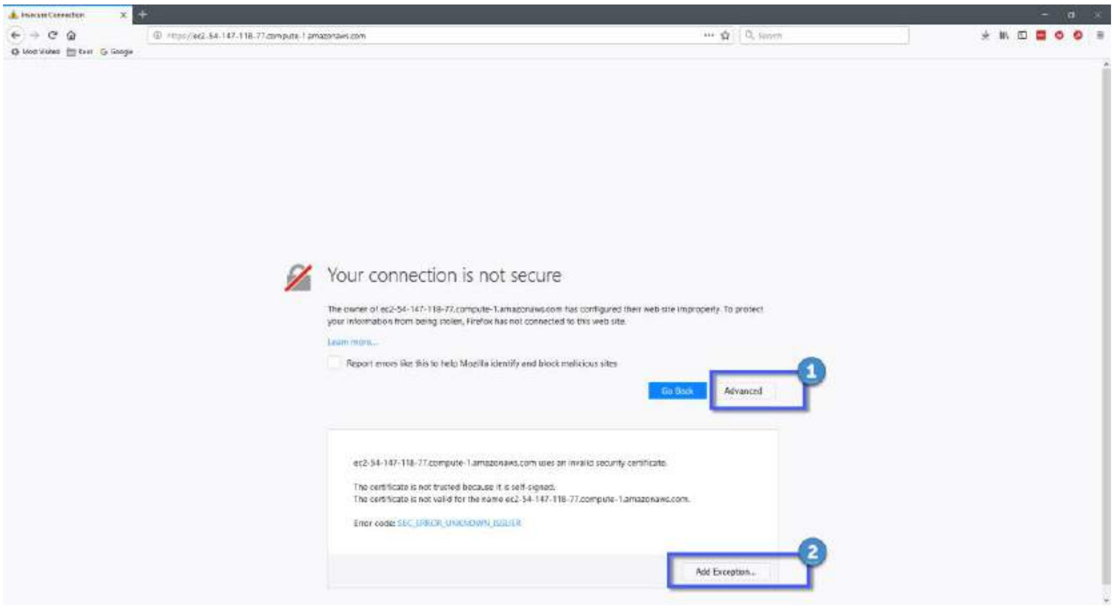
Instance ID i-0b99675617115678f
Instance state running
Instance type t2.micro
Elastic IPs
Availability zone us-east-1c
Security groups recover. view inbound rules

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

Figure 2-1

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:



Your connection is not secure

The owner of ec2-54-147-118-77.compute-1.amazonaws.com has configured their web site improperly. To protect your information from being stolen, Firefox has not connected to this web site.

Learn more...

□ Report errors like this to help Mozilla identify and block malicious sites

Go Back | Advanced

ec2-54-147-118-77.compute-1.amazonaws.com uses an invalid security certificate.

The certificate is not trusted because it is self-signed.
The certificate is not valid for the name ec2-54-147-118-77.compute-1.amazonaws.com.

Error code: SEC_ERROR_UNKNOWN_ISSUER

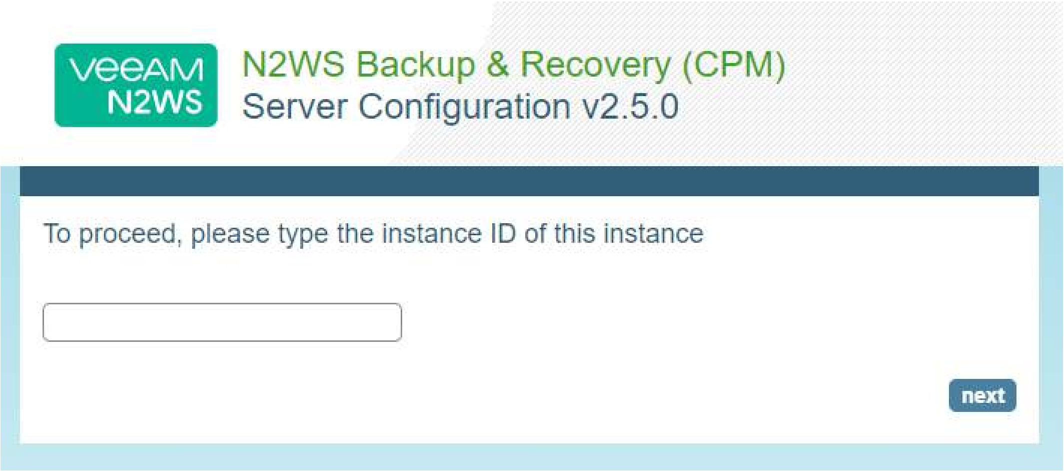
Add Exception...

Figure 2-2

The example in Figure 2-2 is from Firefox Quantum. After you click **Advanced** (1) and add an exception for this server (2), you get the first screen of the N2WS configuration application.

2.1 N2WS Server Configuration

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:



N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

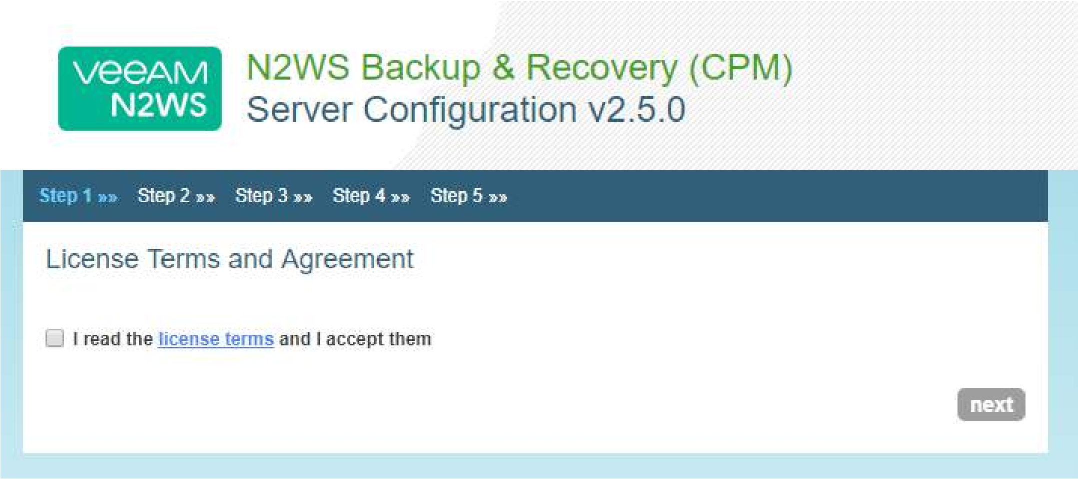
To proceed, please type the instance ID of this instance

Figure 2-3

On the next screen the 5-step N2WS configuration procedure begins.

Step 1: Approve the N2WS license agreement

Review the user license terms, select the check box and click **next**.



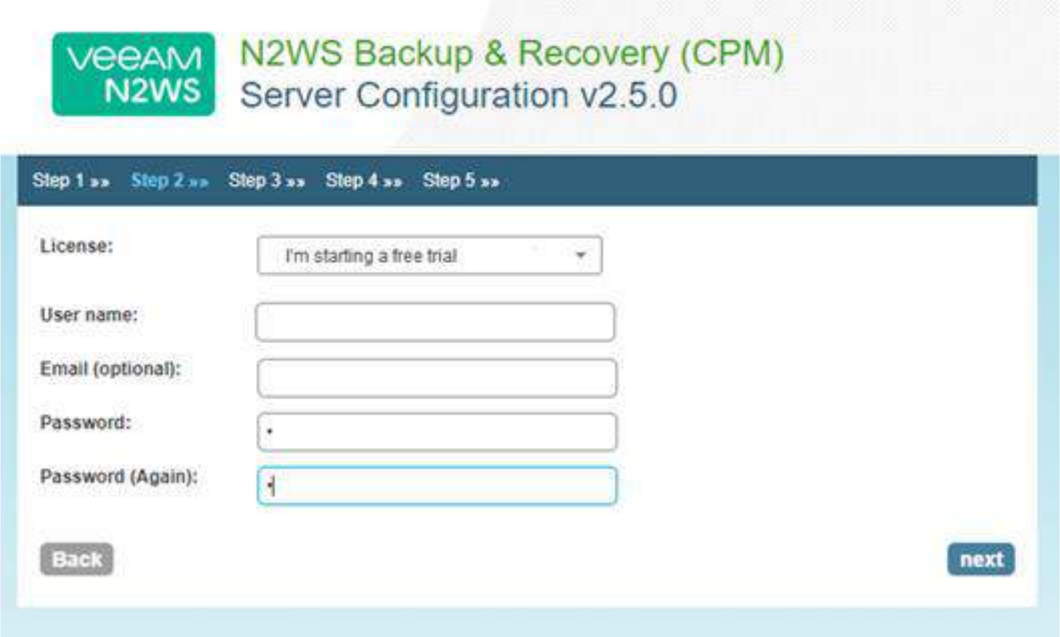
N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

License Terms and Agreement

□ I read the license terms and I accept them

Figure 2-4

Step 2: Configure the N2WS "root" account password and user information


Veeam N2WS
N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0
Step 1 »» Step 2 »» Step 3 »» Step 4 »» Step 5 »»
Back
next

License: I'm starting a free trial

User name:

Email (optional):

Password: •

Password (Again): •

Figure 2-5

To start a 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 connecting to N2WS. Contact support@n2ws.com to resolve.

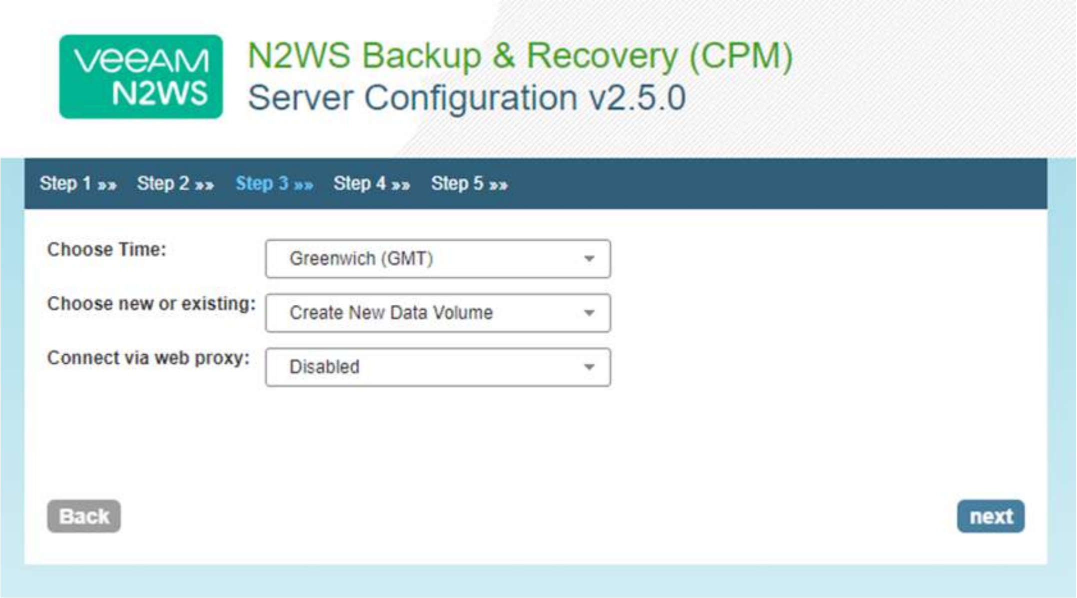
Note: If you are using one of the N2WS paid products on AWS Marketplace, you will not see the License field.

Additionally, you will need to enter a user name, an optional valid email address, and enter a password and verify it. 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 to use passwords that are difficult to guess and to change them regularly.

When you have completed entering the details for Step 2, click **next**.

Step 3: Time zone, new volume, and web proxy settings



N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

Choose Time: Greenwich (GMT)

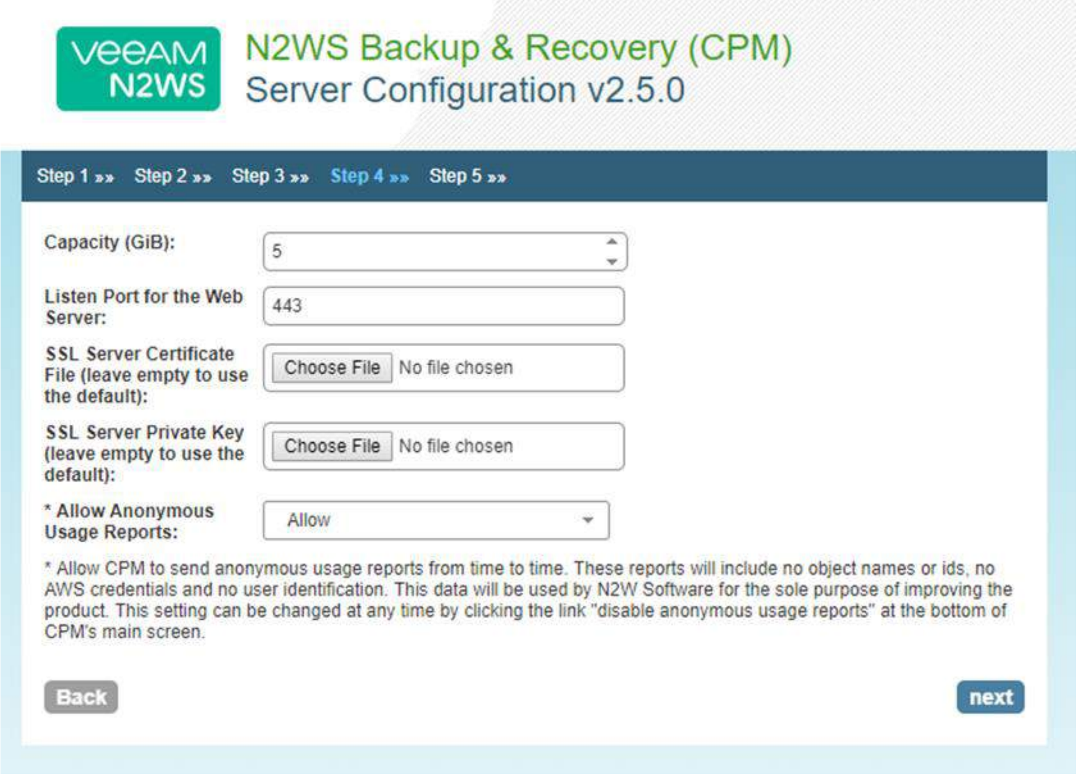
Choose new or existing: Create New Data Volume

Connect via web proxy: Disabled

Figure 2-6

1. Select your time zone.
2. Choose whether to create a new data volume or use an existing one.
3. Click **next**.

Step 4: Data volume, Web Server settings, and anonymous usage reports



N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

Capacity (GiB): 5

Listen Port for the Web Server: 443

SSL Server Certificate File (leave empty to use the default): Choose File No file chosen

SSL Server Private Key (leave empty to use the default): Choose File No file chosen

* Allow Anonymous Usage Reports: Allow

* Allow CPM to send anonymous usage reports from time to time. These reports will include no object names or ids, no AWS credentials and no user identification. This data will be used by N2W Software for the sole purpose of improving the product. This setting can be changed at any time by clicking the link "disable anonymous usage reports" at the bottom of CPM's main screen.

Figure 2-7

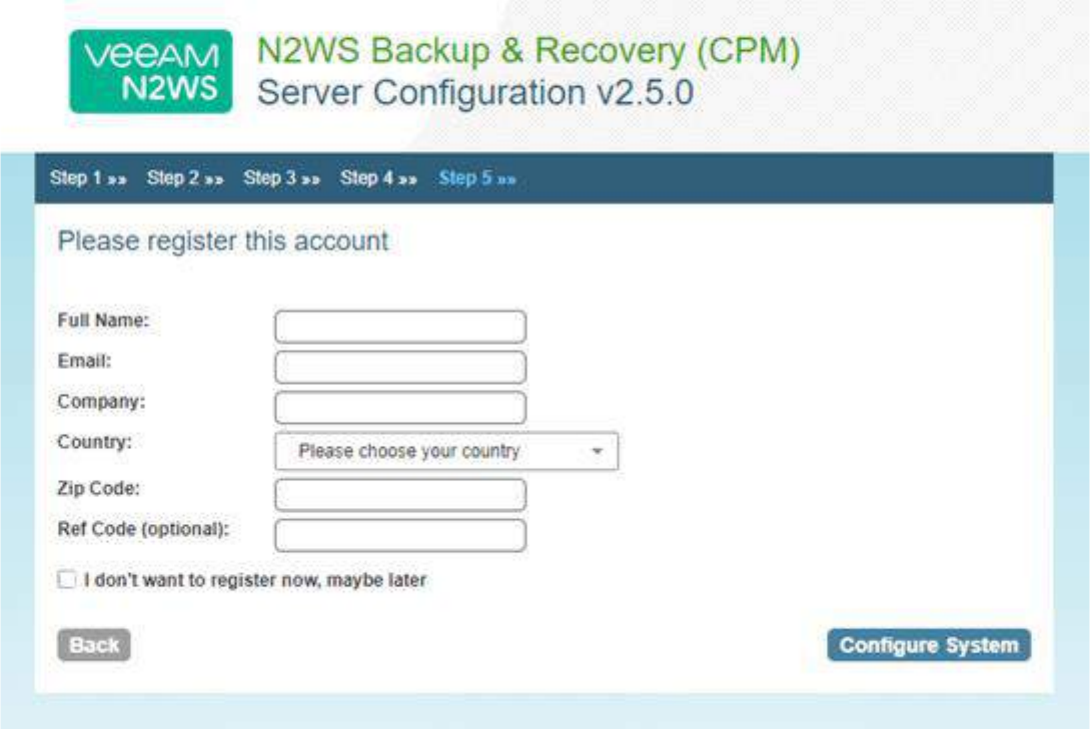
If you chose to create a new volume in the previous step, you will see the Capacity box, or if you chose to use an existing volume, you will see a drop-down volume selection box.

Complete the Web Server settings. The default port 443 is used by the N2WS manager.

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.

Click **next** when finished.

Step 5: Register the account with N2W Software


N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

Please register this account

Full Name:	
Email:	
Company:	
Country:	Please choose your country
Zip Code:	
Ref Code (optional):	

□ I don't want to register now, maybe later

Figure 2-8

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.

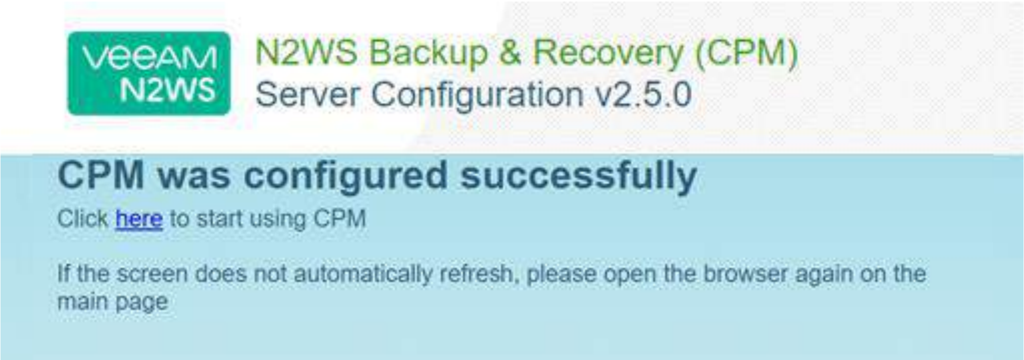
If you have a Reference Code, enter it in the **Ref Code** box.

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

Click **Configure System** when finished.

Please wait while Cloud Protection Manager is being configured!

The registration operation takes approximately 30 seconds after which the success screen appears:



N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

CPM was configured successfully

Click here to start using CPM

If the screen does not automatically refresh, please open the browser again on the main page

Figure 2-9

When you see the screen in

N2WS Backup & Recovery (CPM)
Server Configuration v2.5.0

CPM was configured successfully

Click here to start using CPM

If the screen does not automatically refresh, please open the browser again on the main page

Figure 2-9, you know that the system was configured successfully. You can then click the link to start using the system. It will take a few seconds for the application to start. If, for any reason, you are not directed automatically to the application logon screen, reboot the instance from the management console:

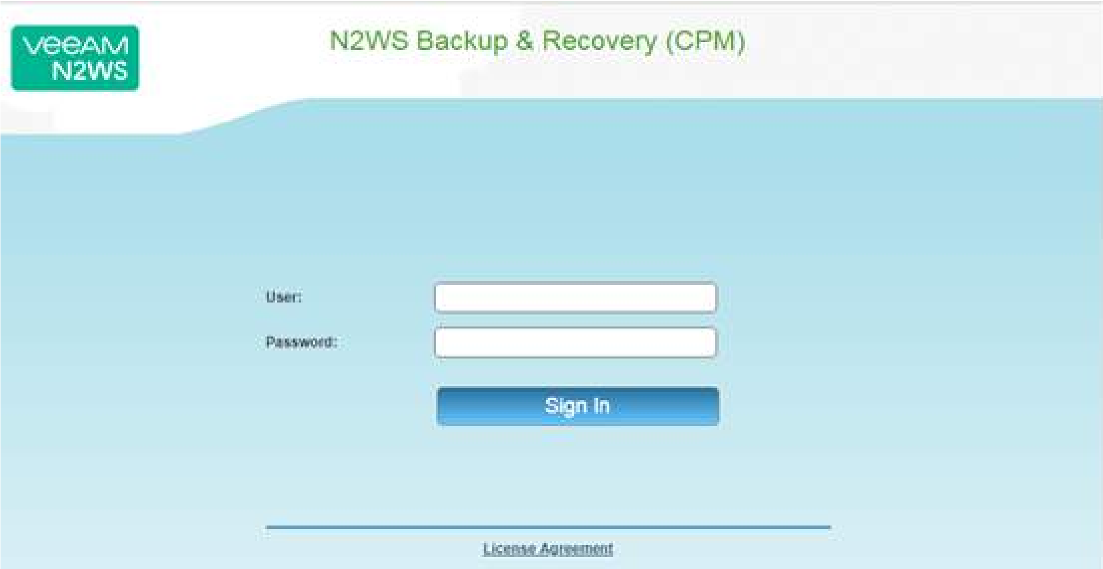


Figure 2-10

You are now ready to log on with the credentials you created in the first screen and begin using N2WS.

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.

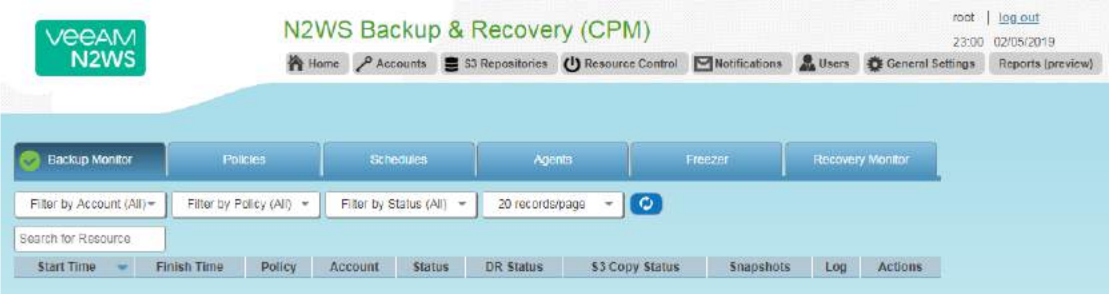


Figure 2-11

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

3.1 Adding an AWS Account

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

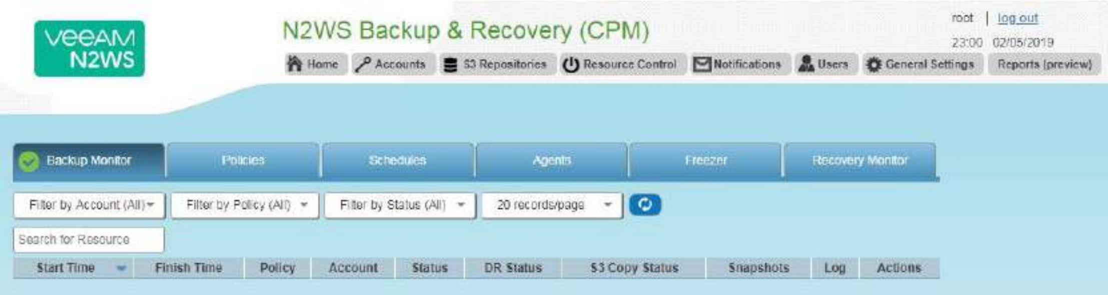
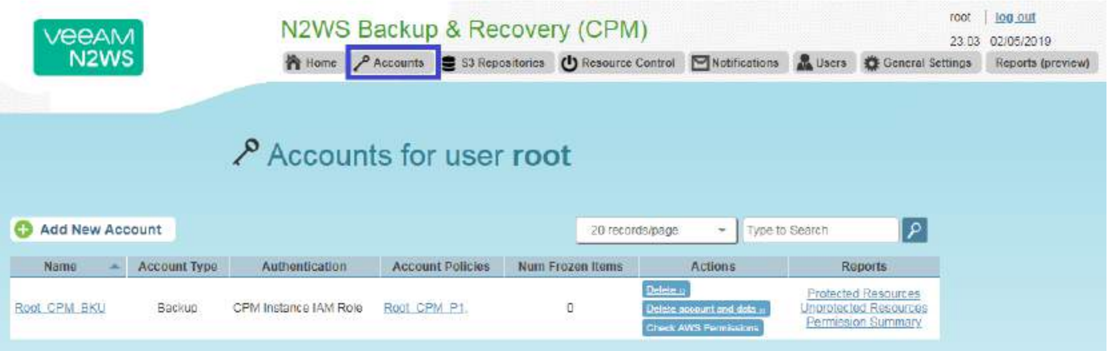


Figure 3-1

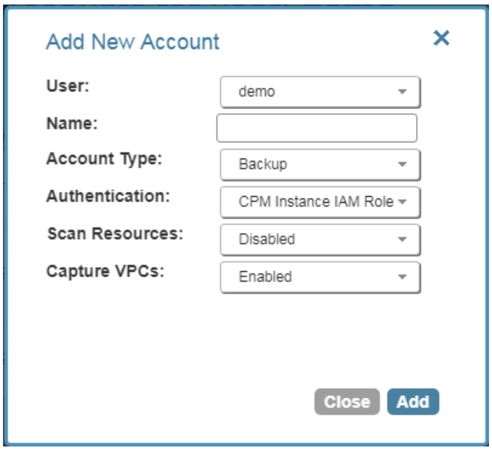
It is currently empty. The first thing you will need to do is to associate an AWS account so you can start backing up EC2 instances. Depending on the edition of N2WS you registered to, you can associate one or more AWS accounts. Click the **Accounts** button in the top panel and then click **Add New Account**.



Accounts for user root

Name	Account Type	Authentication	Account Policies	Num Frozen Items	Actions	Reports
Root_CPM_BKU	Backup	CPM Instance IAM Role	Root_CPM_P1,	0	Delete Delete account and data Check AWS Permissions	Protected Resources Unprotected Resources Permission Summary

Figure 3-2



Add New Account

User: demo

Name:

Account Type: Backup

Authentication: CPM Instance IAM Role

Scan Resources: Disabled

Capture VPCs: Enabled

Figure 3-3

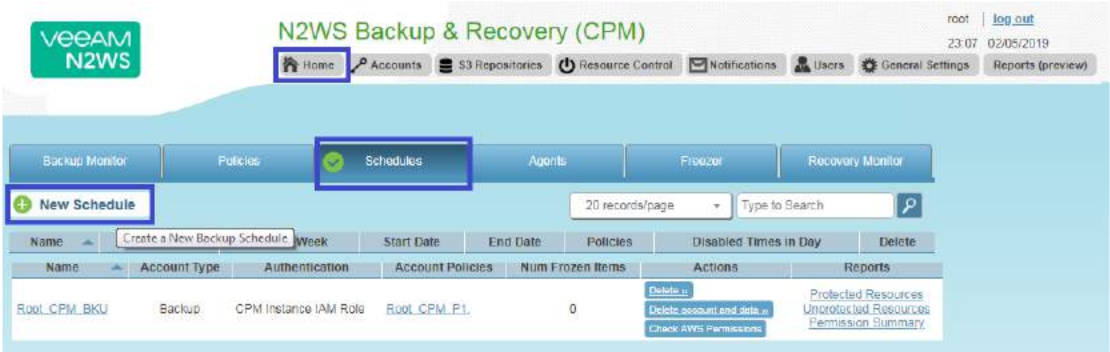
In the **Add New Account** screen (Figure 3-3):

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**. DR accounts relate to cross-account backup and recovery and are 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 **N2WS 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. In the Scan Resources, select **Enabled** to turn on the capability for this account to scan resources.
5. In the **Capture VPCs** list, select **Disabled** to turn off automatic capturing of VPCs for this account.

3.2 Creating a simple backup schedule

Click the **Home** button to go back to the main screen and then click the **Schedules** tab. Currently, the list of schedules is empty.

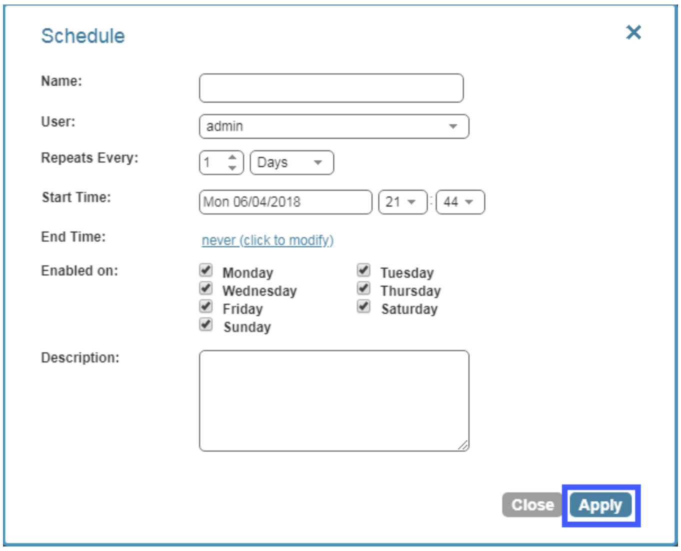


Name	Week	Start Date	End Date	Policies	Disabled Times in Day	Delete

Name	Account Type	Authentication	Account Policies	Num Frozen Items	Actions	Reports
Root_CPM_BKU	Backup	CPM Instance IAM Role	Root_CPM_P1,	0	Delete » Delete account and data » Check AWS Permissions	Protected Resources Unprotected Resources Permission Summary

Figure 3-4

You will now create the first schedule. Click **New Schedule** and then enter a schedule name and description:



Schedule

Name:

User: admin

Repeats Every: 1 Days

Start Time: Mon 06/04/2018 21 : 44

End Time: never (click to modify)

Enabled on:
☑ Monday ☑ Tuesday
☑ Wednesday ☑ Thursday
☑ Friday ☑ Saturday
☑ Sunday

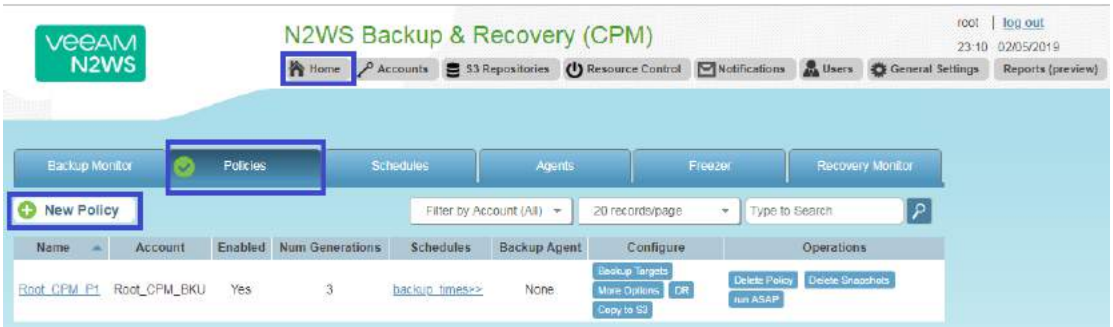
Description:

Figure 3-5

You can also set the start time of this schedule and the frequency. Available units are minutes, hours, days, weeks and months. The default End Time is never. Click the **End Time** link to modify.

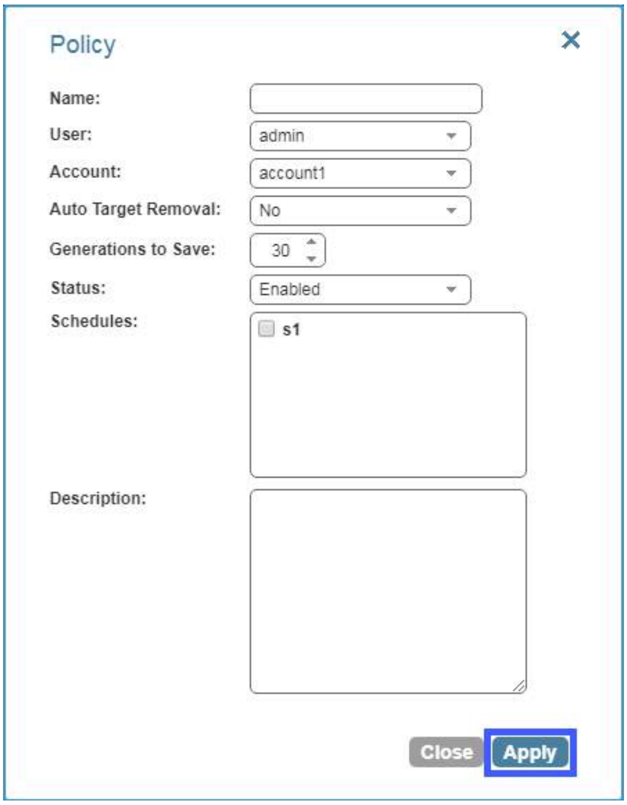
3.3 Creating a simple backup policy

Click the **Home** button to go back to the main screen and then click the **Policies** tab. Currently, the list of policies is empty. You will now create the first policy. Click **New Policy**.



Name	Account	Enabled	Num Generations	Schedules	Backup Agent	Configure	Operations
Root_CPM_P1	Root_CPM_BKU	Yes	3	backup_times>>	None	Backup Targets More Options DR Copy to S3	Delete Policy Delete Snapshots run ASAP

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



Policy

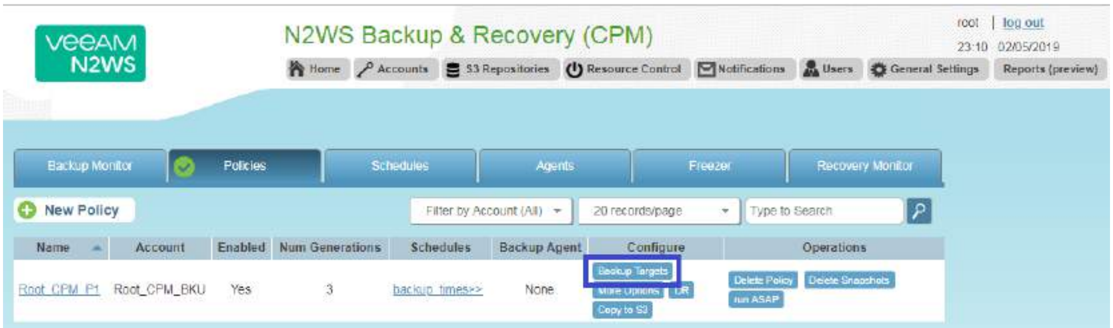
Name:	
User:	admin
Account:	account1
Auto Target Removal:	No
Generations to Save:	30
Status:	Enabled
Schedules:	□ s1
Description:	

Figure 3-6

Other fields in this screen (Figure 3-6) include:

- **Account** – Each policy can be associated with one AWS account.
- **Auto Target Removal** – Whether to auto-remove resources that no longer exist.
- **Generations to Save** – Number of backups of this policy you want to keep. Older backups will be automatically deleted.
- **Status** – By default a policy is **enabled**.
- **Schedules** – Select the schedule you just created.

When finished, click **Apply** and select the **Policies** tab.



Name	Account	Enabled	Num Generations	Schedules	Backup Agent	Configure	Operations
Root_CPM_P1	Root_CPM_BKU	Yes	3	backup_times>>	None	Backup Targets More Options DR Copy to S3	Delete Policy Delete Snapshots run ASAP

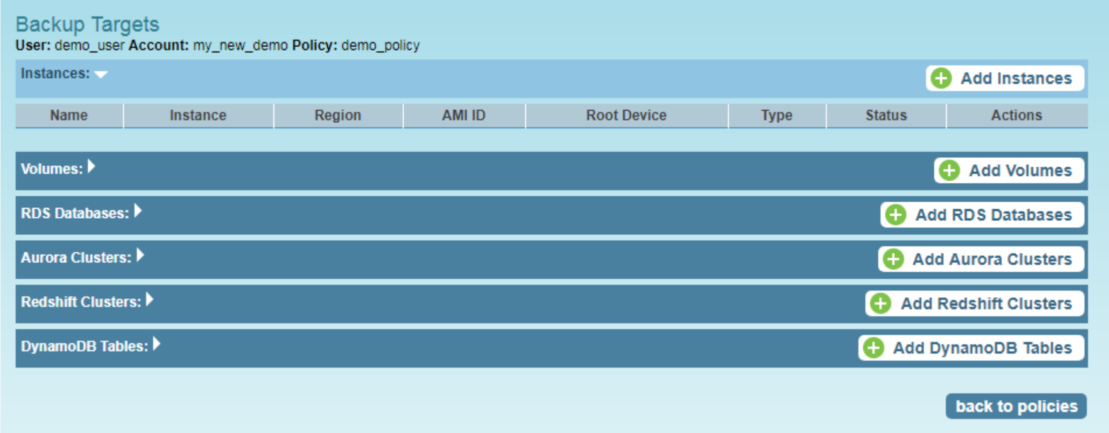
Figure 3-7

When looking at this screen, you can see there are several things you can do with a policy. To edit the basic policy definition, click the link of the policy's name.

To configure the policy, you have three buttons:

- **Backup Targets** - Defines the actual resource objects this policy will back up.
- **More Options -** Defines Linux scripts and settings for the definition of a successful backup and retry parameters.
- **DR -** Defines disaster recovery options.

Click the **Backup Targets** button:



Backup Targets

User: demo_user **Account:** my_new_demo **Policy:** demo_policy

Instances:

Name	Instance	Region	AMI ID	Root Device	Type	Status	Actions

Figure 3-8

As you can see in Figure 3-8, there are numerous types of objects you can back up:

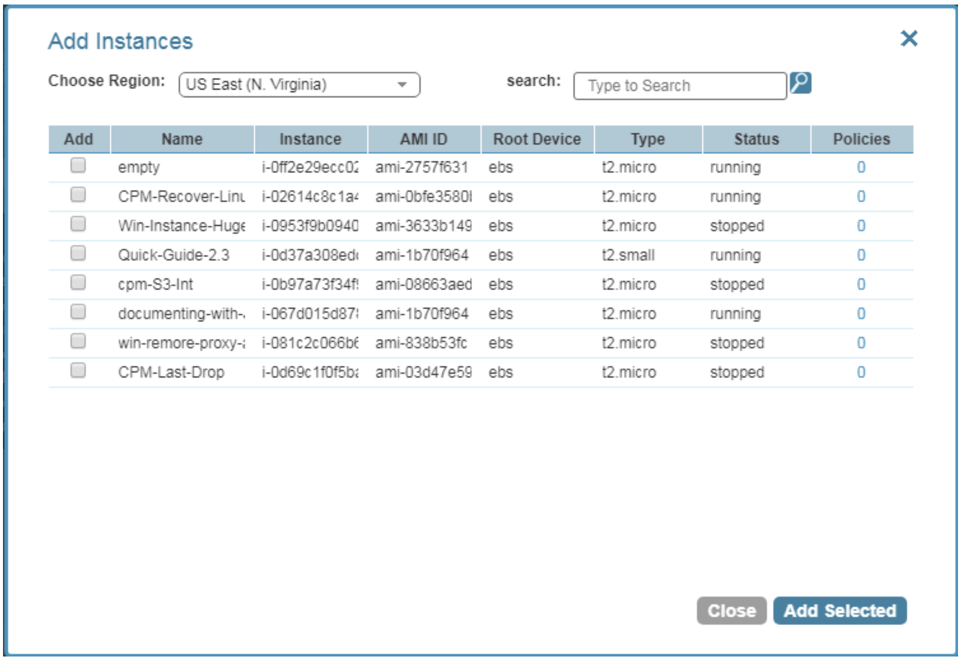
- **Instances** - Back up EC2 instances, including their metadata, and optionally some or all of their data volumes. This is the most common backup target.
- **Volumes** - Back up EBS volumes independently, whether or not they are attached to an instance, and regardless of which instance they are attached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

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

Click **Add Instances.** The list of instances (see Figure 3-9) you have in the policy's account appears. The **Choose 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.



Add Instances

Choose Region: US East (N. Virginia)

search: Type to Search

Add	Name	Instance	AMI ID	Root Device	Type	Status	Policies
☐	empty	i-0ff2e29ecc02	ami-2757f631	ebs	t2.micro	running	0
☐	CPM-Recover-Linu	i-02614c8c1a4	ami-0bfe3580l	ebs	t2.micro	running	0
☐	Win-Instance-Huge	i-0953f9b0940	ami-3633b149	ebs	t2.micro	stopped	0
☐	Quick-Guide-2.3	i-0d37a308ed	ami-1b70f964	ebs	t2.small	running	0
☐	cpm-S3-Int	i-0b97a73f34f	ami-08663aed	ebs	t2.micro	stopped	0
☐	documenting-with-	i-067d015d87	ami-1b70f964	ebs	t2.micro	running	0
☐	win-remore-proxy-	i-081c2c066b	ami-838b53fc	ebs	t2.micro	stopped	0
☐	CPM-Last-Drop	i-0d69c1f0f5b	ami-03d47e59	ebs	t2.micro	stopped	0

Figure 3-9

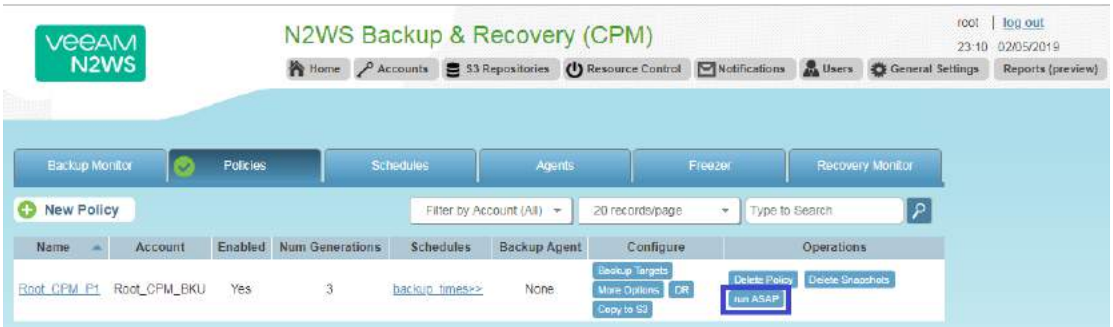
Select an instance you want to back up and click **Add Selected**. This will add the requested instance to the screen in the background and remove it from the popup window, although it does not close the popup. You can add as many instances as you want up to the limit of your licence. Click **Close**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

Back in the **Backup Targets** screen, you can see the instance on the list of instances. You have buttons to remove it from the policy and a **Configure** button.

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. Click **Home** and go to the **Policies** tab again. In the **Schedules** column of the policy, click the **backup times** link. You will see the planned backups for this policy.

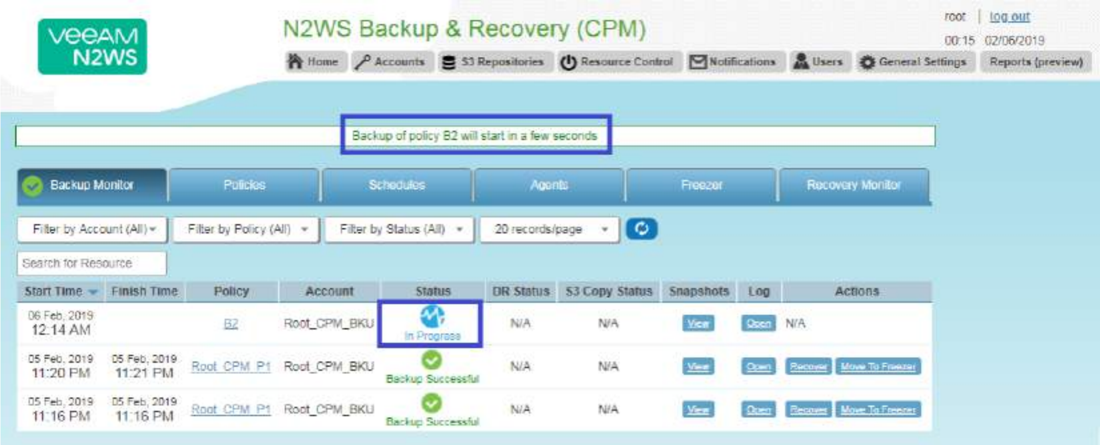
The backups will start automatically at the time configured previously in the schedule.

If you want to initiate an immediate backup, click **run ASAP** in the Operations column.



Name	Account	Enabled	Num Generations	Schedules	Backup Agent	Configure	Operations
Root_CPM_P1	Root_CPM_BKU	Yes	3	backup_times>>	None	Backup Targets More Options DR Copy to S3	Delete Policy Delete Snapshots run ASAP

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



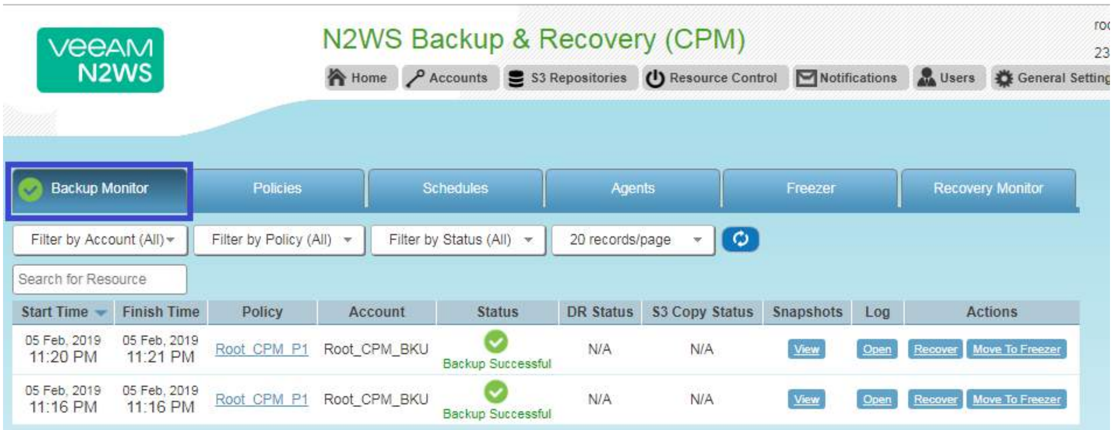
Backup of policy B2 will start in a few seconds

Start Time	Finish Time	Policy	Account	Status	DR Status	S3 Copy Status	Snapshots	Log	Actions
06 Feb, 2019 12:14 AM		B2	Root_CPM_BKU	In Progress	N/A	N/A	View	Open	N/A
05 Feb, 2019 11:20 PM	05 Feb, 2019 11:21 PM	Root_CPM_P1	Root_CPM_BKU	Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer
05 Feb, 2019 11:16 PM	05 Feb, 2019 11:16 PM	Root_CPM_P1	Root_CPM_BKU	Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer

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

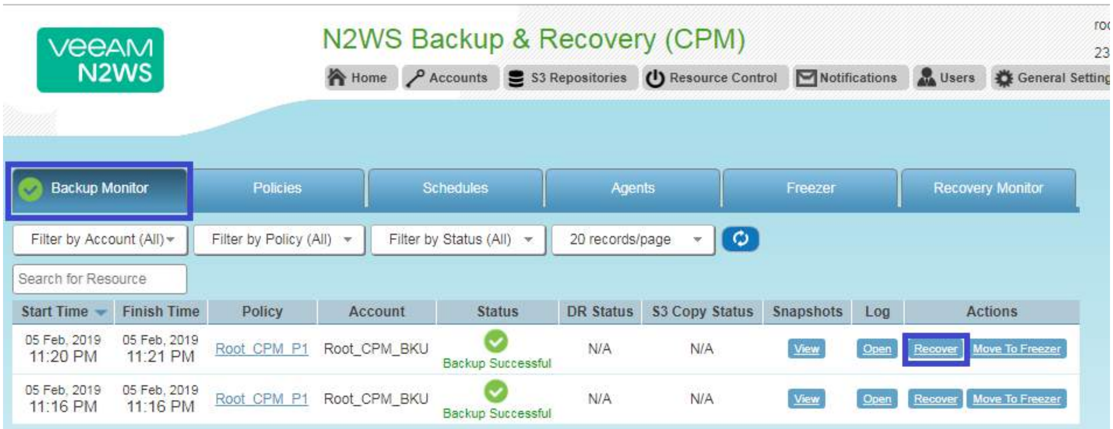
N2WS backs up the requested objects at the requested times. When you return to the main console after a while, you can view the backups in the **Backup Monitor** tab:



Start Time	Finish Time	Policy	Account	Status	DR Status	S3 Copy Status	Snapshots	Log	Actions
05 Feb, 2019 11:20 PM	05 Feb, 2019 11:21 PM	Root_CPM_P1	Root_CPM_BKU	✓ Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer
05 Feb, 2019 11:16 PM	05 Feb, 2019 11:16 PM	Root_CPM_P1	Root_CPM_BKU	✓ Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer

Figure 4-1

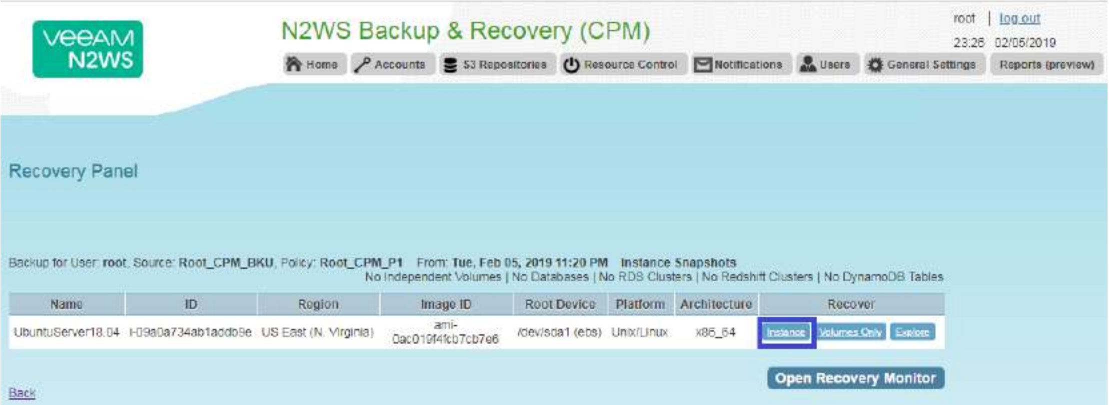
For each backup, you can see exact start and finish times, and status. Click **View** in the **Snapshots** column and see the individual EBS snapshots of all the volumes. Click **Open** in the **Log** column to view the log of this backup with all the details. In order to recover from a particular backup (typically the most recent successful backup), click the **Recover** button in the **Actions** column:



Start Time	Finish Time	Policy	Account	Status	DR Status	S3 Copy Status	Snapshots	Log	Actions
05 Feb, 2019 11:20 PM	05 Feb, 2019 11:21 PM	Root_CPM_P1	Root_CPM_BKU	✓ Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer
05 Feb, 2019 11:16 PM	05 Feb, 2019 11:16 PM	Root_CPM_P1	Root_CPM_BKU	✓ Backup Successful	N/A	N/A	View	Open	Recover Move To Freezer

Figure 4-2

In the **Recovery Panel** screen (Figure 4-3), 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 link to recover them as well. In order to recover an instance, click the **Instance** button. The **Volumes Only** button is for recovering only the EBS volumes of the instance without actually creating a new instance.

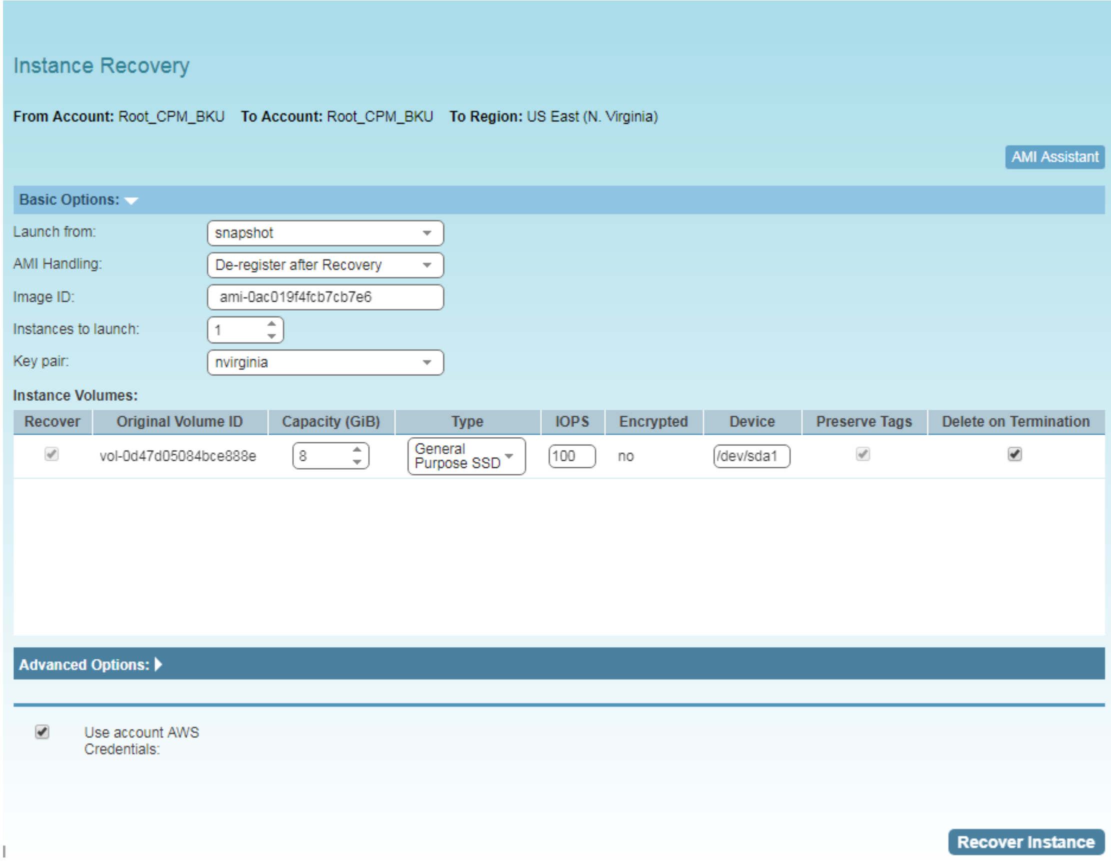


Recovery Panel

Backup for User: **root**, Source: **Root_CPM_BKU**, Policy: **Root_CPM_P1** From: **Tue, Feb 05, 2019 11:20 PM** **Instance Snapshots**
No Independent Volumes | No Databases | No RDS Clusters | No Redshift Clusters | No DynamoDB Tables

Name	ID	Region	Image ID	Root Device	Platform	Architecture	Recover
UbuntuServer18.04	i-09a0a734ab1addb9e	US East (N. Virginia)	ami-0ac019f4fcb7cb7e6	/dev/sda1 (ebs)	Unix/Linux	x86_64	Instance Volumes Only Explore

You will now see the **Instance Recovery** page:



Instance Recovery

From Account: Root_CPM_BKU **To Account:** Root_CPM_BKU **To Region:** US East (N. Virginia)

Basic Options:

Launch from:	snapshot
AMI Handling:	De-register after Recovery
Image ID:	ami-0ac019f4fcb7cb7e6
Instances to launch:	1
Key pair:	nvirginia

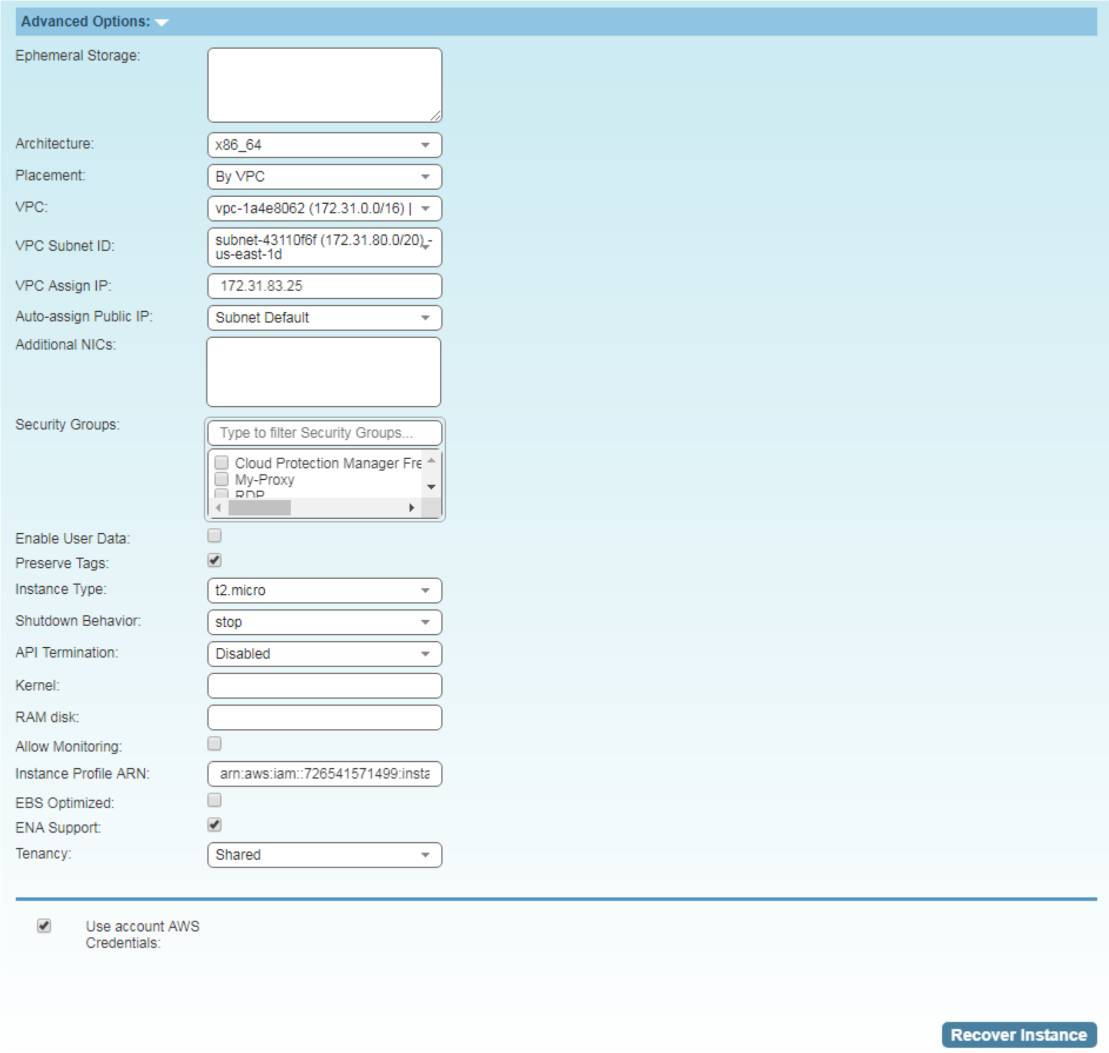
Instance Volumes:

Recover	Original Volume ID	Capacity (GiB)	Type	IOPS	Encrypted	Device	Preserve Tags	Delete on Termination
☑	vol-0d47d05084bce888e	8	General Purpose SSD	100	no	/dev/sda1	☑	☑

Advanced Options:

☑ Use account AWS Credentials:

Click **Advanced Options** for additional recovery parameters.



Advanced Options:

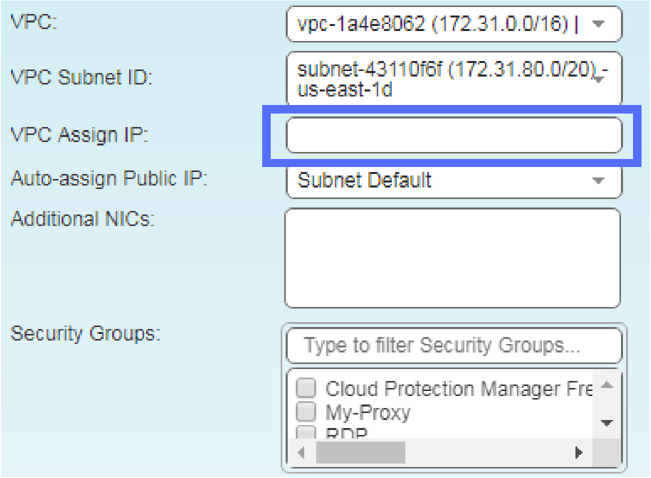
Ephemeral Storage:	
Architecture:	x86_64
Placement:	By VPC
VPC:	vpc-1a4e8062 (172.31.0.0/16) |
VPC Subnet ID:	subnet-43110f6f (172.31.80.0/20) - us-east-1d
VPC Assign IP:	172.31.83.25
Auto-assign Public IP:	Subnet Default
Additional NICs:	
Security Groups:	Type to filter Security Groups... ☐ Cloud Protection Manager Fre ☐ My-Proxy ☐ RDP
Enable User Data:	☐
Preserve Tags:	☑
Instance Type:	t2.micro
Shutdown Behavior:	stop
API Termination:	Disabled
Kernel:	
RAM disk:	
Allow Monitoring:	☐
Instance Profile ARN:	arn:aws:iam::726541571499:insta
EBS Optimized:	☐
ENA Support:	☑
Tenancy:	Shared

☑ Use account AWS Credentials:

Figure 4-3

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. Clicking the **Recover Instance** button will recover an instance exactly like the original one.

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:



VPC: vpc-1a4e8062 (172.31.0.0/16) |

VPC Subnet ID: subnet-43110f6f (172.31.80.0/20) - us-east-1d

VPC Assign IP:

Auto-assign Public IP: Subnet Default

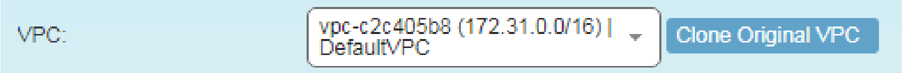
Additional NICs:

Security Groups: Type to filter Security Groups...

□ Cloud Protection Manager Fre
□ My-Proxy
□ RDP

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.

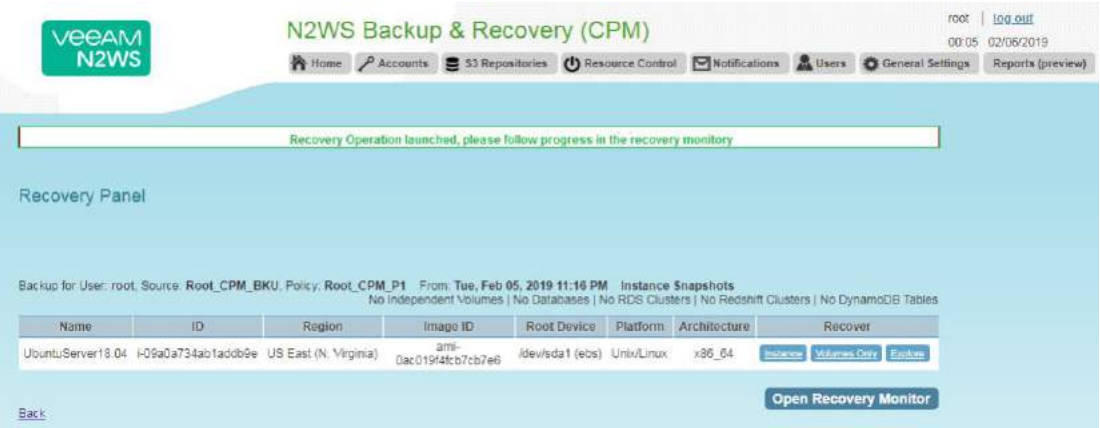
If Capture VPC Environments was enabled in **General Settings**, the **Advanced Options** section will also contain a **Clone Original VPC** option next to the **VPC** box.



VPC: vpc-c2c405b8 (172.31.0.0/16) | DefaultVPC

The **Clone Original VPC** option allows you to recover the instance to a clone of a selected VPC environment. See the *N2WS Backup & Recover (CPM) User Guide* for details on “Recovering to a Cloned Original VPC”.

After you click **Recover Instance** and confirm, you will be directed back to the recovery panel page, and will get a message about the operation success:



Recovery Operation launched, please follow progress in the recovery monitory

Recovery Panel

Backup for User: root, Source: **Root_CPM_BKU**, Policy: **Root_CPM_P1** From: **Tue, Feb 05, 2019 11:16 PM** **Instance Snapshots**
No Independent Volumes | No Databases | No RDS Clusters | No Redshift Clusters | No DynamoDB Tables

Name	ID	Region	Image ID	Root Device	Platform	Architecture	Recover
UbuntuServer18.04	i-09a0a734ab1addb9e	US East (N. Virginia)	ami-0ac019f4fcb7cb7e6	/dev/sda1 (ebs)	Unix/Linux	x86_64	Instance Volumes Only Explore

Figure 4-4

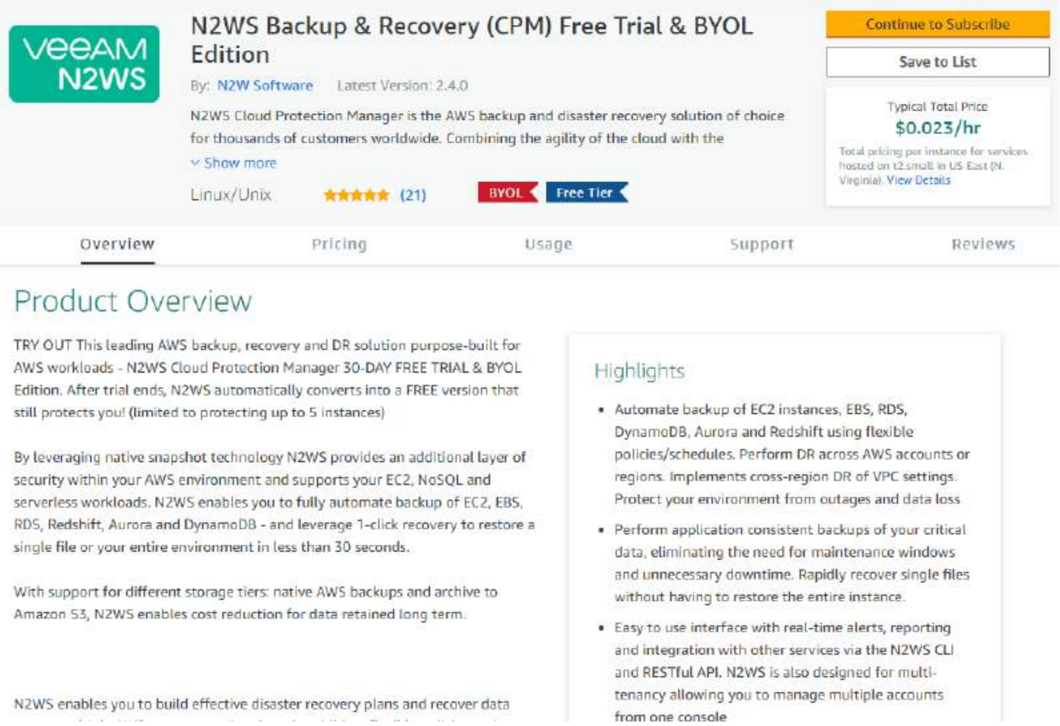
The message will include the instance ID of the new instance, and now you can go and verify the successful recovery in the AWS Management Console. The recovered instance is exactly the same as the original one, with all its EBS volumes.

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/pp/B00UIO8514/ref=_ptnr_qsg
2. Click **Continue to Subscribe**.



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

By: N2W Software Latest Version: 2.4.0

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

Show more

Linux/Unix ★★★★★ (21)

Typical Total Price
$0.023/hr
Total pricing per instance for services hosted on t2.small in US East (N. Virginia). View Details

Product Overview

TRY OUT This leading AWS backup, recovery and DR solution purpose-built for AWS workloads - N2WS Cloud Protection Manager 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 and DynamoDB - and leverage 1-click recovery to restore a single file or your entire environment in less than 30 seconds.

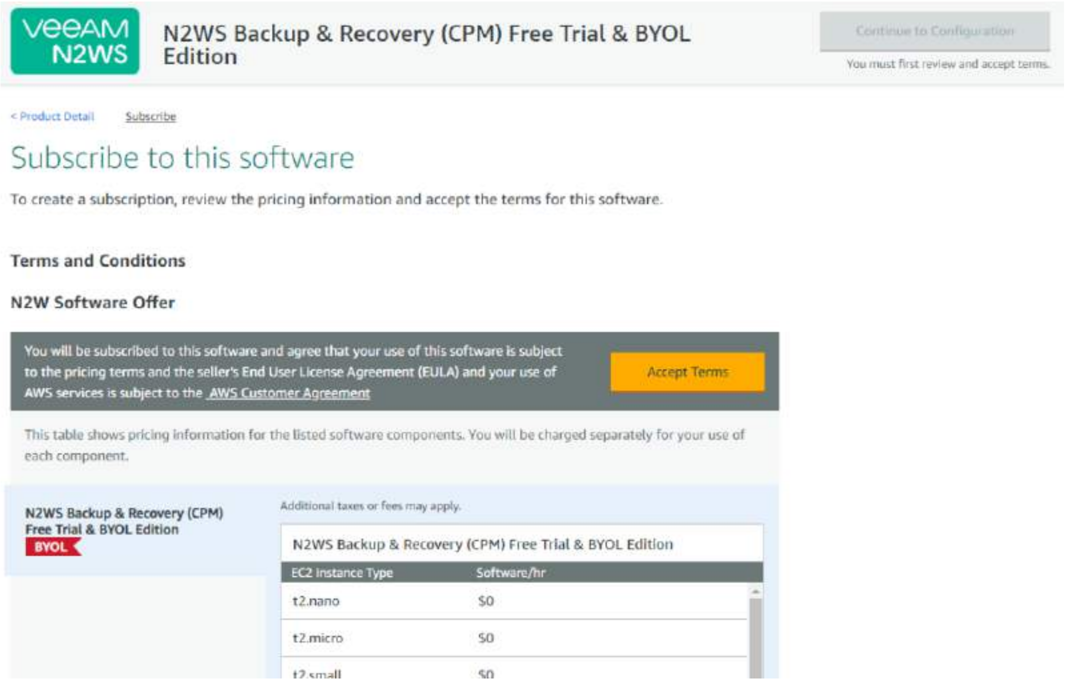
With support for different storage tiers: native AWS backups and archive to Amazon S3, N2WS enables cost reduction for data retained long term.

N2WS enables you to build effective disaster recovery plans and recover data

Highlights

- Automate backup of EC2 instances, EBS, RDS, DynamoDB, Aurora and Redshift using flexible policies/schedules. Perform DR across AWS accounts or regions. Implements cross-region DR of VPC settings. Protect your environment from outages 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

3. Click **Continue to Configuration** and then click **Accept Terms**.



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

You must first review and accept terms.

Subscribe to this software

To create a subscription, review the pricing information and accept the terms for this software.

Terms and Conditions

N2W Software Offer

You will be subscribed to this software and agree that your use of this software is subject to the pricing terms and the seller's End User License Agreement (EULA) and your use of AWS services is subject to the AWS Customer Agreement

This table shows pricing information for the listed software components. You will be charged separately for your use of each component.

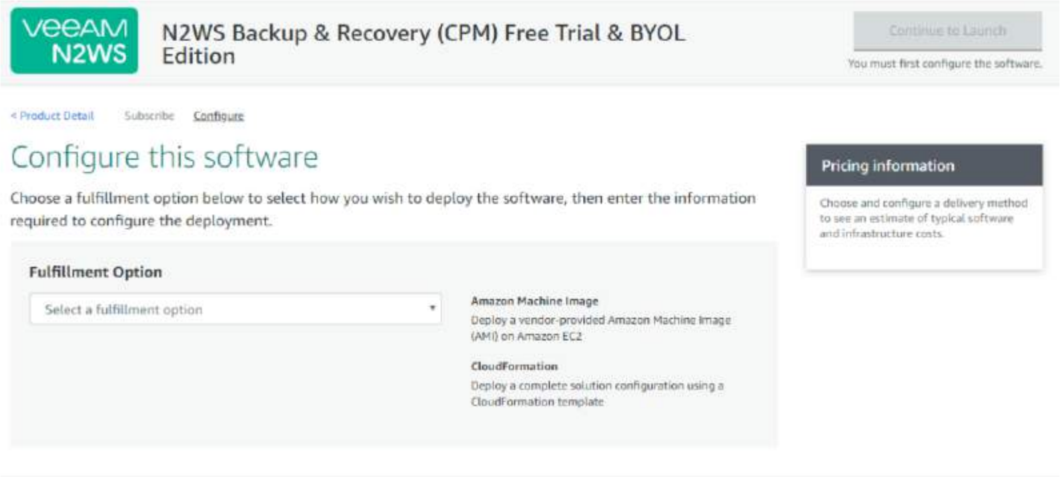
N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition

Additional taxes or fees may apply.

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

EC2 Instance Type	Software/hr
t2.nano	$0
t2.micro	$0
t2.small	$0

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



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

You must first configure the software.

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

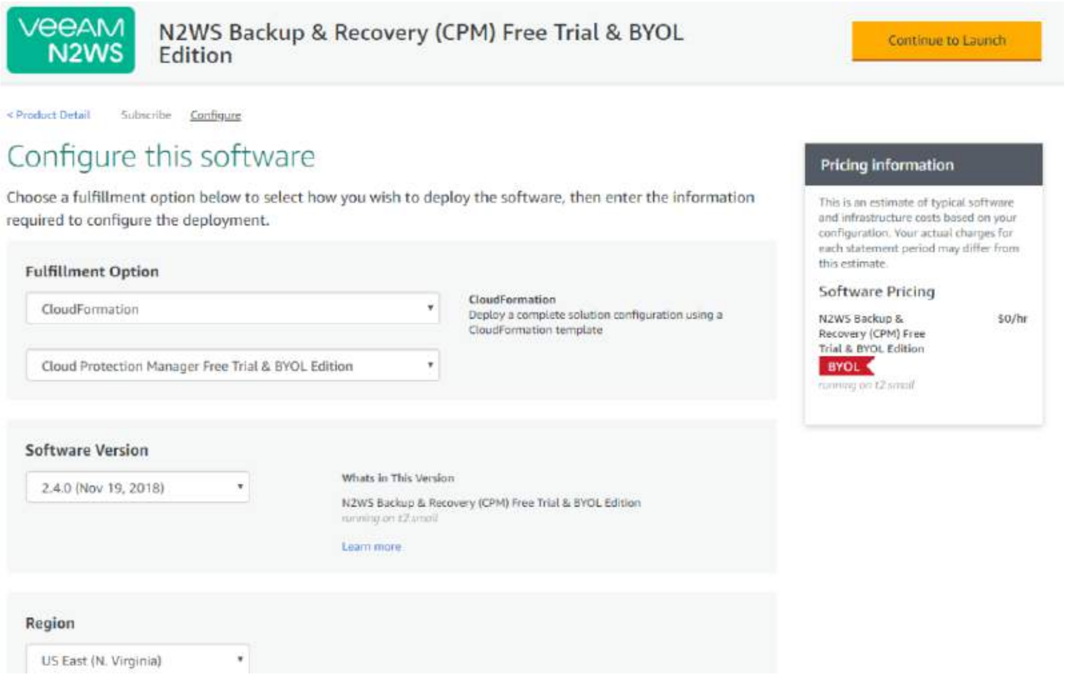
Amazon Machine Image
Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2

CloudFormation
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.

5. Select the relevant **Software Version** and **Region** and then click **Continue to Launch**.



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

Cloud Protection Manager Free Trial & BYOL Edition

CloudFormation
Deploy a complete solution configuration using a CloudFormation template

Software Version

2.4.0 (Nov 19, 2018)

Whats in This Version

N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition
running on t2.small

Learn more

Region

US East (N. Virginia)

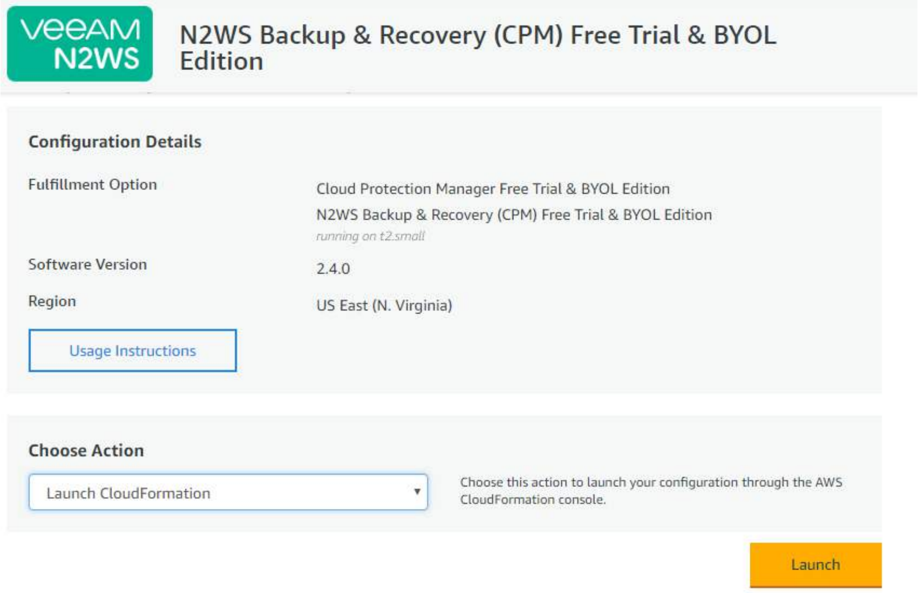
Pricing information

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 BYOL *running on t2.small*	$0/hr

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



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

Configuration Details

Fulfillment Option	Cloud Protection Manager Free Trial & BYOL Edition N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition *running on t2.small*
Software Version	2.4.0
Region	US East (N. Virginia)

Usage Instructions

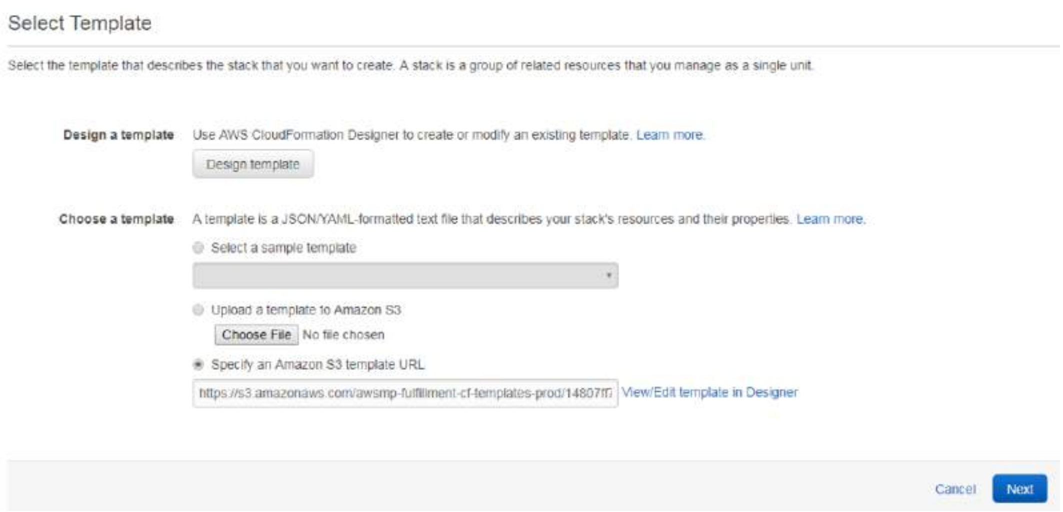
Choose Action

Launch CloudFormation

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

Launch

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



Select Template

Select the template that describes the stack that you want to create. A stack is a group of related resources that you manage as a single unit.

Design a template Use AWS CloudFormation Designer to create or modify an existing template. Learn more.

Choose a template A template is a JSON/YAML-formatted text file that describes your stack's resources and their properties. Learn more.

○ Select a sample template

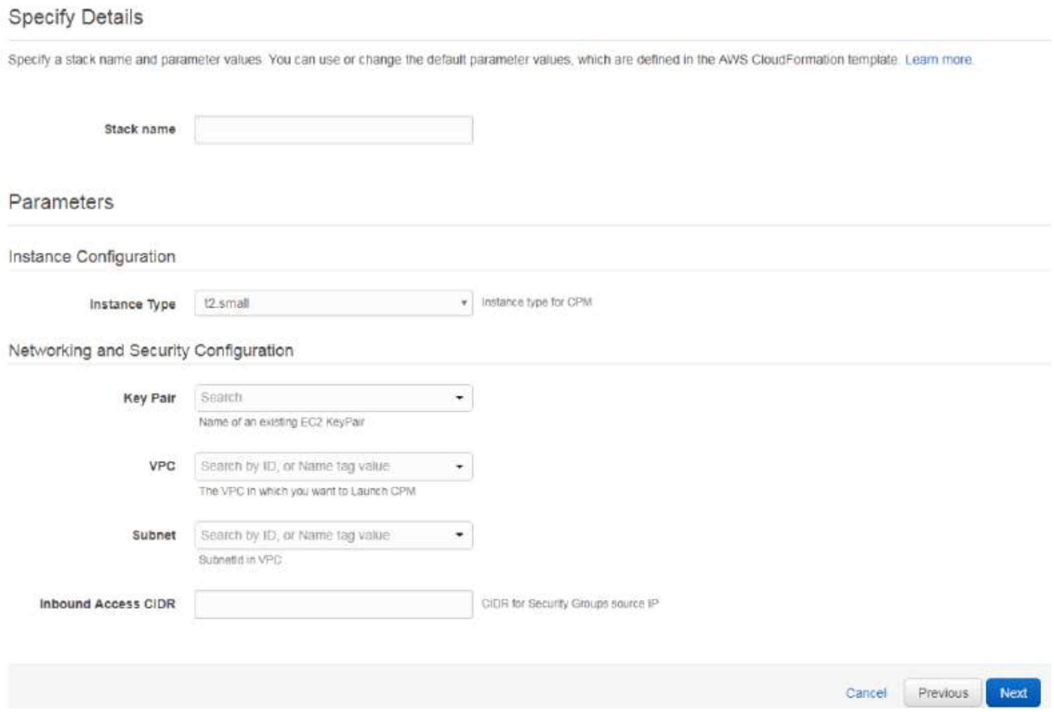
○ Upload a template to Amazon S3

No file chosen

● Specify an Amazon S3 template URL

https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/14807f View/Edit template in Designer

7. Under **Choose a template**, choose **Specify an Amazon S3 template URL**. Select an Amazon S3 template URL and click **Next**. The **Specify Details** page opens.



Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name

Parameters

Instance Configuration

Instance Type t2.small — Instance type for CPM

Networking and Security Configuration

Key Pair Search — Name of an existing EC2 KeyPair

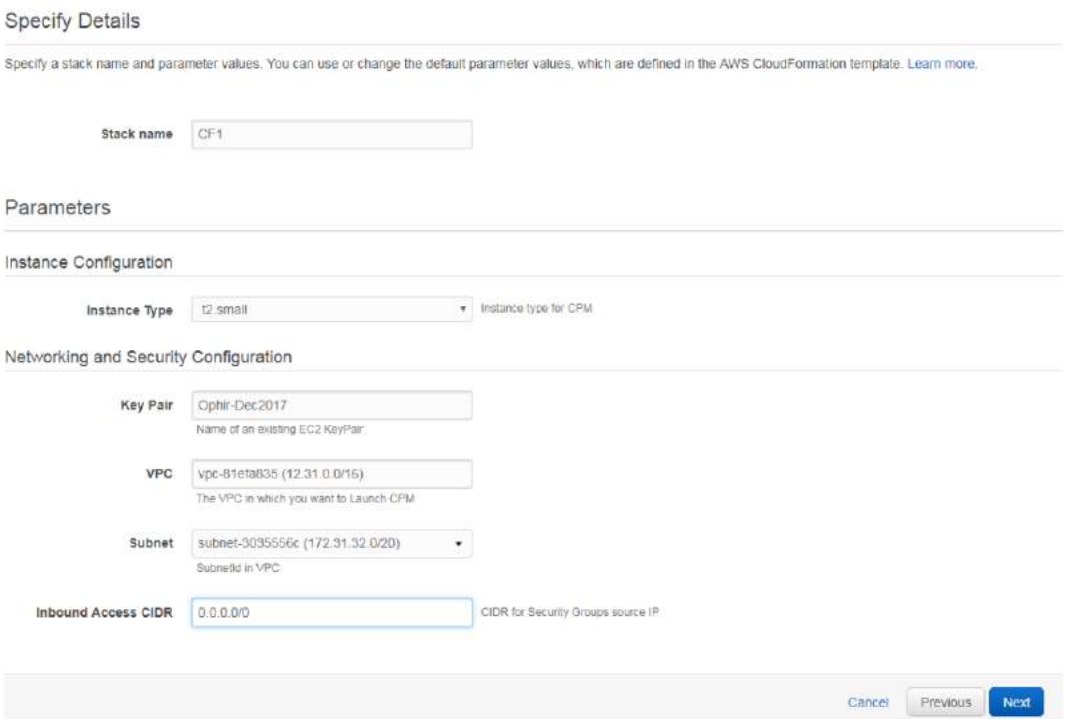
VPC Search by ID, or Name tag value — The VPC in which you want to Launch CPM

Subnet Search by ID, or Name tag value — SubnetId in VPC

Inbound Access CIDR — CIDR for Security Groups source IP

8. 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



Specify Details

Specify a stack name and parameter values. You can use or change the default parameter values, which are defined in the AWS CloudFormation template. Learn more.

Stack name: CF1

Parameters

Instance Configuration

Instance Type: t2.small — Instance type for CPM

Networking and Security Configuration

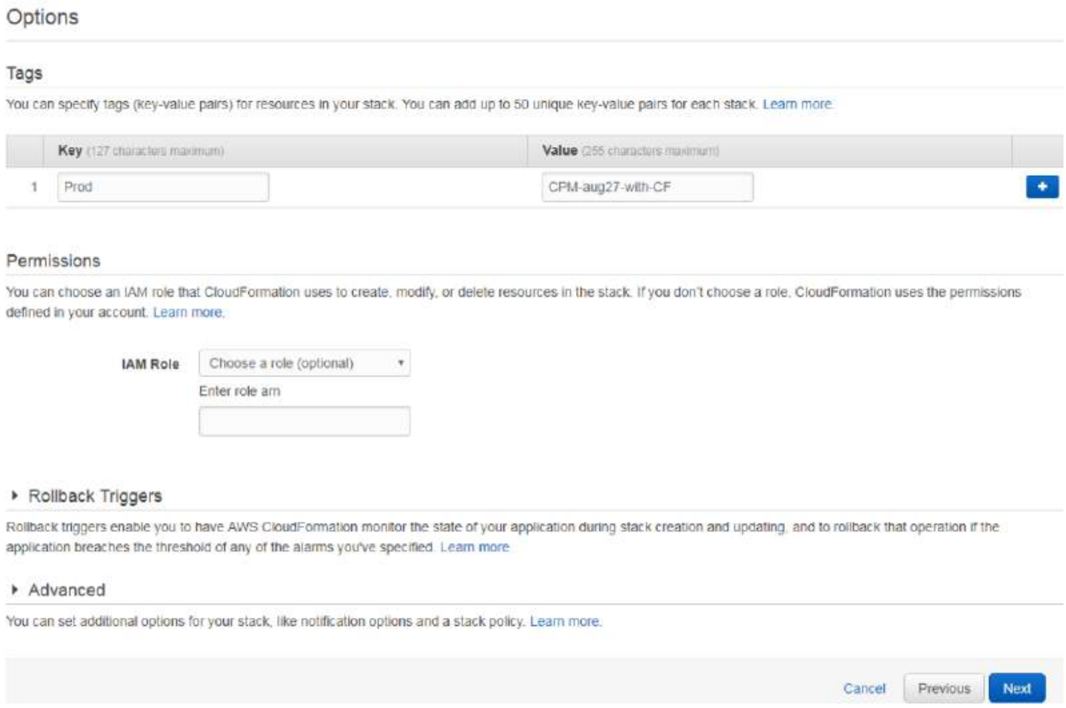
Key Pair: Ophir-Dec2017 — Name of an existing EC2 KeyPair

VPC: vpc-81efa835 (12.31.0.0/16) — The VPC in which you want to Launch CPM

Subnet: subnet-3035556c (172.31.32.0/20) — SubnetId in VPC

Inbound Access CIDR: 0.0.0.0/0 — CIDR for Security Groups source IP

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



Options

Tags

You can specify tags (key-value pairs) for resources in your stack. You can add up to 50 unique key-value pairs for each stack. Learn more.

	Key (127 characters maximum)	Value (255 characters maximum)
1	Prod	CPM-aug27-with-CF

Permissions

You can choose an IAM role that CloudFormation uses to create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses the permissions defined in your account. Learn more.

IAM Role: Choose a role (optional)

Enter role arn

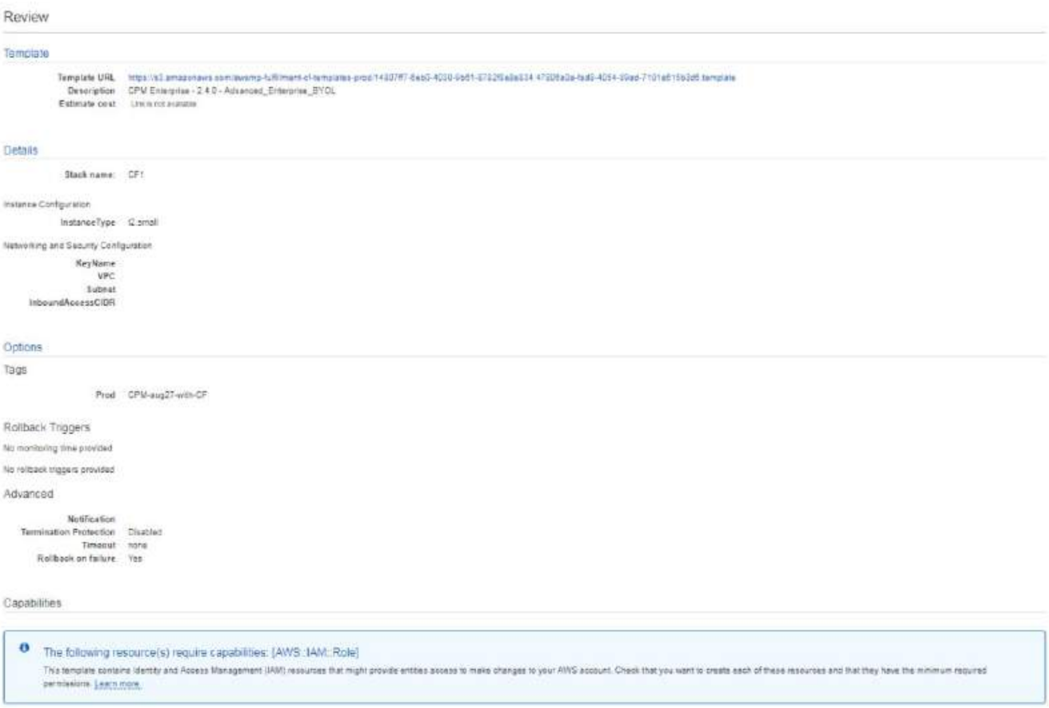
Rollback Triggers

Rollback triggers enable you to have AWS CloudFormation monitor the state of your application during stack creation and updating, and to rollback that operation if the application breaches the threshold of any of the alarms you've specified. Learn more

Advanced

You can set additional options for your stack, like notification options and a stack policy. Learn more.

10. Complete the **Options** and click **Next**. The **Review** page opens.



Review

Template

Template URL https://s3.amazonaws.com/awsmp-fulfillment-cf-templates-prod/14807ff7-6eb0-4030-9b61-87829a8a834.47808a0a-fad6-4054-99ad-7101a615b3d6.template
Description CPM Enterprise - 2.4.0 - Advanced_Enterprise_BYOL
Estimate cost Link is not available

Details

Stack name: CF1

Instance Configuration

InstanceType t2.small

Networking and Security Configuration

KeyName
VPC
Subnet
InboundAccessCIDR

Options

Tags

Prod CPM-aug27-with-CF

Rollback Triggers

No monitoring time provided

No rollback triggers provided

Advanced

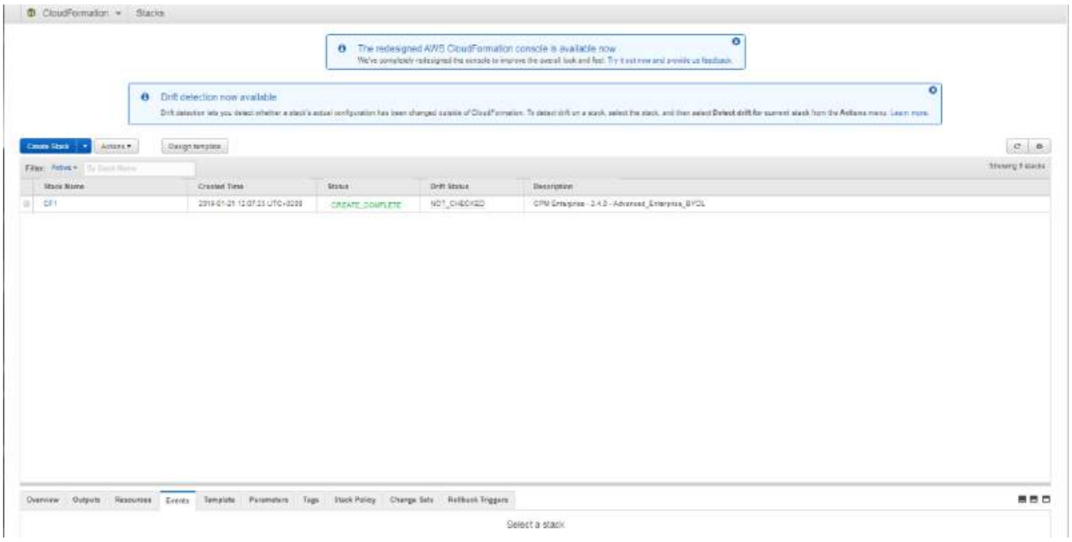
Notification
Termination Protection Disabled
Timeout none
Rollback on failure Yes

Capabilities

The following resource(s) require capabilities: [AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources that might provide entities access to make changes to your AWS account. Check that you want to create each of these resources and that they have the minimum required permissions. Learn more.

11. Select the **I acknowledge that AWS CloudFormation might create IAM resources** check box. Click **Create**. The **CloudFormation Create Stack Events** page opens.



The redesigned AWS CloudFormation console is available now

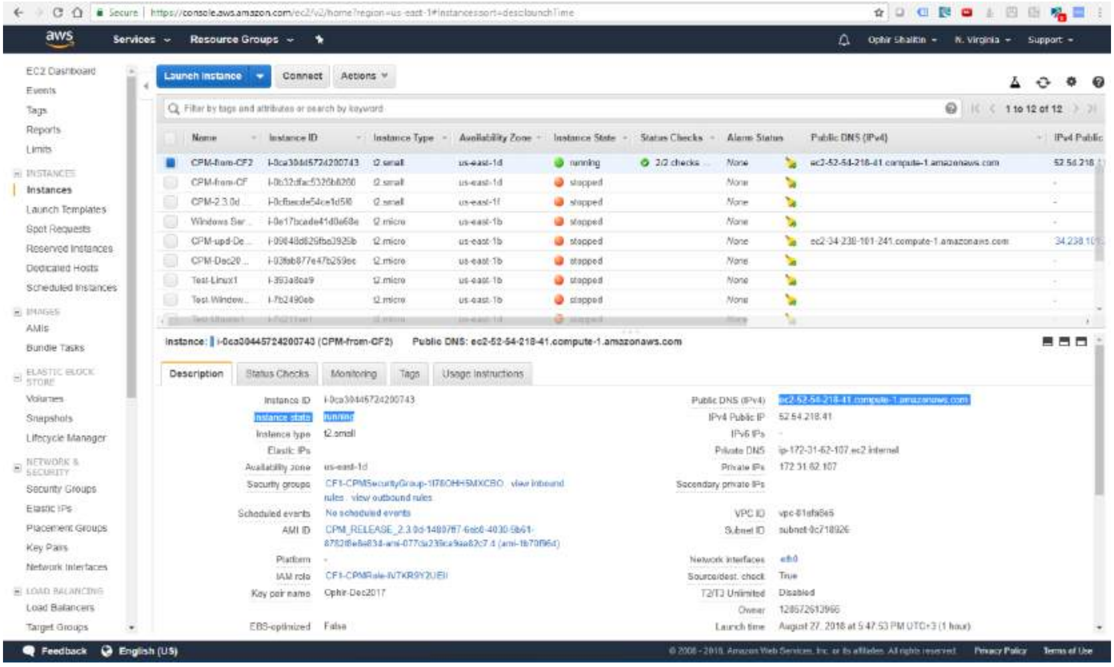
We've completely redesigned the console to improve the overall look and feel. Try it out now and provide us feedback.

Drift detection now available

Drift detection lets you detect whether a stack's actual configuration has been changed outside of CloudFormation. To detect drift on a stack, select the stack, and then select **Detect drift for current stack** from the **Actions** menu. Learn more.

Stack Name	Created Time	Status	Drift Status	Description
CF1	2019-01-21 12:07:23 UTC+0200	CREATE_COMPLETE	NOT_CHECKED	CPM Enterprise - 2.4.0 - Advanced_Enterprise_BYOL

12. Select the new stack. The **Instances** page opens.



Name	Instance ID	Instance Type	Availability Zone	Instance State	Status Checks	Alarm Status	Public DNS (IPv4)	IPv4 Public
CPM-from-CF2	i-0ca304d5724200743	t2.small	us-east-1d	running	2/2 checks ...	None	ec2-52-54-218-41.compute-1.amazonaws.com	52.54.218.41
CPM-from-CF	i-0b32dfac5326b8260	t2.small	us-east-1d	stopped		None		-
CPM-2.3.0d ...	i-0cfbecde54ce1d5f0	t2.small	us-east-1f	stopped		None		-
Windows Ser...	i-0e17bcade41d0a68e	t2.micro	us-east-1b	stopped		None		-
CPM-upd-De...	i-09848d829fba3925b	t2.micro	us-east-1b	stopped		None	ec2-34-238-101-241.compute-1.amazonaws.com	34.238.101
CPM-Dec20...	i-03fab877e47b259ec	t2.micro	us-east-1b	stopped		None		-
Test-Linux1	i-393a8ba9	t2.micro	us-east-1b	stopped		None		-
Test-Window...	i-7b2490eb	t2.micro	us-east-1b	stopped		None		-

Instance: i-0ca30445724200743 (CPM-from-CF2) Public DNS: ec2-52-54-218-41.compute-1.amazonaws.com

Description | Status Checks | Monitoring | Tags | Usage Instructions

Instance ID	i-0ca30445724200743	Public DNS (IPv4)	ec2-52-54-218-41.compute-1.amazonaws.com
Instance state	running	IPv4 Public IP	52.54.218.41
Instance type	t2.small	IPv6 IPs	-
Elastic IPs		Private DNS	ip-172-31-62-107.ec2.internal
Availability zone	us-east-1d	Private IPs	172.31.62.107
Security groups	CF1-CPMSecurityGroup-1I78OHH5MXCBO. view inbound rules. view outbound rules	Secondary private IPs	
Scheduled events	No scheduled events	VPC ID	vpc-81afa8e5
AMI ID	CPM_RELEASE_2.3.0d-1480787-6eb0-4030-9b61-8782f8e8e834-ami-077da236ca9aa82c7.4 (ami-1b70f96d)	Subnet ID	subnet-0c718926
Platform	-	Network interfaces	eth0
IAM role	CF1-CPMRole-IV7KR9Y2UEII	Source/dest. check	True
Key pair name	Ophir-Dec2017	T2/T3 Unlimited	Disabled
		Owner	128572613966
EBS-optimized	False	Launch time	August 27, 2018 at 5:47:53 PM UTC+3 (1 hour)

13. Select the instance. Copy the **Instance ID** value shown in the **Description** tab and click **Launch Instance**. The **N2WS Server Configuration** page opens.

14. Continue as from section 2.1.

This concludes the *Quick Start Guide*. Consult the *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.

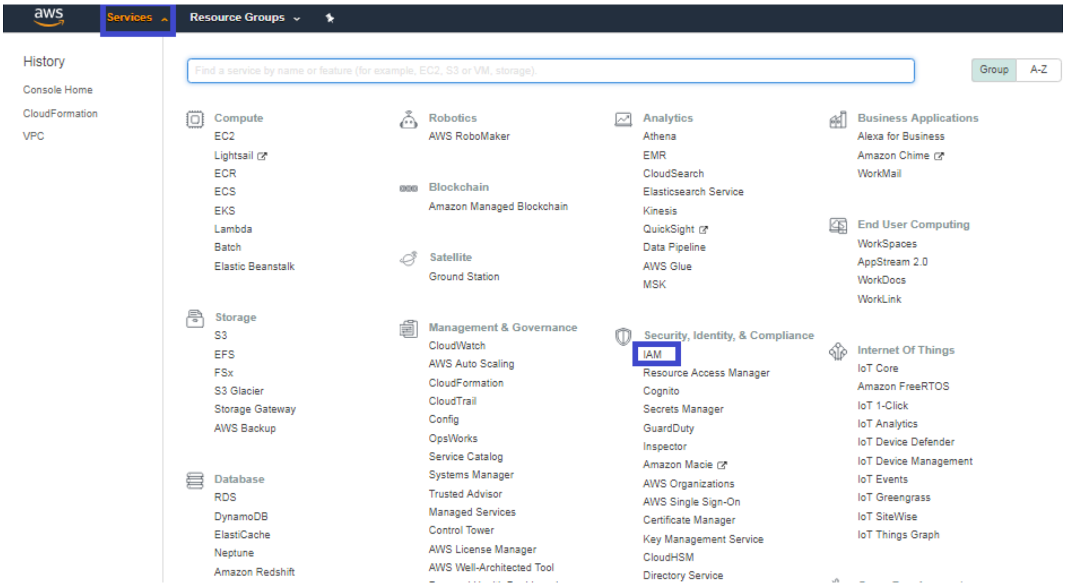
N2WS supports two different types of AWS authentication during setup:

- AccessKey / SecretKey
- Role based authentication (recommended)

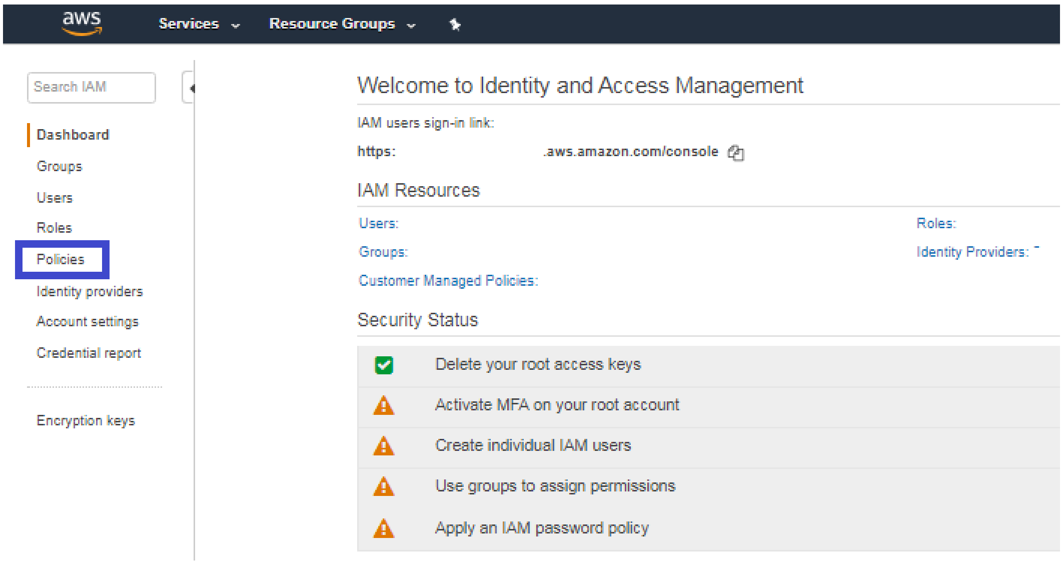
The permissions necessary have been combined into a JSON file for convenience and can be downloaded from the N2WS Knowledge Base:

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**.



Welcome to Identity and Access Management

IAM users sign-in link:

https: .aws.amazon.com/console

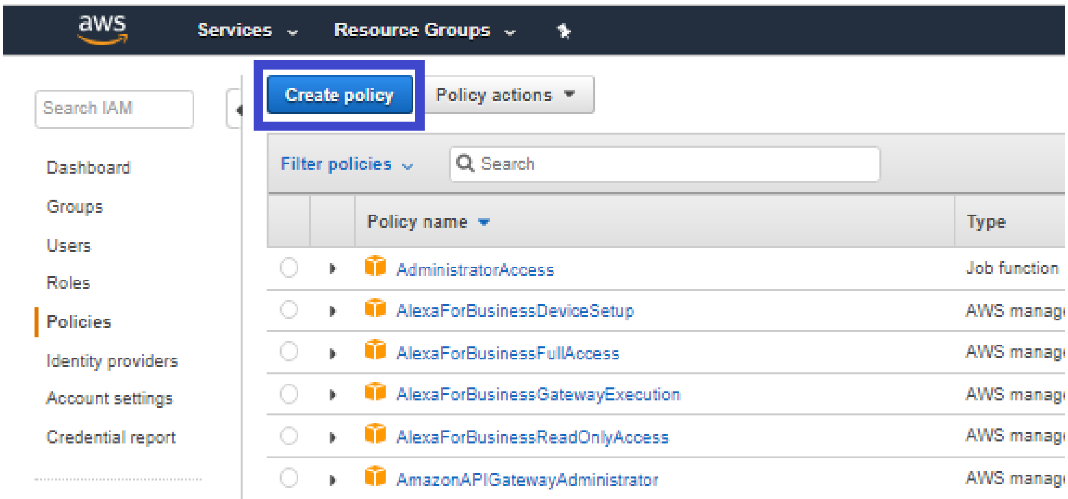
IAM Resources

Users:	Roles:
Groups:	Identity Providers:
Customer Managed Policies:	

Security Status

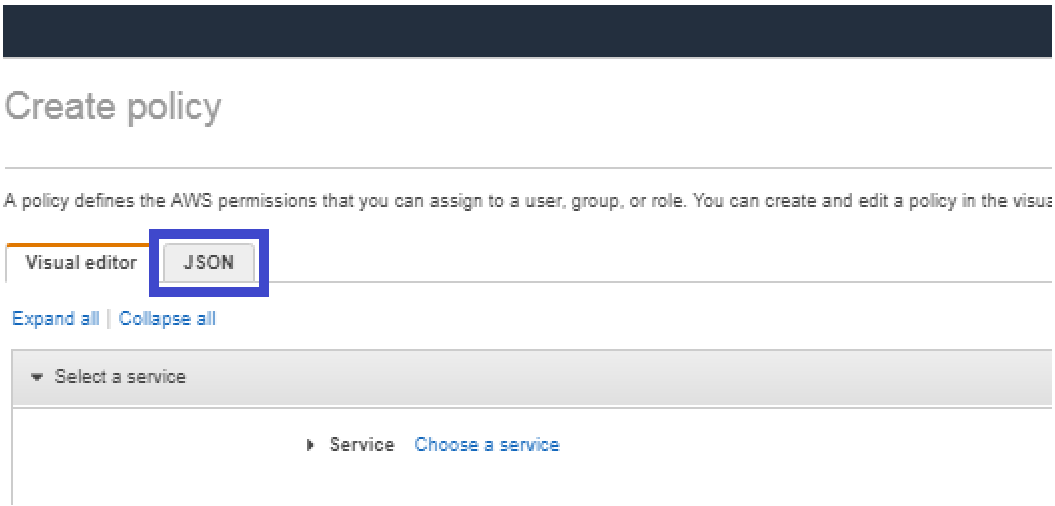
- ✓ Delete your root access keys
- ⚠ Activate MFA on your root account
- ⚠ Create individual IAM users
- ⚠ Use groups to assign permissions
- ⚠ Apply an IAM password policy

3. Click the **Create policy** button.



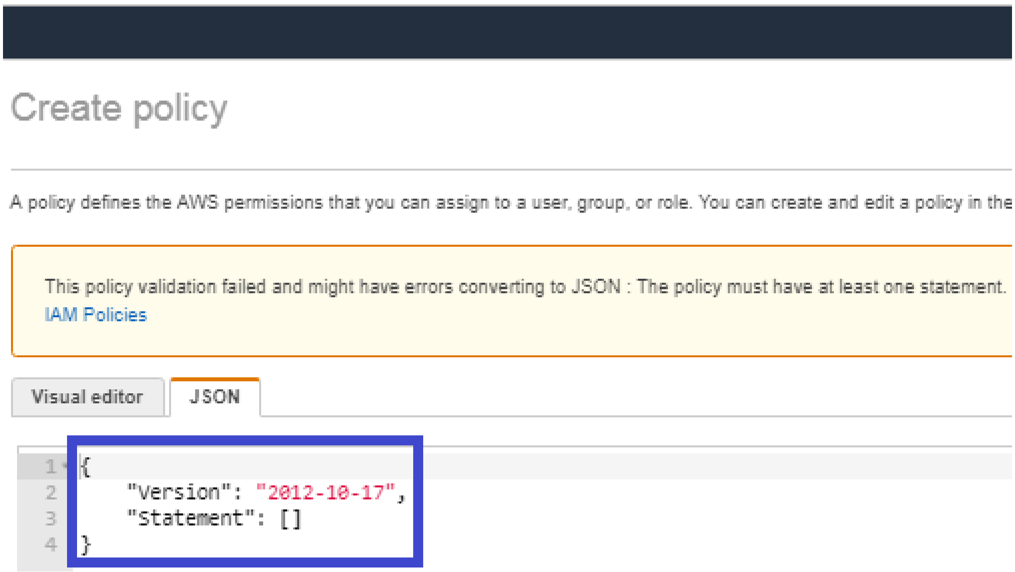
		Policy name	Type
○	▸	AdministratorAccess	Job function
○	▸	AlexaForBusinessDeviceSetup	AWS manag
○	▸	AlexaForBusinessFullAccess	AWS manag
○	▸	AlexaForBusinessGatewayExecution	AWS manag
○	▸	AlexaForBusinessReadOnlyAccess	AWS manag
○	▸	AmazonAPIGatewayAdministrator	AWS manag

4. Select the **JSON** tab.


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 visua

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



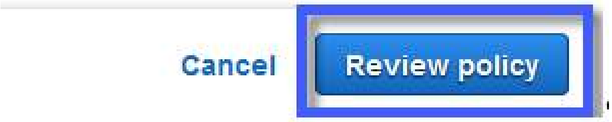
Create policy

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

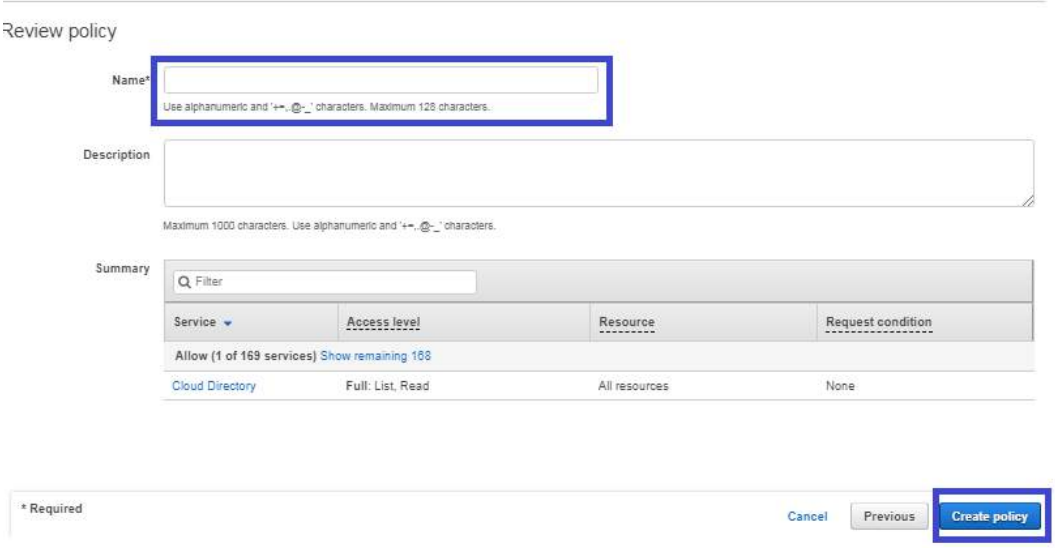
This policy validation failed and might have errors converting to JSON : The policy must have at least one statement.
IAM Policies

```
{
    "Version": "2012-10-17",
    "Statement": []
}
```

6. At the bottom of the screen, click **Review Policy**.



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



Review policy

Name*

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

Description

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

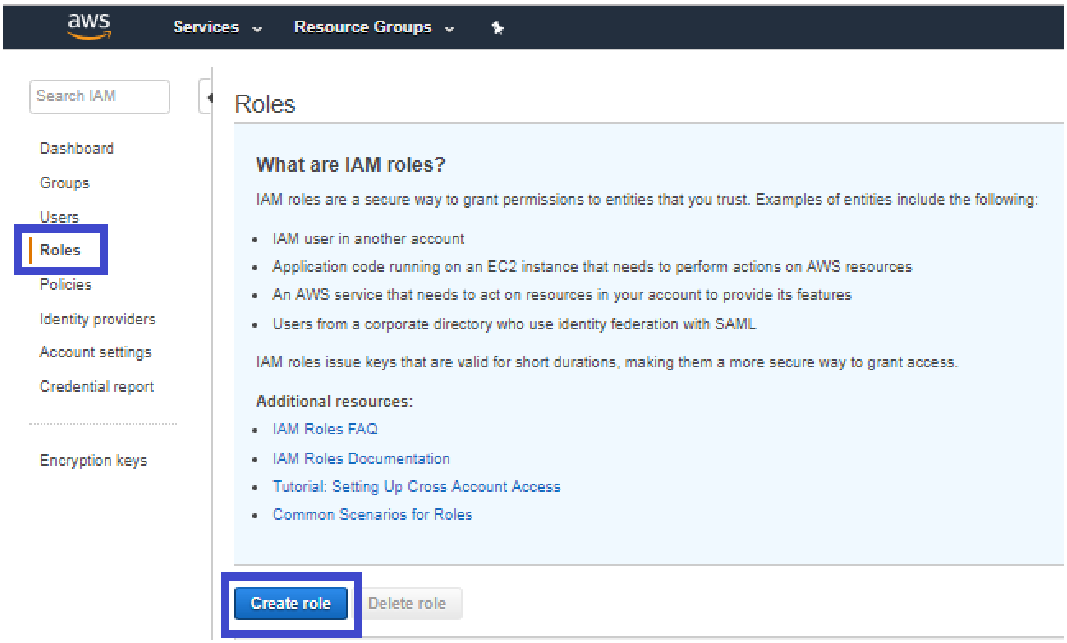
Summary

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

* Required

Next, create a role, and then assign the policy you just created to that role.

8. In the left menu, select **Roles** and click **Create role**.



Roles

What are IAM roles?

IAM roles are a secure way to grant permissions to entities that you trust. Examples of entities include the following:

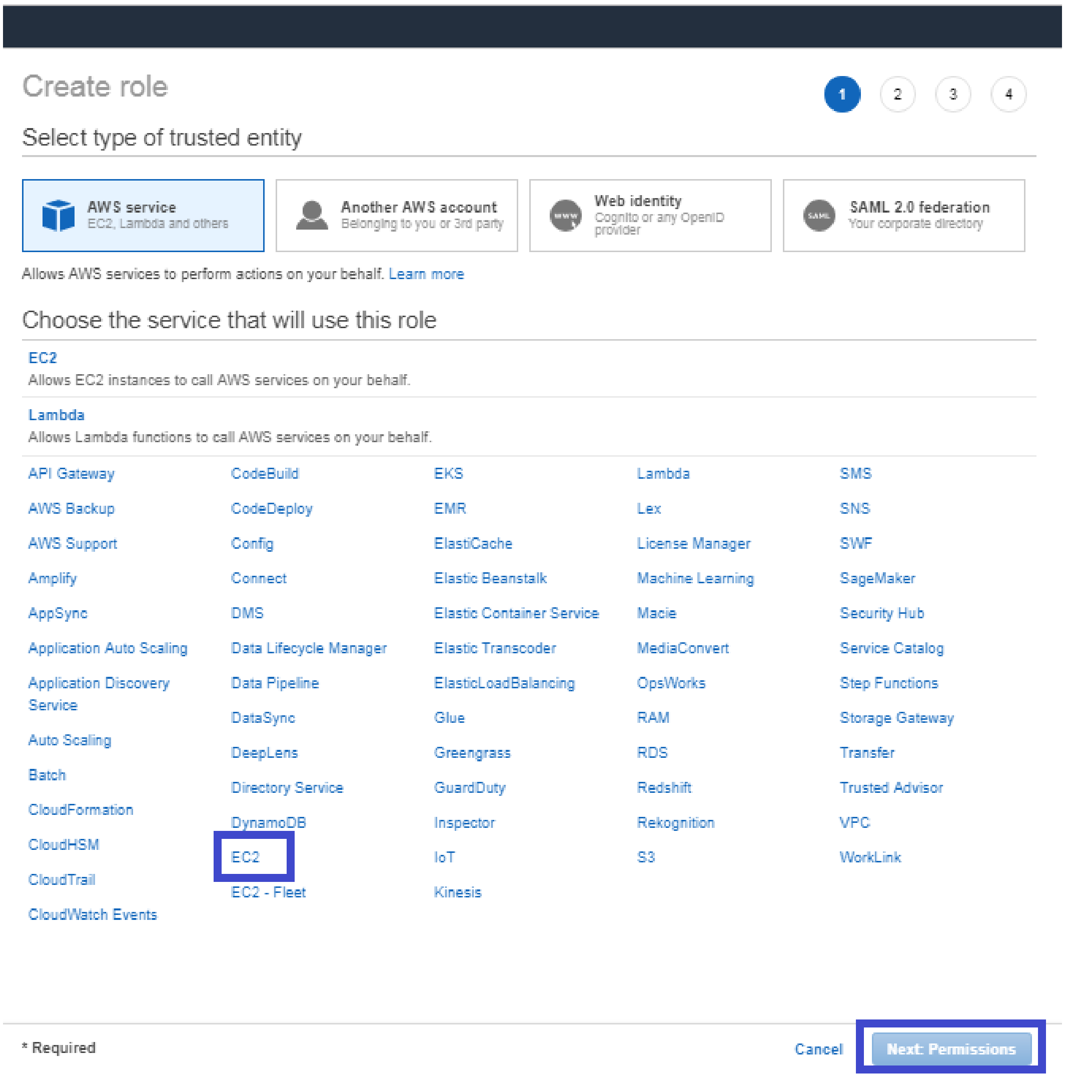
- IAM user in another account
- Application code running on an EC2 instance that needs to perform actions on AWS resources
- An AWS service that needs to act on resources in your account to provide its features
- Users from a corporate directory who use identity federation with SAML

IAM roles issue keys that are valid for short durations, making them a more secure way to grant access.

Additional resources:

- IAM Roles FAQ
- IAM Roles Documentation
- Tutorial: Setting Up Cross Account Access
- Common Scenarios for Roles

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



Create role

Select type of trusted entity

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
AWS Backup
AWS Support
Amplify
AppSync
Application Auto Scaling
Application Discovery Service
Auto Scaling
Batch
CloudFormation
CloudHSM
CloudTrail
CloudWatch Events

CodeBuild
CodeDeploy
Config
Connect
DMS
Data Lifecycle Manager
Data Pipeline
DataSync
DeepLens
Directory Service
DynamoDB
EC2
EC2 - Fleet

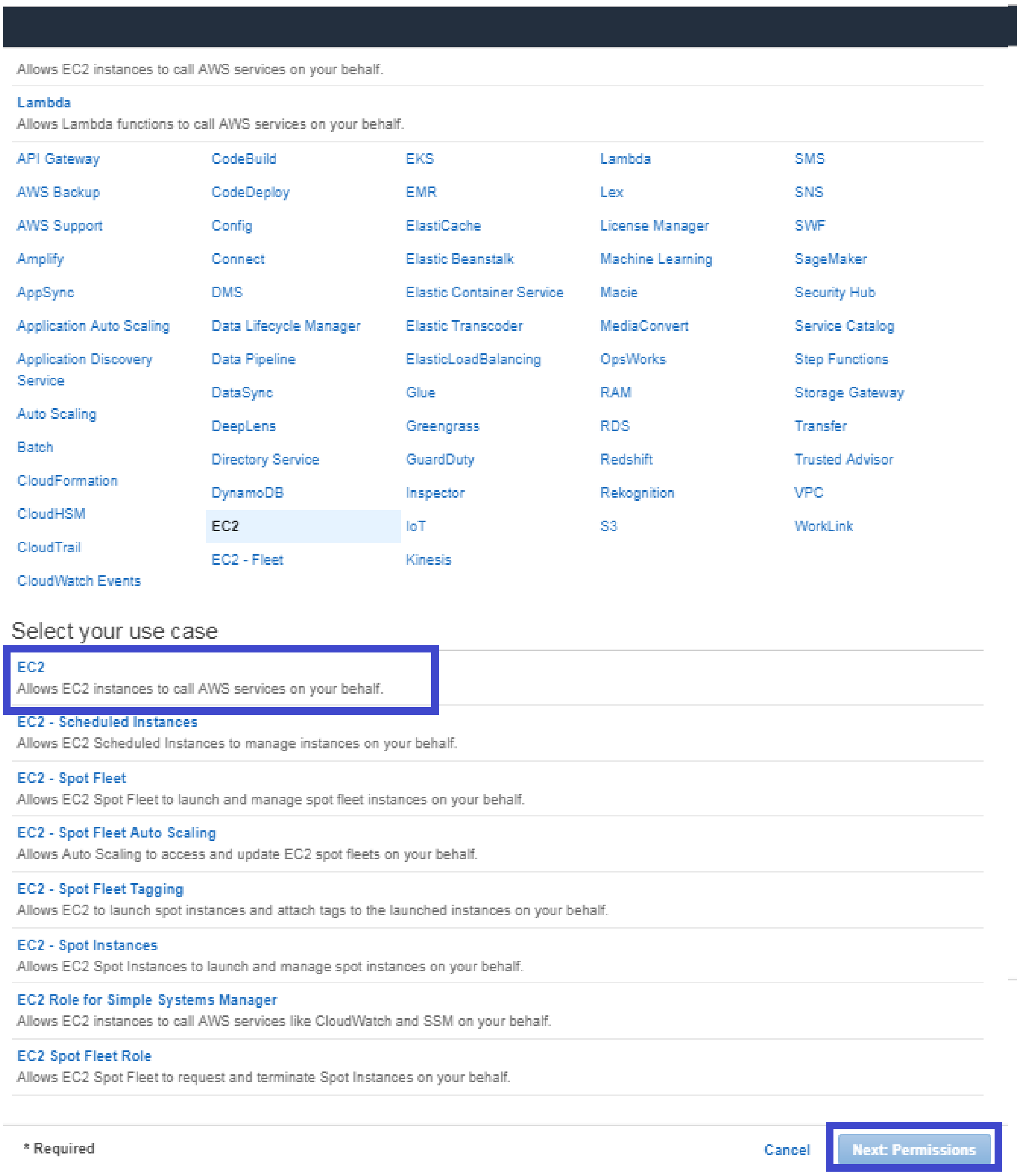
EKS
EMR
ElastiCache
Elastic Beanstalk
Elastic Container Service
Elastic Transcoder
ElasticLoadBalancing
Glue
Greengrass
GuardDuty
Inspector
IoT
Kinesis

Lambda
Lex
License Manager
Machine Learning
Macie
MediaConvert
OpsWorks
RAM
RDS
Redshift
Rekognition
S3

SMS
SNS
SWF
SageMaker
Security Hub
Service Catalog
Step Functions
Storage Gateway
Transfer
Trusted Advisor
VPC
WorkLink

* Required

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

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.

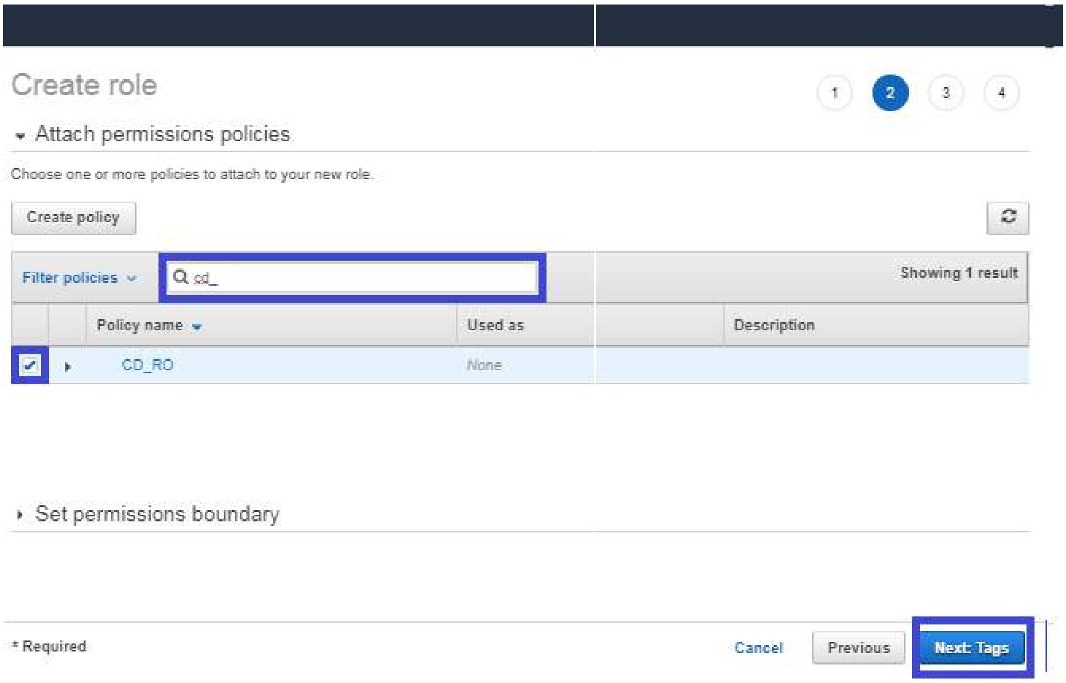
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

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

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



Create role

Attach permissions policies

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

Filter policies: cd_

Showing 1 result

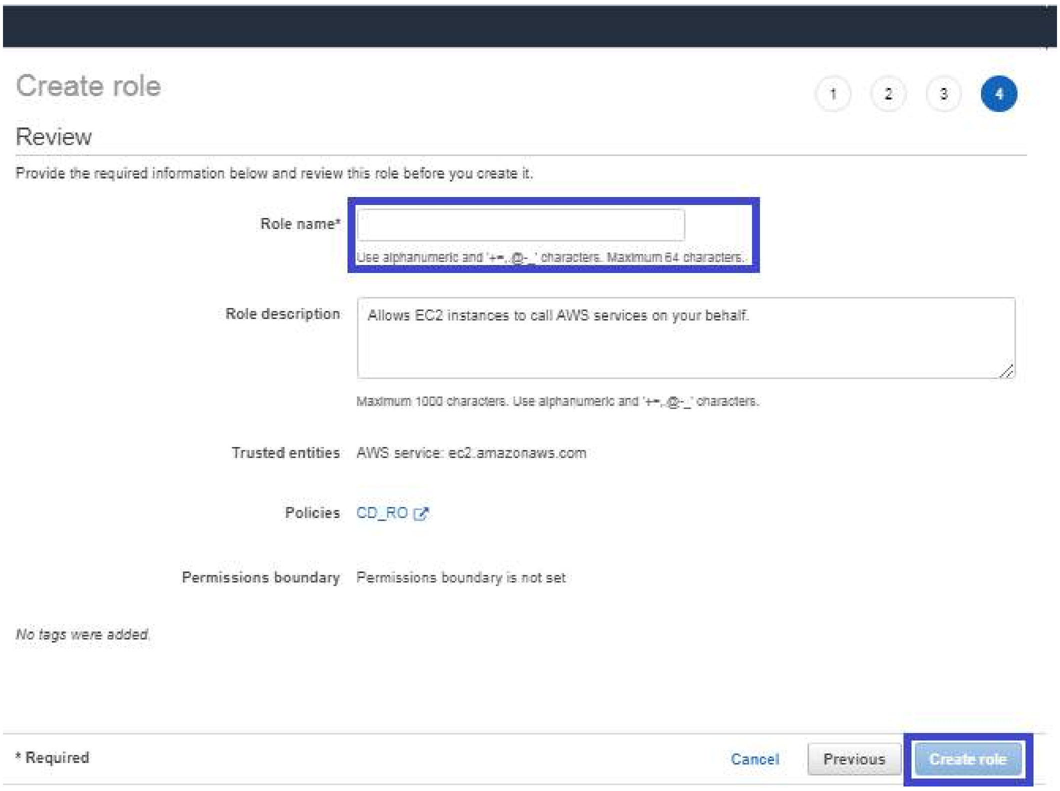
		Policy name	Used as	Description
☑	▸	CD_RO	None	

Set permissions boundary

* Required

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

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



Create role

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

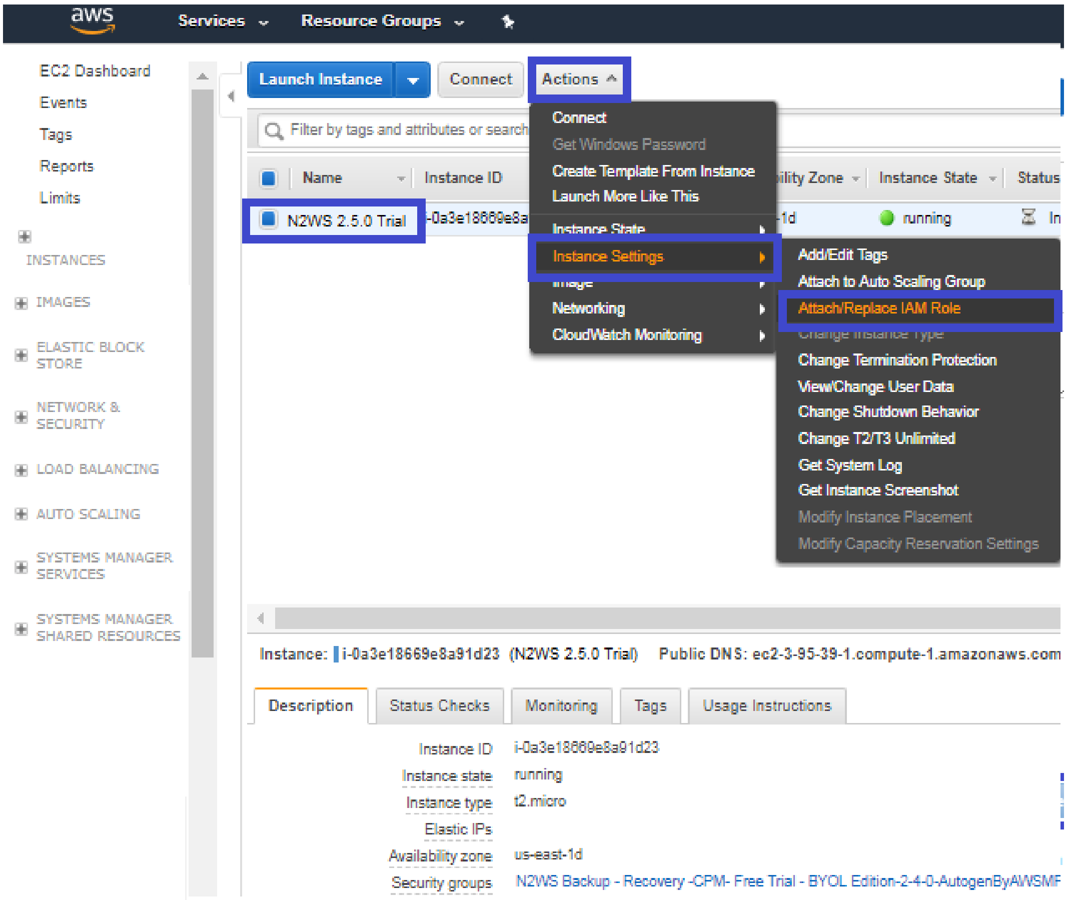
No tags were added.

* Required

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

    a. Select the N2WS instance name.

    b. In the Actions menu, select **Instance Settings** and then **Attach/Replace IAM Role**.



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

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