



# **N2WS Backup & Recovery**

## **User Guide**

**Version 4.0.0**



## Contents

<b>1</b>	<b>Introduction to N2WS Backup &amp; Recovery.....</b>	<b>7</b>
1.1	Purchasing N2WS on the AWS Marketplace.....	8
1.2	N2WS Architecture.....	9
1.3	N2WS Server Instance .....	10
1.4	Upgrading N2WS .....	12
1.5	N2WS Technology .....	16
1.6	Browser Support.....	17
1.7	Viewing Tutorial and Free Installation .....	17
1.8	Customized Free Trial.....	17
1.9	N2WS Support for AWS Outposts .....	17
<b>2</b>	<b>Configuring N2WS.....</b>	<b>19</b>
2.1	Instance ID.....	20
2.2	License Agreement and Root User .....	21
2.3	Defining Time Zone, Data Volume, Force Recovery Mode, Web Proxy ..	22
2.4	Complete Remaining Fields in N2WS Configuration .....	25
2.5	Registering and Finalizing the Configuration .....	28
2.6	Configuration Troubleshooting .....	28
2.7	Modifying the Server Configuration.....	30
2.8	Configuring N2WS in Silent Mode .....	30
2.9	Maintaining N2WS.....	33
2.10	Using the AWS Key Management Service .....	33
<b>3</b>	<b>Start Using N2WS.....</b>	<b>35</b>
3.1	Associating an AWS Account.....	35
3.2	Associating an Azure Account .....	42
3.3	Deleting Accounts.....	42
3.4	Managing Volume Usage.....	43
3.5	Importing Non-N2WS Backups to S3.....	45
3.6	N2WS Help and Support.....	48
<b>4</b>	<b>Defining Backup Policies .....</b>	<b>51</b>
4.1	Schedules.....	51
4.2	AWS Policies .....	56
4.3	Managing Policies.....	67
<b>5</b>	<b>Consistent Backup.....</b>	<b>71</b>
5.1	Crash-Consistent Backup.....	71
5.2	Application-Consistent Backup .....	71
5.3	N2WS and a Point in Time .....	71
5.4	Summary or What Type of Backup to Choose .....	71
<b>6</b>	<b>Windows Instances Backup .....</b>	<b>73</b>
6.1	Configuring N2WS Thin Backup Agents.....	73
6.2	Configuring Simple System Manager (SSM) Agents.....	76
6.3	Using VSS .....	79



6.4	Using Backup Scripts on Windows .....	83
<b>7</b>	<b>Linux/Unix Instances Backup .....</b>	<b>86</b>
7.1	Connecting to the N2WS Server .....	86
7.2	Backup scripts .....	86
<b>8</b>	<b>Using Elastic File System (EFS) with N2WS .....</b>	<b>90</b>
8.1	Configuring EFS .....	90
8.2	Creating IAM Roles in AWS .....	91
8.3	Backup Options for EFS Instances .....	93
<b>9</b>	<b>Additional Backup Topics .....</b>	<b>94</b>
9.1	N2WS in a VPC Environment .....	94
9.2	Backup when an Instance is Stopped .....	94
9.3	The Freezer .....	95
9.4	Running Automatic Cleanup .....	95
9.5	Backing up Independent Volumes .....	96
9.6	Excluding Volumes from Backup .....	96
9.7	Regions Disabled by Default .....	97
9.8	Synchronizing S3 Buckets .....	97
<b>10</b>	<b>Performing Recovery .....</b>	<b>101</b>
10.1	Searching for Backups to Recover From .....	101
10.2	Recovery AWS credentials .....	103
10.3	Instance Recovery .....	103
10.4	Volume Recovery .....	113
10.5	RDS Database Recovery .....	116
10.6	Aurora Cluster Recovery .....	116
10.7	Aurora Serverless Recovery .....	117
10.8	Redshift Cluster Recovery .....	119
10.9	DynamoDB Table Recovery .....	120
10.10	EFS Recovery .....	120
10.11	FSx Recovery .....	122
<b>11</b>	<b>Disaster Recovery (DR) .....</b>	<b>124</b>
11.1	Configuring DR .....	124
11.2	About the DR Process .....	125
11.3	DR and Mixed-region Policies .....	126
11.4	Planning your DR Solution .....	127
11.5	DR Recovery .....	128
11.6	DR Monitoring and Troubleshooting .....	132
<b>12</b>	<b>Cross-Account DR, Backup and Recovery .....</b>	<b>134</b>
12.1	Configuring Cross-Account Backup .....	135
12.2	Cross-Account DR and Clean-Up .....	135
12.3	Cross-Account with Cross-Region .....	136
12.4	Cross-Account Recovery .....	136
<b>13</b>	<b>File-level Recovery .....</b>	<b>137</b>
13.1	Limitations .....	139



13.2	File Level Recovery from S3.....	140
13.3	File-Level Recovery from EFS .....	141
<b>14</b>	<b>Tag-based Backup Management.....</b>	<b>143</b>
14.1	The “cpm backup” Tag .....	143
14.2	Custom Tags .....	148
14.3	Tag Scanning.....	149
14.4	Pitfalls and Troubleshooting .....	150
<b>15</b>	<b>Resource Control .....</b>	<b>152</b>
15.1	Adding a Resource Control Group.....	154
15.2	Adding Resource Targets to a Group .....	155
15.3	Configuring Off/On Scheduler .....	157
15.4	Overriding a Resource Control Schedule .....	158
15.5	Using Scan Tags with Resource Control .....	159
15.6	Resource Control Reporting .....	159
<b>16</b>	<b>Security Concerns and Best Practices.....</b>	<b>162</b>
16.1	N2WS Server.....	162
16.2	Best Security Practices for N2WS .....	162
16.3	Using IAM .....	163
<b>17</b>	<b>Alerts, Announcements, Notifications and Reporting.....</b>	<b>167</b>
17.1	Alerts .....	167
17.2	Pull Alerts.....	169
17.3	Using SNS.....	170
17.4	Push Alerts.....	172
17.5	Daily Summary.....	172
17.6	Resources Summary PDF Report.....	173
17.7	Raw Reporting Data.....	174
17.8	AWS Usage Reports.....	177
17.9	Protected Resources and AWS Unprotected Resources Reports .....	177
17.10	Reports Page.....	178
17.11	Examples of AWS Alerts .....	182
17.12	Announcements .....	184
<b>18</b>	<b>N2WS User Management .....</b>	<b>185</b>
18.1	Independent Users .....	185
18.2	Managed Users.....	186
18.3	User Definitions.....	186
18.4	Delegates .....	188
18.5	Usage Reports .....	189
18.6	Audit Reports.....	190
18.7	Email Configuration .....	190
<b>19</b>	<b>N2WS IdP Integration.....</b>	<b>193</b>
19.1	Configuring IdPs to Work with N2WS .....	193
19.2	Configuring Groups and Group Permissions on the N2WS Side .....	195
19.3	Configuring Groups on the IdP Side .....	198
19.4	N2WS Login Using IdP Credentials .....	201





19.5	Configuring N2WS to Work with Active Directory / AD FS .....	211
19.6	Configuring an AD FS User Claim.....	212
19.7	Configuring Azure AD and N2WS IdP Settings .....	216
<b>20</b>	<b>Configuring N2WS with CloudFormation .....</b>	<b>225</b>
<b>21</b>	<b>Managing Snapshots with Lifecycle Policies.....</b>	<b>230</b>
21.1	Using S3 with N2WS .....	230
21.2	The S3 Repository.....	232
21.3	The S3 Policy.....	234
21.4	The Export RDS to S3 Policy .....	239
21.5	The Glacier Archive.....	245
21.6	Monitoring Lifecycle Activities .....	247
<b>22</b>	<b>Configuring Workers .....</b>	<b>251</b>
22.1	Worker Parameters .....	252
22.2	Worker Tags .....	254
22.3	Testing the Configuration for a Worker .....	255
<b>23</b>	<b>Capturing and Cloning in VPC Environments .....</b>	<b>257</b>
23.1	Overview of VPC and N2WS .....	257
23.2	Features of Capturing and Cloning VPCs.....	257
23.3	Configuring VPC Capturing .....	258
23.4	Updating Accounts for VPC .....	259
23.5	Cloning VPCs.....	259
<b>24</b>	<b>Orchestrating Recovery Scenarios .....</b>	<b>263</b>
24.1	Overview.....	263
24.2	Conditions.....	263
24.3	Creating a Recovery Scenario.....	264
24.4	Testing a Recovery Scenario.....	269
24.5	Managing Recovery Scenarios and Targets.....	270
24.6	Running and Monitoring a Recovery Scenario.....	270
24.7	Recovery Scenario User Scripts .....	272
<b>25</b>	<b>Monitoring Costs and Savings.....</b>	<b>274</b>
25.1	Enabling and Disabling Cost Explorer .....	275
25.2	Monitoring Costs .....	276
25.3	Monitoring Expected Cost Savings .....	277
<b>26</b>	<b>Using N2WS with Azure.....</b>	<b>278</b>
26.1	Setting Up Your Azure Subscription .....	278
26.2	Registering Your Azure App.....	280
26.3	Adding an Azure Account to N2WS.....	281
26.4	Creating an Azure Policy.....	283
26.5	Backing Up an Azure Policy .....	284
26.6	Recovering from an Azure Backup .....	285



<b>Appendix A – Recommended Configuration for Copy to S3 .....</b>	<b>289</b>
<b>Appendix B – Agents Configuration Format .....</b>	<b>294</b>
<b>Appendix C – Time Zones .....</b>	<b>295</b>
<b>Appendix D – Datadog Integration Support .....</b>	<b>296</b>
D.1    Activating Datadog and Monitoring N2WS .....	296
D.2    Monitoring N2WS with Web Proxy .....	300
<b>Appendix E – Splunk Integration Support .....</b>	<b>301</b>
E.1    Configure N2WS Server for Splunk .....	301
E.2    Installation on Splunk .....	301
E.3    Configuration of TA for N2WS .....	302
E.4    Viewing Dashboards .....	306



# 1 Introduction to N2WS Backup & Recovery

N2WS Backup & Recovery (CPM), known as N2WS, is an enterprise-class backup, recovery and disaster recovery solution for the Amazon Web Services (AWS). Designed from the ground up to support AWS, N2WS uses cloud-native technologies (e.g. EBS snapshots) to provide unmatched backup and, more importantly, restore capabilities in AWS.

N2WS also supports backup and recovery for Microsoft Azure Virtual Machines and Disks.

N2WS is sold as a service. When you register to use the service, you get permission to launch a virtual Amazon Machine Image (AMI) of an EC2 instance. Once you launch the instance, and after a short configuration process, you can start backing up your data using N2WS.

Using N2WS, you can create backup policies, schedules, and import non-N2WS backups to Amazon Simple Storage Service (S3). Backup policies define what you want to back up (i.e. Backup Targets) as well as other parameters, such as:

- Frequency of backups
- Number of backup generations to maintain
- Whether to copy the backup data to other AWS regions, etc.
- Whether to back up a resource immediately

Backup targets can be of several different types, for example:

- EC2 instances (including some or all of the instance's EBS volumes)
- Independent EBS volumes (regardless of whether they are attached and to which instance)
- Amazon Relational Database Service (RDS) databases
- RDS Aurora clusters, including Aurora Serverless
- Redshift clusters
- DynamoDB tables
- Elastic File System (EFS)
- FSx File Systems
- S3 Sync to copy objects between S3 buckets
- For Azure policies, Virtual Machines (VM) and Disks

In addition to backup targets, you also define backup parameters, such as:

- In Windows achieving application consistency using Microsoft Volume Shadow Copy Service (VSS)
- Running backup scripts
- Number of retries in case of a failure

Schedules are used to define how you want to time the backups. You can define the following:

- A start and end time for the schedule, including time zone of data
- Backup frequency, e.g. every 15 minutes, every 4 hours, every day, etc.
- Days of the week to run the policy
- Special times to disable the policy

A policy can have one or more schedules associated with it. A schedule can be associated with one or more policies. As soon as you have an active policy defined with a schedule, backups will start automatically.



N2WS provides monitoring at multiple levels. The Dashboard displays key performance indicators for backups, disaster recoveries, volume usage, backups to S3, and other metrics. Operation-specific monitors allow you to view details. And support for additional monitoring using Datadog and Splunk is available.

## 1.1 Purchasing N2WS on the AWS Marketplace

N2WS is available in several different editions that support different usage tiers of the solution, e.g. number of protected instances, number of AWS accounts supported, etc. The price for using the N2WS software is a fixed monthly price which varies between the different N2WS editions.

To see the different features for each edition, along with pricing and details, go to the [N2W Software Web site](#). Once you subscribe to one of the N2WS editions, you can launch an N2WS Server instance and begin protecting your AWS environment. Only one N2WS Server per subscription will actually perform a backup. If you run additional instances, they will only perform recovery operations (section 1.3.3).

### 1.1.1 Moving between N2WS Editions

If you are already subscribed and using one N2WS edition and want to move to another that better fits your needs, you need to perform the following steps:

**Note:** Before proceeding, it is highly recommended to create a snapshot of your CPM data volume. You can delete that snapshot once your new N2WS Server is up and running. The data volume is typically named **N2WS – Data Volume**.

1. Terminate your existing N2WS instance. It is recommended that you do so while no backup is running.
2. Unsubscribe from your current N2WS edition. It is important since you will continue to be billed for that edition if you don't cancel your subscription. You will only be able to unsubscribe if you don't have any running instances of your old edition. You manage your subscriptions on the AWS Marketplace site on the [Your Software](#) page.
3. Subscribe to the new N2WS Edition and launch an instance. You need to launch the instance in the same Availability Zone (AZ) as the old one. If you want to launch your new N2WS Server in a different zone or region, you will need to create a snapshot of the data volume and either create the volume in another zone or copy the snapshot to another region and create the volume there.
4. During configuration, choose **Use Existing Data Volume** and select the existing data volume.
5. Once configuration completes, continue to work with your existing configuration with the new N2WS edition.

### 1.1.2 Downgrading

If you moved to a lower N2WS edition, you may find yourself in a situation where you exceed the resources your new edition allows. For example, you used N2WS Advanced Edition and you moved to N2WS Standard Edition, which allows fewer instances. N2WS will detect such a situation as a compliance issue, will cease to perform backups, display a message, and issue an alert detailing the problem.



### To fix the problem:

- Move back to an N2WS edition that fits your current configuration, or
- Remove the excessive resources, e.g. remove users, AWS accounts, or instances from policies.

Once the resources are back in line with the current edition, N2WS will automatically resume normal operations.

## 1.2 N2WS Architecture

The N2WS Server is a Linux-based virtual appliance. It uses AWS APIs to access your AWS account. It allows managing snapshots of EBS volumes, RDS instances and clusters, Redshift clusters, and DynamoDB tables. Except in cases where the user chooses to install our Thin Backup Agent for Windows Servers or the AWS Simple System Manager (SSM) Remote Agent, N2WS does not directly access your instances. Access is performed by the agent, or by a script that the user provides, which performs application quiescence.

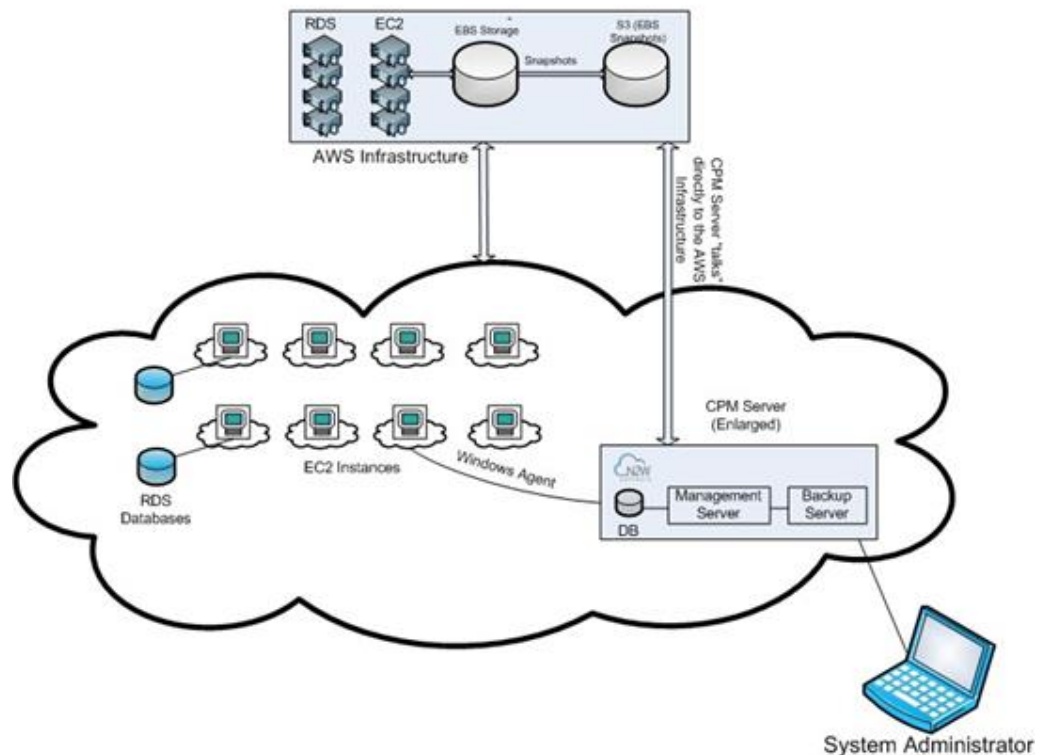
N2WS consists of three parts, all of which reside on the N2WS virtual server:

- A database that holds your backup related metadata.
- A Web/Management server that manages metadata.
- A backup server that actually performs the backup operations. These components reside in the N2WS server.

The N2WS architecture is shown below. N2WS Server is an EC2 instance inside the cloud, but it also connects to the AWS infrastructure to manage the backup of other instances. N2WS does not need to communicate or interfere in any way with the operation of other instances. The only case where the N2WS server communicates directly with and has software installed on, an instance, is when backing up Windows Servers for customers who want to use Microsoft VSS for application quiescing.

- If you wish to have VSS or script support for application quiescence, you need to install the AWS SSM Agent or the N2WS Thin Backup Agent. The agent gets its configuration from the N2WS server, using the HTTPS protocol.
- The SSM agent doesn't require any inbound ports to be opened. All communication from the agent is outbound from HTTPS to the SSM and EC2 Message endpoints in the region where your instances are registered.

## N2WS Solution Architecture



## 1.3 N2WS Server Instance

The N2WS instance is an EBS-based instance with two EBS volumes. One is the root device, and the other is the CPM data volume. All persistent data and configuration information reside on the data volume. From N2WS's perspective, the root device is dispensable. You can always terminate your N2WS instance and launch a new one, then using a short configuration process continue working with your existing data volume.

### 1.3.1 Root Volume

Although you have access to the N2WS Server instance via SSH, N2W Software expects the N2WS Server instance will be used as a virtual appliance. N2W Software expects you not to change the OS and not to start running additional products or services on the instance. If you do so and it affects N2WS, N2W Software will not be able to provide you with support. Our first requirement will be for you to launch a clean N2WS server.

**Note:** Remember that all your changes in the OS will be wiped out as soon as you upgrade to a new release of N2WS, which will come in the form of a new image (AMI). If you need to install software to use with backup scripts (e.g. Oracle client) or you need to install a Linux OS security update, you can. N2W Software recommends that you consult [N2W Software support](#) before doing so.




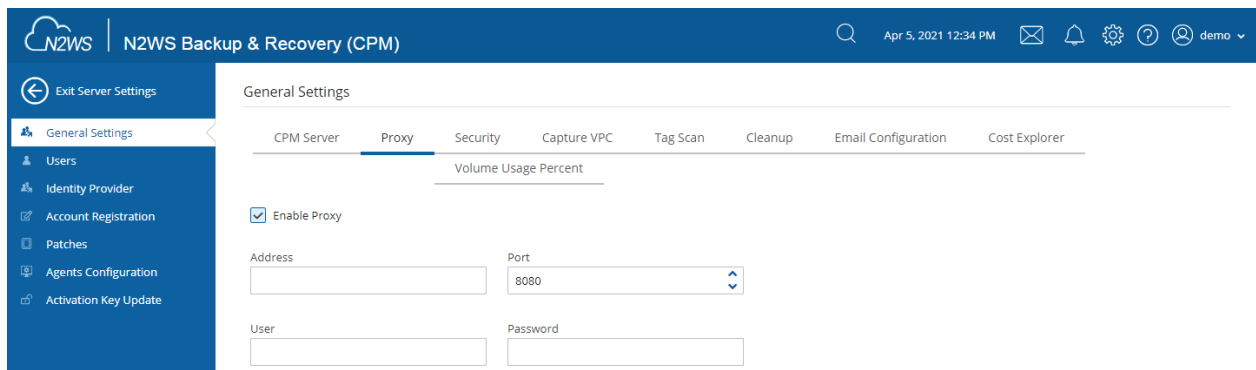
### 1.3.2 Backing up the N2WS Server

N2WS server runs on an EBS-based instance. This means that you can stop and start it whenever you like. But if you create an image (AMI) of it and launch a new one with the system and data volume, you will find that the new server will not be fully functional. It will load and will allow you to perform recovery, but it will not continue performing backup as this is not the supported way to back up N2WS servers. What you need to do, is to back up only the data volume, launch a fresh N2WS server, and connect it to a recovered data volume. See section 11.4.3.

### 1.3.3 N2WS Server with HTTP Proxy

N2WS needs connectivity to AWS endpoints to be able to use AWS APIs. This requires Internet connectivity. If you need N2WS to connect to the Internet via an HTTP Proxy, that is fully supported. During configuration, you will be able to enable proxy use and enter all the required details and credentials: proxy address, port, user, and password. User and password are optional and can be left empty if the proxy server does not require authentication. Once you configure proxy settings at the configuration stage, they will also be set for use in the main application.

The proxy setting can be modified at any time in the **Proxy** tab of N2WS  **Server Settings** > **General Settings**. Select or clear **Enable Proxy**. If enabled, enter the requested proxy information.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title "N2WS Backup & Recovery (CPM)", a search icon, the date and time "Apr 5, 2021 12:34 PM", and several utility icons (mail, bell, gear, question mark, and a user profile labeled "demo"). A left sidebar contains a list of settings: "Exit Server Settings", "General Settings" (selected), "Users", "Identity Provider", "Account Registration", "Patches", "Agents Configuration", and "Activation Key Update". The main content area is titled "General Settings" and features a tabbed interface with tabs for "CPM Server", "Proxy" (active), "Security", "Capture VPC", "Tag Scan", "Cleanup", "Email Configuration", and "Cost Explorer". Under the "Proxy" tab, there is a section "Volume Usage Percent" and a checkbox labeled "Enable Proxy" which is checked. Below this, there are input fields for "Address", "Port" (a dropdown menu showing "8080"), "User", and "Password".

### 1.3.4 Multiple N2WS Servers

If you are trying to launch multiple N2WS servers of the same edition in the same account, you will find that from the second one on, no backup will be performed. Each such server will assume it is a temporary server for recovery purposes and will allow only recovery. Typically, one N2WS server should be enough to back up your entire EC2 environment. If you need more resources, you should upgrade to a higher edition of N2WS. If you do need to use more than one N2WS server in your account, contact [N2W Software support](#).



## 1.4 Upgrading N2WS

**Note:** We strongly recommend that you read this *entire* section **BEFORE** starting the upgrade and that you follow **every step** in these sections to ensure that version 3.x is configured correctly and with no loss of data.

The upgrade process consists of 4 phases:

1. Before starting the upgrade, refer to instructions specific to your current version in section 1.4.1.
2. Terminate the old version instance and launch the new version as described in section 1.4.2.
3. Configure the new version instance according to instructions in section 1.4.3.
4. After the upgrade, there are still a few steps to ensure a complete transition. See section 1.4.4.

If you have any questions or encounter issues, visit the [N2WS Support Center](#) where you will find helpful resources in a variety of formats or can open a Support Ticket.

### 1.4.1 Before Upgrading to N2WS V3.X

The following sections outline the steps required to upgrade to N2WS Backup & Recover version 3.x.

#### GENERAL

##### Permissions

Due to new functionality in v3.x, you may need to update your permission policies. If you have more than one AWS Account added to the N2WS console, you will have to update the IAM Policies for each account. See the JSON templates at <https://support.n2ws.com/portal/kb/articles/what-are-the-required-minimal-aws-permissions-roles-for-cpm-operation>

##### **Before starting:**

1. Have the username and password for the root/admin user ready.
2. If you are using a proxy in the N2WS settings, write down the details.
3. Take a screenshot of the N2WS EC2 instance network settings: IP, VPC, Subnet, Security Groups, and IAM Role and Keypair name.
4. Take a screenshot of the Tags if you have more than a few.
5. Verify that there are no backups, DRs, or Cleanup running or scheduled to run within the next 15-30 minutes.
6. Shut down the N2WS EC2 instance.
7. Take a snapshot of the N2WS Data Volume. Only the Data Volume is important, as it contains all your settings, backup entries, etc.
8. Download the latest [IAM permissions](#) and update the IAM Policies from your role.





## UPGRADE FROM 2.7.X, 3.X, 2.3.X, 2.2.X, 2.1x

- **For 3.0.0/3.0.0a Customers, *after* upgrading to v3.0.0b or later versions:**
  - If you created or modified an S3 policy in v3.0.x or earlier versions, **TO AVOID a POSSIBLE DATA LOSS**, you **must** apply the workaround listed at [S3 backups may be stored for X days instead of X months](#).
  - Policies created or modified in v3.0.0b and later will not experience this issue.
- **For Customers upgrading from other versions**, perform the upgrade as usual. See section [1.4.2](#).

## UPGRADE FROM 2.4, 2.5, 2.6

- **Customers that did *not* use Copy to S3** do not need to perform any additional actions and should perform the upgrade as usual. See section [1.4.2](#).
- **Customers that *did* use Copy to 3 *must*** proceed according to the following steps:

### IMPORTANT NOTICE FOR 2.4, 2.5, 2.6 CUSTOMERS USING COPY TO S3:

- All data previously archived to S3 (using versions 2.4-2.6) **cannot** be recovered using version 3.0. To recover this data in the future, you will need to create an AMI of the existing N2WS instance **before** completing the upgrade process.
- You **must** complete the following **mandatory** steps:

### Mandatory Steps for 2.4, 2.5, 2.6 Customers using Copy to S3:

#### ***Before shutting down the 2.4.x, 2.5.x, or 2.6.x N2WS server:***

1. Verify that no backup/DR/Cleanup/S3 is in process or scheduled within the next 30 minutes.
2. Disable the local CPM Agent.
3. Connect to CPM in SSH.
4. Type:

```
sudo mv
/opt/n2wsoftware/cpmagent/agent.pyo/opt/n2wsoftware/cpmagent/agent.p
yo.disabled
```
5. Use the AWS Console to create an AMI of the existing N2WS instance. Retain this AMI to ensure that you can recover data previously archived to S3, using any version before 2.7. Retain this AMI for as long as you need to recover the pre-v2.7 legacy data from S3.

**Note:** Launch this AMI, which defaults to *recover-only* mode, whenever you need to recover from the old S3 repository:

1. Navigate to the EC2 console.
2. Select the running N2WS instance.
3. Under the **Actions** menu, select **Image**.
4. Create Image.

6. Launch version 3.x using the normal upgrade process. See section [1.4.2](#).



#### Notice for customers using Copy to S3:

- Once version 3.0 is launched, the first archive to S3 will be FULL. All subsequent backups will be incremental as usual.
- You can maximize cost savings by moving previously archived data (pre-v2.7) from S3 to S3 Intelligent Tiering, or IA if preferred.

#### Cleaning Up Your Pre-2.7 S3 Repository

**Note:** Once version 3.x is launched, all data previously archived to S3 (using versions 2.4 - 2.6) will not be deleted by the N2WS cleanup operation.

When based on your retention policy you no longer need any of the archived backups in your older repository using versions 2.4-2.6, you can manually delete it.

#### To delete a repository named 'Repository\_to\_Delete' located at 'Configured\_S3\_Bucket':

1. Use the AWS console to access the S3 console.
2. The repository, '**Rep\_to\_Delete**', will be located under **Configured\_S3\_Bucket > Veeam > Backup > Rep\_to\_Delete**
3. Select the '**Rep\_to\_Delete**' folder and delete it using the S3 console.

### 1.4.2 Terminating the Old Instance and Launching the New Instance

1. Verify that no backup, DR, or Cleanup is being performed or is about to be started within the next 15 to 30 minutes.
2. Terminate the existing CPM instance.
3. Launch a new N2WS Server instance in the same region and AZ as the old one. You can launch the instance using the [Your Marketplace Software](#) page on the AWS web site.
4. To determine the AZ of the new instance, launch the instance using the EC2 console rather than using the 1-click option.
5. Wait until the old CPM instance is in the **terminated** state.

### 1.4.3 Configuring the New N2WS Server Instance

#### To upgrade/restart the N2WS Server Instance:

1. About 1 minute after launching the new instance, it should be in the **running** state. Connect to the UI with a browser using [https://\[ip-of-your-new-instance\]](https://[ip-of-your-new-instance]).
2. Confirm the Instance ID of your newly launched instance.
3. Accept the Terms and Conditions.
4. Enter the username and password of the admin/root user.
5. Approve the exception to the SSL certificate.
6. Choose the time zone and select **Use Existing Data Volume** in step #4, "Data Volume and Proxy".
7. Select your old data volume from the **Existing CPM Data Volume** list in step #5, "Server Configuration".
8. Select **Configure System** in step #6, "Register Your Account". N2WS will automatically resume operations. Wait until the login mask appears.



Note: See section 2 for complete details for the Server Configuration.

## 1.4.4 Completing the Upgrade

### **After upgrading:**

- If you were using N2WS Thin Backup Agents to perform app-consistent backups:
  - Check the Agents tab and see if “last heard from” is updated with a recent date and time.
  - If not, you may have to download and install the N2WS Thin Backup Agent on your Windows EC2 instances.
- If you were using the AWS SSM Remote Agent to perform app-consistent backups, note that the SSM Agent will not appear in the **Agents** tab. You will need to verify the SSM Agent separately.
- If you were using backup scripts that utilize SSH, you may need to log in to the N2WS Server once and run the scripts manually so that the use of the private key will be approved.
- If you have more than one AWS Account added to the N2WS console:
  - Update the IAM Policies for each Account. See step 8 in the Before Warning in section 1.4.1.
  - Confirm using Check AWS Permissions for each Account.

### **UPGRADE FROM 2.7.X, 3.X, 2.3.X, 2.2.X, 2.1x**

- For 3.0.0/3.0.0a Customers, *after* upgrading to v3.0.0b or later versions:
  - If you created or modified an S3 policy in v3.0.x or earlier versions, **TO AVOID a POSSIBLE DATA LOSS**, you **must** apply the workaround listed at [S3 backups may be stored for X days instead of X months](#).
  - Policies created or modified in v3.0.0b and later will not experience this issue.
- For Customers upgrading from other versions, perform the upgrade as usual. See section [1.3.6](#).

### **UPGRADE FROM 2.4, 2.5, 2.6**

- **Customers that did *not* use Copy to S3** do not need to perform any additional actions and should perform the upgrade as usual. See section [1.3.6](#).
- **Customers that *did* use Copy to 3 *must*** proceed according to the following steps:

#### **IMPORTANT NOTICE FOR 2.4, 2.5, 2.6 CUSTOMERS USING COPY TO S3:**

All data previously archived to S3 (using versions 2.4-2.6) *cannot* be recovered using version 3.0. To recover this data in the future, you will need to create an AMI of the existing N2WS instance **before** completing the upgrade process.

You *must* complete the following **mandatory** steps:



## Mandatory Steps for 2.4, 2.5, 2.6 Customers using Copy to S3:

**Before** shutting down the 2.4.x, 2.5.x, or 2.6.x N2WS server:

1. Verify that no backup/DR/Cleanup/S3 is in process.
2. Disable the local CPM Agent.
3. Connect to CPM in SSH.
4. Type:

```
sudo mv
/opt/n2wsoftware/cpmagent/agent.pyo/opt/n2wsoftware/cpmagent/agent.p
yo.disabled
```
5. Use the AWS Console to create an AMI of the existing N2WS instance. Retain this AMI to ensure that you can recover data previously archived to S3, using any version before 2.7. Retain this AMI for as long as you need to recover the pre-v2.7 legacy data from S3.

**Note:** Launch this AMI, which defaults to *recover-only* mode, whenever you need to recover from the old S3 repository:

1. Navigate to the EC2 console.
2. Select the running N2WS instance.
3. Under the **Actions** menu, select **Image**.
4. **Create Image**.

6. Launch version 3.x using the normal upgrade process. See section [1.3.6](#).

### Notice for customers using Copy to S3:

- Once version 3.0 is launched, the first archive to S3 will be FULL. All subsequent backups will be incremental as usual.
- You can maximize cost savings by moving previously archived data (pre-v2.7) from S3 to S3 Intelligent Tiering, or IA if preferred.

## Cleaning Up Your Pre-2.7 S3 Repository

**Note:** Once version 3.x is launched, all data previously archived to S3 (using versions 2.4 - 2.6) will not be deleted by the N2WS cleanup operation.

When based on your retention policy you no longer need any of the archived backups in your older repository using versions 2.4-2.6, you can manually delete it.

### To delete a repository named 'Repository\_to\_Delete' located at 'Configured\_S3\_Bucket':

1. Use the AWS console to access the S3 console.
2. The repository, '**Rep\_to\_Delete**', will be located under **Configured\_S3\_Bucket > Veeam > Backup > Rep\_to\_Delete**
3. Select the '**Rep\_to\_Delete**' folder and use the S3 console to delete it.

## 1.5 N2WS Technology

As part of the cloud ecosystem, N2WS relies on web technology. The management interface through which you manage backup and recovery operations is web-based. The APIs which



N2WS uses to communicate with AWS, are web-based. All communication with the N2WS server is performed using the HTTPS protocol, which means it is all encrypted. This is important, since sensitive data will be communicated to/from the N2WS server, for example, AWS credentials, N2WS credentials, object IDs of your AWS objects (instances, volumes, databases, images, snapshot IDs, etc.).

## 1.6 Browser Support

Most interactions with the N2WS server are performed via a web browser.

- Since N2WS uses modern web technologies, you will need your browser to be enabled for JavaScript.
- N2WS supports Microsoft Chromium Edge, Mozilla Firefox, and Google Chrome.
- Other browsers are not supported.

## 1.7 Viewing Tutorial and Free Installation

If you want to view a getting-started tutorial, or to try the fully-functional N2WS free for 30 days, go to <https://n2ws.com/support/video-tutorials/getting-started>.

Follow the instructions in the 'Getting Started with N2WS Backup & Recovery for AWS' video.

**Note:** It is not necessary to reinstall N2WS after purchasing a license.

## 1.8 Customized Free Trial

It is now possible to have a free trial of N2WS with the usage limitations customized for your specific AWS infrastructure. Contact N2W Software sales at [info@n2ws.com](mailto:info@n2ws.com) to start your customized free trial. The N2W Software sales team may provide a reference code for your customized installation.

## 1.9 N2WS Support for AWS Outposts

N2WS provides customers the ability to backup and recover on-premise workloads running on AWS Outposts as well as workloads on AWS. N2WS can run the core backup application on the AWS cloud and protect workloads running either on regions outside of AWS Outposts or protect applications that need to be backed up on AWS Outposts.

N2WS supports the following AWS services running on Outposts:

- EC2/EBS/RDS/SES/S3/VPC
- The services can be deployed in all AWS regions.

### 1.9.1 Deployment

N2WS is available on AWS Marketplace with different editions ready to support any size environment:

<https://aws.amazon.com/marketplace/search/results?x=29&y=9&searchTerms=n2ws>

You can launch N2WS as an AMI directly from the AWS Marketplace or use a pre-configured



CloudFormation template. Configuration takes a few minutes. See

<https://n2ws.com/support/video-tutorials/install-and-configure-n2ws-backup-recovery-3-0>

For further information regarding the AWS Outposts service, go to

<https://console.aws.amazon.com/outposts/>

## 1.9.2 Supported Use Cases

The prerequisite for support is complete installation of N2WS Backup & Recovery. Use cases are:

- **Backup**

N2WS can either backup applications, such as a media server, that run on AWS Outposts by storing the backup data on Outposts, as well as protect applications running outside of AWS Outposts by storing backup data in the same AWS region.

- **Disaster Recovery (DR)**

In the case of Disaster Recovery, N2WS protects resources running on AWS Outposts and copies data to another AWS Region or AWS account.

- Another option is to use N2WS Backup & Recovery to backup resources running in a specific AWS region to Amazon Outposts.
- DR failback reverses the workflow.



## 2 Configuring N2WS

**Important:** BEFORE upgrading to version 3.0 from versions 2.4-2.7, Copy to S3 customers must review section 2.3.2 (Step 4) about special conditions for data recovery.

The N2WS management console is accessed via a web browser over HTTPS.

- When a new N2WS Server is launched, the server will automatically generate a new self-signed SSL certificate. This certificate will be used for the web application in the configuration step.
- If no other SSL certificate is uploaded to the N2WS Server, the same certificate will be used also for the main N2WS application.
- Every N2WS Server will get its own certificate.
- Since the certificate is not signed by an external Certificate Authority, you will need to approve an exception in your browser to start using N2WS.

When configuring the N2WS server, define the following settings:

- AWS Credentials for the N2WS root user.
- Time zone for the server.
- Whether to create a new CPM data volume or attach an existing one from a previous N2WS server.
- Whether to create an additional N2WS server from an existing data volume during Force Recovery Mode.
- Proxy settings. Configure proxy settings in case the N2WS server needs to connect to the Internet via a proxy. These settings will also apply to the main application.
- The port the web server will listen on. The default is 443. See section 1.3.3.
- Whether to upload an SSL certificate and a private key for the N2WS server to use. If you provide a certificate, you will also need to provide a key, which must not be protected by a passphrase.
- Register the AWS account with N2W Software. This is mandatory only for free trials but is recommended for all users. It will allow N2W Software to provide quicker and enhanced support. Registration information is not shared.

For the configuration process to work, as well as for normal N2WS operations, N2WS needs to have outbound connectivity to the Internet, for the HTTPS protocol. Assuming the N2WS server was launched in a VPC, it needs to have:

- A public IP, or
- An Elastic IP attached to it, or
- Connectivity via a NAT setup, Internet Gateway, or HTTP proxy.

If an access issue occurs, verify that the:

- Instance has Internet connectivity.
- DNS is configured properly.
- Security groups allow outbound connections for port 443 (HTTPS) or other (if you chose to use a different port).



**Following are the configuration steps:**

1. Approve the end-user license agreement.
2. Define the root user name, email, and password.
3. Define the time zone of the N2WS Server and usage of data volumes.
4. Fill in the rest of the information needed to complete the configuration process.

## 2.1 Instance ID

To initially be identified as the owner of this instance, you are required to type or paste the N2WS server instance ID. This is just a security precaution.

The image shows a screenshot of the N2WS Server Configuration interface. At the top, there is a blue header bar with the N2WS logo and the text "Server Configuration" and "N2WS Backup & Recovery (CPM)". Below the header, there is a horizontal progress bar with six steps: "Instance Confirmation", "End User License Agreement", "License and Root User", "Data Volume and Proxy", "Server Configuration", and "Register Your Account". The "Instance Confirmation" step is currently selected and highlighted. Below the progress bar, there is a text prompt: "To begin, please enter the instance ID of this instance:" followed by a text input field. A "Next" button is located at the bottom right of the form area.

**In the next step of the configuration process,** you will also be required to approve the end-user license agreement.





The screenshot shows the 'End User License Agreement' step in the N2WS Server Configuration wizard. At the top, a progress bar indicates the sequence of steps: Instance Confirmation, End User License Agreement (current step), License and Root User, Data Volume and Proxy, Server Configuration, and Register Your Account. The main content area displays the 'End User License Agreement' with a version number 'Version x.x.x - dd/mm/yyyy'. The text of the agreement is visible, including a section titled '1. License Grant'. At the bottom, there is a checkbox labeled 'I read the license terms and I accept them' and a 'Next' button.

## 2.2 License Agreement and Root User

The **License** field is presented. Select **I'm starting a free trial** for a free trial. Otherwise, select the appropriate license option in the list, such as Bring Your Own License (BYOL) Edition. Alternatively, if your organization purchased a license directly from N2W Software, additional instructions are shown.

The AWS root user (IAM User) is no longer allowed to control the operation of the N2WS server. A user with the Authentication credentials for **N2WS Instance IAM Role** is the only user allowed to install N2WS, log on to the system server, and operate it. As shown below, you need to define the root user name, email, and password. This is the third step in the configuration process. The email may be used when defining Amazon Simple Notification Service (SNS) based alerts. Once created, choose to automatically add this email to the SNS topic recipients.



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

License:

User name:

Email (optional):

Password:

Confirm Password:

**Note:** Passwords: N2W Software does not enforce any password policy, however, it is recommended that you use passwords that are difficult to guess and that are changed from time to time.

## 2.3 Defining Time Zone, Data Volume, Force Recovery Mode, Web Proxy

In the fourth step of the configuration process, you can:

- Set the time zone of the N2WS Server.
- If using a paid license, choose whether to create a new data volume or to use an existing one. Your AWS credentials will be used for the data volume setup process.
- Create an additional N2WS server in recovery mode only, by choosing an existing data volume and set **Force Recovery Mode**.
- Configure proxy settings for the N2WS server. See section 2.3.3.

As you will see in section 4.1.3, all scheduling of backup is performed according to the local time of the N2WS Server. You will see all time fields displayed by local time; however, all time fields are stored in the N2WS database in UTC. This means that if you wish to change the time zone later, all scheduling will still work as before.

As you can see below, the choice of new or existing data volume is made here. Actual configuration of the volume will be accomplished at the next step.

AWS credentials are required to create a new Elastic Block Storage (EBS) data volume if needed and to attach the volume to the N2WS Server instance.

- If you are using AWS Identity and Access Management (IAM) credentials that have limited permissions, these credentials need to have permissions to view EBS volumes in your account, to create new EBS volumes, and to attach volumes to instances. See section 16.3. These credentials are kept for file-level recovery later on and are used only for these purposes.



- If you assigned an IAM Role to the N2WS Server instance, and this role includes the needed permissions, select **Use Instance's IAM Role** and then you will not be required to enter credentials.

here.' At the bottom are 'Back' and 'Next' buttons."/>

### 2.3.1 New Data Volume

When creating a new data volume, the only thing you need to define is the capacity of the created volume. You also have the option to encrypt the volume, as described in section 2.4.1. The volume is going to contain the database of N2WS's data, plus any backup scripts or special configuration you choose to create for the backup of your servers. The backup itself is stored by AWS, so normally the data volume will not contain a large amount of data. The default size of the data volume is 5 GiB.

- This is large enough to manage roughly 50 instances and about 3 times as many EBS volumes.
- If your environment is larger than 50 instances, increase the volume at about the ratio of 1 GiB per 10 backed-up instances.

The new volume will be automatically created in the same AZ as the N2WS instance. It will be named **N2WS Data Volume**. During the configuration process, the volume will be created and attached to the instance. The N2WS database will be created on it.

### 2.3.2 Existing Data Volume

#### Important notice for Copy to S3 customers BEFORE upgrading to version 3.0:

- All data previously archived to S3, using versions 2.4-2.6.x, **cannot** be recovered using version 3.0.
- To allow recovery of such data in the future, create an AMI of your current N2WS instance **BEFORE upgrading** to version 3.0.
- To do this, follow all the steps outlined in the version 3.0 [Upgrade Instructions](#) **BEFORE continuing** your upgrade.



- For additional information, see [Release Notes](#).

The **Existing data volume** option is used if:


- You have already run N2WS and terminated the old N2WS server, but now wish to continue where you stopped.
- You are upgrading to new N2WS releases.
- You are changing some of the configuration details.
- You want to configure an additional N2WS server in recovery mode only. See section 2.3.4.

The select box for choosing the volumes will show all available EBS volumes in the same AZ as the N2WS Server instance. When choosing the volumes, consider the following:

- It is important to create the instance in the AZ your volume was created in the first place.
- Another option is to create a snapshot from the original volume, and then create a volume from it in the AZ you require.

**Note:** Although CPM data volumes typically have a special name, it is not a requirement. If you choose a volume that was not created by an N2WS server for an existing data volume, the application will *not* work.

### 2.3.3 Proxy Settings

If the N2WS server needs an HTTP proxy to connect to the Internet, define the proxy address, port, user, and password. The proxy settings will be kept as the default for the main application. In the N2WS UI, proxy settings are made in the **Proxy** tab of  **Server Settings > General Settings**.

**Note:** Make sure to enable SSH connections (port 22) through your proxy.

### 2.3.4 Force Recovery Mode

You can configure an additional N2WS server, in recovery mode only, by choosing an existing data volume:

- In step 4, choose to use an existing volume and in the **Force Recovery Mode**, select **Yes**.
- In step 5, in the **Existing CPM Data Volume** list, select the volume that holds your backup records.



**Note:** The N2WS server configured for recovery mode will NOT:

- Perform backups.
- Perform Data Lifecycle Management operations.
- Perform Recovery Scenario.
- Have Resource Control management.
- Perform any scheduled operations.

## 2.4 Complete Remaining Fields in N2WS Configuration

In the fifth step, you will fill in the rest of the information needed for the configuration of the data volume for the N2WS Server.



If you chose to create a new volume, you can choose the volume capacity, type, and whether to encrypt.

N2WS

Server Configuration  
N2WS Backup & Recovery (CPM)

Instance Confirmation

End User License Agreement

License and Root User

Data Volume and Proxy

Server Configuration

Register Your Account

Capacity (GiB):

5

EBS Volume Type:

General Purpose SSD (gp2)

Encrypt Volume:

Not Encrypted

Web Server Port:

443

SSL Server Certificate File:

No file chosen

SSL Server Private Key:

No file chosen

Anonymous Usage Reports:

Allow

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

Leave empty for default self-signed certificate

Back

Next

If you chose to use an existing volume, you will see a drop-down volume selection box instead of the volume capacity field:

N2WS

Server Configuration  
N2WS Backup & Recovery (CPM)

Instance Confirmation

End User License Agreement

License and Root User

Data Volume and Proxy

Server Configuration

Register Your Account

Existing CPM Data Volume:

vol-0572ed603db0b2f08 (N2WS - Data Volume)

Web Server Port:

443

SSL Server Certificate File:

No file chosen

SSL Server Private Key:

No file chosen

Anonymous Usage Reports:

Allow

Leave empty for default self-signed certificate

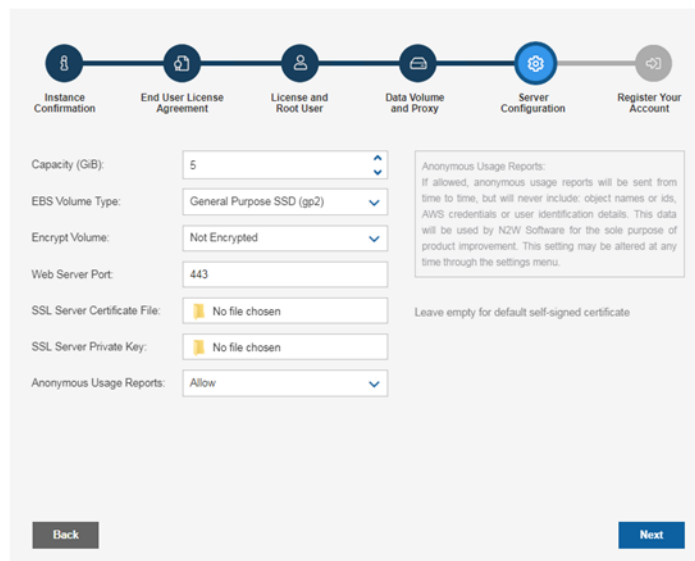
If allowed, anonymous usage reports will be sent from time to time, but will never include: object names or ids, AWS credentials or user identification details. This data will be used by N2W Software for the sole purpose of product improvement. This setting may be altered at any time through the settings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

Back

Next

### 2.4.1 Encrypting a New Data Volume

If you choose a new data volume, you have an option to encrypt CPM user data. You also have the option to encrypt a new data volume if using the silent configuration mode. See section 2.8.



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.

## 2.4.2 Web Server Settings

Port 443 is the default port for the HTTPS protocol, which is used by the N2WS manager. If you wish, you can configure a different port for the web server. But, keep in mind that the specified port will need to be open in the instance's security groups for the management console to work, and for any Thin Backup Agents that will need to access it.

The final detail you can configure is an SSL certificate and private key.

- If you leave them empty, the main application will continue to use the self-signed certificate that was used so far.
- If you choose to upload a new certificate, you need to upload a private key as well. The key cannot be protected by a passphrase, or the application will not work.

**Warning:** If a corrupted SSL certificate is installed, it will prevent the N2WS server from starting.

## 2.4.3 Anonymous Reports Setting

Leaving the Anonymous Usage Reports value as **Allow** permits N2WS to send anonymous usage data to N2W Software. This data does not contain any identifying information:

- No AWS account numbers or credentials.
- No AWS objects or IDs like instances or volumes.
- No N2WS names of objects names, such as policy and schedule.

It contains only details like:

- How many policies run on an N2WS server
- How many instances per policy
- How many volumes



- What the scheduling is, etc.

## 2.5 Registering and Finalizing the Configuration

After filling in the details in the last step, you are prompted to register. This is mandatory for free trials and optional for paid products.

Select **Configure System** to finalize the configuration. The configuration will take between 30 seconds and 3 minutes for new volumes, and usually less for attaching existing volumes. After the configuration is complete, a 'Configuration Successful – Starting Server ...' message appears. It will take a few seconds until you are redirected to the login screen of the N2WS application.

If you are not redirected, refresh the browser manually. If you are still not redirected, reboot the N2WS server via AWS Management Console, and it will come back up, configured, and running.

## 2.6 Configuration Troubleshooting

Most inputs you have in the configuration steps are validated when you select **Next**. You will get an informative message indicating what went wrong.





A less obvious problem you may encounter is if you reach the third step and get the existing volume select box with only one value in it: **No Volumes found**. This can arise for two reasons:

- If you chose to use an existing volume and there are no available EBS volumes in the N2WS Server's AZ, you will get this response. In this case, you probably did not have your existing data volume in the same AZ.

To correct this:

- Terminate and relaunch the N2WS server instance in the correct zone and start over the configuration process, or
- Take a snapshot of the data volume, and create a volume from it in the zone the server is in.
- If there is a problem with the credentials you typed in, the "No Instances found" message may appear, even if you chose to create a new data volume. This usually happens if you are using invalid credentials, or if you mistyped them. To fix, go back and enter the credentials correctly.

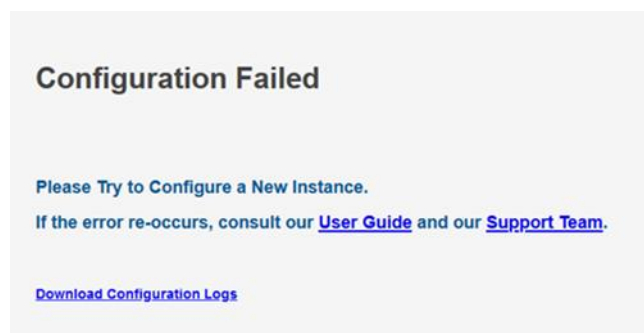
In rare cases, you may encounter a more difficult error after you configured the server. In this case, you will usually get a clear message regarding the nature of the problem. This type of problem can occur for several reasons:

- If there is a connectivity problem between the instance and the Internet (low probability).
- If the AWS credentials you entered are correct, but lack the permissions to do what is needed, particularly if they were created using IAM.
- If you chose an incorrect port, e.g. the SSH port which is already in use.
- If you specified an invalid SSL certificate and/or private key file.

If the error occurred after completing the last configuration stage, it is recommended that you:

1. Terminate the N2WS server instance.
2. Delete the new data volume (if one was already created).
3. Try again with a fresh instance.

If the configuration still fails, the following message will display. If configuring a new instance does not solve the problem, see the *User Guide* and contact [N2W Software Support Team](#). To access configuration error details, select **Download Configuration Logs**.





## 2.7 Modifying the Server Configuration

If you need to change the configuration of your N2WS server after it has already been created, you may need to:

- Change the time zone
- Reset the N2WS root user password
- Change SSL credentials
- Change the HTTPS port

The process to make these changes is to terminate the current N2WS server instance and create a new one. After you terminate the N2WS server, the data volume becomes available. Configure the server as needed and connect to the old (existing) data volume.

**Note:** Remember to launch the new server in the same AZ.

For the N2WS root user, you may change the email or the password. The username of the root user cannot be changed. If, during the configuration process, you type a different username than the original, N2WS will assume you forgot the root username. In that case, the username will not change, and a file named `/tmp/username_reminder` will be created on the N2WS server. It will contain the username. You can connect to N2WS server using SSH to view this file. See section 7.1.

## 2.8 Configuring N2WS in Silent Mode

Launching an EC2 instance in AWS can optionally be set with User Data. See the description of how such user data can be utilized at

<https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/user-data.html>.

The N2WS instance can also use this user data when launching.

- If the string 'CPMCONFIG' exists in the user data text, then the text following it is used for the CPM configuration.
- The extraction is until the string 'CPMCONFIGEND' or the end of the data.
- The extracted text is assumed to be in '.ini' file format.
- The extracted configuration text of the new N2WS instance should start with a [SERVER] section, followed by the configuration details.
- For the relevant `time_zone` parameter value, see Appendix C

Following is an example of the whole script:

```
[any-script-before-cpmconfig]

CPMCONFIG

[SERVER]

user=<username for the N2WS user>

password=<password>

volume_option=<new or existing>
```



```
volume_size=<in GB, used only for the new volume option>

volume_id=<Volume ID for the data volume, used only in the existing
volume option>

volume_type=<set your storage performance and cost.
The default is "gp3". It can be set to "io1", "io2", "gp2", or "gp3">

snapshot_id=<snapshot ID to create the data volume from, used only with
the existing volume option, and only if volume_id is not present>

encryption_key=<encrypt user-data volume by setting the ARN of the
KMS key. used only for the new volume option>

time_zone=<set N2WS server's local time.
The default time zone is GMT. See Appendix C for available time zones.>

allow_anonymous_reports=<send anonymous usage data to N2W Software.
The default is "False">

force_recovery_mode=<allow additional N2WS server to perform recovery
operations only. The default is "False". If it set to "True" - it
requires volume_option=existing>
CPMCONFIGEND

[any-script-after-cpmconfig]
```

Additionally, if you need the N2WS server to connect to the Internet via an HTTP proxy, add a proxy section:

```
[PROXY]

proxy_server=<address of the proxy server>

proxy_port=<proxy port>

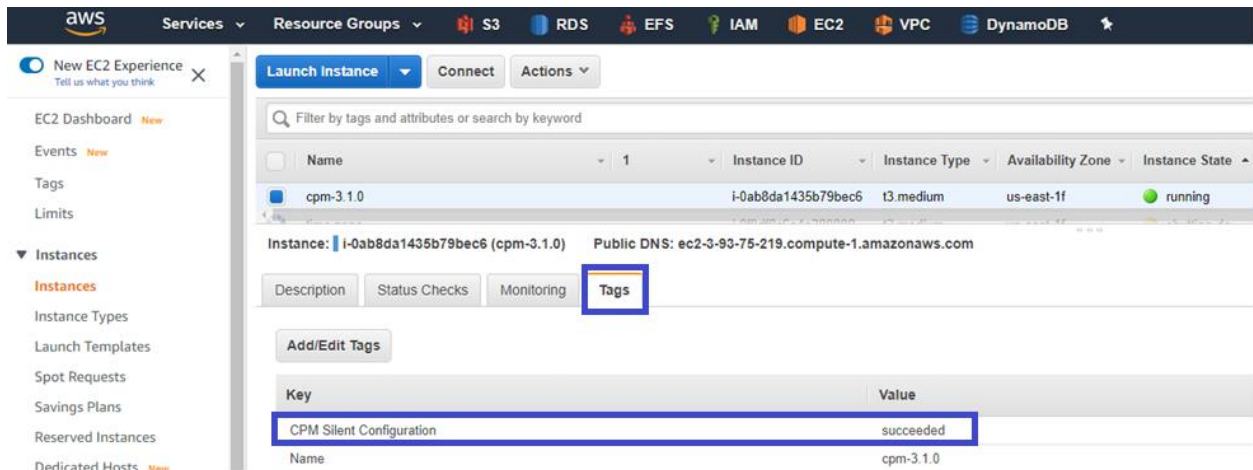
proxy_user=<user to authenticate, if needed>

proxy_password=<password to authenticate, if needed>
```

The snapshot option does not exist in the UI. It can be used for automation of a Disaster Recovery (DR) server recovery. Additionally, if you state a volume ID from another AZ, N2WS will attempt to create a snapshot of that volume and migrate it to the AZ of the new N2WS server. This option is for DR only.

**Note:** You are not required to select the license terms when using the silent configuration option, since you already approved the terms when subscribing to the product on AWS Marketplace.

After executing the configuration, on the AWS **Instances** page, select the **Tags** tab. If the **CPM Silent Configuration** key value equals 'succeeded', then the CPM instance was successfully launched with the user data configured in silent mode.

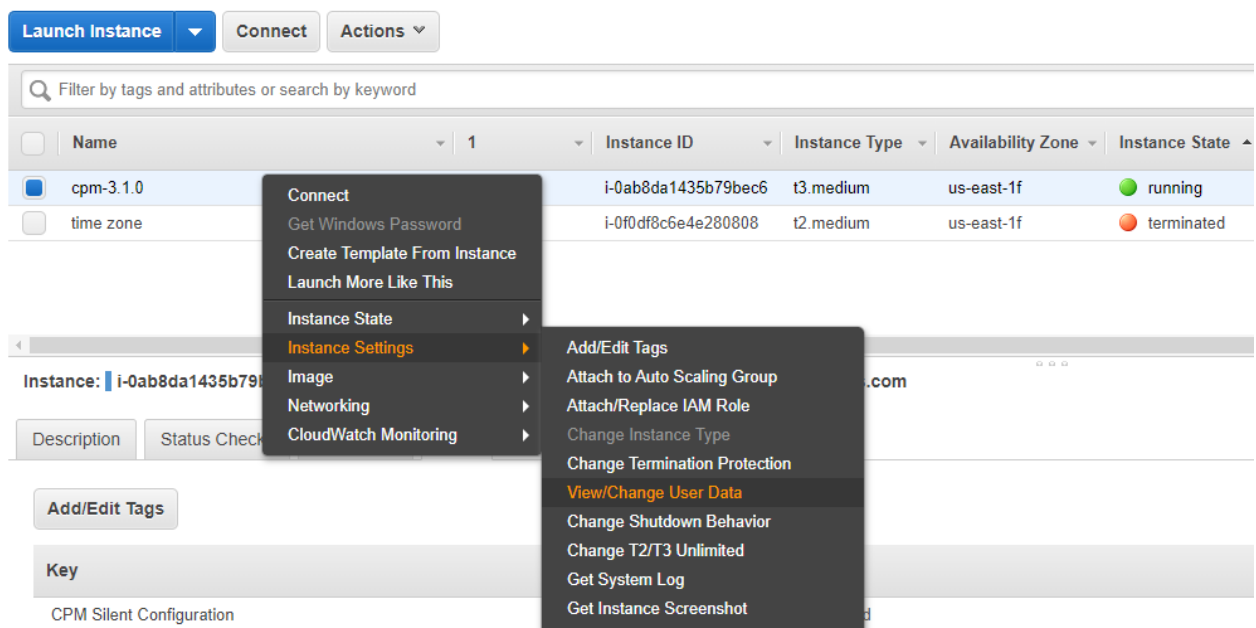


The screenshot shows the AWS Management Console interface. On the left, the 'Instances' menu is expanded, and 'Instances' is selected. The main panel displays a list of EC2 instances. The instance 'cpm-3.1.0' with ID 'i-0ab8da1435b79bec6' is highlighted. Below the list, the 'Tags' tab is selected, showing a table with one tag: 'CPM Silent Configuration' with the value 'succeeded'.

Key	Value
CPM Silent Configuration	succeeded

**To verify configuration user data:**

1. In AWS, select the CPM instance.
2. In the right-click menu, select **Instance Settings**, and then select **View/Change User Data**.



The screenshot shows the AWS Management Console interface with the right-click context menu open for the 'cpm-3.1.0' instance. The 'Instance Settings' option is highlighted, and its sub-menu is displayed, showing 'View/Change User Data' as the selected option.

Name	Instance ID	Instance Type	Availability Zone	Instance State
cpm-3.1.0	i-0ab8da1435b79bec6	t3.medium	us-east-1f	running
time zone	i-0f0df8c6e4e280808	t2.medium	us-east-1f	terminated



**View/Change User Data** ✕

Instance ID: i-0ab8da1435b79bec6

User Data:

```
CPMCONFIG
[SERVER]
user=demo
password=1
volume_option=new
time_zone=Asia/Jerusalem
```

To edit your instance's user data you first need to stop your instance.

Cancel Save

## 2.9 Maintaining N2WS

To keep your N2WS running at its highest efficiency, N2WS will occasionally send you notification of the existence of a patch through an Announcement or an email. Download the patch according to the notification instructions.

**To install patches:**

1. Select  **Server Settings** and then select **Patches**.

2. Select **Choose file** to select the patch file.
3. Select **Upload and Install**.

## 2.10 Using the AWS Key Management Service

The AWS Key Management Service allows you to securely share custom encryption keys between accounts. For details on enabling shared custom keys, see <https://aws.amazon.com/blogs/security/share-custom-encryption-keys-more-securely-between-accounts-by-using-aws-key-management-service/>.

The use of custom keys is required in the following cases:

- Authentication of `cpmuser` to N2WS server using a non-default certificate with a private key.

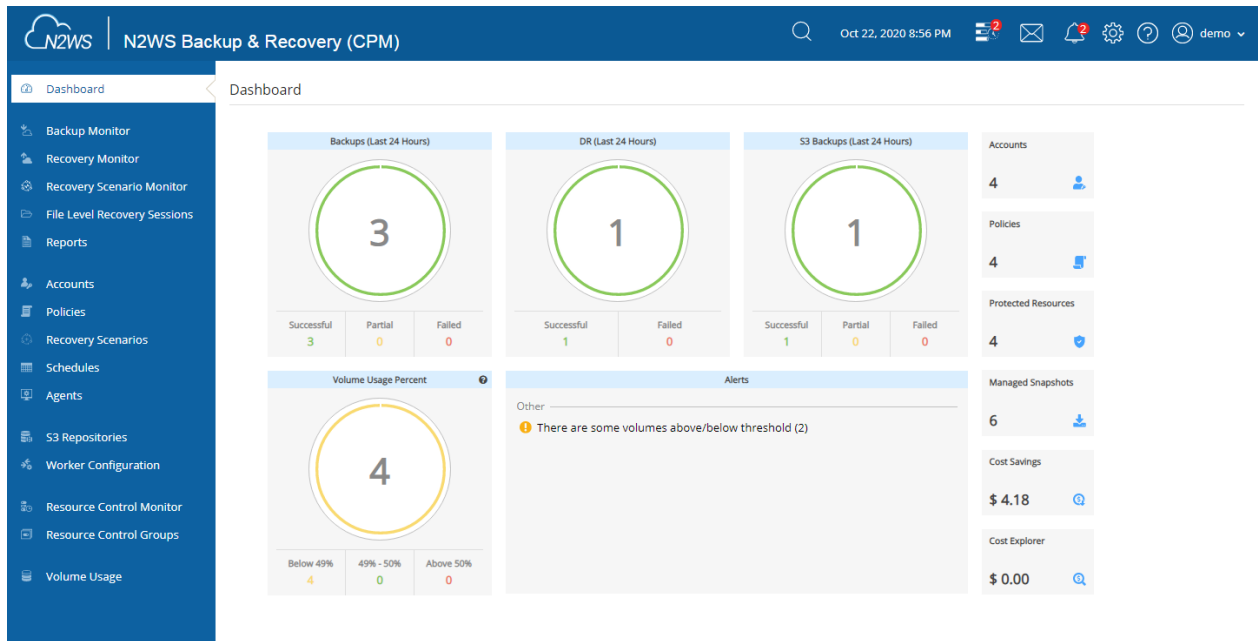


- Encrypting new volumes.
- Associating an account for File Level Recovery.
- Authentication of IAM User.
- Running scripts.
- Performing Recoveries, DR, and Cross-Account activities for RDS, EC2, and EFS resources.




## 3 Start Using N2WS

N2WS opens to the Dashboard – an overview of recent backups, recoveries, alerts, resources, and costs.



Depending on your device resolution, the **Alerts** tile may not appear in the Dashboard.

Regardless of resolution, all Alerts are available by selecting  in the toolbar.

The first step in using N2WS is to associate one or more of your cloud accounts with N2WS.

- With AWS accounts you will be able to:
  - Perform backup and recovery operations for a variety of AWS resource types
  - Perform Disaster Recovery (DR)
  - Copy to S3
  - Manage volume usage
  - Monitor costs and savings
- With Azure accounts you will be able to:
  - Perform backup and recovery operations for Azure VMs and Disks. See section 26 for complete details.

### 3.1 Associating an AWS Account

To associate an AWS account for Recovery, you will need to either:

- Enter AWS credentials consisting of an access key and a secret key, or
- Use an IAM role, either on the N2WS server instance or cross-account roles.

Following are the steps to associate an N2WS account with an AWS account:



1. To manage your users and roles and obtain AWS credentials, go to the IAM console at <https://console.aws.amazon.com/iam/home?#users>
  - a. Follow the directions to either add a new account or view an existing account.
  - b. Capture the AWS credentials.
2. If the AWS account will be operating in special regions, such as China Cloud or US Government Cloud, see section 3.1.5 *before* adding the account in N2WS.
3. To associate the AWS account with an N2WS account, go to N2WS:
  - a. In the left panel, select the Accounts tab.
  - b. In the + New menu, select AWS account.
  - c. Complete the fields, entering the required information for the Account Type and Authentication method.

### 3.1.1 Account Type

If you are using the Advanced or Enterprise Edition or a free trial, you will need to choose an account type.

- The **Backup** account is used to perform backups and recoveries and is the default 3333.
- The **DR** account is used to copy snapshots to as part of cross-account functionality.
  - You choose whether this account is allowed to delete snapshots. If the account not allowed to delete snapshots when cleaning up, the outdated backups will be tagged. Not allowing N2WS to delete snapshots of this account implies that the presented IAM credentials do not have the permission to delete snapshots.
  - Enable **Use Secured DR Account** to select specific permissions for resource types and activities for prohibition. The **Secured DR Account Check** operation warns the N2WS user about the existence of Prohibited Permissions in IAM policies of the DR account. Turn on the **Check Secured DR Account Periodically** toggle to perform a periodic





check of whether the DR account backups are compromised by the presence of the prohibited permissions. For details about periodic and immediate checking of the account, see section 3.1.3.

For accounts operating in special regions, in the **AWS Cloud Type** list, select the type of AWS cloud. See section 3.1.5.

### 3.1.2 Authentication

N2WS Supports three methods of authentication:

- **IAM User** - Authentication using IAM credentials, access and secret keys.

Warning: Using IAM User credentials is not recommended as they are less secure than using IAM roles.

- **CPM Instance IAM Role** – If an IAM role was assigned to the N2WS server at launch time or later, you can use that IAM role to manage backups in the same AWS account the N2WS server is in.

Note: Only the root/admin N2WS user is allowed to use the IAM role.

- **Assume Role** – This type of authentication requires another AWS account already configured in N2WS. If you want to use one account to access another, you can define a cross-account role in the target account and allow access from the first one. The operation of using one account to take a role and accessing another account is called **assume role**.

Note: You can add as many AWS accounts as your N2WS edition permits.

#### To allow account authentication using Assume Role in N2WS:

1. In the **Authentication** box, choose **Assume Role**.
2. In the **Account Number** box, type the 12-digit account number, with no hyphens, of the target account.
3. In the **Role to Assume** box, type the role name, not the full Amazon Resource Name (ARN) of the role. N2WS cannot automatically determine what the role name is, since it is defined at the target account, which N2WS has no access to yet.
4. The **External ID** box is optional unless the cross-account role was created with the **3rd party** option.
5. In the **Assuming Account** list, choose the account that will assume the role of the target account.



N2WS Backup & Recovery (CPM)

Accounts > New Account

Name:  User:  + New

Account Type:

Authentication:

Account Number:  Role to Assume:  External ID:

Assuming Account:

☐ Scan Resources

☒ Capture VPCs

Save Cancel

If you are the root user or independent user and have managed users defined, an additional selection list will appear enabling you to select the user.

6. Select **Scan Resources** to include the current account in tag scans performed by the system.

Once **Scan Resources** is **Enabled**:

- a. In the Scan Regions list, select the regions to scan. To select all regions, select the checkbox at the top of the list. To filter regions, start typing in the search box.

☒ Scan Resources

Scan Regions

18 Regions Selected

☐ us

☒ US East (N. Virginia)

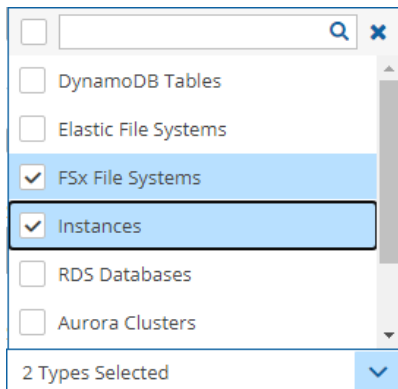
☒ US East (Ohio)

☒ US West (Oregon)

☒ US West (N. California)

- b. In the Scan Resource Types list, select the types of resources to scan. Select the top checkbox for all, or use the search box to filter types.

**Note:** Scanning only specific resource types can reduce tag scan processing time and is useful when user permissions are limited to certain resource types.



7. The **Capture VPCs** option defaults to enabled. Clear **Capture VPCs** to disable for this account. See section 23.

### 3.1.3 Secured DR Account

The DR account is a secure entity. In N2WS version 3.2.0, N2WS has taken the security to a higher level with the N2WS Secured DR feature, which hardens N2WS security. It allows the N2WS user to better protect the backups of his resources by making sure that backups kept in the DR account are not compromised through the use of unwanted permissions. N2WS can perform a periodic check to alert the user about IAM Users/Roles of the DR account that have unwanted IAM permissions.

The risk of unwanted permissions is demonstrated in the following example:

- If an IAM Role of a DR account has an attached policy that includes the “**ec2:DeleteSnapshot**” permission, the snapshot is in danger of getting deleted.

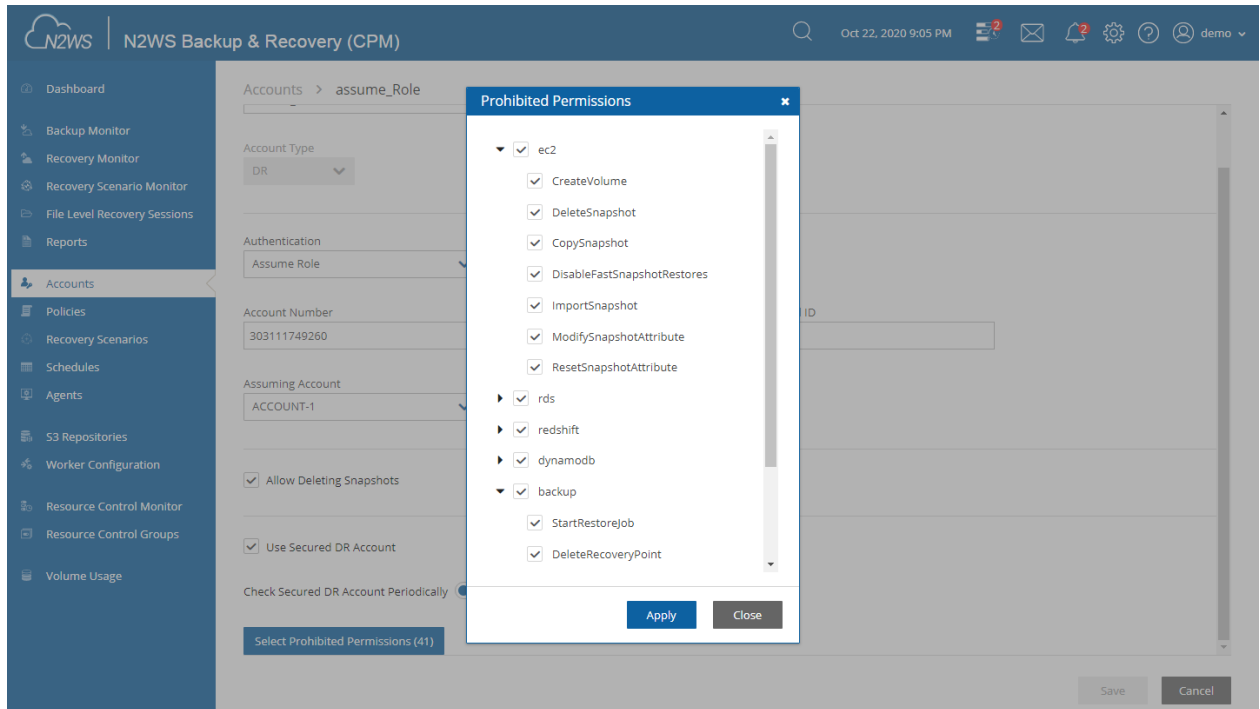
The N2WS user has the flexibility of defining risky permissions for an account.

Name	Account Type	Authentication	Policies
ACCOUNT-1	Backup	CPM Instance IAM Role	4 policies
ACCOUNT-2	Backup	CPM Instance IAM Role	
ACCOUNT-3	Backup	CPM Instance IAM Role	
<input checked="" type="checkbox"/> assume_Role	DR (Secured)	Assume DR-Role	



### To define a 'Secured' DR Account and prohibited permissions:

1. In the **Accounts** tab, select a DR account and then select **Edit**.
2. Select **Use Secured DR Account** and then select **Prohibited Permissions**. By default, *all* permissions are prohibited.
3. For each type of target or action, clear the permissions to be 'allowed', and then select **Apply**.
4. Select **Save**.



N2WS will check for policies whose account has permissions defined as 'prohibited' and list them as compromised in the check log. The user can then generate the Secured DR Account Report to identify the accounts and policies at risk. See section 3.1.4.

The required IAM permissions for the DR account to check its users and roles are:

- iam:ListUsers
- iam:ListRoles
- iam:SimulatePrincipalPolicy
- iam:ListAccessKeys, for authentication

**Note:** Removing permissions may compromise the safety of N2WS backups. If permissions are removed, a warning alert for the secured DR account will appear as a potential backup risk.





### 3.1.4 Checking Secured DR Accounts



Two reports are available for checking Secured DR Accounts. If the **Check Secured DR Account 'Show Log'** indicates that there are compromised permissions, then you can run the **Generate Secured DR Report** to view the policies and users with the compromised permissions.

- **Check Secured DR Account** – Creates a summary status log (**Show Log**) showing the number of policies and accounts with compromised permissions. The check can be run periodically throughout the day or run immediately.
- **Secured DR Report** - A detailed list of the AWS policies and the prohibited permissions that are compromised for an account of the current user.

#### To check Secured DR Accounts:

1. In the **General Settings** tab, select the **Security** tab.
2. To check the DR accounts periodically during the day, select **Check Secured DR Account**, select an hourly interval in the **Secured DR Check Interval** list, and then select **Save**.
3. To run the report immediately, select **Check Secured DR Account Now** and **confirm**.
  - a. To view the progress and status of the Secured DR Check Settings operation, select **Background Tasks**  in the toolbar. Background Tasks only appears after the first Check Secured DR Account or Clone VPC operation. Select **View All Tasks**.
4. To view the log, select **Show Log**. To download, select  **Download Log** in the upper right corner of the log. The `Secured_DR_Account_check_log_<date>_<time>.csv` file contains Log Time, security Level Type, and Log Message.

#### To generate Secured DR Account reports:

1. In the **Accounts** tab, select a DR (Secured) account.
2. To check the status of the Secured DR Account periodically during the day:
  - a. Select  **Edit**.
  - b. If not enabled, select **Use Secured DR Account**.
  - c. Turn on the **Check Secured DR Account Periodically** toggle.
  - d. To view the interval for checking Secured DR Accounts, select **Secured DR Check Settings**.
  - e. Select **Save**.
3. To run the detailed report, in the **Accounts** tab list, select a DR (Secured) Account and then select  **Generate Secured DR Report**.

The downloaded file (`Secured_DR_Account_check_<account>_<date>_<time>.csv`) contains a list with the following data:

- AWS IAM Policy
- AWS Policy's User/Role
- Compromising Permission

### 3.1.5 Special Regions

If the account that you are about to create will be operating with non-standard AWS regions, such as China or US government clouds, it is necessary to first contact N2WS Support (see



section 3.6) to adjust the N2WS configuration. After N2WS Support has made the adjustment, when you create the N2WS account, you will be prompted for the **AWS Cloud Type**.

N2WS Backup & Recovery (CPM)

Accounts > New AWS Account

Name:

User:  + New

Account Type:

AWS Cloud Type:

☐ Scan Resources

The type of cloud will appear in the **Cloud** column in the list of policies.

N2WS Backup & Recovery (CPM)

Accounts

Name	Cloud	Account Type	Authentication
std	AWS	Backup	CPM Instance IAM Role
gov	AWS (US GovCloud)	Backup	CPM Instance IAM Role
china	AWS (AWS China)	Backup	CPM Instance IAM Role
assume-gov	AWS (US GovCloud)	Backup	Assume DR-Role

## 3.2 Associating an Azure Account

To associate an Azure account with an N2WS account, see section 26.

## 3.3 Deleting Accounts

There are two options when deleting an account:

- Delete the CPM account and all its resources and metadata, BUT leave the AWS account and all its related data on AWS. Select **Delete**.
- Delete the CPM account and all its resources and metadata, AND delete the AWS account and all its data, including S3 Repositories. Select **Delete Account and Data**.



In each case, you will be provided with an explanation of the scope of the delete and a prompt to confirm. In the **Delete Account** confirmation dialog box, type the phrase '**delete me**' and then select **Delete**.

The dialog box is titled "Delete Account" and contains the following text:

Are you sure you want to delete account 'a1'?

All related policies, backups, scheduled reports, resource control groups, etc., will be deleted along with it

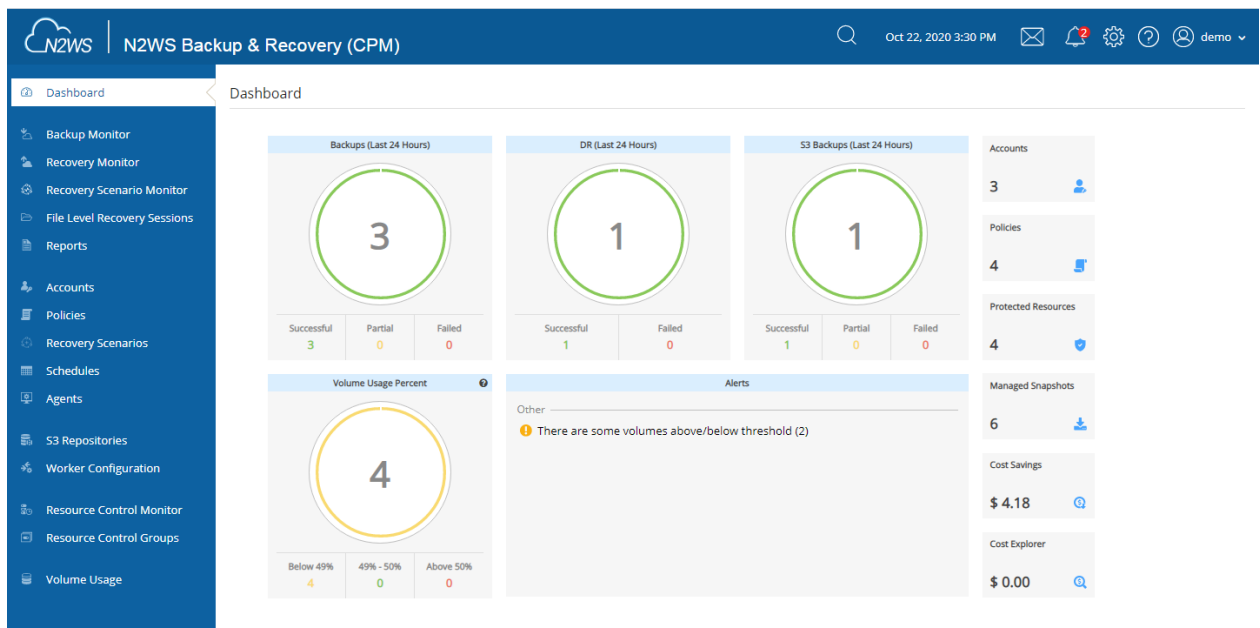
In order to confirm deletion of the selected accounts, please type the phrase '**delete me**'

At the bottom right, there are two buttons: "Delete" and "Cancel".

## 3.4 Managing Volume Usage


As part of starting to use N2WS, you might want to enable alerts for when volume usage exceeds high and low thresholds. Volume usage reporting can become an integral part of the Dashboard.

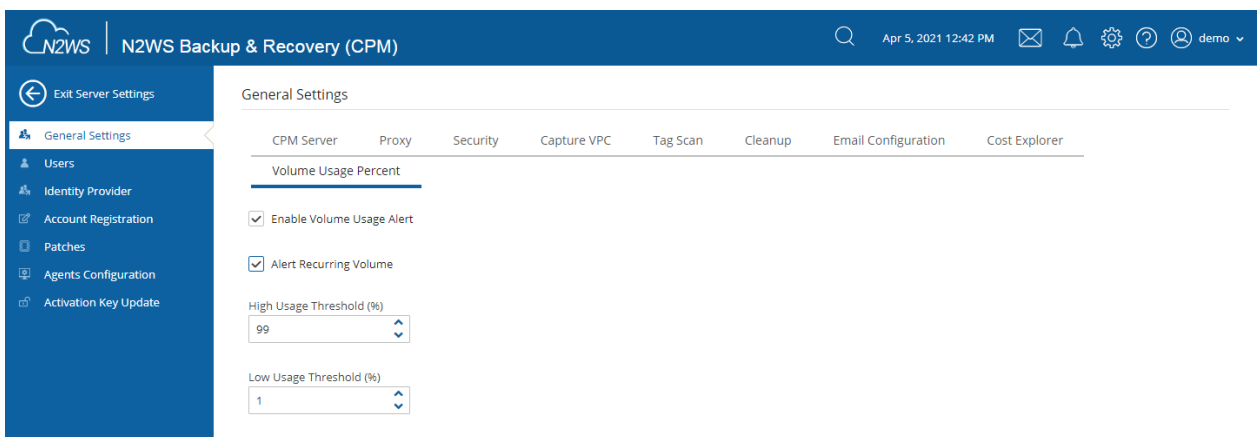
If the **Volume Usage Alert** is enabled, a generic message for volumes exceeding the threshold will appear on the Dashboard Alerts tile. In the **Volume Usage Percent** tile, the number of volumes below, within, and above the thresholds are shown.





## To report volume usage:

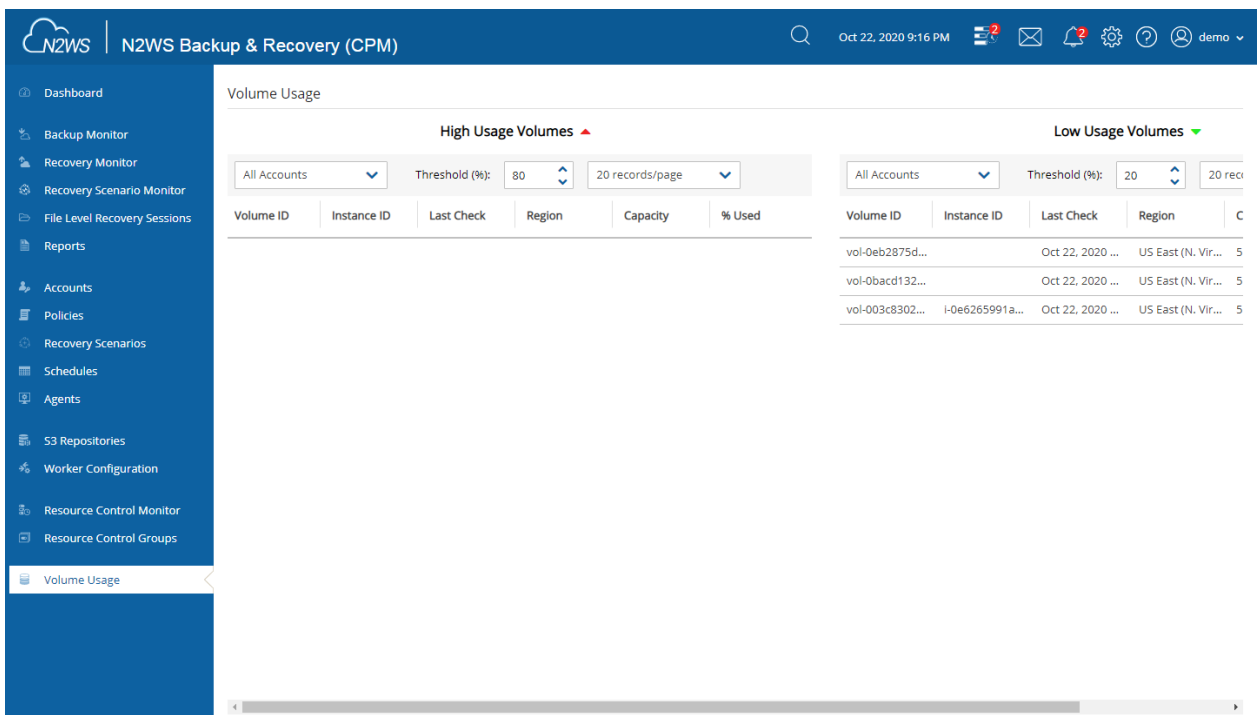
1. In **General Settings** of the  **Server Settings**, select the **Volume Usage Percent** tab.
2. Select **Enable Volume Usage Alert**.
3. Enter a percentage in the **High Usage Threshold** and **Low Usage Threshold (%)** boxes for when to initiate an alert.
4. To enable an alert for each time a backup is run on a volume with usage exceeding the **High** or **Low Usage Threshold**, select **Alert Recurring Volume**. The recurring alert is turned off by default, and the alert initiated only when there is a change in the usage or a change in the threshold that has caused the initiation.
5. Select **Save**.



The screenshot shows the 'General Settings' page for 'N2WS Backup & Recovery (CPM)'. The 'Volume Usage Percent' tab is selected. The settings include:

- ☒ Enable Volume Usage Alert
- ☒ Alert Recurring Volume
- High Usage Threshold (%): 99
- Low Usage Threshold (%): 1

If there is a volume usage alert, select the **Volume Usage** tab in the main screen to view the specific volume and percentage which initiated the message.



The screenshot shows the 'Volume Usage' tab in the 'N2WS Backup & Recovery (CPM)' interface. It displays two tables: 'High Usage Volumes' and 'Low Usage Volumes'.

**High Usage Volumes** (Threshold: 80%)

Volume ID	Instance ID	Last Check	Region	Capacity	% Used
-----------	-------------	------------	--------	----------	--------

**Low Usage Volumes** (Threshold: 20%)

Volume ID	Instance ID	Last Check	Region	Capacity	% Used
vol-0eb2875d...		Oct 22, 2020 ...	US East (N. Vir...		5
vol-0bacd132...		Oct 22, 2020 ...	US East (N. Vir...		5
vol-003c8302...	i-0e6265991a...	Oct 22, 2020 ...	US East (N. Vir...		5





You can evaluate whether additional volumes are nearing the alert thresholds by adjusting the **High Usage** and **Low Usage Thresholds** in the Volume Usage screen and selecting the **Enter** key.

If a volume's usage changes from high to low, or low to high, there will be an additional alert for that volume.

Notes: Changing the usage thresholds in the **Volume Usage** tab does not change the alert thresholds set in the **General Settings** tab.

Enabling and configuring usage thresholds while adding a user will **override** the alert thresholds set in the **General Settings** tab.

### 3.5 Importing Non-N2WS Backups to S3

You can quickly lower your storage costs for existing non-N2WS backups by moving them to a more economical S3 storage class. After successfully importing your snapshots with the AnySnap Archiver feature, you can then safely delete the original snapshots.

Note: Currently, the Import to S3 feature supports only EBS snapshots.

Importing consists of the following steps:

1. In AWS, apply custom tags to backups to import.
2. In N2WS, create an S3 Repository. See section 21.1.
3. In the **Policies** tab, create an Importer Policy with identical custom tags. The maximum number of custom tags per policy is 20.
4. Verify a scan of the snapshots to import by executing **Import Dry Run**.
5. Start the import. Review the progress in the **Policies** tab.
6. If necessary, pause the import to change the S3 configuration or to postpone the migration process. See section 21.2.1.
7. Review the import process **Show Imported Backups** or **Show Import Log** for snapshots imported to S3.
8. After the import process, N2WS attaches an `import_policy_name` tag with the name of the policy to the snapshot. The tag excludes the snapshot from additional importing.
  - a. If necessary, to restart the import, remove the `import_policy_name` tag using the AWS Snapshot console.
  - b. For bulk tag removals, use the AWS Resource Group service. Verify that you have the correct tag key/value pair.

The **Import Dry Run** scans all AWS snapshots defined in the Importer Policy and marks for import those meeting the following criteria:

- Snapshot date is within the Start/End Time Range.
- AWS tag values equal the Import by Tags values defined in the Policy.
- Snapshot date is the latest within the Record Duration. N2WS marks for import the last backup made within the number of hours defined as record duration. If the duration is set



for 2 and there are 3 snapshots with import tags within a 2-hour period, only the last snapshot will be imported.

### 3.5.1 Creating an Importer Policy

**Note:** Expiration of storage for S3 snapshots is computed from their EBS snapshot creation date. The retention period is determined by the **Keep backups in S3 for at least** configuration value. If the retention period is set for 12 months and there are 2 imported snapshots, one 11 months old and the other 10 months old, the 11-month-old snapshot will be deleted from S3 in 1 month and the other in 2 months.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation links: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies (selected), Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Policies' and includes a search bar, filters for 'All Accounts' and 'All Schedules', and a '20 records/page' dropdown. Below these are action buttons: New, Edit, Delete, Run ASAP, Backup Times, Stop S3 / Archive Operations, Delete Snapshots, New Importer Policy, and Refresh. A table lists existing policies:

<input type="checkbox"/>	Name	Account	Enabled	Backup Generations	Schedules	Cost (\$)
<input type="checkbox"/>	CE-LINUX-111	a1	Yes	30		N/A
<input type="checkbox"/>	CE-LINUX-222	a1	Yes	30		N/A
<input type="checkbox"/>	CE-LINUX-333	a1	Yes	30		N/A
<input type="checkbox"/>	CE-WINDOWS	a1	Yes	30		2.86
<input type="checkbox"/>	cpmdata	a1	Yes	30		N/A
<input type="checkbox"/>	Importer-1	a1				N/A

At the bottom, it shows '0 of 6 items selected'.

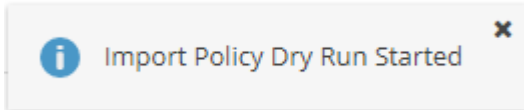
1. In the **Policies** tab, select **New Importer Policy**.
2. In the **Policy Details** tab:
  - a. Enter the policy Name, and select the User and Account.
  - b. The optional Description box would be an excellent place to identify details of the import.
3. In the **Import Parameters** tab:
  - a. Select the Start/End Source Data Time Range. End Time defaults to Up to Import Start.
  - b. In the Backup Record Interval (Hours) list, select the number of hours from which to select the latest snapshot. For example, if you select 6 and there are 4 snapshots within a period of 6 hours, only the last one of the 4 snapshots is imported.
  - c. Enter at least 1 Import by Tags. All regions in the specified account will be scanned.
4. In the **S3 Storage Configuration** tab, there must be at least 1 retention condition:
  - a. In the Keep backups in S3 for at least lists, select a minimum retention period.
  - b. To move S3 backups for archival in Glacier, turn on the Archive to Glacier toggle and select the archiving frequency and retention period.
  - c. In the Target repository list, select the repository to import to.
  - d. In the S3 Storage class list, select the storage type for this import. Default is Standard.



- e. If Archive to Glacier is enabled, select an Archive Storage Class.
5. Select **Save**. After saving, the **Import Dry Run** and **Start Import** buttons are enabled, and the import status in the far-right column is Not Started.

### 3.5.2 Testing Import with Dry Run

After creating the Importer policy, select the policy, and then select **Import Dry Run**. In the

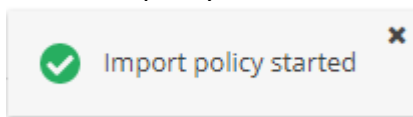
upper right corner, the Dry Run Started message  appears. Shortly after the Dry Run completes and the Started message has automatically closed, the `Import Snapshots Dry Run [policy name] yyyy mm dd hh mn.CSV` file downloads. The report contains the list of the snapshots scanned and whether they meet the criteria for import. Fields include Backup Record number, CPM Account number, AWS Account number, Import (Yes or No), Region, Type (Resource), Volume, Snapshot ID, Start Time, Volume Size in GB, and the Dry Run Parameters.

Review and make adjustments to the Import policy or tags as needed.

### 3.5.3 Running the Migration

**To perform the actual import:**

1. Select the policy, and then select **Start Import**. The Import policy started message



appears.

2. To view progress details of the import process:
  - a. Select Show Import Log.
  - b. In the far-right column, view the migration status symbol. Refer to the table of status symbols in section 3.5.4.
3. If it is necessary to pause the import to S3, in the **Policies** tab, select **Pause Import**. To resume, select **Resume Import**, and the process will restart the copy of the snapshot from scratch.
4. If it is necessary to stop the import to S3, in the **Backup Monitor**, when the **Lifecycle Status** is 'Storing in S3 ...', select **Abort Copy to S3**. To resume, in the **Policies** tab, select **Resume Import**, and the process will restart the copy of the snapshot from the beginning.
5. In the **Backup Monitor**, you can view the final status of the import in the **Lifecycle Status** column. For statuses other than **Stored in S3**, hover over the symbol for a description of the status.
6. In the **Policies** tab, when the import is finished:
  - a. Select Show Imported Snapshots.
  - b. To lower costs, you can Delete EBS Snapshots. The icon is active only if the import was 100% successful.



**Note:** Before deleting any snapshots, it is recommended that you perform a test recovery for each region/account that you imported from to verify that everything is working as expected.

Snapshots imported to S3 are included in the Backup and Snapshot reports. See section [17.7](#).

### 3.5.4 Migration Status Symbols

During the actual migration, you can monitor the progress in the **Policies** tab by viewing the following migration status symbol in the far-right column. A symbol indicates that the policy is an importer policy, and its color indicates its migration status.

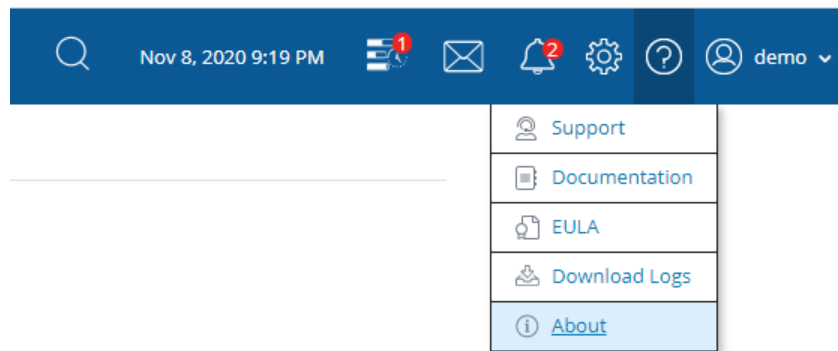
**Note:** To view status details, hover over the symbol.

Symbol	Importer Policy Migration Status	Next Actions
	Not started	<b>Start Import</b>
	Scanning for custom tags, import criteria	<b>Show Import Log</b>
	Copying	<b>Show Import Log</b>
	Completed without finding snapshots	Reconfigure; <b>Import Dry Run</b>
	Copy completed	<b>Show Imported Snapshots</b> If needed, <b>Delete EBS Snapshots</b>
	Deleting EBS snapshots	<b>Show Import Log</b>
	Moved to S3	<b>Show Imported Snapshots</b>
	Pausing	If needed, <b>Abort Copy to S3</b>
	Paused	<b>Resume Import</b> to continue, or <b>Abort Copy to S3</b> to stop
	Failed	<b>Show Import Log</b>
[No symbol]	Indicates a backup policy	

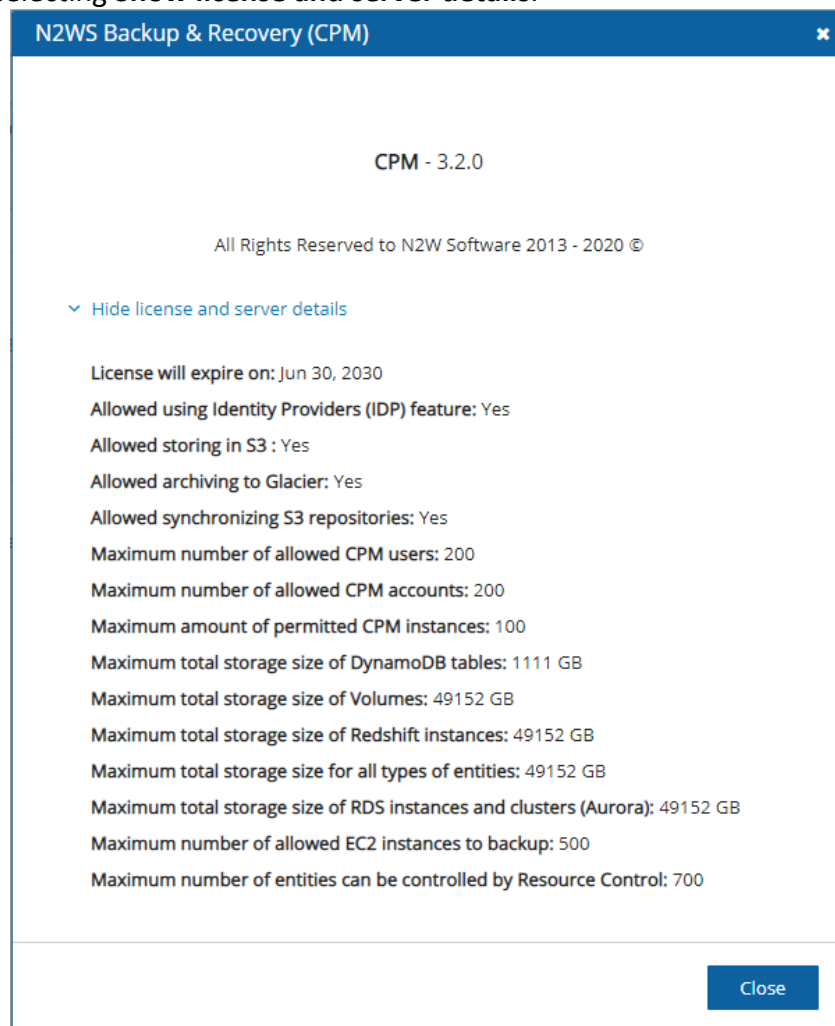
## 3.6 N2WS Help and Support

You can email support issues to [N2W Software support](#).

For online help and support, select **Help & Support** in the upper right toolbar.




You can view your current privileges on the N2WS licensed server or activation key by selecting **About** and then selecting **Show license and server details**.



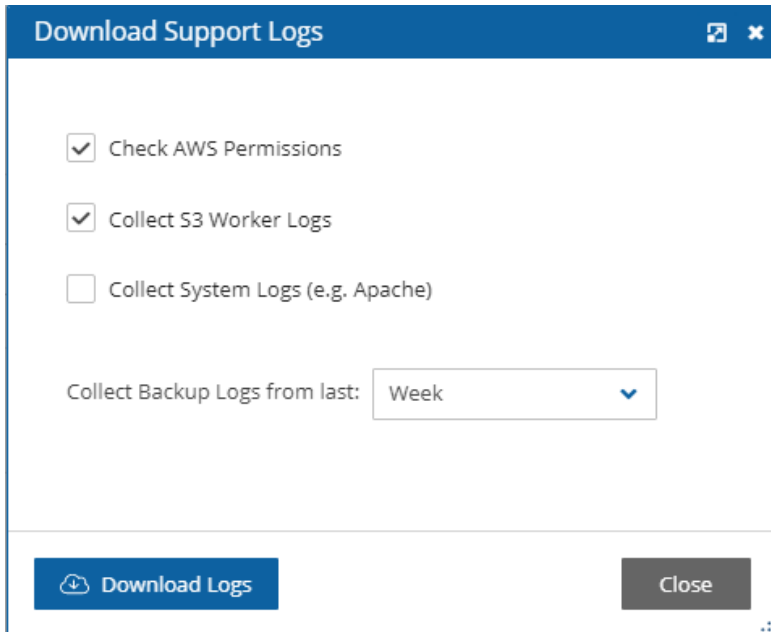
For self-service support using the N2WS knowledge base, documentation, how-to guides, and tutorial videos go to the N2WS Support Center by selecting **Support**.

To go directly to the docs and guides, select **Documentation**.



To collect and download support logs, select **Download Logs**. In the **Download Support Logs** dialog box, select the relevant logs and time frame, and then select  **Download Logs**.

- **Check AWS permissions** – Against the required permissions for AWS services and resources.
- **Collect S3 Worker Logs** – When S3 support is needed.
- **Collect System Logs** – For comprehensive system debugging.
- **Collect Backup Logs from Last** - Select Day, Week, or Month in the list.



**Note:** N2WS support covers all N2W Software users including AWS Outposts.



## 4 Defining Backup Policies

The backbone of the N2WS solution is the backup policy. A backup policy defines everything about a logical group of backed-up objects. A policy defines:

- What will be backed up - **Backup Targets**.
- How many generations of backup data to keep
- When to back up – **Schedules**.
- Whether to use backup scripts.
- Whether VSS is activated (Windows Servers 2008, 2012, 2016, and 2019 only).
- Whether backup is performed via a backup agent (Windows only)
- The retry policy in case of failure.
- DR settings for the policy.
- Lifecycle events: Copy to S3, Archive to Glacier

The following sections explain the stages for defining an N2WS policy and its schedule. Schedule definition is addressed first as it one of the attributes of a policy and Scheduled Reports.

For Azure policy definition, backup, and recovery, see section 26.

N2WS Backup & Recovery (CPM)

Search Policies

All Accounts All Schedules 20 records/page Cost Period (Last Month)

+ New Edit Delete Run ASAP Backup Times Stop S3 / Archive Operations Delete Snapshots New Importer Policy Refresh

<input type="checkbox"/>	Name	Account	Enabled	Backup Generations	Schedules	Cost (\$)
<input type="checkbox"/>	CE-LINUX-111	a1	Yes	30		N/A
<input type="checkbox"/>	CE-LINUX-222	a1	Yes	30		N/A
<input type="checkbox"/>	CE-LINUX-333	a1	Yes	30		N/A
<input type="checkbox"/>	CE-WINDOWS	a1	Yes	30		2.86
<input type="checkbox"/>	cpmdata	a1	Yes	30		N/A
<input type="checkbox"/>	importer-1	a1				N/A

0 of 6 items selected

### 4.1 Schedules

Schedules are the objects defining **when** to perform a backup

- Schedules are defined separately from policies and Scheduled Reports.
- One or more schedules can be assigned to both policies and Scheduled Reports.



Schedules can be managed in the **Schedules** tab found in the left panel. They can be added also during the creation of a new Policy.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with the following items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules (highlighted), Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Schedules' and features a search bar, a dropdown for 'All Policies', and a '20 records/page' selector. Below these are '+ New', 'Edit', and 'Delete' icons, along with a 'Refresh' button. A table lists the following schedule:

<input type="checkbox"/>	Name	Scheduling	Days In Week	First Run	Expires	Policies	Scheduled Repo...	Recovery Scenar...	Time Z
<input type="checkbox"/>	Daily_Sched	Every Day	Mon-Sun	Oct 22, 2020 9:21 ...	Never				Italy (E

At the bottom, it indicates '0 of 1 items selected'.

Or, added when creating a new scheduled report in the **Scheduled Reports** tab of the **Reports** tab in the left panel.

The screenshot shows the 'New Scheduled Report' form in the N2WS Backup & Recovery (CPM) interface. The left sidebar is the same as in the previous screenshot, with 'Reports' highlighted. The main content area is titled 'Reports > New Scheduled Report' and contains the following fields:

- Name:
- Report Type:  (dropdown)
- User:  (dropdown) with a '+ New' link and a refresh icon.
- ☒ Enabled
- Schedules:  (dropdown) with a '+ New' link and a refresh icon.
- Recipients:
- User to Filter by:  (dropdown)
- Description:

At the bottom right, there are 'Save' and 'Cancel' buttons.

**Note:** Both interfaces include all defined schedules and the same definition options.





You can define schedules to:

- Run for the first time at a date and time in the future.
- Run forever or have a specific date and time to stop.
- Repeat every 'n' minutes, hours, days, weeks, months.
- Selectively enable for certain minutes, hours, and days of the week, but not for weeks and months.
- Repeat every day of the week, or only run on certain days.
- Exclude running a report or policy during certain time ranges within the scheduled times.

For the root/admin user, if you have created additional managed users, you can select the user to whom the schedule belongs.

**Important:** For weekly or monthly backups and report generation, the start time will determine the day of the week of the schedule and *not* the days of week checkboxes.

#### 4.1.1 Defining Schedules

The same schedule can be used in all of the following:

- Policy backup operations.
- Recovery Scenarios for policies with schedules.
- Generating **Scheduled Reports**.


**Note:** All start times are derived from the **First Run** time. The time set in First Run becomes the regular start time for the defined schedule.

You can add a schedule from a number of places:

- In the **Schedules** tab, select **+ New**.
- While creating or editing a policy in the **Policies** tab, in the Policy Details tab, select **+ New** above the Schedules list.
- While creating or editing a schedule report in the **Scheduled Reports** tab of the **Reports** tab, select **+ New** above the Schedules list.



## To define a schedule:

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.

**Note:** The time set in **First Run** becomes the regular start time for the defined schedule.


- If you want a daily backup to run at 10:00 AM, set **Repeats Every** to one day and the start time to 10:00 AM.
  - If you want an hourly backup to run at 17 minutes after the hour, set **Repeats Every** to one hour and **First Run** to `nn:17`, where `nn` is the hour of the **First Run**.
3. If this schedule expires, turn on the **Expires** toggle and select the date and time the schedule ends. By default, schedules never expire.
  4. In the **Repeats Every** list, select the frequency of the backups for this schedule. The possible units are months, weeks, days, hours, and minutes.
  5. In the **Enabled On** section, select the day-of-week checkboxes on which to run the schedule.
  6. To exclude time ranges within the defined schedule, turn on the **Exclude Time Ranges** toggle. See section 4.1.4.
  7. Select **Save**.

### 4.1.2 Overriding Schedules

It is possible to override existing schedules and run backups and Scheduled Reports immediately:

- Ad hoc backups are initiated by the  **Run ASAP** command in the **Policies** tab. See section 4.3.2.



- Ad hoc generation of Scheduled Reports is initiated by the  **Run Now** command in the **Reports** page. See section 17.10.3.

### 4.1.3 Scheduling and Time Zones

When you configure an N2WS server, its time zone is set. See section 2.3. In the N2WS management application, all time values are in the time zone of the N2WS server. Schedule times, however, may be set and executed according to a specific time zone. A policy's **Backup Times** will be according to the time zone.

**Important:** Even when you are backing up instances that are in different time zones, the backup time that is shown on the monitor and Backup Log is always according to the N2WS server's local time.

In the N2WS database, times are saved in UTC time zone (Greenwich). So, if, at a later stage, you start a new N2WS server instance, configure it to a different time zone, and use the same CPM data volume as before, it will still perform backup at the same times as before.

### 4.1.4 Disabled Times

While or after defining a schedule, you can set specific times when the schedule should not start a backup or generate a Scheduled Report. For example, you want a backup or report to run every hour, but not on Tuesdays between 01:00 PM and 3:00 PM. You can define that on Tuesdays, between these hours, the schedule is disabled.

You can define a disabled time where the finish time is earlier than the start time. The meaning of disabling the schedule on **Monday** between 17:00 and 8:00 is that it will be disabled every Monday at 17:00 until the next day at 8:00. The meaning of disabling the schedule for **All** days between 18:00 and 6:00 will be that every day the schedule will be disabled after 18:00 until 6:00.

**Note:** Be careful not to create contradictions within a schedule's definition:

- It is possible to define a schedule that will never start backups or generate a report.
- You can define a weekly schedule which runs on Mondays, and then deselect Monday from the weekdays.
- It is also possible to create different "disabled times", which would effectively mean that the schedule is always disabled.

#### 4.1.4.1 Defining Disabled Times

For each schedule, you can define as many excluded time ranges as you need.

**To define disabled times:**

1. In **New Schedule** screen, turn on the **Exclude Time Ranges** toggle.
2. In the **Day** list, select a day of the week to exclude from the schedule.



3. In the **Start Time** and **End Time** lists, select the start and end time of the exclusion.

The screenshot shows the 'Exclude Time Ranges' section of the N2WS interface. A modal is open for selecting a time range. The modal has 'Hours' and 'Minutes' dropdowns, AM/PM radio buttons, and 'Apply' and 'Cancel' buttons. The background shows a table with columns for 'Day', 'Start Time', and 'End Time'.

4. Select **Apply** after each definition. To add another time range, select **+ New**.
5. Select the checkboxes of the excluded time ranges to enable, and then select **Save**.

## 4.2 AWS Policies

Policies are the main objects defining backups. A policy defines:

- What to back up
- How to back it up
- When to perform the backup by assigning schedules to the policy

Policy definitions are spread among the following tabs:

- **Policy Details** – Basic policy details: name, user, account, enabled, schedules, auto-target removal, backup generations, and description
- **Backup Targets** – Choose and configure backup targets. Application consistency is applied at the instance level.
- **More Options** – Backup options, such as activate Linux backup scripts, define successful backup, retry parameters, and the number of failures to trigger an alert
- **DR** – Enable DR
- **Lifecycle Management (Snapshot /S3 / Glacier)** – Configure Lifecycle operations, including number of backup generations, copy to S3, and archive to Glacier.

A policy named `cpmdata` must exist for backing up Windows instances and the N2WS server, DR, and Copy to S3. For the `cpmdata` policy, the relevant tabs are **Policy Details** and **DR**.

### 4.2.1 Creating an AWS Policy

**Note:** As of version 2.7.0, the `cpmdata` policy is no longer using scripts as the default. Users can enable application-consistent scripts for cpm data by selecting **Application Consistent** for the `cpmdata` policy in the **Policy Details** tab.

**To define a new policy:**

1. In the left panel, select **Policies**.



2. In the **+ New** menu, select **AWS policy**. The **Policy Details** tab opens.

3. In the **Name** box, type a name for the policy.
4. For the root/admin user, if you have created additional managed users, select the policy owner in the **User** box.
5. If you have more than one account, in the **Account** list, select the account that the policy is associated with. The account cannot be modified after the policy has been created.

**Note:** To avoid a Policy creation error, if the **Account** does not exist yet, select **+ New** to create the policy and then return to the Policy creation.

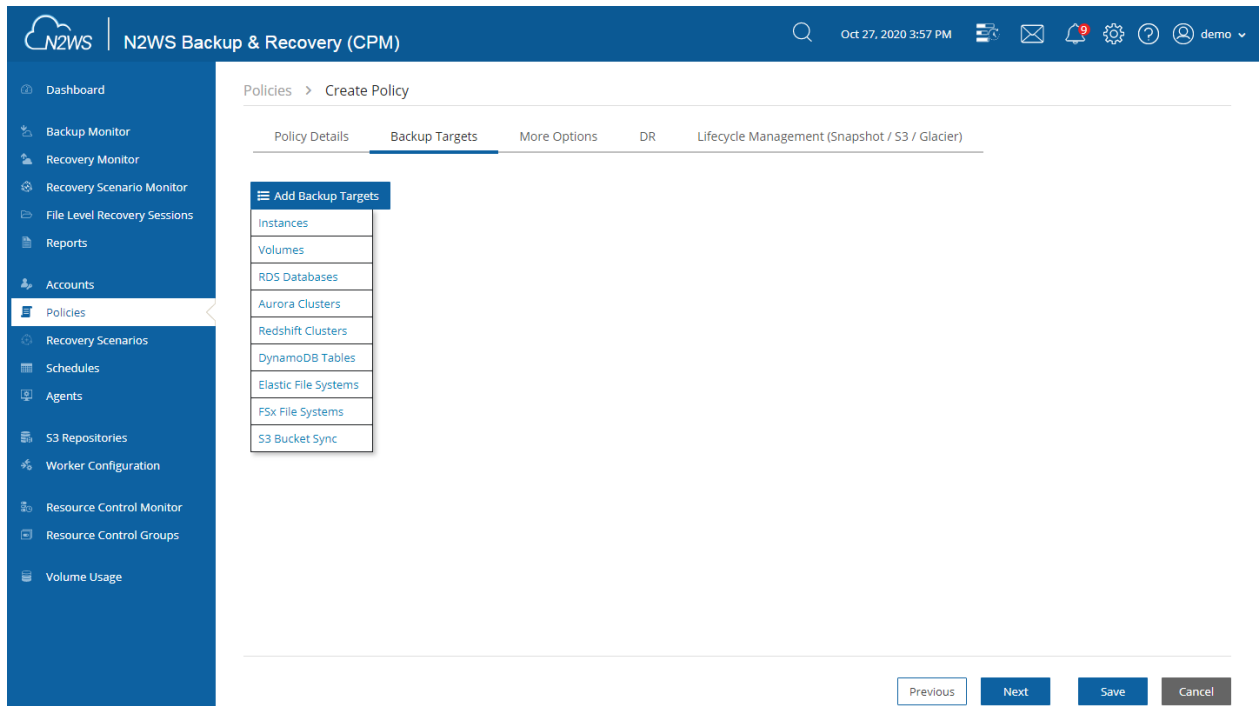
6. In the **Auto Target Removal** list, specify whether to automatically remove resources that no longer exist. If you enable this removal, if an instance is terminated, or an EBS volume deleted, the next backup will detect that and remove it from the policy. Choose **yes and alert** if you want the backup log to include a warning about such removal.
7. To use application-consistent scripts as the default for cpm data, in the `cmpdata` policy, select **Application Consistent**.

☐ **Application Consistent**

8. In the **Description** box, optionally type a description.
9. To add Backup Targets now, select the **Backup Targets** tab. See section 4.2.2. The policy will be saved when you save the Backup Targets definition.
10. To add Backup Targets later, in the **Policy Details** tab, select **Save**. The new policy is included in the list of policies in the **Policies** screen. To add Backup Targets, select the new policy, select **Edit** and then select the **Backup Targets** tab.

## 4.2.2 Adding AWS Backup Targets

Backup targets define what a policy is going to back up. You define backup targets by selecting the **Backup Targets** tab of the **Create Policy** screen.



Following are the types of backup targets:

- **Instances** – This is the most common type. You can choose as many instances as you wish for a policy up to your license limit. For each instance, allowed under your license, define:
  - Whether to back up all its attached volumes, some, or none.
  - Whether to take snapshots (default for Linux), take snapshots with one initial AMI (default for Windows), or just create AMIs.See section 4.2.3.
- **EBS Volumes** – If you wish to back up volumes, not depending on the instance they are attached to, you can choose volumes directly. This can be useful for backing up volumes that may be detached part of the time or moved around between instances (e.g. cluster volumes).
- **RDS Databases** – You can use N2WS to back up RDS databases using snapshots. There are advantages to using the automatic backup AWS offers. However, if you need to use snapshots to back up RDS, or if you need to back up databases in sync with instances, this option may be useful.
- **Aurora Clusters** – Even though Aurora is part of the RDS service, Aurora is defined in clusters rather than in instances. Use this type of backup target for your Aurora clusters and Aurora Serverless.
  - Aurora cluster storage is calculated in increments of 10 GiB with the respect to the license. For example, if you have over 10 GiB of data but less than 20 GiB, your data is computed as 20 GiB.
  - Keep in mind that clusters can grow dynamically and may reach the storage limits of your license. If the total storage is approaching your license limit, N2WS will issue a warning.



- For Aurora Serverless, capacity units will appear in the **Class** column when adding RDS Clusters as Backup Targets.
- **Redshift Clusters** – You can use N2WS to back up Redshift clusters. Similar to RDS, there is an automatic backup function available, but using snapshots can give an extra layer of protection.
- **DynamoDB Tables** – You can use N2WS to back up DynamoDB tables. The recommended best practice is a backup limit of 10 DynamoDB tables per policy.
  - When defining your backup targets, keep in mind that DynamoDB table storage is calculated in increments of 10 GiB with the respect to the license. For example, if you have over 10 GiB of data but less than 20 GiB, your data is computed as 20 GiB.
  - Tables can grow dynamically and may reach the storage limits of your license. If the total storage is approaching your license limit, N2WS will issue a warning.
- **Elastic File Systems (EFS)** – You can use N2WS to back up and restore your EFS snapshot data to AWS using AWS Backup service. Configuration options include backup vault, IAM role, transition to cold storage, and expiration.
- **FSx File Systems** – Use N2WS to back up and restore your FSx File Systems to the same region and the same account. Following are the FSx types:
  - Lustre (Linux) file system.
  - Windows file system with managed Active Directory (Win-AD)
  - Windows file system with self-managed Active Directory (Win-SMAD)

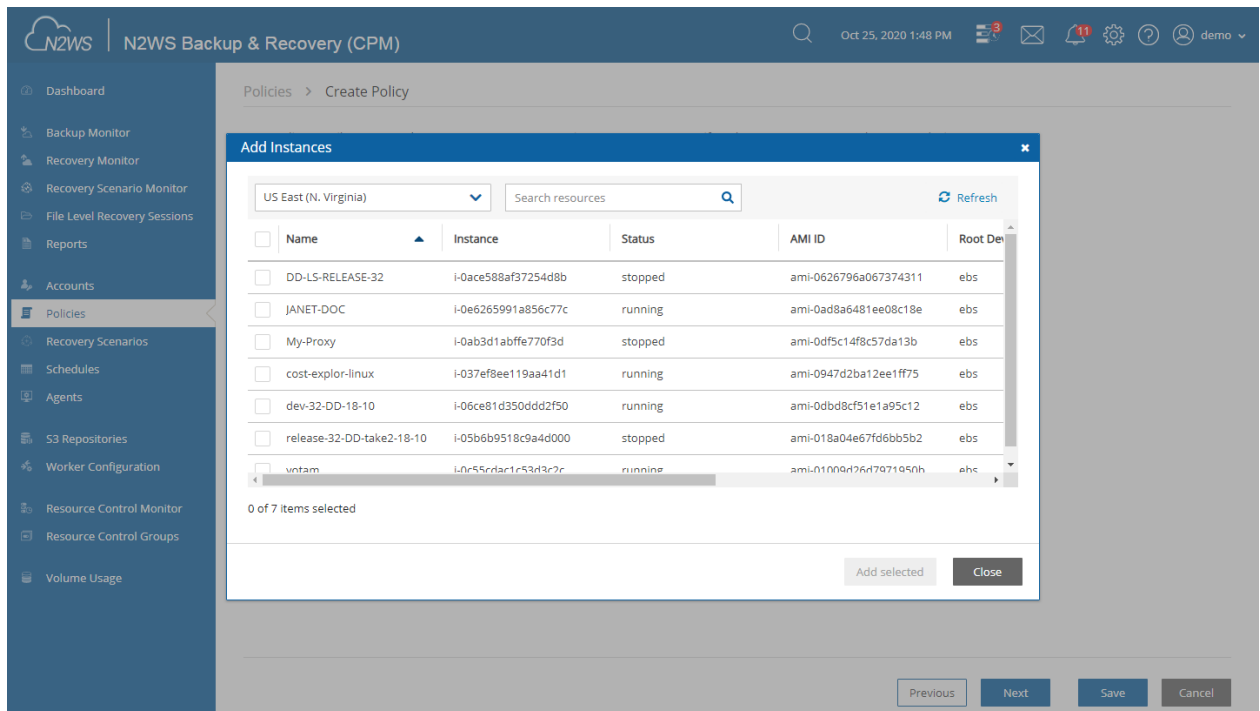
For AWS FSx backup limitations, see section 4.2.7.

See section 10.11 for recovery options.


Also, see <https://aws.amazon.com/fsx>.

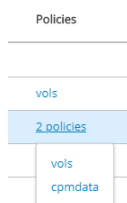
- **S3 Bucket Sync** – You can use N2WS to synchronize a source S3 bucket to a destination bucket. Since a snapshot is not created, there is no recovery or movement to the Freezer. The buckets require configuration. See section 9.8.

In the **Add Backup Targets** drop-down menu, select the relevant resource type. A window containing a list of the available resources for the selected type and region opens. To view additional columns and rows, move the scroll bars as needed.




When adding backup targets of the resource type to the policy:

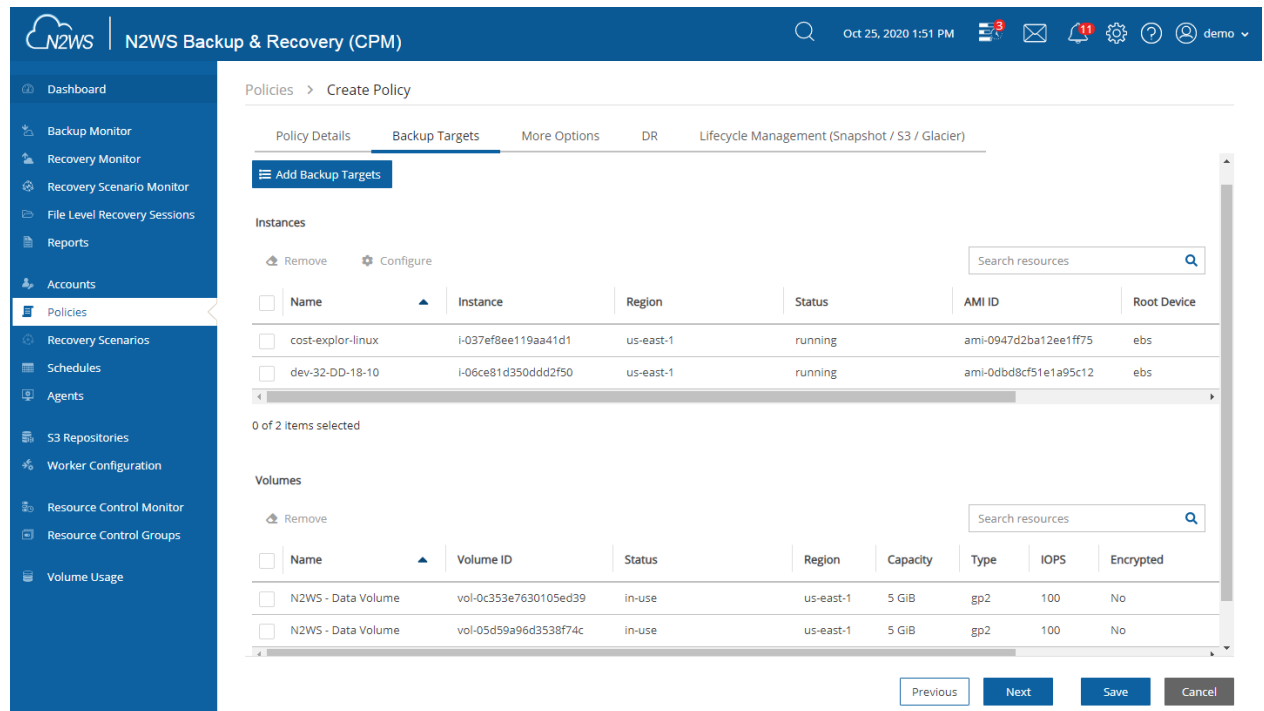
- You will see all the backup targets of the requested type that reside in the current region, except the ones already in the policy.
- You can select targets in another region by choosing from the region drop-down list.
- If there are many targets, you have the ability to:
  - Filter by typing part of a resource name in the search box and select **Search** . To clear a search, select **x**.
  - Sort by a column by selecting its heading. Select it again to change the sort direction.
  - Scroll between pages.
- For each backup target, the **Policies** column shows the policy, or the number of policies, the target is already in. Select the link to see which policies the target is in.




### To add a backup target to the policy:

1. Select a region in the drop-down list. The resources in the selected region are shown.
2. To filter the resources in the region, enter all or part of a resource name in the Search resources box and select **Search** .
3. Select the checkbox of the desired target resources.
4. Select **Add selected**. The selected objects are added to the policy's backup target list.
5. Repeat as many times as needed, from multiple regions if relevant.
6. Select **Close** when finished. The selected targets are listed in the **Backup Targets** tab.





The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', and a search bar. The left sidebar contains various navigation options. The main content area is titled 'Policies > Create Policy' and has tabs for 'Policy Details', 'Backup Targets', 'More Options', 'DR', and 'Lifecycle Management (Snapshot / S3 / Glacier)'. The 'Backup Targets' tab is selected, and a 'Add Backup Targets' button is visible. Below this, there are two sections: 'Instances' and 'Volumes'. Each section has a 'Remove' button and a 'Configure' button. The 'Instances' section shows a table with columns: Name, Instance, Region, Status, AMI ID, and Root Device. The 'Volumes' section shows a table with columns: Name, Volume ID, Status, Region, Capacity, Type, IOPS, and Encrypted. At the bottom right, there are buttons for 'Previous', 'Next', 'Save', and 'Cancel'.

7. For Instances, Volumes, EFS, and S3 Bucket Sync targets, select  **Configure** and complete the backup options.
8. In the **Backup Targets** screen, select **Save** to save the listed selections to the policy.


### 4.2.3 Instance Configuration

**Note:** With N2WS you can now create multi-volume snapshots, which are point-in-time snapshots for all EBS volumes attached to a single EC2 instance. After it's created, a multi-volume snapshot behaves like any other snapshot. You can perform all operations, such as restore, delete, and copy across Regions and Accounts. After creating your snapshots, they appear in your EC2 console created at the exact point-in-time.

In the case of EC2 instances, you can set options for any instance.

By default, Copy to S3 is performed incrementally. To ensure the correctness of your data, you can force a copy of the full data for a single iteration to your S3 Repository. While defining the **Backup Targets** for a policy with Copy to S3, select **Force a single full copy to S3**.

**To configure an instance:**

1. Select a policy, select the **Backup Targets** tab, and then select an instance.
2. Select  **Configure**. The Policy Instance and Volume Configuration screen opens.



N2WS Backup & Recovery (CPM)

Policy Instance and Volume Configuration

Backup From: i-037ef8ee119aa41d1

Which Volumes: All Volumes

Backup Options:

- Snapshots Only
- Snapshots With Initial AMI
- AMIs Only

Apply Close

3. In the **Which Volumes** list, choose whether to back up all the volumes attached to this instance, or include or exclude some of them. By default, N2WS will back up all the attached storage of the instance, including volumes that are added over time.
4. If **All Volumes** is selected, the **Remote Agent** list is enabled. Select **N2WS Thin Backup Agent** or **Simple System Manager (SSM)** depending on what you have configured. See section 6.
5. If **All Volumes** was not selected, in the volumes table, clear or select the volume checkboxes.

N2WS Backup & Recovery (CPM)

Policy Instance and Volume Configuration

Backup From: i-037ef8ee119aa41d1

Which Volumes: Include Selected

<input type="checkbox"/>	Device	Name	Volume ID	Capacity	Type	IOPS	Encrypted
<input checked="" type="checkbox"/>	/dev/sdc	cost-explor-linux	vol-005b9dce242ff5a08	22 GiB	gp2	100	Yes
<input type="checkbox"/>	/dev/sdb	cost-explor-linux-vol	vol-0d62e0cc15dfd5a2d	88 GiB	gp2	264	No
<input checked="" type="checkbox"/>	/dev/xvda	cost-explor-linux	vol-0c7bb56136732199f	77 GiB	gp2	231	No

Backup Options: Snapshots Only

Apply Close

6. In the **Backup Options** list, select one of the following:



- **Snapshots Only** - Default for Linux-based instances.
- **Snapshots with Initial AMI** - Take an initial AMI and then snapshots. Default for Windows-based instances.
- **AMIs Only** - Just schedule AMI creation. If a reboot is required after the backup, select **Reboot**. See section 4.2.3.1.

Backup Options

☐ Reboot

7. When Copy to S3 is enabled for the policy, to have a full copy of the data copied to your S3 Repository, select **Force a single full copy to S3**.
8. Select **Apply**.
9. Continue to add instances from other regions, and select **Close** when finished with the resource type. Control returns to the **Backup Targets** tab list.
10. At the bottom of the **Backup Targets** tab list, select **Save** to update the policy for all listed targets.

#### 4.2.3.1 AMI Creation


If you choose to just create AMIs:

- N2WS will create AMIs for that instance instead of taking direct snapshots. App-aware backup per agent does not apply for AMI creation.
- You can choose whether to reboot the instance during AMI creation or not to reboot, which leaves a risk of data corruption. As opposed to AMI creation in the EC2 console, the default in N2WS is no reboot.

**Note:** Try not to schedule AMI creations of an instance in one policy, while another policy running at the same time backs up the same instance using snapshots. This will cause the AMI creation to fail. N2WS will overcome this issue by scheduling a retry, which will usually succeed. However, it is recommended that you avoid such scheduling conflicts.

#### 4.2.3.2 Initial/Single AMI

Single or Initial AMIs are meant to be used mainly for Windows instance recovery.

- N2WS will keep a single AMI for each instance with this setting. A single AMI will contain *only* the root device (boot disk).
- N2WS will rotate single AMIs from time to time. It will create a new AMI and delete the old one. N2WS aims to optimize costs by not leaving very old snapshots in your AWS account.
- By default, N2WS will rotate single AMIs every 90 days. That value can be configured in the  **Server Settings > General Settings > Cleanup** tab to any number of days, or to 0 if you prefer no rotation at all.



#### 4.2.3.3 Limitations with AMI creation:

AMIs will be copied across regions for DR, but they will not be copied across accounts.

**Important:** If you use cross-account backup, be aware that if you need to recover the instance at the remote account, you need to make sure you have an AMI ready in that account.

#### 4.2.4 More Options

To see more policy options, select the **More Options** tab for a policy in the **Policies** tab. The options consist of:

- Activating Linux backup scripts and defining script timeout and output
- Defining backup success, retries, and failures for alerting

Backup scripts refer to those running on the N2WS server. See section 7.2.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options like Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main panel is titled 'Policies > Create Policy' and has tabs for Policy Details, Backup Targets, More Options (selected), DR, and Lifecycle Management (Snapshot / S3 / Glacier). Under the 'More Options' tab, there is a checkbox for 'Activate Linux Backup Scripts'. Below this, there are three dropdown menus: 'Backup Successful when' (set to 'Success Without Any Issues'), 'Number of Retries' (set to 3), and 'Wait Between Retries (minutes)' (set to 10). There is also a dropdown for 'Failures to Trigger Alert' (set to 1). At the bottom, there is a 'Custom Tags' section with a '+ New' button, a 'Delete' button, and a table with columns for 'Tag Key', 'Name Is Prefix', 'Tag Value', and 'Value Is Prefix'. At the bottom right of the main panel, there are buttons for 'Previous', 'Next', 'Save', and 'Cancel'.

- **Activate Linux Backup Scripts** – This option is turned off by default. If you select **Activate Linux Backup Scripts**, the following options appear:
  - **Scripts Timeout** – Timeout (in seconds) to let each script run. When a backup script runs, after the timeout period, it will be killed, and a failure will be assumed. The default is 30 seconds.
  - **Collect Scripts Output** – N2WS can collect the output of backup scripts to the standard error (stderr). This may be useful for debugging. It can also be used by a script to log the operations it is performing and write useful information. This output is captured, saved in the N2WS database, and can be viewed from the Recovery Panel screen. To turn this option on, choose Collect. The default option is Ignore.

**Note:** The output of a script is typically a few lines. However, if it gets really big (MBs), it can affect the performance of N2WS. If it gets even larger, it can cause crashes



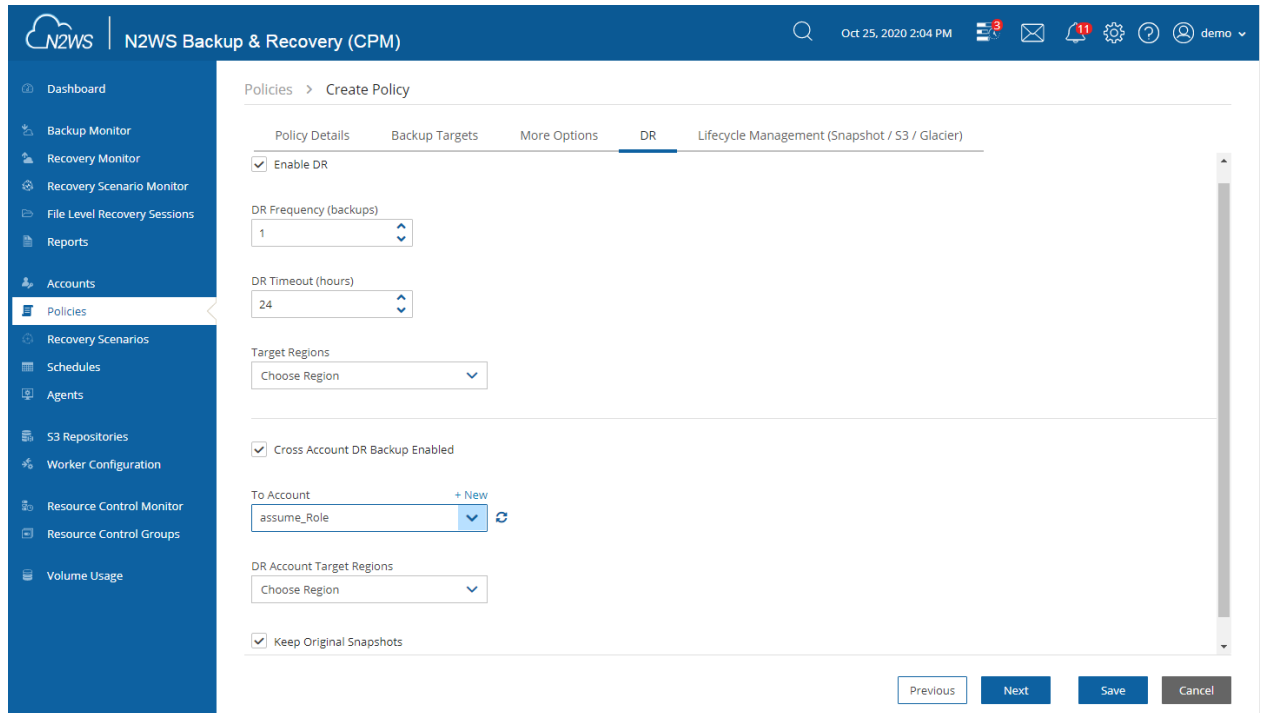
in N2WS processes. To avoid the risk of too much data going to `stderr`, redirect the output elsewhere.

- **Backup Successful when** - This indicates whether a backup needs its scripts/VSS to complete, to be considered a valid backup. This has a double effect:
  - For retries, a successful backup will not result in a retry;
  - For the automatic retention management process, a backup that is considered successful is counted as a valid generation of data.The possible values are:
  - **Success Without Any Issues** – If scripts and/or VSS are defined for this policy, the backup will be considered successful only if everything succeeds. If backup scripts or VSS fails and all snapshots succeed, the backup is not considered successful. You can still recover from it, but it will cause a retry (if any are defined), and the automatic retention management process will not count it as a valid generation of data. This is the stricter option and is also the default.
  - **Snapshot Succeeded with Possible VSS or Script Failure** – This is the less strict option and can be useful if scripts or VSS fail often, which can happen in a complex environment. Choosing this option accepts the assumption that most applications will recover correctly even from a crash-consistent backup.
- **Retry information** – The next three options deal with what to do when a backup does not succeed:
  - **Number of Retries** – The maximal number of retries that can be run for each failed backup. The default is three. After the retries, the backup will run again at the next scheduled time.
  - **Wait Between Retries (minutes)** – Determines how much time N2WS will wait after a failure before retrying. Backup scripts and VSS may sometimes fail or timeout because the system is busy. In this case, it makes sense to substantially extend the waiting time until the next retry when the system may be more responsive.
  - **Failures to Trigger Alert** – The minimum number of failures to trigger an alert.
- **Custom Tags** – You can add custom tags for the policy. Define the **Tag Name** and **Tag Value**. if the Name and/or Value is a prefix, select **Name is Prefix**. For details about Custom Tags, see section 14.2.

#### 4.2.5 Enabling Disaster Recovery

To enable Disaster Recovery for the policy:

1. Select the **DR** tab for a policy in the **Policies** tab screen.



2. Select **Enable DR**.
3. Select the **DR Frequency** for backups, **DR Backup Timeout**, and **Target Regions**.
4. To enable **Cross Account DR Backups**, select the checkbox, and:
  - a. Choose the To Account and DR Account Target Regions in the lists.

**Note:** If the DR **To Account** does not exist yet, select **+ New** to create the account and then return to the policy creation.

- b. To Keep Original Snapshots, select the checkbox.

## 4.2.6 Managing Lifecycle

The **Lifecycle Management** tab for a policy allows you to do the following:

- Set retention policy for snapshots: **Keep n (Native) Backup Generations**.
- **Backup to S3** – Enable, set copy and retention policies, choose storage options, and optionally delete EBS backup snapshots after a backup to S3. See section 21.3.
- **Archive to Glacier** - Enable, set copy and retention policies, and choose the Archive Storage Class. See section 21.5.3.

**Note:** **Archive to Glacier** requires that the **Backup to S3** option is enabled first.

- **Storage settings** – Define the Target repository and S3 Storage class, or Archive Storage class if relevant. See section 21.3.1.



## 4.2.7 AWS Backup Limitations to FSx

**Note:** FSx is *not* currently supported in AWS GovCloud (US) regions.

Following are limitations on backups of FSx for Lustre:

- Backups are not supported on scratch file systems because these file systems are designed for temporary storage and shorter-term processing of data.
- Backups are not supported on file systems linked to an Amazon S3 bucket because the S3 bucket serves as the primary data repository, and the Lustre file system does not necessarily contain the full data set at any given time.

For further information, see <https://docs.aws.amazon.com/fsx/latest/LustreGuide/using-backups-fsx.html>

## 4.3 Managing Policies

The following actions are available for both AWS and Azure policies.

### 4.3.1 Viewing Policy Backup Times

In the **Policies** tab, select a policy and then select **Backup Times** to open the Planned Backups window, which is ordered by Time Zone. You can change the **Time Period** from the default 'Next Day' to a number of days, weeks, or the next month.



**Planned Backups**

Time Zone: Indonesia - Jayapura

Time Period:  
Next Day

Run Time	Schedule
Fri 01/17/2020 11:48 AM	sch1

**Backup Times** are relevant to the schedules of the selected policy.

### 4.3.2 Running an Ad Hoc Backup

An ad hoc backup will execute the selected Policy and create backups of all its targets.

**Note:** An ad hoc backup counts as another generation if it completes successfully.

**To run a backup immediately:**

1. In the left panel, select the **Policies** tab and then select a policy in the list.
2. To start the backup, select **Run ASAP**.
3. To follow the progress of the backup, select **Open Backup Monitor** in the 'Backup started' message **Backup started (Open Backup Monitor)** at the top right corner, or select the **Backup Monitor** tab.
  - a. To update the list, select **Refresh**.

**Backup Monitor**

Search backups  by instance  All Policies  All Accounts  All Backup Statuses

20 records/page  Show:

<input type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle
<input type="checkbox"/>	Oct 25, 2020 2:12 PM		P1	ACCOUNT-1	In Progress		
<input type="checkbox"/>	Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P3	ACCOUNT-3	Successful		
<input type="checkbox"/>	Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/>	Oct 25, 2020 11:03 AM	Oct 25, 2020 11:13 AM	P1	ACCOUNT-1	Successful		
<input type="checkbox"/>	Oct 25, 2020 11:03 AM	Oct 25, 2020 11:04 AM	CPMDATA	ACCOUNT-1	Successful		
<input type="checkbox"/>	Oct 24, 2020 2:43 PM	Oct 24, 2020 2:44 PM	P3	ACCOUNT-3	Successful		
<input type="checkbox"/>	Oct 24, 2020 1:37 PM	Oct 24, 2020 1:39 PM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/>	Oct 24, 2020 1:37 PM	Oct 24, 2020 1:49 PM	P1	ACCOUNT-1	Successful		
<input type="checkbox"/>	Oct 24, 2020 1:37 PM	Oct 24, 2020 1:37 PM	CPMDATA	ACCOUNT-1	Successful		
<input type="checkbox"/>	Oct 22, 2020 8:22 AM	Oct 22, 2020 8:24 AM	P2	ACCOUNT-1	Successful	Completed	
<input type="checkbox"/>	Oct 22, 2020 8:21 AM	Oct 22, 2020 8:22 AM	P1	ACCOUNT-1	Successful		

0 of 11 items selected

- b. You can switch between showing backup records 'in the Freezer' by turning on and off the toggle key and backup records 'not in the Freezer' by turning on and off the toggle key in the Show area to the right of the filters.
4. To view or download backup details, select **Log**. Select **Refresh** as needed.





The screenshot shows the 'Backup Log' window in the N2WS interface. It displays a table of backup events with columns for Time, Level, and Message. The events are listed in chronological order, showing the start of the backup, the completion of individual snapshots for various instances and volumes, and the final completion of the backup process.

Time	Level	Message
10/25/2020 2:12:32 PM	Info	Backup is agentless, managed by CPM Server
10/25/2020 2:12:32 PM	Info	Starting. Fired by schedule: Immediate/ASAP
10/25/2020 2:12:36 PM	Info	All snapshots started successfully
10/25/2020 2:13:25 PM	Info	snapshot of instance cost-explor-linux, volume cost-explor-linux (vol-005b9dce242ff5a08) completed successfully.
10/25/2020 2:13:25 PM	Info	snapshot of instance cost-explor-linux, volume cost-explor-linux-vol (vol-0d62e0cc15dfd5a2d) completed successfully.
10/25/2020 2:13:25 PM	Info	snapshot of instance cost-explor-linux, volume cost-explor-linux (vol-0c7bb56136732199f) completed successfully.
10/25/2020 2:14:10 PM	Info	snapshot of instance 310-milan-CPM, volume 310-milan-CPM (vol-0c81cb9a670fa6aa9) completed successfully.
10/25/2020 2:14:10 PM	Info	snapshot of instance 310-milan-CPM, volume N2WS - Data Volume (vol-08e36a1cb7bf72a4f) completed successfully.
10/25/2020 2:14:10 PM	Info	Backup Finished successfully on all volumes/databases.
10/25/2020 2:14:10 PM	Info	starting CBT for volume snapshots
10/25/2020 2:14:16 PM	Info	CBT successfully processed for 5 volume snapshots

5. To delete a particular snapshot in AWS or to delete all AWS snapshots after a successful run, select **View Snapshots**. Select one or more backups and then select **Delete**.

The screenshot shows the 'Snapshots' window in the N2WS interface. It displays a list of 'Regular Snapshots' with columns for Instance, Snapshot Type, Snapshot ID, Volume, and Finished at. The snapshots are listed in chronological order, showing the completion of individual snapshots for various instances and volumes.

Instance	Snapshot Type	Snapshot	Volume	Finished at	Succeeded?
i-037ef8ee119aa41d1	EBS	snap-08d524d3ed98d29bc	vol-005b9dce242ff5a08	Oct 25, 2020 2:13 PM	Yes
i-037ef8ee119aa41d1	EBS	snap-0bee9c339fde854ee	vol-0d62e0cc15dfd5a2d	Oct 25, 2020 2:13 PM	Yes
i-037ef8ee119aa41d1	EBS	snap-0797d8bc13f02b824	vol-0c7bb56136732199f	Oct 25, 2020 2:13 PM	Yes
i-0d93e780248d9f1c4	EBS	snap-0807b979e0a2981de	vol-0c81cb9a670fa6aa9	Oct 25, 2020 2:14 PM	Yes
i-0d93e780248d9f1c4	EBS	snap-04cff52d6af6bd57a	vol-08e36a1cb7bf72a4f	Oct 25, 2020 2:14 PM	Yes

### 4.3.3 Deleting a Policy

**Note:** When deleting a policy, all related snapshots and data are deleted.

To delete a policy, select it in the **Policies** table and then select **Delete**. In the **Delete Policy** confirmation dialog box, type '**delete all**' and then select **Delete**.



### Delete Policy



Are you sure you want to delete policy 'p1'? All related snapshots and data will be deleted.

In order to confirm deletion of the selected policies with their related snapshots, please type the phrase 'delete all'

Delete

Cancel



## 5 Consistent Backup

This guide explains a few key concepts to help you use N2WS correctly.

### 5.1 Crash-Consistent Backup

By default, snapshots taken using N2WS are Crash-consistent. When you back up an EC2 instance at a certain time, and later want to restore this instance from backup, it will start the same as a physical machine booting after a power outage. The file system and any other applications using EBS volumes were not prepared or even aware that a backup was taking place, so they may have been in the middle of an operation or transaction.

Being in the middle of a transaction implies that this backup will not be consistent, but actually, this is not the case. Most modern applications that deal with important business data are built for robustness. A modern database, be it MySQL, Oracle, or SQL Server, has transaction logs. Transaction logs are kept separately from the data itself, and you can always play the logs to get to a specific consistent point in time. A database can start after a crash and use transaction logs to get to the most recent consistent state. NTFS in Windows and EXT3 in Linux have implemented journaling, which is not unlike transaction logs in databases.

### 5.2 Application-Consistent Backup

During application-consistent backups, any application may be informed about the backup progress. The application can then prepare, freeze and thaw **in minimal-required time** to perform operations to make sure the actual data on disk is consistent before the backup starts., making minimal changes during backup time (**backup mode**) and returning to full-scale operation as soon as possible.

There is also one more function that application-consistent backups perform especially for databases. Databases keep transaction logs which occasionally need to be deleted to recover storage space. This operation is called **log truncation**. When can transaction logs be deleted without impairing the robustness of the database? Probably after you make sure you have a successful backup of the database. In many cases, it is up to the backup software to notify the database it can truncate its transaction logs.

### 5.3 N2WS and a Point in Time

When taking snapshots, the **point in time** is the exact time that the snapshot started. The content of the snapshot reflects the exact state of the disk at that point in time, regardless of how long it took to complete the snapshot.

### 5.4 Summary or What Type of Backup to Choose

The type of backup to choose depends on your needs and limitations. Every approach has its pros and cons:



### 5.4.1 Crash-Consistent

Pros:

- Does not require writing any scripts.
- Does not require installing agents in Windows Servers.
- Does not affect the operation and performance of your instances and applications.
- Fastest.

Cons:

- Does not guarantee a consistent state of your applications.
- Does not guarantee the exact point in time across multiple volumes/disks.
- No way to automatically truncate database transaction logs after backup.

### 5.4.2 Application-Consistent

Pros:

- Prepares the application for backup and therefore achieves a consistent state.
- Can ensure one exact point in time across multiple volumes/disks.
- Can truncate database transaction logs automatically.

Cons:

- May require writing and maintaining backup scripts.
- Requires installing an N2WS Thin Backup Agent or the AWS SSM Agent for Windows Servers.
- May slightly affect the performance of your application, especially for the freezing/flushing phase.



## 6 Windows Instances Backup

From the point of view of the AWS infrastructure, there is not much difference between backing up Linux/Unix instances or Windows instances. You can still run snapshots on EBS volumes. However, there is one substantial difference regarding recovering instances:

- In Unix/Linux instances, you can back up system volumes (root devices), and later launch instances based on the snapshot of the system volume. You can create an image (AMI) based on the system volume snapshot and launch instances.
- This option is currently not available for Windows Servers. Although you can take snapshots of the system volume of a Windows Server, you cannot create a launchable image (AMI) from that snapshot.

Because of this limitation, N2WS needs an AMI to start the recovery of a Windows instance. N2WS will still make sure all the volumes, including the root device (OS volume), will be from the point-in-time of the recovered backup. By default, N2WS will create an initial AMI when you start backing up a Windows instance. That AMI will be used as the default when recovering this instance.

If crash-consistent backup is sufficient for your needs, you do not need to install any agent. However, to use VSS for application-consistent backups or to run backup scripts, you will need to install the N2WS proprietary Thin Backup Agent or the AWS SSM Agent. AWS's SSM Agent can be installed and configured for EC2 instances, on-premise servers, or virtual machines (VMs).

**Note:** When using SSM for VSS:

- Certain AWS roles are required. See section 6.2.
- SSM is only applicable for Windows instances with the 'All Volumes' option.
- Upon success, the description 'VSS snapshot' is added to the snapshot. For example, "CPM policy p3|instance: i0a9ebd86122a0eab2| VSS snapshot".
- If SSM is not configured, the agent will get an exception from AWS and will back up using 'multi-volume' but without our VSS agent.
- If `ec2-vss-agent.exe` is not configured, it will be detected too late and the backup of that target will fail.
- The SSM Agent does *not* appear in the **Agents** tab. Check the system directly to verify installation and status.

### 6.1 Configuring N2WS Thin Backup Agents

The N2WS Thin Backup Agent is used for Windows instances that need to perform application quiescence using VSS or backup scripts.

- The agent communicates with the N2WS Server using the HTTPS protocol.
- No sensitive information passes between the backup agent and the N2WS Server.


Any Windows instance in a policy can have a backup agent associated with it.





### 6.1.1 Associating an Agent with a Policy

After adding your Windows instance to the backup targets page (section 4.2.2), the next step is to configure its agent by associating it with a policy.

**To associate an agent with the policy:**

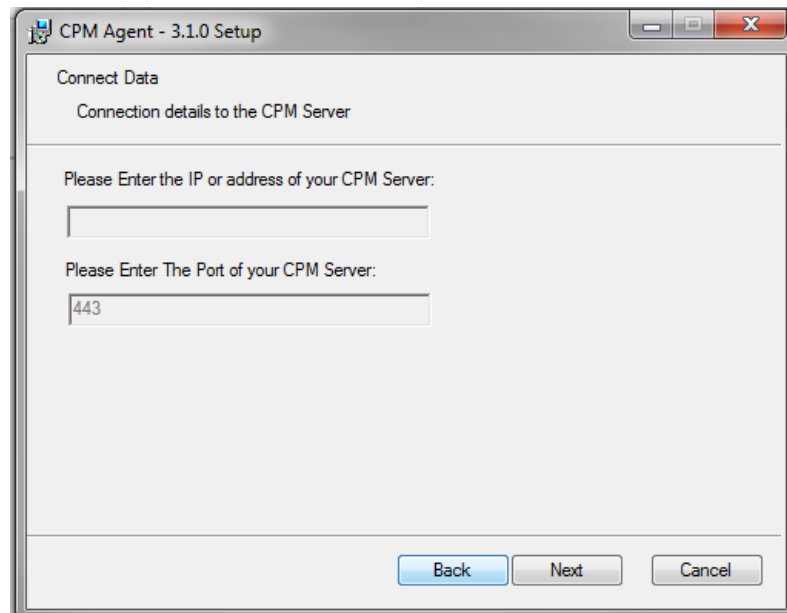
1. In the **Policies** tab, select the 'cpmdata' policy and then select  **Edit**.
2. In the **Backup Targets** tab, select the Windows instance and select **Configure**.
3. In the configuration screen, select **Application Consistent Backup**.
4. In the **Remote Agent Type** list, select AWS SSM and N2WS Thin Agent

### 6.1.2 Downloading and Distributing an N2WS Thin Backup Agent Configuration

1. You can download the installation package of the agent from the **Agents** tab in the left panel. Select  **Download Thin Backup Agent** to download a standard Windows package (CPMAgentService.msi) to the Downloads folder.
2. After downloading the agent installation package, select  **Server Settings** and then select **Agents Configuration**.
3. Enter the configuration syntax as described in Appendix B (page 294), and select **Publish**.

### 6.1.3 Installing an N2WS Thin Backup Agent

The agent can be installed on any Windows 2003, 2008, 2012, 2016, or 2019 instance, 32 or 64-bit. After accepting the license agreement, the Setup screen opens.



The required fields are:

- The address of the N2WS server that is reachable from this instance.
- The default port is 443 for HTTPS communication. Change it if you are using a custom port.



After finishing the installation, the N2WS agent will be an automatic service in your Windows system.

**Note:** The N2WS Thin Backup Agent is known as **CPM Agent Service** in the Windows Task Manager.

**Important:** After the N2WS Thin Backup Agent is installed and configured and a policy with a target that points at it is configured and enabled, the users must wait to see it registered in the remote **Agents** screen in the N2WS. It may take a few minutes until the N2WS connects.

The screenshot shows the N2WS Backup & Recovery (CPM) web interface. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date 'Oct 25, 2020 7:53 PM', and several status icons. The left sidebar contains a list of navigation items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents (highlighted), S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Agents' and features a search bar, a dropdown for '20 records/page', and a 'Download Thin Backup Agent' link. Below this is a table with columns: Name, Instance ID, Last Heard From, and Policies. The table contains one entry: 'win-tag-CE' with Instance ID 'i-081567f5c1d249787', Last Heard From 'Oct 25, 2020 7:52 PM', and Policy 'windows-vss-backu'. A 'Refresh' button is located at the top right of the table.

Name	Instance ID	Last Heard From	Policies
win-tag-CE	i-081567f5c1d249787	Oct 25, 2020 7:52 PM	windows-vss-backu

## 6.1.4 Changing an N2WS Thin Backup Agent Configuration

To change the configuration of the backup agent after installation, edit the backup agent configuration file.

**To change the agent configuration file:**

1. Before proceeding, it is recommended that you make a copy of the `cpmagent.cfg` file, which resides in the N2WS Agent installation folder.
2. If the address or port of the N2WS Server had changed, edit the agent configuration file manually. Make the change after the equation sign.
3. After making the changes, restart the **CPM Agent Service**, in the Windows Service Manager console.
4. As an alternative, you could uninstall and reinstall the agent.

## 6.1.5 Using the N2WS Thin Backup Agent with an HTTP Proxy

N2WS supports configurations where the backup agent for a Windows instance can reach the CPM server only through a proxy.



### To configure the agent with an HTTP proxy:

1. See section 6.1.4 about editing `cpmagent.cfg`, and:
2. Add the following lines under the general section:  

```
proxy_address=<dns name or ip address of the proxy server>  
proxy_port=<port for the proxy (https)>
```
3. If your proxy server requires authentication, add the following two lines as well:  

```
proxy_user=<proxy user name>  
proxy_password=<proxy password>
```
4. Restart the **CPM Agent Service** from the Windows Service Manager.

## 6.2 Configuring Simple System Manager (SSM) Agents

Following are the general steps to run a VSS snapshot backup:

- Define an SSM IAM Role.
- Define a VSS IAM Role.
- Associate an SSM Agent with an N2WS policy.
- Install the latest SSM Agent.
- Install and run the latest VSS app.
- Backup scripts for Windows targets must be PowerShell scripts.

To use the SSM agent with VSS, the following AWS permissions are required:

- **AmazonSSMFullAccess** – For N2WS and the instance to use the SSM remote agent for VSS and scripts.
- **AmazonSSMFullAccess** and **CreateVssSnapshot** - For creating VSS.

### 6.2.1 Associating an SSM Agent with a Policy

To enable SSM in an N2WS policy, when configuring a Windows instance in the Policy Instance and Volume Configuration screen, select **All Volumes** in the **Which Volumes** list and **Simple Systems Manager (SSM)** in the **Remote Agent** list. See section 4.2.3.

### 6.2.2 Defining and Attaching an IAM Instance Profile for SSM

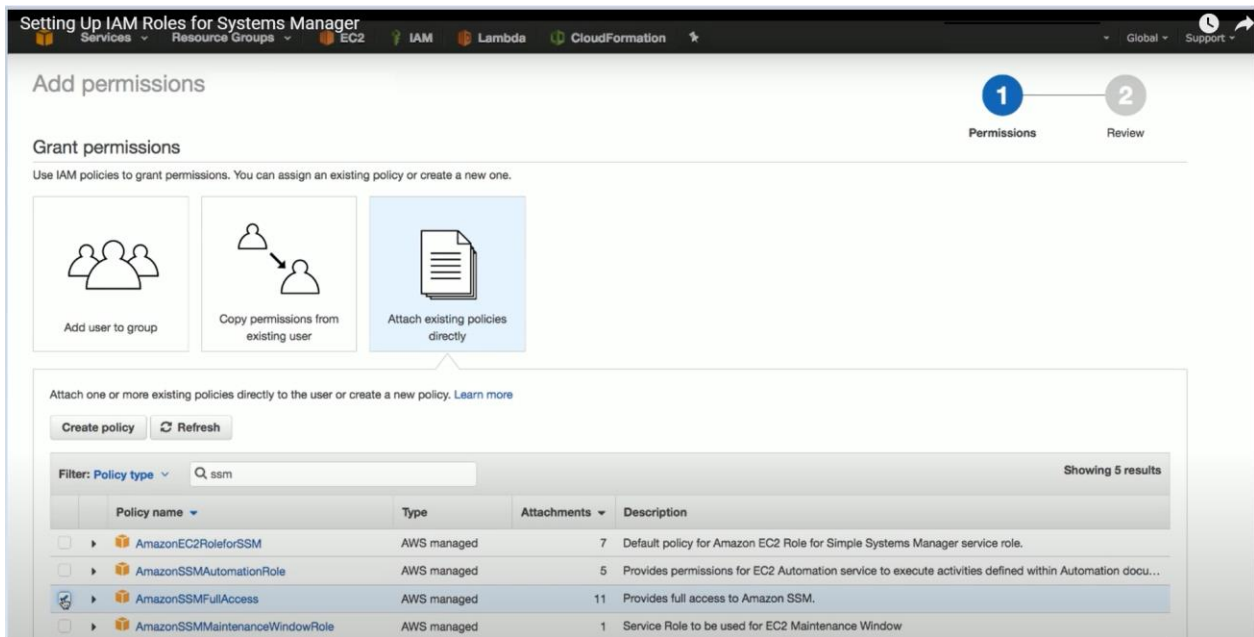
To create an IAM instance profile for SSM, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-instance-profile.html>

To attach an IAM instance profile to an EC2 instance, see

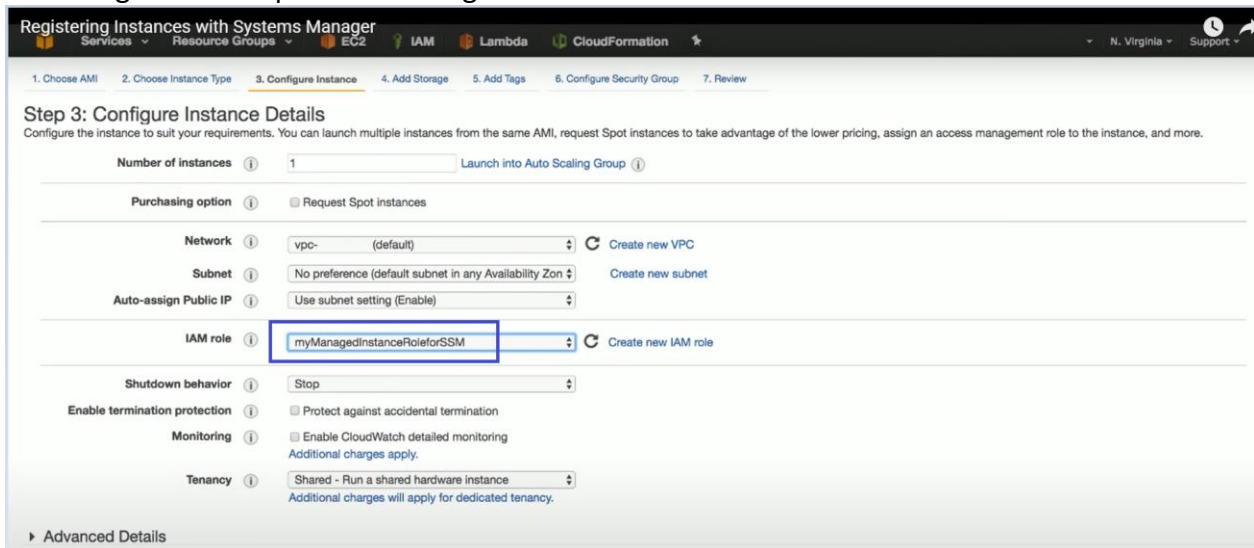
<https://docs.aws.amazon.com/systems-manager/latest/userguide/setup-launch-managed-instance.html>

Following is an example of adding SSM permissions to an IAM policy on AWS:





Following is an example of attaching an SSM role to an EC2 Instance on AWS:

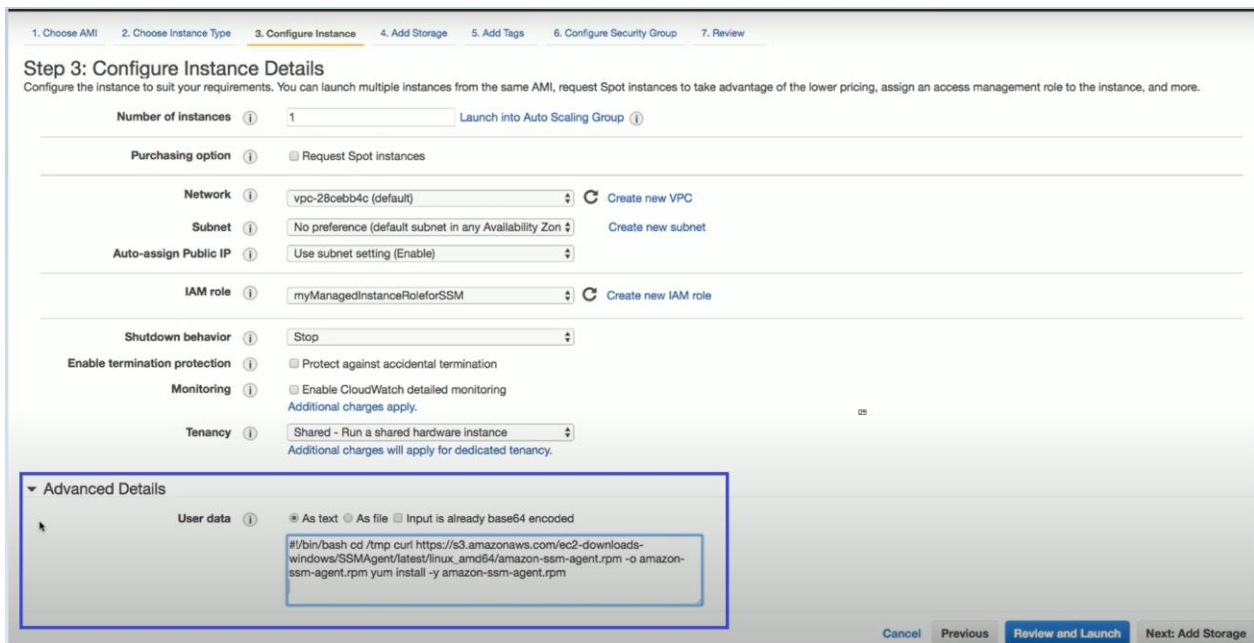


## 6.2.3 Installing SSM Agents

To manually install an SSM Agent on EC2 instances:

- For Windows Servers, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-install-win.html>
- For Linux, see <https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-manual-agent-install.html>

Following is an example of how to install an SSM Agent during EC2 launch:



1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

### Step 3: Configure Instance Details

Configure the instance to suit your requirements. You can launch multiple instances from the same AMI, request Spot instances to take advantage of the lower pricing, assign an access management role to the instance, and more.

Number of instances: 1 [Launch into Auto Scaling Group](#)

Purchasing option: ☐ Request Spot instances

Network: vpc-28cebb4c (default) [Create new VPC](#)

Subnet: No preference (default subnet in any Availability Zone) [Create new subnet](#)

Auto-assign Public IP: Use subnet setting (Enable)

IAM role: myManagedInstanceRoleforSSM [Create new IAM role](#)

Shutdown behavior: Stop

Enable termination protection: ☐ Protect against accidental termination

Monitoring: ☐ Enable CloudWatch detailed monitoring  
Additional charges apply.

Tenancy: Shared - Run a shared hardware instance  
Additional charges will apply for dedicated tenancy.

**Advanced Details**

User data: ☒ As text ☐ As file ☐ Input is already base64 encoded

```
#/bin/bash cd /tmp curl https://s3.amazonaws.com/ec2-downloads-windows/SSMAgent/latest/linux_amd64/amazon-ssm-agent.rpm -o amazon-ssm-agent.rpm yum install -y amazon-ssm-agent.rpm
```

[Cancel](#) [Previous](#) [Review and Launch](#) [Next: Add Storage](#)

## 6.2.4 Defining an IAM VSS Role and Installing VSS App

To create an IAM role for VSS-enabled snapshots and to download and install VSS components on Windows for an EC2 instance, except for US government cloud regions, see <https://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/application-consistent-snapshots-getting-started.html#run-command-vss-role>

For US government cloud regions, the IAM role needs to be updated with 'aws-us-gov' as shown below:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ec2:CreateTags",
      "Resource": [
        "arn:aws-us-gov:ec2:::snapshot/",
        "arn:aws-us-gov:ec2:::image/"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:CreateSnapshot",
        "ec2:CreateImage",
        "ec2:DescribeImages"
      ],
      "Resource": "*"
    }
  ]
}
```



## 6.2.5 Using Backup Scripts on Windows Targets

When using an SSM remote agent for Windows instance targets, all before or after backup scripts must be PowerShell scripts. Each script's content must consist of valid PowerShell commands. Saving the files with the '.ps' extension is not necessary.

## 6.3 Using VSS

VSS, or Volume Shadow Copy Service, is a backup infrastructure for Windows Servers. It is beyond the scope of this guide to explain how VSS works. You can read more at <http://technet.microsoft.com/en-us/library/cc785914%28v=WS.10%29.aspx>. However, it is important to state that VSS is the standard for Windows application quiescence, and all recent releases of many of the major applications that run on Windows use it, including Microsoft Exchange, SQL Server, and SharePoint. It is also used by Windows versions of products not developed by Microsoft, like Oracle.

N2WS supports VSS for backup on Windows Servers 2008, 2012, 2016, and 2019 *only*. Trying to run VSS on other Windows OSs will always fail. VSS is turned on by default for every Windows agent. For unsupported OSs, you will need to disable it yourself. This can be done in the instance configuration screen, see section 6.1.1.

Any application that wishes to be **backup aware** has a component called **VSS Writer**. Every vendor who would like to support copying the actual backup data (making shadow copies) provides a component called a **VSS Provider**. The operating system comes with a **System Provider**, which knows how to make shadow copies to the local volumes. Storage hardware vendors have specialized **Hardware Providers** that know how to create shadow copies using their own hardware snapshot technology. Components that initiate an actual backup are called **VSS Requestors**.

When a requestor requests a shadow copy, the writers flush and freeze their applications. At the point of time of the shadow copy, all the applications and the file systems are frozen. They all get thawed after the copy is started (copy-on-write mechanisms keep the point in time consistent, similar to EBS snapshots). When the backup is complete, the writers get notified that they have a consistent backup for the point in time of the shadow copy. For example, Microsoft Exchange automatically truncates its transaction logs when it gets notified that a backup is complete.

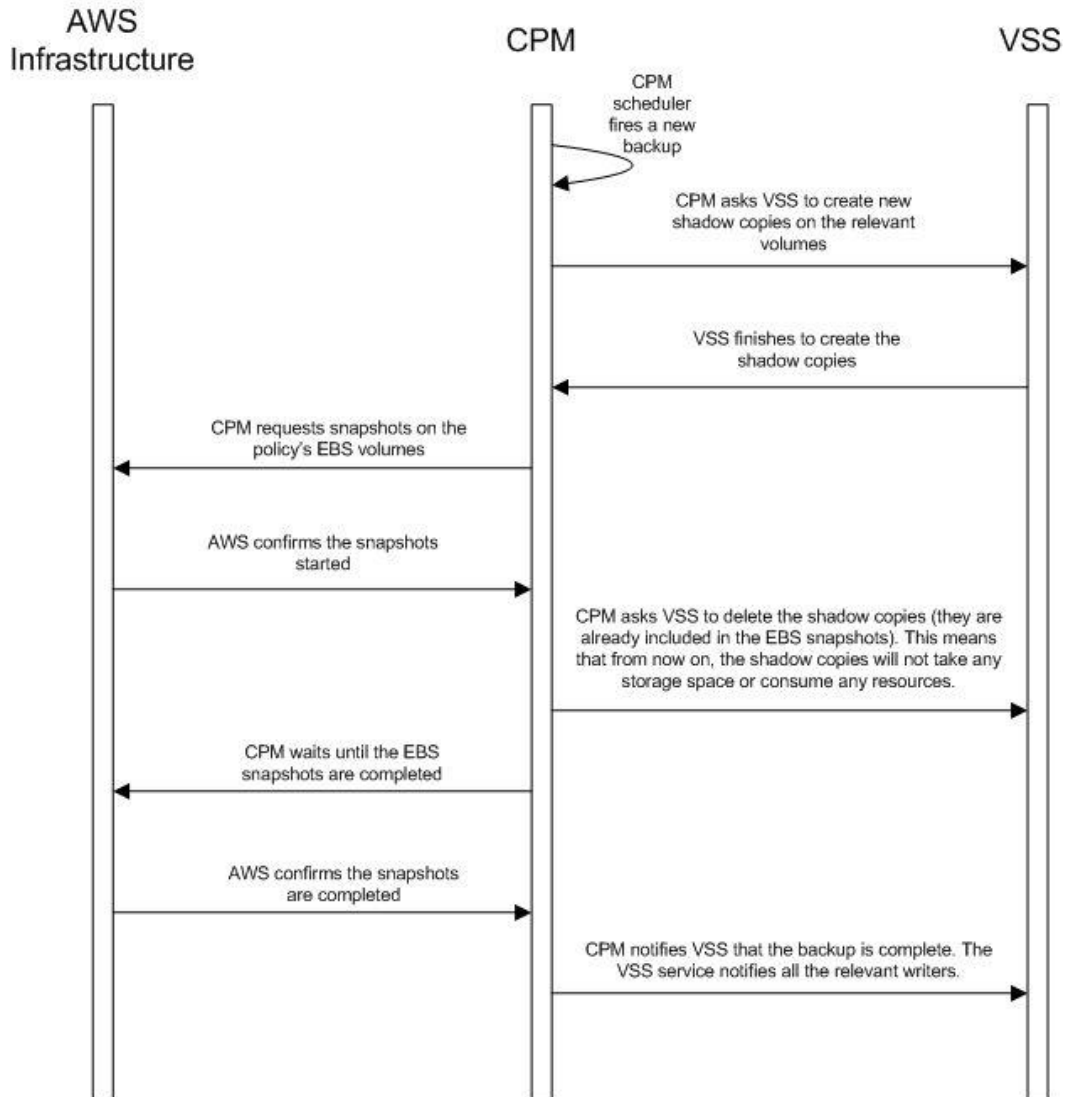
### 6.3.1 How N2WS Uses VSS

The N2WS Agent or SSM Agent performs under the role of a **VSS Requestor** to request the VSS **System Provider** to perform shadow copies. The process is:

- When N2WS initiates a backup, it **requests** a backup agent to invoke a backup of all relevant volumes. The agent then requests the VSS System Provider to start the shadow copy.
- VSS only creates differential copies, which means that in order for the N2WS to fully backup each volume, a few extra MBs are needed for the backup to complete. The amount of MBs depends on the size of the volume and the amount of data written since the last backup. Once the backup is complete, the backup agent will request the VSS Provider to delete the shadow copies. The agent will notify all relevant VSS writers that

the backup is complete, only after making sure all the EBS snapshots are completed successfully.

You can see the process depicted below.



### 6.3.2 Configuring VSS

By default, VSS is enabled when a backup agent is associated with an instance in a policy. In many cases, you will not need to do anything. By default, VSS will take shadow copies of all the volumes. However, you may want to exclude some volumes. For example, since the system volume (typically C:\) cannot be used to recover the instance in a regular scenario, you may want to exclude it from the backup.

**To make shadow copies of only some of the volumes:**

1. In the Instance and Volume configuration screen, change the value of **Volumes for shadow copies**.
2. Type drive letters followed by a colon, and separate volumes with a comma, e.g. **D:**, **E:**, **F:**.



### 6.3.3 Excluding and Verifying VSS Writers

Writer exclusions and inclusions are configured using a text file, not the UI.

You may wish to exclude **VSS Writers** from the backup process in cases where the writer is:

- Failing the backup.
- Consuming too many resources.
- Not essential for the backup's consistency.

#### To exclude VSS writers:

In the subfolder `scripts` under the installation folder of the agent (on the backed-up instance), create a text file named `vss_exclude_writers_<policy-name>.txt` with the following structure:

- Each line will contain a writer ID (including the curly braces)
- If you write in one of the lines `all`, all writers will be excluded. This can be handy sometimes for testing purposes.

In some cases, you want to make sure that certain writers are included (verified) in the shadow copy, and if not, fail the operation.

#### To verify writers:

In the subfolder `scripts` under the installation folder of the agent (on the backed-up instance), create a text file named `vss_verify_writers_<policy-name>.txt` with the following structure:

- Each line will contain a writer ID (including the curly braces).
- `all` is not an option.

An example of a line in either of the files is:


```
{4dc3bdd4-ab48-4d07-adb0-3bee2926fd7f}
```

### 6.3.4 Troubleshooting VSS Issues

When a VSS-enabled policy runs, you will see its record in the **Backup Monitor** tab.

- If it finished with no issues, the status of the record will be **Backup Successful**.
- If there were issues with VSS, the status will be **Backup Partially Successful**.

#### To troubleshoot:

- To view the errors that VSS encountered, look in the backup log.
- To view the output of the exact VSS error, select  **Recover**.
- To view the VSS Disk Shadow log, select its link in the recovery panel. There is a link for each of the agents in the policy, with the instance ID stated.
- In most cases, VSS will work out of the box with no issues. There can be a failure from time to time in stressed system conditions.
- If the writers do not answer the **freeze** request fast enough, the process times out and fails. Often, the retry will succeed.
- When VSS is constantly failing, it is usually a result of problems with one of the writers. This could be due to some misconfiguration in your Windows system.
- In most cases, the problem is out of the scope of N2WS. The best way to debug such an issue is to test VSS independently. You can run the Diskshadow utility from a command



line window and use it to try and create a shadow copy. Any issue you have with VSS using N2WS should also occur here.

- To learn how to use the Diskshadow utility, see: <https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/diskshadow>
- You may see failures in the backup because VSS times out or is having issues. You will see that the backup has status **Backup Partially Successful**. Most times you will not notice it since N2WS will retry the backup and the retry will succeed.
- If the problem repeats frequently, check that your Windows Server is working properly. You can check the application log in Window's Event Log. If you see VSS errors reported frequently, contact [N2W Software support](#).

### 6.3.5 VSS Recovery

Recovering instances using N2WS is covered in section 10. When recovering a Windows Server that was backed up with VSS, you need to revert back to the shadow copies in the recovery volumes to get the consistent state of the data.

**To revert back to shadow copies after VSS recovery:**

1. Connect to the newly recovered instance.
2. Stop the services of your application, e.g. SQL Server, Exchange, SharePoint, etc.
3. Open an administrator command line console and type `diskshadow`.
4. In the recovery panel screen, select the **VSS DiskShadow Data** link to find the IDs of the shadow copies made for the required backup.
5. Type `revert {shadow id}` for each of the volumes you are recovering, except for the system volume (C: drive). After finishing, the volumes are in a consistent state.
6. Turn the services on and resume work.

If you wish to recover a system disk, it cannot be reverted to the shadow copy using this method. The system volume should not contain actual application data as it is not a recommended configuration, and, therefore, you should be able to skip this revert operation. However, you can expose the system disk from the shadow and inspect its contents.

**To expose the system disk from the shadow:**

1. In the Diskshadow utility, type: `expose {shadow id} volletter:`
2. After finishing, remember to unexpose the disk.
3. To avoid unnecessary resource consumption, delete the shadow: `(delete shadow {shadow id})`.

### Reverting to a shadow copy for a system volume

If you have a strict requirement to recover the consistent shadow copy for the system volume as well, do the following:

1. Before reverting for other volumes, stop the instance; wait until it is in **stopped** state.
2. Using the AWS Console, detach the EBS volume of the C: drive from the instance and attach it to another Windows instance as an "additional disk".
3. Using the Windows Disk Management utility, make sure the disk is online and exposed with a drive letter.



4. Go back to the process in the previous section (VSS Recovery), and revert to the snapshot of drive C which will now have a different drive letter. Since it is no longer a system volume, it is possible to do so.
5. Detach the volume from the second Windows instance, reattach to the original instance using the original device, which is typically `/dev/sda1`, and turn the recovered instance back on.

**Note:** Shadow copy data is stored by default in the volume that is being shadowed. However, in some cases, it is stored on another volume. In order for you to be able to recover, you need to make sure that the volume the shadow copy is on is included in the backup and the recovery operation.

**Important:** If you revert a volume that contains another volume's shadow data, the reversion will take the volume to a state where it no longer contains the second volume's backup data, as the second volume would need to be reverted before the first volume can be reverted. If you accidentally restore the shadow copies in the wrong order, just delete the recovered instance and its data volumes and begin the recovery operation again from N2WS, taking care to revert the shadow copies in the correct order.

## 6.4 Using Backup Scripts on Windows

Besides VSS, there is also the option to run backup scripts to achieve backup consistency. It is also possible to add backup scripts in addition to VSS.

**Note:** PowerShell backup scripts for use with an SSM agent do not require the 'ps' file extension.

- You enable backup scripts in the Instance and Volume Configuration screen of the instance in the policy and select the type of agent that you want to execute the scripts.
- All scripts are named with a prefix plus the name of the policy.
- There are 3 types of events. If scripts are used, a script must be provided for each of these events. If all of the scripts are not defined, N2WS will treat the missing script as a failing script.
  - Before the VSS backup - `BEFORE_<policy-name>.<ext>`
  - After the VSS backup started - `AFTER_<policy-name>.<ext>`
  - After the VSS backup has completed - `COMPLETE_<policy-name>.<ext>`
- Scripts can have any extension as long as they are executable. They can be batch scripts, VBS scripts, PowerShell, or even binary executables. However, N2WS cannot run PowerShell scripts directly as Windows scripts.
- All scripts must be set with exit code zero 0.

### 6.4.1 Location and Execution of Scripts

When using the N2WS Thin Backup Agent:





- As opposed to Linux, Windows backup scripts run directly on the agent. All the scripts are located in the subfolder `scripts` under the installation folder of the N2WS Thin Backup Agent.
- If the N2WS user that owns the policy is not the root user, the scripts will be under another subfolder with the user name (e.g. `...\scripts\cpm_user1`).
- Scripts are launched by N2WS Thin Backup Agent, so their process is owned by the user that runs the agent service. By default, this is the local system account. However, if you need to run it under a different user you can use the service manager to change the logged-on user to a different one. For example, you might want to run it with a user who has administrative rights in a domain.

When using the SSM Agent:

- Scripts are saved locally on the N2WS server and invoked remotely.
- Scripts must be saved in `/cpmdata/scripts/<username>/<instance_id>/`
- Script names are the same as for the N2WS Thin Backup Agent. The PowerShell file extension is not required.

### 6.4.2 Before Script

The `before_<policy-name>.<ext>` runs before the backup begins. Typically, this script is used to move applications to backup mode. The **before** script leaves the system in a **frozen** state. This state will stay for a very short while, until the snapshots of the policy start, which is when the **after** script is started.

### 6.4.3 After Script

The `after_<policy-name>.<ext>` script runs after all the snapshots of the policy start. It runs shortly after the **before** script, generally less than 2-3 seconds. This script releases anything that may have been frozen or locked by the **before** script.

This script accepts the success status of the **before** script. If the **before** script succeeded, the argument will be one `1`. If it failed, crashed, or timed out, the argument will be zero `0`.

**Note:** This is the opposite of the exit status. Think of it as an argument that is true when the **before** script succeeded.

### 6.4.4 Complete Script

The `complete_<policy-name>.<ext>` script runs after all snapshots are completed.

Usually, the script runs quickly since snapshots are incremental. This script can perform clean-up after the backup is complete and is typically used for transaction log truncation.

The script accepts one argument. If the entire backup was successful and all the previous scripts were successful, it will be one `1`. If any issues or failures happened, it will be zero `0`. If this argument is `1`, truncate logs.

**Important:** When you enable backup scripts, N2WS assumes you implemented all three scripts. Any missing script will be interpreted as an error and be reflected in the backup status. Sometimes the “complete” script is often not needed. In this case,





write a script that just exits with the code zero 0, and the policy will not experience errors.

### **6.4.5 Capturing the Output of Backup Scripts**

You can have the output of backup scripts collected and saved in the N2WS Server. See section 4.2.4.



## 7 Linux/Unix Instances Backup

Making an application-consistent backup of Linux instances does not require any agent installation. Since the N2WS server is Linux based, backup scripts will run on it. Typically, such a script would use SSH to connect to the backed-up instance and perform application quiescence. However, this can also be accomplished using custom client software. There is no parallel to VSS in Linux, so the only method available is by running backup scripts.

### 7.1 Connecting to the N2WS Server

To create, test, and install backup scripts, you will need to connect to the N2WS server using SSH with `cpmuser`. The only way to authenticate `cpmuser` is by using the private key from the key pair you used when you launched the N2WS server instance. As long as your key is not compromised, no unauthorized person will be able to connect to the N2WS server. With `cpmuser`, you will be able to copy (using secure copy), create, and test your scripts. `cpmuser` is the same user N2WS will use to run the scripts. If you need to edit your scripts on the N2WS Server, you can use Vim or nano editors. Nano is simpler to use.

### 7.2 Backup scripts

**Note:** If an SSM remote agent for a Windows instance target is running, all before and after backup scripts must be PowerShell scripts.

Backup scripts should be placed in the path `/cpmdata/scripts`. If the policy belongs to an N2WS user other than the root user, scripts will be located in a subfolder named like the user (e.g. `/cpmdata/scripts/cpm_user1`). This path resides on the CPM data volume and will remain there even if you terminate the N2WS server instance and wish to launch a new one. Backup scripts will remain on the data volume, together with all other configuration data. As `cpmuser`, you have read, write, and execute permissions in this folder.

- All scripts should exit with the code 0 when they succeed and 1 (or another non-zero code) when they fail.
- All scripts have a basename (detailed for each script in the coming sections) and may have any addition after the basename. The delimiter between the base part of the name and the file extension is a period (.). For example:  
`before_policy1.v11.5.bash`  
where 'before\_policy1' is the base name, 'v11.5' is the optional additional part of the name, and 'bash' is the file extension.
- Scripts can be written in any programming language: shell scripts, Perl, Python, or even binary executables.
- You only have to make sure the scripts can be executed and have the correct permissions.



**Warning:** Having more than one script with the same base name can result in unexpected behavior. N2WS does not guarantee which script it will run, and even to run the same script every backup.

There are three scripts for each policy:

- Before
- After
- Complete

### 7.2.1 Before Script

The `before_<policy-name>[.optional_addition].<ext>` script runs before backup begins. Typically, this script is used to move applications to backup mode. The **before** script typically leaves the system in a frozen state for a short time until the snapshots of the policy are fired. One option is to issue a `freeze` command to a file system like `xfs`.

### 7.2.2 After Script

The `after_<policy-name>[.optional_addition].<ext>` script runs after all the snapshots of the policy fire. It runs within a few seconds after the **before** script. This script releases anything that may have been frozen or locked by the **before** script. This script accepts the success status of the **before** script. If the **before** script succeeded, the argument will be `1`. If it failed, crashed, or timed out, the argument will be `0`.

**Note:** This is the opposite of the exit status. Think of this as an argument that is true when the **before** script succeeds.

### 7.2.3 Complete Script

The `complete_<policy-name>[.optional_addition].<ext>` script runs after all snapshots are completed. Usually, it runs quickly since snapshots are incremental. This script can perform clean-up after the backup is complete and is typically used for transaction log truncation. The script accepts one argument. If the entire backup was successful and all the previous scripts were successful, it will be `1`. If any issues or failures happened, it will be `0`. If this argument is `1`, truncate logs.

### 7.2.4 Capturing the Output of Backup Scripts

You can have the output of backup scripts collected and saved in the N2WS Server, see section 4.2.4.

### 7.2.5 Troubleshooting and Debugging Backup Scripts

**Note:** Verify that if an SSM remote agent is in use for a Windows instance all scripts are PowerShell.

You can use the output collected by N2WS to debug backup scripts. However, the recommended way is to run them independently of N2WS, on the N2WS Server machine using



SSH. You can then view their outputs and fix what is needed. Once the scripts work correctly, you can start using them with N2WS. Assuming these scripts are using SSH, during the first execution you will need to approve the SSH key by answering `yes` at the command line prompt. If you terminate your N2WS Server and start a new one, you will need to run the scripts again from the command line and approve the SSH key.

## 7.2.6 Example Backup Scripts

Following is an example of a set of backup scripts that use SSH to connect to another instance and freeze a MySQL Database:

- The **before** script will flush and freeze the database.
- The **after** script will release it.
- The **complete** script will truncate binary logs older than the backup.

**Note:** These scripts are presented as an example *without* warranties. Test and make sure scripts work in your environment as expected before using them in your production environment.

The scripts are written in `bash`:

**before\_MyPolicy.bash**

```
#!/bin/bash

ssh -i /cpmdata/scripts/mysshkey.pem sshuser@ec2-host_name.compute-1.amazonaws.com "mysql -u root -p<MySQL root password> -e 'flush tables with read lock; flush logs;'"

if [ $? -gt 0 ]; then
    echo "Failed running mysql freeze" 1>&2
    exit 1
else
    echo "mysql freeze succeeded" 1>&2
fi
```

This script connects to another instance using SSH and then runs a MySQL command. Another approach would be to use a MySQL client on the N2WS Server, and then the SSH connection will not be necessary.

After that script is executed, the N2WS server will start the snapshots, and then call the next script:

**after\_MyPolicy.bash**

```
#!/bin/bash

if [ $1 -eq 0 ]; then
    echo "There was an issue running first script" 1>&2
fi

ssh -i /cpmdata/scripts/mysshkey.pem sshuser@ec2-host_name.compute-1.amazonaws.com "date +%F %H:%M:%S > sql_backup_time; mysql -u root -p<MySQL root password> -e 'unlock tables;'"

if [ $? -gt 0 ]; then
```



```
echo "Failed running mysql unfreeze" 1>&2
exit 1
else
    echo "mysql unfreeze succeeded" 1>&2
fi
```

This script checks the status in the first argument and then does two things:

- First, it saves an exact timestamp of the current backup of the frozen database to a file,
- Then, it releases the lock on the MySQL table.

After that, when all snapshots succeed, N2WS runs the **complete** script:

**complete\_MyPolicy.bash**

```
#!/bin/bash
if [ $1 -eq 1 ]; then
    cat /cpmdata/scripts/complete_sql_inner |ssh -i
/cpmdata/scripts/mysshkey.pem sshuser@ec2-host_name.compute-
1.amazonaws.com "cat > /tmp/complete_ssh; chmod 755 /tmp/complete_ssh;
/tmp/complete_ssh"
    if [ $? -gt 0 ]; then
        echo "Failed running mysql truncate logs" 1>&2
        exit 1
    else
        echo "mysql truncate logs succeeded" 1>&2
    fi
else
    echo "There was an issue during backup - not truncating logs" 1>&2
fi
```

It calls an inner script, **complete\_sql\_inner**:

```
butime=`<sql_backup_time`
mysql -u root -p<MySQL root password> -e 'PURGE BINARY LOGS BEFORE
"$butime"'
```

These two scripts purge the binary logs only if the **complete** script receives 1 as the argument. They purge logs earlier than the time in the timestamp files.

## 7.2.7 Scripts and SSH Access in a Multi-user Environment

If your N2WS configuration requires multiple users, which are separated from each other, you may wish to allow users to access N2WS using SSH to create and debug backup scripts:

- Create additional Linux users in the N2WS instance and allowing each user access to their own scripts folder only.
- `cpmuser` will need to be able to access and execute the scripts of all users. This can be achieved by assigning the user `cpmuser` as the group of all user subfolders and scripts. Then, if given **executable** permissions for the group, `cpmuser` will be able to access and execute all scripts.



## 8 Using Elastic File System (EFS) with N2WS

Configuring EFS on N2WS allows you to determine backup:

- Schedule and frequency
- Retention
- Lifecycle policy, including moving backups to cold storage, defining expiration options, and deleting them at end of life.

With AWS Backup, you pay only for the amount of backup storage you use and the amount of backup data you restore in the month. There is no minimum fee and there are no set-up charges.

**Important:** EFS Backup and Restore is performed by AWS Backup Service.


When adding an EFS target for the first time in a region, you must create the default backup vault in AWS. Go to the AWS Backup console and choose **Backup vaults**.

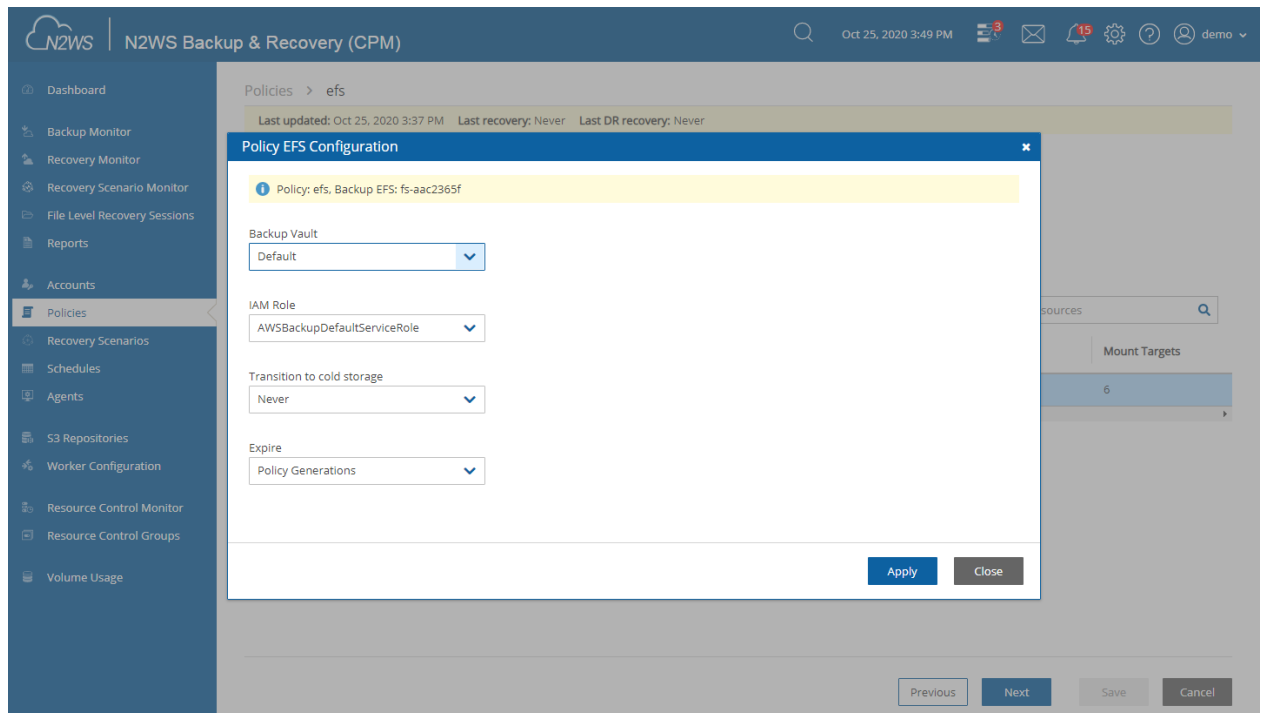
For more information regarding the AWS Backup Service, refer to <https://docs.aws.amazon.com/efs/latest/ug/awsbackup.html>

**Notes:** Before continuing, consider the following:

- Currently, AWS Backup service doesn't support cross-account DR for EFS resources.
- Check AWS for regions that are available for EFS backup on the AWS Backup service. Currently, regions EU (Milan) and Africa (Cape Town) are not supported by AWS for cross-region DR.
- AWS Backup is not available for EFS in the following regions: Asia Pacific (Hong Kong), Europe (Stockholm), South America (Sao Paulo), and Middle East (Bahrain).
- Backup transitions and expirations are performed automatically according to the configured lifecycle.
- A default or custom IAM role must exist in AWS to create and manage backups on behalf of N2WS. The IAM identity contains the backup and restore policies allowing operations on EFS. If a default was not automatically created, or you prefer to use a custom IAM role, see section 8.2.

### 8.1 Configuring EFS

1. In the AWS Console, create the EFS in one of the available regions listed in section 8.
2. In N2WS, in the **Backup Targets** tab of a Policy, select **Elastic File Systems** in the **Add Backup Targets** menu.
3. In the **Add Elastic File System** screen list, select one or more EFS targets and then select **Add selected**.
4. In the **Backup Targets** tab, select an EFS target and then select  **Configure**.
5. Configure the EFS backup and restore options and select **Apply**.



- **Backup Vault** – A logical backup container for your recovery points (your EFS snapshots) that allows you to organize your backups.

Note: Default Backup vaults are created in AWS: **AWS Backup > Backup vaults**.

- **IAM Role** – An IAM identity that has specific permissions for all supported AWS backup services. The following AWS backup permissions should be attached to your IAM role:
  - **AWSBackupServiceRolePolicyForBackup** - Create backups on your behalf across AWS services.
  - **AWSBackupServiceRolePolicyForRestores** - Perform restores on your behalf across AWS services.

If a default IAM role was not automatically created by AWS, or you require a custom IAM role, see section 8.2. Selecting the preferred IAM role is only required during the EFS policy configuration.

Note: If adding or removing IAM Role permissions for immediate use, reboot the instance to have the change take effect quickly.

- **Transition to cold storage**– Select the transition lifecycle of a recovery point (your EFS snapshots). The default is **Never**.
- **Expire** – When does a protected resource expire. The default is **Policy Generations**.

Note: Moving a backup to the Freezer will set **Expire** to **Never**.

6. When finished, select **Apply**.
7. Select **Save** in the Backup Targets screen to save the configuration to the policy.

## 8.2 Creating IAM Roles in AWS

A default or custom IAM role is necessary for AWS to perform EFS operations on behalf of N2WS.



**Note:** If adding or removing IAM Role permissions for immediate use, reboot the instance to have the change take effect promptly.

#### To create a default IAM Role:

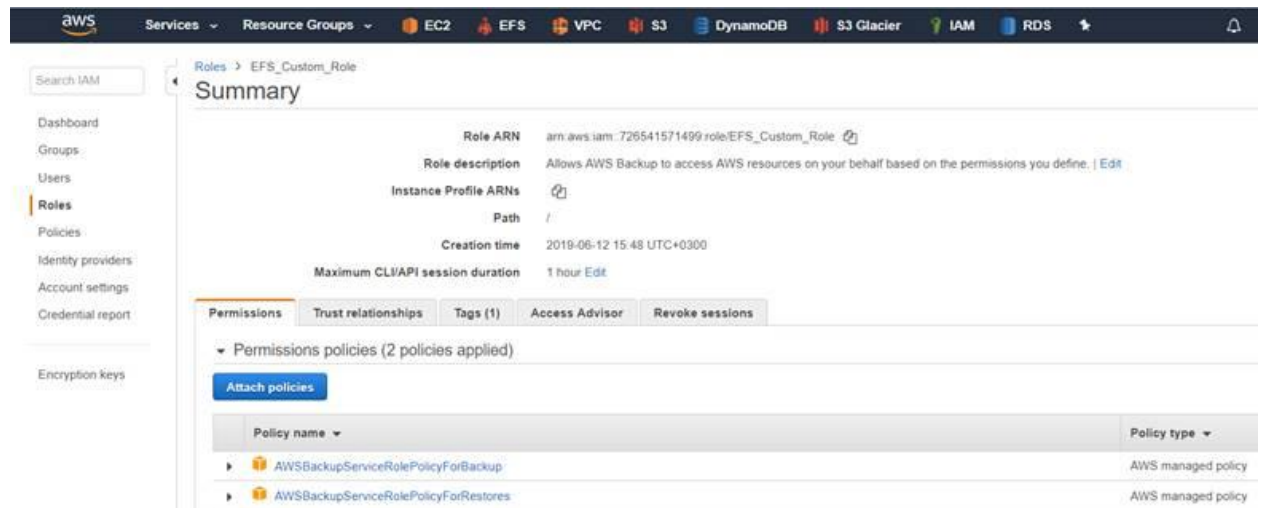
1. Go to the AWS Backup Service:  
<https://us-east-1.console.aws.amazon.com/backup/>
2. Select **Create an on-demand backup**.
3. For **Resource type**, select **EBS**.
4. For **Volume ID**, select **any EBS volume to backup**.
5. Select **Default IAM Role**.
6. Select **Create on-demand backup**. Ignore the error provided by AWS.
7. Verify that the following role was created on AWS IAM Service:



#### To create a custom IAM Role:

1. Go to AWS IAM Service:  
<https://console.aws.amazon.com/iam/home#/roles>
2. Select **Create role**.
3. Select **AWS Backup** and then select **Next: Permissions**.
4. Search for **BackupService**.
5. Select the following AWS managed policies:  
**AWSBackupServiceRolePolicyForBackup**  
**AWSBackupServiceRolePolicyForRestores**
6. Select **Next: Tags** and then select **Next: Review**.
7. Enter a **Role name** and select **Create role**.





Search IAM

Dashboard

Groups

Users

**Roles**

Policies

Identity providers

Account settings

Credential report

Encryption keys

Services ▾ Resource Groups ▾ EC2 EFS VPC S3 DynamoDB S3 Glacier IAM RDS ↗

Roles > EFS\_Custom\_Role

### Summary

**Role ARN** arn:aws:iam::726541571499:role/EFS\_Custom\_Role

**Role description** Allows AWS Backup to access AWS resources on your behalf based on the permissions you define. [Edit](#)

**Instance Profile ARNs** /

**Path** /

**Creation time** 2019-06-12 15:48 UTC+0300

**Maximum CLI/API session duration** 1 hour [Edit](#)

Permissions Trust relationships Tags (1) Access Advisor Revoke sessions

▼ Permissions policies (2 policies applied)

[Attach policies](#)

Policy name ▾	Policy type ▾
<a href="#">AWSBackupServiceRolePolicyForBackup</a>	AWS managed policy
<a href="#">AWSBackupServiceRolePolicyForRestores</a>	AWS managed policy

## 8.3 Backup Options for EFS Instances

EFS can be configured by creating the **cpm backup** tag with the following options. In this case, N2WS will override the EFS configuration with the tag values. See section 14.1.4 for keys and values.



## 9 Additional Backup Topics

### 9.1 N2WS in a VPC Environment

The N2WS Server runs in a VPC, except in old environments utilizing EC2 Classic. For N2WS to work correctly, it will need outbound connectivity to the Internet. To use AWS endpoints, see [AWS Regions and Endpoints](#).

- You will need to provide such connectivity using one of the following methods:
  - Attaching an Elastic IP
  - Using a dynamic public IP, which is not recommended unless there is a dynamic DNS in place
  - Enabling a NAT configuration, or
  - Using a proxy
- You will need to access it using HTTPS to manage it and possibly SSH as well, so some *inward* access will need to be enabled.
- If you will run Linux backup scripts on it, it will also need network access to the backed-up instances.
- If N2WS backup agents will need to connect, they will need access to it (HTTPS) as well.
- If backup scripts are enabled for a Linux backed-up instance, it will need to be able to get an *inbound* connection from the N2WS Server.
- If a Thin Backup Agent is used in a Windows backed-up instance, the agent will need *outbound* connectivity to the N2WS Server.

### 9.2 Backup when an Instance is Stopped

N2WS continues to back up instances even if they are stopped. This may have important implications:

- If the policy has backup scripts and they try to connect to the instance, they will fail, and the backup will have **Backup Partially Successful** status.
- If the policy has no backup scripts and VSS is not configured, or if the policy's options indicate that **Backup Partially Successful** is considered successful (section 4.2.2), the backup can continue running, and automatic retention will delete older backups. Every new backup will be considered a valid backup generation.
- Snapshots will soon take no storage space since there will be no changes in the volumes, and EBS snapshots are incremental.
- Assuming the instance was shut down in an orderly manner and did not crash, backups will be consistent by definition.

**Note:** It is recommended that if you are aware of an instance that will be stopped for a while, you disable the policy by selecting its name and changing **status** to **disabled**.

Another way to proceed is to make sure the policy is not entirely successful when the instance is stopped by using backup scripts and to keep the default stricter option that treats script



failure as a policy failure. This will make sure that the older generations of the policy, before it was stopped, will not be deleted.

**Important:** If you disable a policy, you need to be aware that this policy will not perform backup until it is enabled again. If you disable it when an instance is stopped, make sure you enable it again when you need the backup to resume.


## 9.3 The Freezer

Backups belonging to a policy eventually get deleted. Every policy has its number of generations, and the retention management process automatically deletes older backups. To keep a backup indefinitely and make sure it is not deleted, move it to the Freezer. There can be several reasons to freeze a backup:




- An important backup of an instance you already recovered from so you will be able to recover the same instance again if needed.
- A backup of interest, such as the first backup after a major change in the system or after an important update.
- You want to delete a policy and only keep one or two backups for future needs.
- Elements in the freezer will not be deleted by the automatic **Cleanup** process.





### To move a backup to the Freezer:

**Note:** Once a backup is moved to the freezer, you will *not* be able to move it back.

1. In the left panel, select the **Backup Monitor** tab.
2. Select the backup and then select  **Move to Freezer**.
3. Type a unique name and an optional description for identification and as keywords for searching and filtering later.

After a backup is in the Freezer:

- Frozen backups are identified by the frozen symbol  in the **Lifecycle Status** column of the **Backup Monitor** tab.
- It will only be deleted if you do so explicitly. Use  **Delete Frozen Item**.
- It will still remain even if you delete the whole policy, frozen backups from the policy will still remain.
- It is recovered the same way as from a regular backup.
- You can search and filter frozen backups using as keywords the name or description. To change the name or description, select  **Edit Frozen Item**.

While in the **Backup Monitor**, you can switch between showing backup records 'in the Freezer' by turning on and off the  toggle key and backup records 'not in the Freezer' by turning on and off the  toggle key in the **Show** area   on the far right of the filters line.

## 9.4 Running Automatic Cleanup

Automatic Cleanup allows you to manage the frequency of the cleanup process and the:


- Number of days to keep backup records, even if the backup is deleted.



- Number of days after which to rotate single AMIs.

**Note:** Keeping backups for long periods of time can cause the N2WS database to grow and therefore affect the size you need to allocate for the CPM data volume. N2W Software estimates that every GiB will accommodate the backup of 10 instances. N2W Software estimates that 10 instances are correct when every record is kept for around 30 days. If you want to keep records for 90 days, triple the estimate, i.e. for 10 instances make the estimate 3 GiB, for 20 make the estimate 6 GiB, etc.

#### To manage the number of generations saved:

1. In the toolbar, select  **Server Settings**.
2. In the **General Settings** tab, select **Cleanup**.
3. In the **Cleanup Interval** list, select the number of hours between cleanup runs. Select **Cleanup Now** to start a cleanup immediately.
4. In each list, select the number of days to:
  - Rotate Single AMIs
  - Keep Deleted Records
  - Keep User Audit logs
  - Keep Resource Control Records

**Note:** The number of days is counted since the backup was created and not deleted. If you want to make sure every backup record is saved for 90 days after creation, even if it was already deleted, select 90.

5. To keep retry backup records for reporting, select **Keep Retry Backup Records**. The S3 Cleanup runs independently according to the retention period configured for the policy in the backup copy settings. See section 21.1. The last S3 Cleanup Log however, is available in the **Cleanup** tab.

## 9.5 Backing up Independent Volumes

Backing up independent volumes in a policy is performed regardless of the volume's attachment state. A volume can be attached to any instance or not attached at all, and the policy will still back it up. Backup scripts can determine which instance is the active node of a cluster and perform application quiescence through it.


## 9.6 Excluding Volumes from Backup

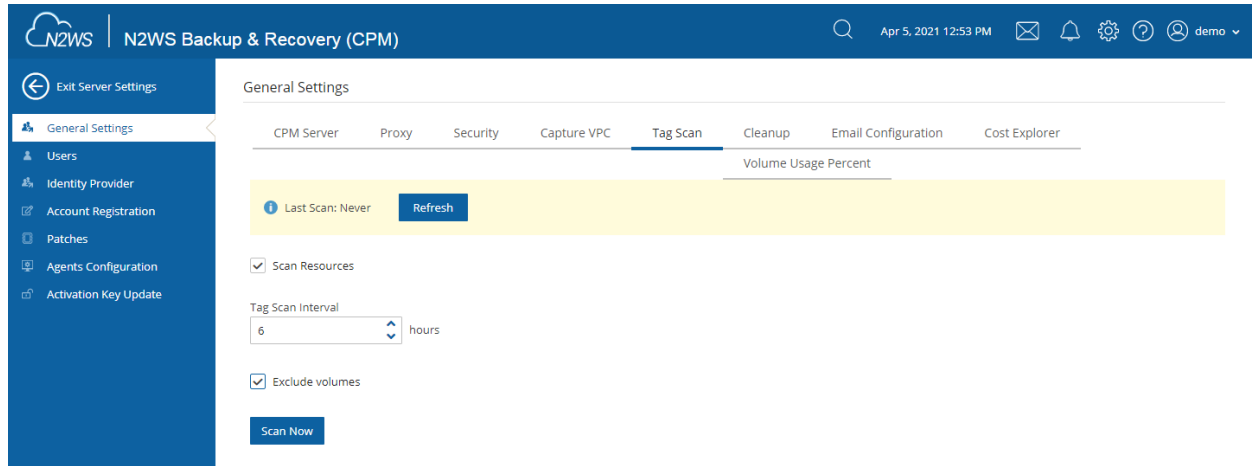
**Note:** If you enable the **Exclude volumes** option in the **Tag Scan** tab of the **General Settings**:

- The **Exclude volumes** option overrides the exclusion of volumes performed through the UI.
- Tagged instances are not included in the **Exclude volumes** option and are excluded from backup *only* when tagged with '**#exclude**' for the policy.

Following are the ways to exclude volumes from backup:



- Enabling the **Exclude volumes** option in **General Settings**:
  - In the toolbar, select  **Server Settings** > **General Settings**.
  - In the **Tag Scan** tab, select **Exclude volumes** and then select **Scan Now**.



- Excluding a volume from a policy configuration in the UI. See section 4.2.3
- Disabling a scheduled backup time. See section 4.1.4.
- Using an '#exclude' tag for the policy. See section 14.1.6.

## 9.7 Regions Disabled by Default

To perform certain actions on Asia Pacific (Hong Kong) and Middle East (Bahrain) AWS regions, managing Session Token Services (STS) is required, as Session Tokens from the global endpoint (<https://sts.amazonaws.com>) are only valid in AWS Regions that are enabled by default. For AWS Regions not enabled by default, users have to configure their AWS Account settings.

**To configure AWS Account settings to enable Session Tokens for all regions:**

1. Go to your AWS console and sign in at <https://console.aws.amazon.com/iam>
2. In the navigation pane, select **Account settings**.
3. In the 'Security Token Service (STS)' section, select Change Global endpoint.
4. In the Change region compatibility of session tokens for global endpoint dialog box, select Valid in all AWS Regions.

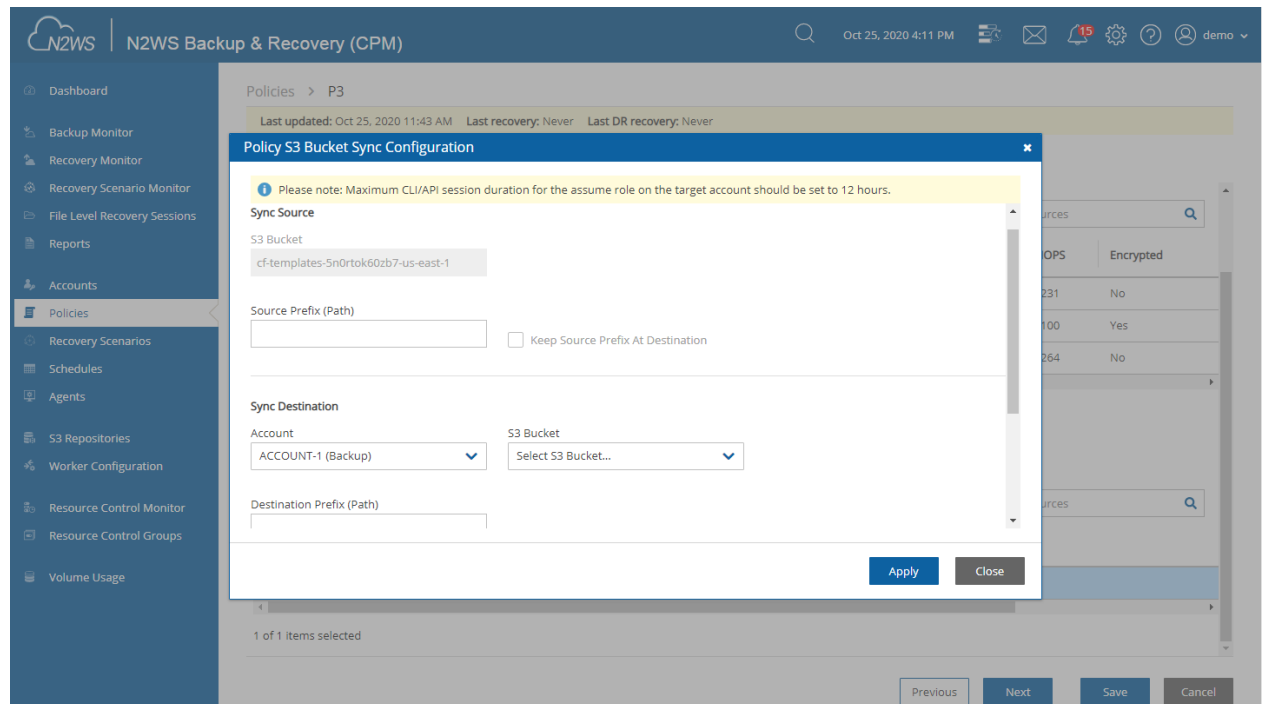
**Note:** Session tokens that are valid in all AWS regions are larger. If you store session tokens, these larger tokens might affect your system.

For more information on how to manage your STS, see [https://docs.aws.amazon.com/IAM/latest/UserGuide/id\\_credentials\\_temp\\_enable-regions.html](https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp_enable-regions.html)

## 9.8 Synchronizing S3 Buckets

You can automatically synchronize S3 buckets using the N2WS S3 Bucket Sync feature. When the policy backup runs, N2WS will copy the source bucket to the destination bucket, without creating a backup. The buckets are selected and configured in **Backup Targets** of the **Policies** tab.





5. In the Sync Source section, you have options to enter a **Source Prefix (Path)** and to select whether to **Keep Source Prefix at Destination**. This option will allow you to combine the source prefix with the destination prefix. For example, if the source prefix is '/a/b/' and the destination prefix is '/c/d/', the objects will be synchronized to 'a/b/c/d'.
6. In the Sync Destination section, configure the following:
  - **Region** – Select the destination region to copy to.
  - **Account** – Select the destination account to copy to.
  - **S3 Bucket** – Select the destination bucket. The account for the destination bucket may be different than the account for the source bucket.


**Note:** For a cross-account S3 Bucket Sync:

- Allow access for source account in destination bucket by adding to **Access Control List** in AWS S3 console. To find the **Canonical ID**, in the AWS **Account** menu, go to **My security credentials** and scroll to **Account identifiers**.
- If using a custom KMS, allow the same in the destination bucket policy.
- Cross-account S3 Bucket Sync is executed with the account of the policy, not the account of the destination S3 bucket, and requires cross-account access permissions to objects that are stored in the destination S3 bucket. For further information, see: <https://aws.amazon.com/premiumsupport/knowledge-center/cross-account-access-s3/>
- **Destination Prefix (Path)** – Enter the destination prefix, if any. If a prefix is entered, the dynamic message under the box will display the destination prefix. If **Keep Source Prefix at Destination** was selected, the prefix will be the concatenation of the source and destination prefixes. For example, source prefix 'abc' and destination 'xyz' will result in a destination prefix of 'abc/xyz'.



- **Storage Class** – Select the S3 Storage Class or S3 Reduced Redundancy Storage:
  - **Standard** – For low latency and high throughput.
  - **Reduced Redundancy** - Enables customers to store non-critical, reproducible data at lower levels of redundancy than Amazon S3's standard storage.
  - **Standard IA** - For data that is accessed less frequently, but requires rapid access. Ideal for long-term storage.
- **Delete Extra** – Select to delete files that exist in the destination but not in the source during synchronization.

7. Select **Apply**.

**Note:** If you change the Storage Class of an S3 Bucket in the **Policies** tab, the Storage Class of an existing destination bucket will not automatically update during the next S3Sync run. In the **Policies** tab, select the S3 Bucket Sync object and then select  **Configure**.

After the Policy has run, view the backup log to see the S3Sync details:

Backup Log

Time	Level	Message
05/27/2020 3:25:52 PM	✓ Info	Backup is agentless, managed by CPM Server
05/27/2020 3:25:52 PM	✓ Info	Starting. Fired by schedule: Immediate/ASAP
05/27/2020 3:25:54 PM	✓ Info	S3Sync: Source bucket: cf-templates-5n0rtok60zb7-us-east-1 to Destination bucket: 1234567890 started
05/27/2020 3:25:54 PM	✓ Info	All snapshots started successfully
05/27/2020 3:26:10 PM	✓ Info	S3Sync: Source bucket: cf-templates-5n0rtok60zb7-us-east-1 to Destination bucket: 1234567890 - 1 objects copied, 0 objects deleted





## 10 Performing Recovery

N2WS offers several options for data recovery. Since all N2WS backup is based on AWS's snapshot technology, N2WS can offer rapid recovery of instances, volumes, and databases. Since a backup is not created for S3 Bucket Sync targets, recovery is neither needed nor possible.

**Recommendation:** N2W Software strongly recommends that you perform recovery drills occasionally to make sure your recovery scenarios work. It is not recommended to try it for the first time when your servers are down. Each policy on the policy screen shows the last time recovery was performed on it. Use the last recovery time data to track recovery drills.


### 10.1 Searching for Backups to Recover From

N2WS provides an enhanced search box to quickly find backup snapshots to recover from. In the Backup Monitor, you can search for snapshots based on the **Backup Target** type or policy, including frozen images.


To search for all backup snapshots:

1. Select **Backup Monitor**.
2. In the **Search backups** box, enter a string to search by. The string can be part of the resource ID or part of the resource tag value.
3. To filter by resource type, select a resource type in the list, such as RDS database.

The screenshot displays the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation links: Dashboard, Backup Monitor (selected), Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Backup Monitor' and features a search bar with the text 'Search backups'. Below the search bar is a dropdown menu for '20 records/page'. To the right of the search bar are three filter dropdowns: 'by instance', 'All Policies', 'All Accounts', and 'All Backup Statuses'. Below these filters is a table of backup records. The table has columns: 'policy / Frozen Item', 'Account', 'Status', 'DR Status', and 'Lifecycle'. The first row is highlighted in blue. Below the table, it says '1 of 8 items selected'.

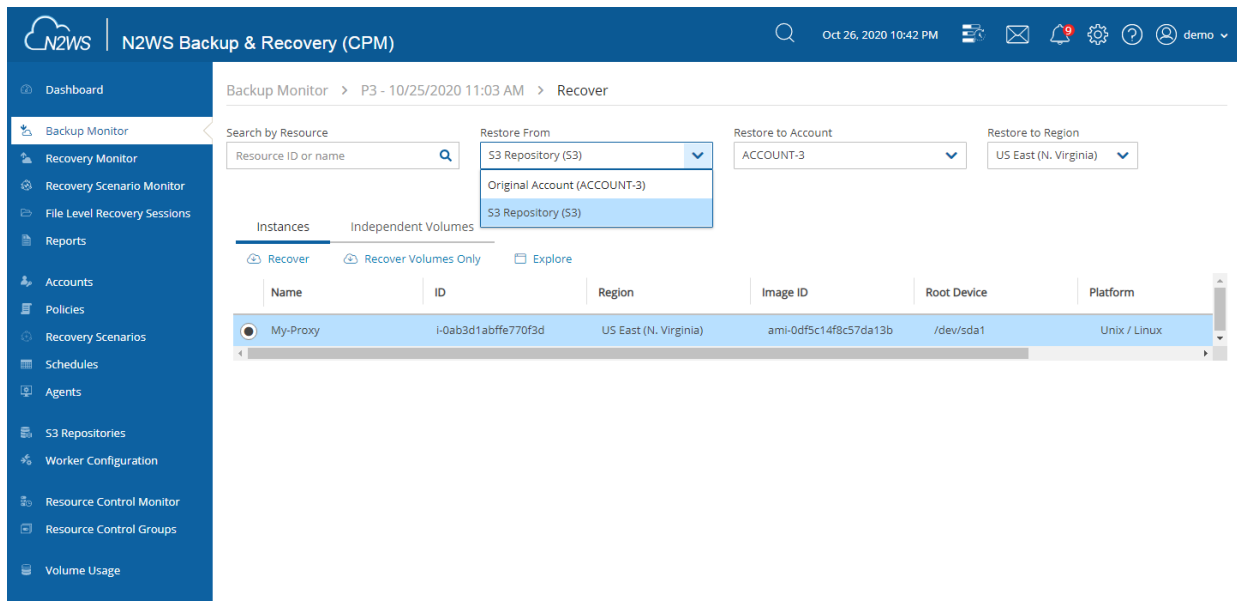
4. Select  and then choose a backup in the list.



When you select  **Recover** for a certain backup, you are directed to the **Backup Monitor Recover** screen. You can Search by Resource using the resource ID or name.

For backups with multiple resource types as targets, the Recover screen will have a separate tab for each type. Select a backup. The **Recover** screen opens.

To restore from an S3 Repository, select the repository in the **Restore From** list. For other considerations when recovering from an S3 Repository, see section 21.3.2.

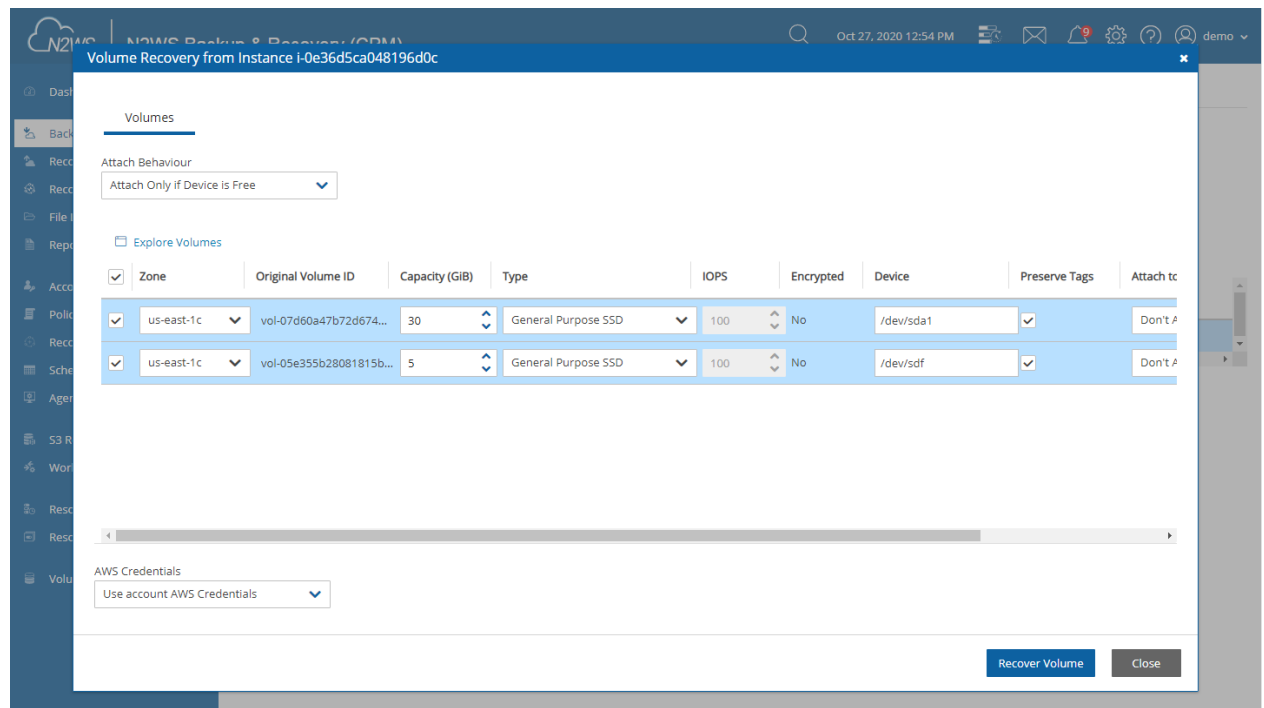


Depending on the specifics of the backup, the Recover screen includes:

- A search box for locating a resource by ID or name.
- Tabs for recovering the backed-up instances, independent volumes, databases, etc.
- Outputs of any backup scripts and VSS if it exists. These reference outputs may be important during a recovery operation.
- If this backup includes DR to another region, there will be a **Restore to Region** drop-down menu to choose in which region to perform the recovery.
- If you have cross-account functionality enabled for your N2WS license, there are two other drop-down menus:
  - **Restore to Account** list where you can choose to restore the resources to another account.
  - If you defined cross-account DR for this policy, you will have the **Restore from Account** list for choosing from which account to perform recovery.

**Note:** All the choices about regions and accounts you make in the recover screen apply to all the recovery operations that you initiate from this screen.

Choose the backups to recover and then select the **Recover** resource type button.



## 10.2 Recovery AWS credentials

All recovery screens have a drop-down list at the bottom labeled **AWS Credentials**. By default, the account AWS credentials used for backup will be used for recovery operations also. Depending on the backup, you can select **Provide Alternate AWS Credentials** and fill in different credentials for recovery. This can be useful if you want to use IAM-created backup credentials that do not have permissions for recovery. See section 16.3. When using custom credentials, N2WS verifies that these credentials actually belong to the recovery account.

**To use custom credentials:**

1. Select **Provide Alternate AWS Credentials** in the list. The custom credential boxes appear.
2. In the **AWS Access Key** box, enter your access key.
3. In the **AWS Secret Key** box, enter your secret key.

## 10.3 Instance Recovery

With Instance recovery, you can recover a complete instance with its data for purposes, such as:

- An instance crashed or is corrupted and you need to create a new one
- Creating an instance in a different AZ
- Creating an instance in a different region. See section 11.5.1.
- Creating an instance from a frozen image

When you recover an instance, by default, you recover it with its configuration, tags, and data, as they were at the time of the backup. However, you can change these elements:

- Instance type
- Placement



- Number of CPU cores and threads
- Architecture
- User data, etc.

You can also choose how to recover the system itself:

- For Linux EBS-based instances: if you have a snapshot of the boot device, you will, by default, use this snapshot to create the boot device of the new instance. You can, however, choose to create the new instance from its original image or a different one.
- For instance-store-based: you will only have the image option. This means you cannot use the snapshot of the instance's root device to launch a new instance.
- For EBS-based Windows Servers: there is a limitation in AWS, prohibiting launching a new instance from a snapshot, as opposed to from an AMI.

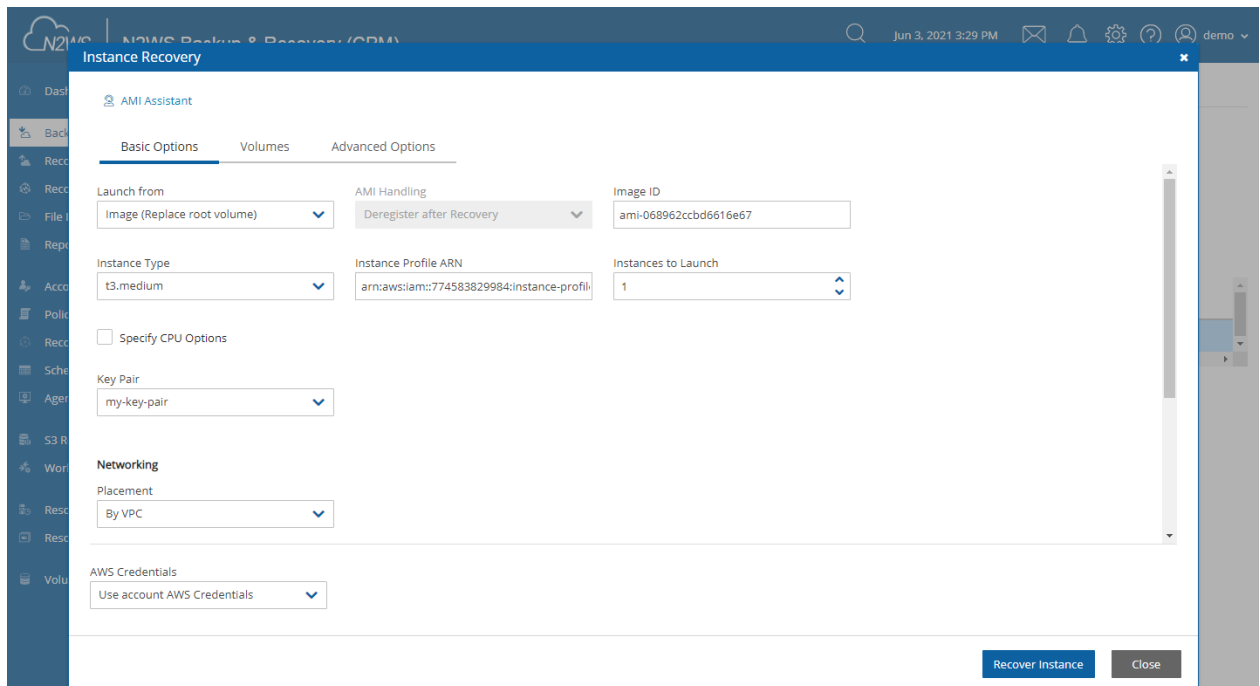
Note: N2WS knows how to overcome this limitation. You can recover an instance from a snapshot, but you also need an AMI for the recovery process. By default, N2WS will create an initial AMI for any Windows instance it backs up and use that AMI for the recovery process. Usually, you do not need to change anything to recover a Windows instance.

- Your data EBS volumes will be recovered by default to create a similar instance as the source. However, you can choose:
  - To recover some or none of the volumes.
  - To enlarge volume capacity, change their device name, or IOPS value.
  - To preserve tags related to the instance and/or data volumes, or not.

The instance recovery screen has tabs for **Basic Options**, **Volumes**, and **Advanced Options**. At the bottom of each screen, there is an option to change **AWS Credentials**.

### 10.3.1 Basic Options

The **Basic Options** tab is divided into the general section and the Networking section:



The screenshot shows the 'Instance Recovery' console with the 'AMI Assistant' tab selected. The configuration is as follows:

- Launch from:** Image (Replace root volume)
- AMI Handling:** Deregister after Recovery
- Image ID:** ami-068962ccbd6616e67
- Instance Type:** t3.medium
- Instance Profile ARN:** arn:aws:iam::774583829984:instance-profile
- Instances to Launch:** 1
- Specify CPU Options:** (unchecked)
- Key Pair:** my-key-pair
- Networking:** Placement: By VPC
- AWS Credentials:** Use account AWS Credentials

Buttons at the bottom right: 'Recover Instance' and 'Close'.

- **AMI Assistant** – Select to view the details of the AMI used to launch your instance and find similar AMIs.
- **Launch from** – Whether to launch the boot device (**Image**) from an existing image, a snapshot, or whether to launch the device using the original volume configuration (**Image (Replace root volume)**) which will contain the Billing Code, if available.
  - The **Snapshot** option is available only if this is an EBS-based instance, and a snapshot of the boot device is available in this backup.
  - See table below for all options.

Note: Launching from a snapshot is not available on Windows.

Launch from	Snapshots Only	Snapshots + Initial AMI	AMI Only
Image	Possible if supply AMI ID	Possible	Default
Image (Replace root volume)	Windows: <b>Default</b> Other OS: Possible if supply AMI ID	<b>Default</b>	<b>Not possible</b>
Snapshot [Create AMI from root snapshot]	Windows: <b>Not possible</b> Other OS: <b>Default</b>	Windows: <b>Not possible</b> Other OS: Possible	<b>Not possible</b>

- **AMI Handling** – This option is relevant only if **Launch from** is set to **snapshot**. If this instance is launched from a snapshot, a new AMI image will be registered and defined as follows:
  - **Deregister after Recovery** – This is the default. The image will only be used for this recovery operation and will be automatically deregistered at the end. This option will not leave any images behind after the recovery is complete.
  - **Leave Registered after Recovery** – The newly created image will be left after recovery. This option is useful if you want to hold on to this image to create future instances. The snapshots the image is based on will not be deleted by the automatic retention process.



However, if you want to keep this image and use it in the future, move the whole backup to the Freezer. See section 9.3.

- **Create AMI without Recovery** – This option creates and keeps the image but does not launch an instance from it. This is useful if you want to launch the instance/s from outside N2WS. If you wish to keep using this image, move the backup to the Freezer.
- **Image ID** – This is only relevant if **Launch from** is set to **Image** or **Image (Replace root volume)** or if you are recovering a Windows instance. By default, this will contain the initial AMI that N2WS created, or if it does not exist, the original AMI ID from which the backed-up instance was launched. You can type or paste a different AMI ID here, but you cannot search AMIs from within N2WS. You can search for it with the AWS Management Console.
- **Instance Type** – Choose the instance type of the new instance/s. The instance type of the backed-up instance is the default.
  - If you choose an instance type that is incompatible with the image or placement method, the recovery operation will fail.

**Note:** Since not all instance types are available in all AWS regions, recovery of an unsupported instance type in a certain region might fail. Where the instance type is not yet supported by AWS, we recommend that you configure a supported instance type.

- **Instance Profile ARN** – The ARN of the instance role (IAM Role) for the instance. To find the ARN, select the Role name in IAM Management Console and then select the **Summary** tab. The default will be the instance role of the backed-up instance if it had one.
- **Instances to Launch** – Specifies how many instances to launch from the image. The default is one, which is the sensible choice for production servers. However, in a clustered environment you may want to launch more than one. It is not guaranteed that all the requested instances will launch. Check the message at the end of the recovery operation to see how many instances were launched, and their IDs.
- **Specify CPU Options** – Enable to select **Core Count** and **Threads per Core** for recovery target.
- **Key Pair** – The key pair you want to launch the instance with. The default is the key that the backed-up instance was created with. You can choose a different one from the list. Keys are typically needed to connect to the instance using SSH (Linux).

**Note:** Keys cannot be used to decrypt the Windows password of a restored instance.

#### 10.3.1.1 Networking Section

The main purpose of the **Networking** section is to define what will be the placement of the instance. By default, it will be the same placement as the backed-up instance. An instance can be placed using three methods which are not all necessarily available.

- **By VPC** – Default placement if you have VPC subnets defined in your account.
- **By Availability Zone** – This is the most basic type and the only one which is always available. You can choose in which AZ to launch the instance. Additional options are:
  - You can choose a different AZ from the backed-up instance.
  - By default, if the backed-up instance was not in a VPC, it will have the same zone as the backed-up instance. Choose a different AZ from the list.



- **By Placement Group** – If you have placement groups defined, this option is available. This is an instance type that can be placed in a placement group. See AWS documentation for details.

If you chose **By VPC** in **Placement**, the following fields are available:

- **VPC** – You can choose the VPC the instance is to be recovered to. By default, it will contain the VPC of the original instance.
- **Clone VPC** - Option to recover to a clone of the selected VPC environment. Control switches to the Account's Clone VPC screen. Choose the date of the source VPC capture for the clone and an optional new destination name. See section 10.3.5. After the cloning process is completed, the name of the newly cloned VPC will appear in the VPC box.
- **VPC Subnet** – This will hold all the subnets in the currently selected VPC.
- **Security Group** – Choose security groups to be applied to the new instance. This is a multiple-choice field. By default, the security groups of the backed-up instance will be chosen.

**Note:** Security groups for VPC instances are different than groups of non-VPC instances. This field has a filter to help you find the security group that you need.

- **VPC Assign IP** – If the backed-up instance was in a VPC subnet, the default value will be the IP assigned to the original instance.
  - If the assigned IP is still taken, it can fail the recovery operation. You can type a different IP here. When you begin recovery, N2WS will verify the IP belongs to the chosen subnet.
  - If this field is empty, an IP address from the subnet will be automatically allocated for the new instance.

If you chose **By Availability Zone** in **Placement**:

- **Availability Zone** - By default, if the backed-up instance was not in a VPC, it will have the same zone as the backed-up instance. However, you can choose a different one from the list.
- **Security Group** - Choose security groups to be applied to the new instance. This is a multiple-choice field. By default, the security groups of the backed-up instance will be chosen.

If you chose **By Placement Group**:

- **Placement Group** - Choose the placement group from the list.

For all Placement options, the following boxes are also available:

- **Additional NICs** - If you want to add additional NICs.
- **AWS Credentials** - You can choose to use different AWS credentials for the recovery operation.

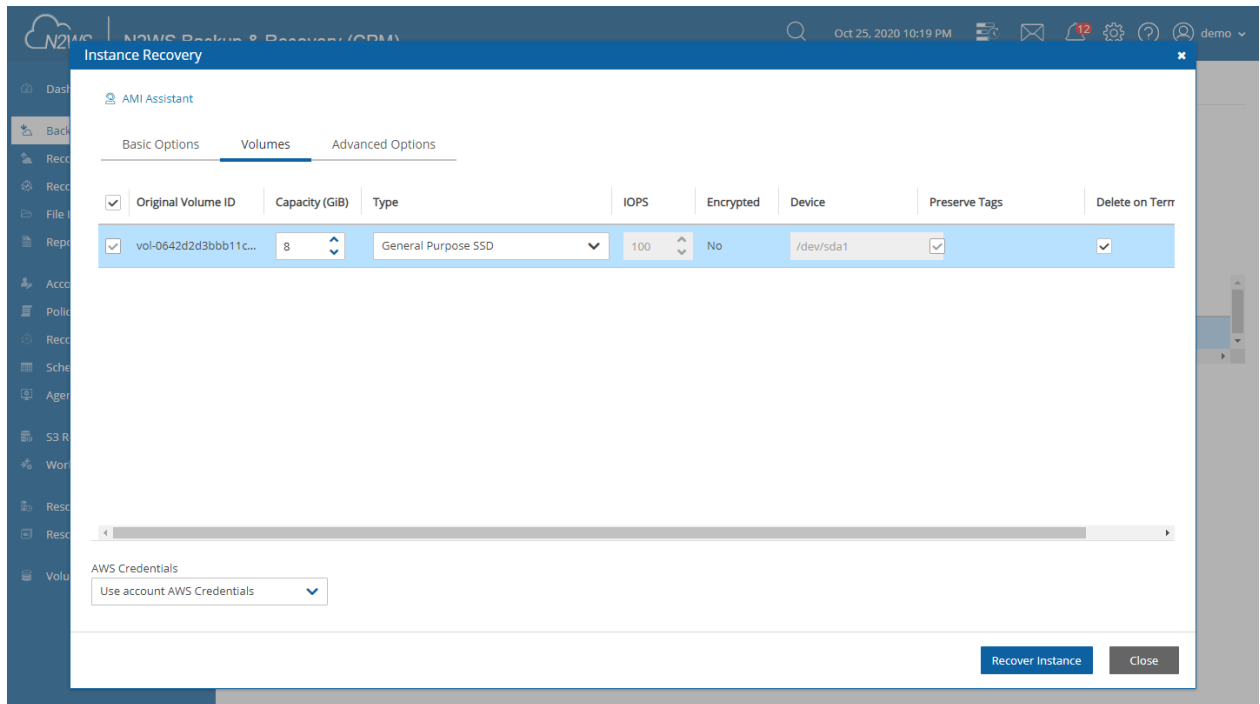
### 10.3.2 Volumes

**Note:** If the policy contains an instance target that99999 has a volume that is also defined as a volume target:

- The volume will not be available under the **Independent Volumes** tab.

- Recover the volume by selecting the relevant instance in the **Instances** tab and then selecting **Recover Volumes Only**. See section 10.4.

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



All data volumes in the policy except the boot device are listed here. Their default configuration is the same as it was in the backed-up instance at the time of the backup.

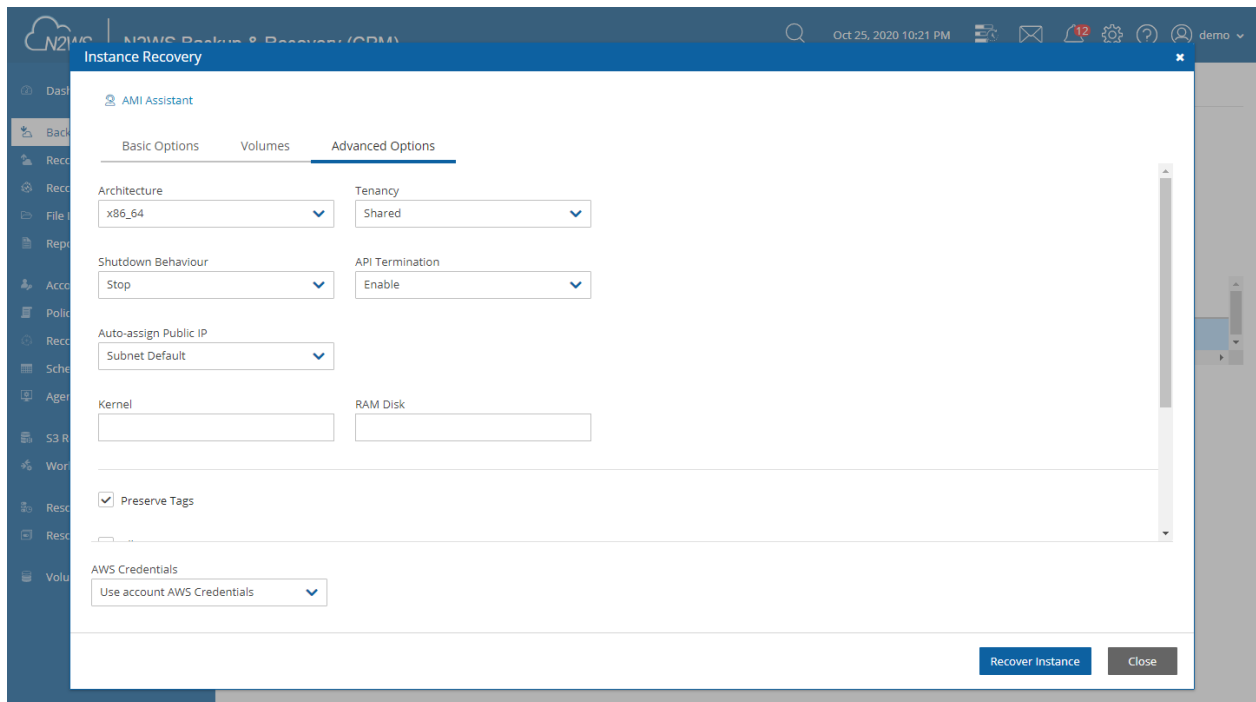
Select a volume to include it in the recovery. You can make adjustments to the volumes, as follows:

- Enlarge capacity of the volume.
- Change the device and device type.
- Change IOPS.
- Exclude any tags associated with the volume, such as its name.
- By default, tags associated with the volume, such as names, are preserved. Clear **Preserve Tags** to exclude all tags.
- By default, the volumes are not deleted on termination of instances recovered from a snapshot. Select **Delete on Termination** to delete the volume on termination of the instance.

### 10.3.3 Advanced Options

**Note:** It is possible to recover to a different account and region by recovering to a clone of an original VPC environment. See the **Clone VPC** option below.





The screenshot shows the N2WS Instance Recovery console. The 'Advanced Options' tab is selected, displaying various configuration fields for recovering an instance. The fields include:

- Architecture:** A dropdown menu currently set to 'x86\_64'.
- Tenancy:** A dropdown menu currently set to 'Shared'.
- Shutdown Behaviour:** A dropdown menu currently set to 'Stop'.
- API Termination:** A dropdown menu currently set to 'Enable'.
- Auto-assign Public IP:** A dropdown menu currently set to 'Subnet Default'.
- Kernel:** An empty text input field.
- RAM Disk:** An empty text input field.
- Preserve Tags:** A checkbox that is checked.
- AWS Credentials:** A dropdown menu currently set to 'Use account AWS Credentials'.

At the bottom right of the form, there are two buttons: 'Recover Instance' (in blue) and 'Close' (in grey).

Advanced options include the following:

- **Architecture** – The default will be the architecture of the backed-up instance. Options are:
  - i386 – which is X86 – 32-bit
  - x86\_64 – which is X86 – 64-bit

**Note:** Changing the architecture may result in an error if the image is incompatible with the requested architecture. For example, if your image is a native 64-bit image and you choose **i386**, the recovery operation will fail.

- **Tenancy** – Choose the tenancy option for this instance.
- **Shutdown Behavior** – The value of the original instance is the default. If the recovered instance is instance-store-based, this option is not used. The choices are:
  - **stop** – If the instance is shut down, it will not be terminated and will just move to **stopped** state.
  - **terminate** – If the instance is shut down, it will also be terminated.
- **API Termination** – Whether terminating the new instance by API is enabled or not. The backed-up instance value is the default.
- **Auto-assign Public IP** - Whether to assign a public IP to the new instance. This is for public subnets. By default, it will behave as the subnet defines.
- **Kernel** – Will hold the Kernel ID of the backed-up instance. You can type or paste a different one. However, you cannot search for a kernel ID from within N2WS. Change this option only if you know exactly which kernel you need. Choosing the wrong one will result in a failure.
- **RAM Disk** - Will hold the RAM Disk ID of the backed-up instance. You can type or paste a different one. However, you cannot search for a RAM Disk ID from within N2WS. Change this option only if you know exactly which RAM Disk you need. Choosing the wrong one will result in a failure.



- **Preserve Tags** – Whether to associate the same tags, such as the volume name, to the recovered volume. The default is yes.
- **Allow Monitoring** – Select if monitoring should be allowed for the new instance. The value in the backed-up instance is the default.
- **ENA** – Select to support Extended Network Adaptor.
- **EBS Optimized** – Select to launch an EBS Optimized instance. The value from the backed-up instance is the default.
- **Enable User Data** – Whether to use user data for this instance launch. If selected, the **User Data** box opens. Enter the text. The text of the user data. Special encoding or using a file as the source is not currently supported from within N2WS.

**Advanced Options** include different additional choices depending on whether **Placement** is **By VPC**, **By Availability Zone** or **By Placement Group**.

To complete the recovery operation, select **Recover Instance** and then confirm. If there are errors that N2WS detects in your choices, you will return to the Recover instance screen with error messages. Otherwise, you will be redirected back to the recovery panel screen, and a message will be displayed regarding the success or failure of the operation.

### 10.3.4 AMI Assistant

The AMI Assistant is a feature that lets you view the details of the AMI used to launch your instance, as well as find similar AMIs. N2WS will record the details of the AMI when you start backing up the instance. If the AMI is deleted sometime after the instance started backing up, N2WS will remember the details of the original AMI.



AMI Assistant

AMI ID	ami-011facbea5ec0363b
Region	ap-northeast-1
Image Name	amzn2-ami-hvm-2.0.20191217.0-x86_64-gp2
Image Description	Amazon Linux 2 AMI 2.0.20191217.0 x86_64 HVM gp2
Owner ID	137112412989 (amazon)
Root	/dev/xvda
Type	ebs
Virtualization	hvm
Hypervisor	xen

Exact Matches    Partial Matches

AMI ID	ami-011facbea5ec0363b
Region	ap-northeast-1
Image Name	amzn2-ami-hvm-2.0.20191217.0-x86_64-gp2
Image Description	Amazon Linux 2 AMI 2.0.20191217.0 x86_64 HVM gp2
Owner ID	undefined (undefined)
Root	/dev/xvda
Type	ebs
Virtualization	hvm
Hypervisor	xen

After selecting **AMI Assistant** in the instance recovery screen, you will see these details:

- AMI ID
- Region
- Image Name
- Image Description
- Owner ID
- Root – Device
- Type
- Virtualization
- Hypervisor

To find AMIs with properties that are exactly like the original, select the **Exact Matches** tab. If the **Exact Matches** search does not find matches, select the **Partial Matches** tab which will search for AMIs similar to the original.

AMI Assistant searches can be useful in the following scenarios:

- You want to recover an instance by launching it from an image, but the original AMI is no longer available.
- You want to recover an instance by launching it from an image, but you want to find a newer version of the image. The fuzzy search will help you.
- You are using DR (section 11) and you need to recover the instance in a different region. You may want to find the matching AMI in the target region to use it to launch the



instance, or you may need its kernel ID or ramdisk ID to launch the instance from a snapshot.

### 10.3.5 Recovering to a Cloned VPC

When you select **Clone VPC** in the **Basic Options** tab, the **Clone VPC** screen opens.


The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title "N2WS Backup & Recovery (CPM)", a search icon, the date "Oct 25, 2020 10:26 PM", and several utility icons. The left sidebar contains a list of navigation items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area displays the "Clone VPC" configuration screen. It has a breadcrumb trail: "Backup Monitor > P2 - 10/25/2020 11:03 AM > Recover > Clone VPC". The configuration is divided into two sections: "Capture Source" and "Clone to Destination". The "Capture Source" section includes a "Region" dropdown menu set to "US East (N. Virginia)", a "VPC" dropdown menu set to "vpc-5d093327", and a "Captured At" dropdown menu set to "Sun 10/25/2020 11:08 AM". The "Clone to Destination" section includes a "Region" dropdown menu set to "US East (N. Virginia)", a "VPC Name" text input field containing "Clone of vpc-5d093327", and an "Account" dropdown menu set to "ACCOUNT-1". At the bottom right of the main content area, there are four buttons: "Download Log", "Cloud Formation Template", "Clone VPC" (highlighted in blue), and "Close".

N2WS will have pre-set the following fields according to the selections made in the **Advanced Options** section:

- **Capture Source:**
  - Region and VPC
  - Captured at date and time – You can select a different date and time to clone in the drop-down list of captures.
- **Clone to Destination:**
  - Region and Account
  - VPC Name – You can change the suggested name for the new VPC.

**Note:** As part of the cloning process, N2WS uses CloudFormation. If the CloudFormation template is over 50 kB, select **Cloud Formation Template**. It requires an existing S3 bucket for uploading. See section 23.5.

When finished, select **Clone VPC**. If you changed the suggested **VPC Name**, it will appear in the **VPC** box.

- To view the cloning progress and status, select **Background Tasks**  in the toolbar. **Background Tasks** only appears after the first **Clone VPC** or **Check Secured DR Account** operation. Select **View All Tasks**.




Background Tasks	Background Tasks
<div>Recent Tasks</div> <div>Clone VPC for account account-1 Started At: Sep 23, 2020 8:34 PM</div>	<div>Recent Tasks</div> <div>Clone VPC for account account-1 Cloning VPC 'vpc-5d093327' completed s... Started At: Sep 23, 2020 8:34 PM Ended At: Sep 23, 2020 8:35 PM</div>

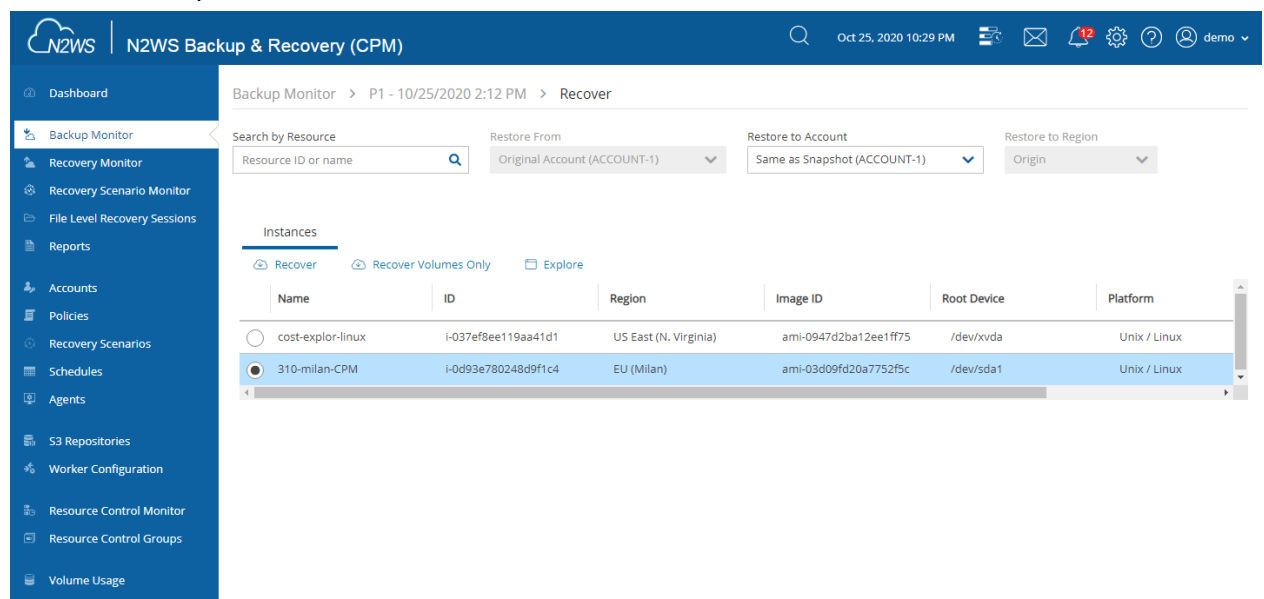
- To view the results of the Clone VPC operation in case manual changes are required, select **Download Log**.

## 10.4 Volume Recovery

Volume recovery means creating EBS volumes out of snapshots. In N2WS, you can recover volumes that were part of an instance's backup or recover EBS volumes that were added to a policy as an independent volume. The recovery process is basically the same.


**To recover volumes belonging to an instance:**

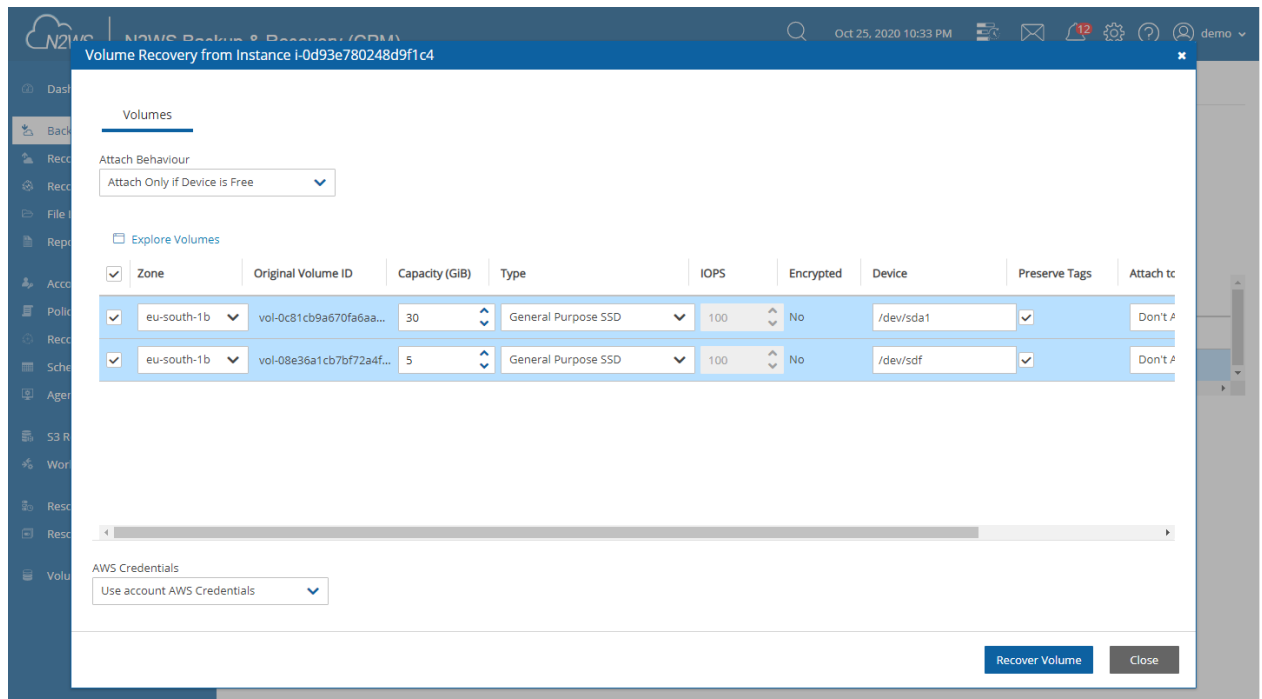
1. In the left panel, select the **Backup Monitor**.
2. Select a backup and then select  **Recover**.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options like Dashboard, Backup Monitor, Recovery Monitor, etc. The main panel is titled 'Backup Monitor > P1 - 10/25/2020 2:12 PM > Recover'. It features search and restore filters at the top and a table of instances below. The '310-milan-CPM' instance is selected.

Name	ID	Region	Image ID	Root Device	Platform
cost-explor-linux	i-037ef8ee119aa41d1	US East (N. Virginia)	ami-0947d2ba12ee1ff75	/dev/xvda	Unix / Linux
310-milan-CPM	i-0d93e780248d9f1c4	EU (Milan)	ami-03d09fd20a7752f5c	/dev/sda1	Unix / Linux

3. Select an instance and then select  **Recover Volumes Only**.



Zone	Original Volume ID	Capacity (GiB)	Type	IOPS	Encrypted	Device	Preserve Tags	Attach to
eu-south-1b	vol-0c81cb9a670fa6aa...	30	General Purpose SSD	100	No	/dev/sda1	<input checked="" type="checkbox"/>	Don't Attach
eu-south-1b	vol-08e36a1cb7b72a4f...	5	General Purpose SSD	100	No	/dev/sdf	<input checked="" type="checkbox"/>	Don't Attach


4. In the Volume Recover from Instance screen, change the fields as needed:

- **Attach Behaviour** – This applies to all the volumes you are recovering if you choose to attach them to an instance:
  - **Attach Only if Device is Free** – If the requested device is already taken in the target instance, the attach operation will fail. You will get a message saying the new volume was created but was not attached.
  - **Switch Attached Volumes** – This option will work only if the target instance is in **stopped** state. If the instance is running, you will get an error message. N2WS will not try to forcefully detach volumes from a running instance since this can cause systems to crash.
  - **Switch Attached Volumes and Delete Old Ones** – This option will work only on stopped instances. This option will also delete the old volumes that are detached from the instance.


**Important:** If you choose **Switch Attached Volumes and Delete Old Ones**, make sure you do not need the old volumes. N2WS will delete them after detaching them from the target instance.

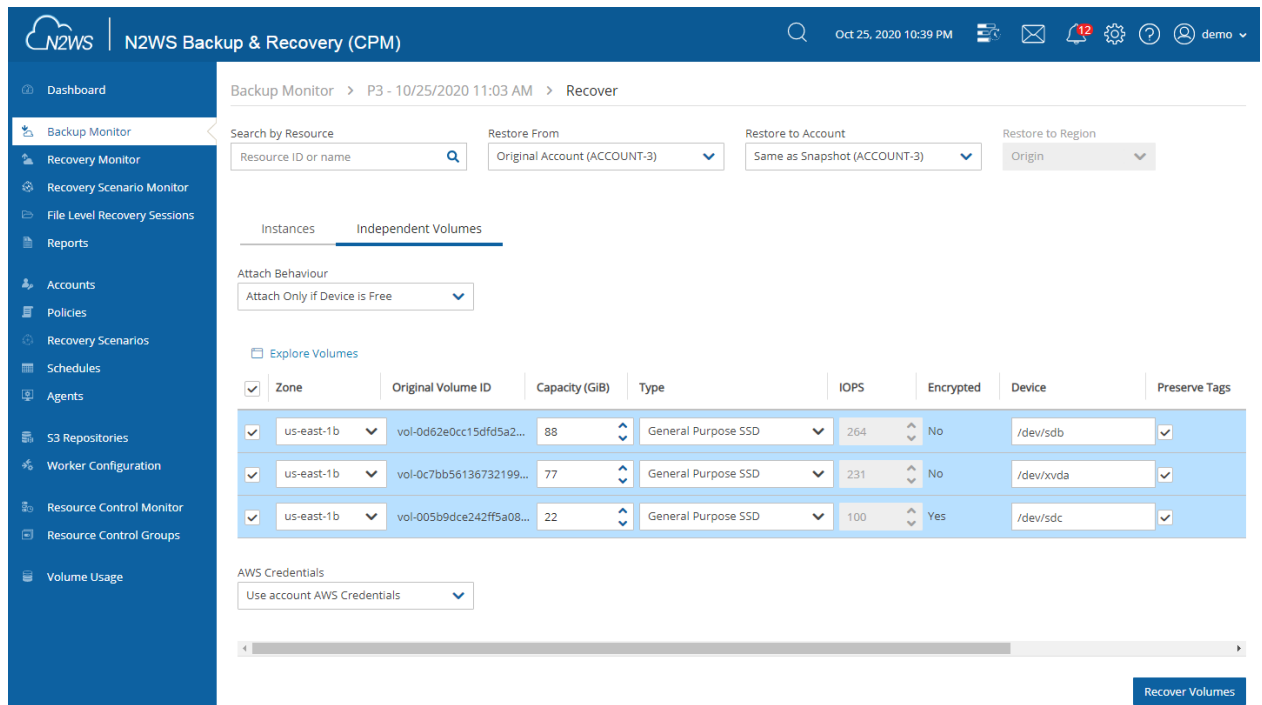
- **Recover** – Enabled by default. Clear **Recover** if you do not want that volume recovered.
- **Zone** – AZ. The default is the original zone of the backed-up volume.
- **Original Volume ID** – ID of the original volume.
- **Capacity** – Enlarge the capacity of a volume. You cannot make it smaller than the size of the original volume, which is the default.
- **Type** – Type of the EBS volume.
- **IOPS** – Number of IOPS. This field is used only if the type of volume you chose is **Provisioned IOPS SSD**. The default will be the setting from the original volume. Values for IOPS should be at least 100, and the volume size needs to be at least 1/10 that number in GiBs. For example, if you want to create a 100 IOPS volume, its size needs to be at least 10 GiB. If you will not abide to this rule, the recovery operation will fail.



- **Encrypted** – Whether device is encrypted.
  - **Device** – Which device it will be attached as. This is only used if you choose to automatically attach the recovered volume to an instance. If the device is not free or not correct, the attach operation will fail.
  - **Preserve Tags** – Whether to associate the same tags, such as the volume name, to the recovered volume. The default is yes.
  - **Attach to Instance** – Whether to attach the newly recovered volume to an instance. Start typing in the list to initiate a filter. The list holds instances that are in the same AZ as the volume. Changing the **Zone** will refresh the content of this list.
  - **AWS Credentials** - As with other recovery screens, you can choose to use different AWS credentials for the recovery operation.
5. After selecting **Recover Volumes** and confirming, if there was an error in a field that N2WS detected, you will be returned to the screen with an error notification.
  6. To follow the progress of the recovery, select the **Open Recovery Monitor** link in the 'Recovery started' message  **Recovery Started (Open Recovery Monitor)** at the top right corner, or select the **Recovery Monitor** tab.

#### To recover independent volumes:

1. In the left panel, select the **Backup Monitor**.
2. Select a backup and then select  **Recover**. The recover volumes screen opens.
3. In the **Independent Volumes** tab, select a volume or Search by Resource.
4. Complete the From/To options as available.



N2WS Backup & Recovery (CPM)

Backup Monitor > P3 - 10/25/2020 11:03 AM > Recover

Search by Resource: Resource ID or name

Restore From: Original Account (ACCOUNT-3)

Restore to Account: Same as Snapshot (ACCOUNT-3)

Restore to Region: Origin

Instances Independent Volumes

Attach Behaviour: Attach Only if Device Is Free

Explore Volumes

<input checked="" type="checkbox"/>	Zone	Original Volume ID	Capacity (GiB)	Type	IOPS	Encrypted	Device	Preserve Tags
<input checked="" type="checkbox"/>	us-east-1b	vol-0d62e0cc15dfd5a2...	88	General Purpose SSD	264	No	/dev/sdb	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	us-east-1b	vol-0c7bb56136732199...	77	General Purpose SSD	231	No	/dev/xvda	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	us-east-1b	vol-005b9dce242ff5a08...	22	General Purpose SSD	100	Yes	/dev/sdc	<input checked="" type="checkbox"/>


AWS Credentials: Use account AWS Credentials

Recover Volumes

5. Select **Recover Volumes**. A screen similar to the recover instance volumes opens. See 10.3.2.



## 10.5 RDS Database Recovery


When a backup includes snapshots of RDS databases, selecting  **Recover** to bring you to the RDS Databases tab. You will see a list of all RDS databases in the current backup. You can change the following options:

- **Recover** – Clear **Recover** to *not* recover the current database.
- **Zone** – The AZ of the database. By default, it will be the zone of the backed-up database, but this can be changed. Currently, recovering a database into a VPC subnet is not supported by N2WS. You can recover from the snapshot using AWS Management Console.
- **DB Instance ID** – The default is the ID of the original database. If the original database still exists, the recovery operation will fail. To recover a new database, type a new ID.
- **DB Instance Class** – The default is the original class, but you can choose another.
- **Storage Type** – Type of storage.
- **IOPS** - Number of IOPS. This field is used only if the type of volume you chose is **Provisioned IOPS SSD**. The default will be the setting from the original volume. Values for IOPS should be at least 100, and the volume size needs to be at least 1/10 that number in GiBs.
- **Port** – The default is the port of the original backed-up database, but you can choose another.
- **Multi AZ** – Whether to launch the database in a multi-AZ configuration or not. The default is the value from the original backed-up database.
- **Subnet Group** – Whether to launch the database in a VPC subnet or not and to which subnet group. The default will be the value from the original backed-up database. You can recover a database from outside a VPC to a VPC subnet group, but the other way around is not supported and will return an error.
- **Publicly Access.** – Whether the database will be publicly accessible or not. The default is the access from the original backed-up database.
- **AWS Credentials** - As in other types of recovery, you can choose to use different AWS credentials and enter your keys.

## 10.6 Aurora Cluster Recovery

Aurora recovery is similar to RDS recovery, with a few important differences.

- Aurora introduces the concept of clusters to RDS. You no longer launch and manage a DB instance, but rather a DB cluster that contains DB instances.
- An Aurora cluster may be created in a single AZ deployment, and the cluster will contain one instance.
- Or, as in production deployments, the cluster will be created in a multi-AZ deployment, and the cluster will have reader and writer DB instances.
- When recovering an Aurora cluster, N2WS will recover the DB cluster and then will create the DB instances for it.

After selecting a backup with Aurora Clusters, select  **Recover**. The **Aurora Clusters Recover** screen opens. In this screen, all Aurora clusters that were backed up are listed. You can change the following options:






- **Recover** – Clear to not recover the current Aurora cluster.
- **RDS Cluster ID** – The default will be the ID of the original cluster. If the original cluster still exists, the recovery operation will fail, unless you change the ID.
- **RDS Instance ID** – The default will be the ID of the original instance.
  - If the original instance still exists, the recovery operation will fail.
  - Type a new ID to recover a new database. N2WS will use this instance ID for the writer, and in the case of multi-AZ, it will create the reader with this name with `_reader` added at the end.
- **RDS Cluster Snapshot ID** – Displays the snapshot ID.
- **Instance Type** – The type or class of the DB instances.
- **Port** – The port of the database. The default is the port of the original backed-up database.
- **Zone** – The AZ of the cluster in case of single AZ. If using a subnet group, leave as is.
- **Subnet Group** – Whether to launch the cluster in a VPC subnet or not and to which subnet group. The default is the value from the original backed-up cluster.
- **Publicly Access** – Whether the cluster will be publicly accessible or not. The default is the access from the original backed-up instance.

Select **Recover Aurora Clusters** when finished.

## 10.7 Aurora Serverless Recovery

Recovery of Aurora Serverless is somewhat different than for an Aurora Cluster. As part of the recovery, you can define actions for setting capacity:

- **Force scaling** the capacity to the specified values in **Minimum/Maximum Aurora capacity unit** when the **Timeout for force scaling** is reached. When you change the capacity, Aurora Serverless tries to find a scaling point for the change.
  - Enable to force capacity scaling as soon as possible.
  - Disable to cancel the capacity changes when the timeout is reached.
- **Pause compute** capacity after consecutive minutes of inactivity. You are only charged for database storage while the compute capacity is paused.
  - Specify the amount of time (**Timeout for force scaling**) with no database traffic to scale to zero processing capacity.
  - When database traffic resumes, Aurora automatically resumes processing capacity and scales to handle the traffic.

1. After selecting a backup with Aurora Serverless in the **Backup Monitor**, select  **Recover**. The **Recover** screen opens.

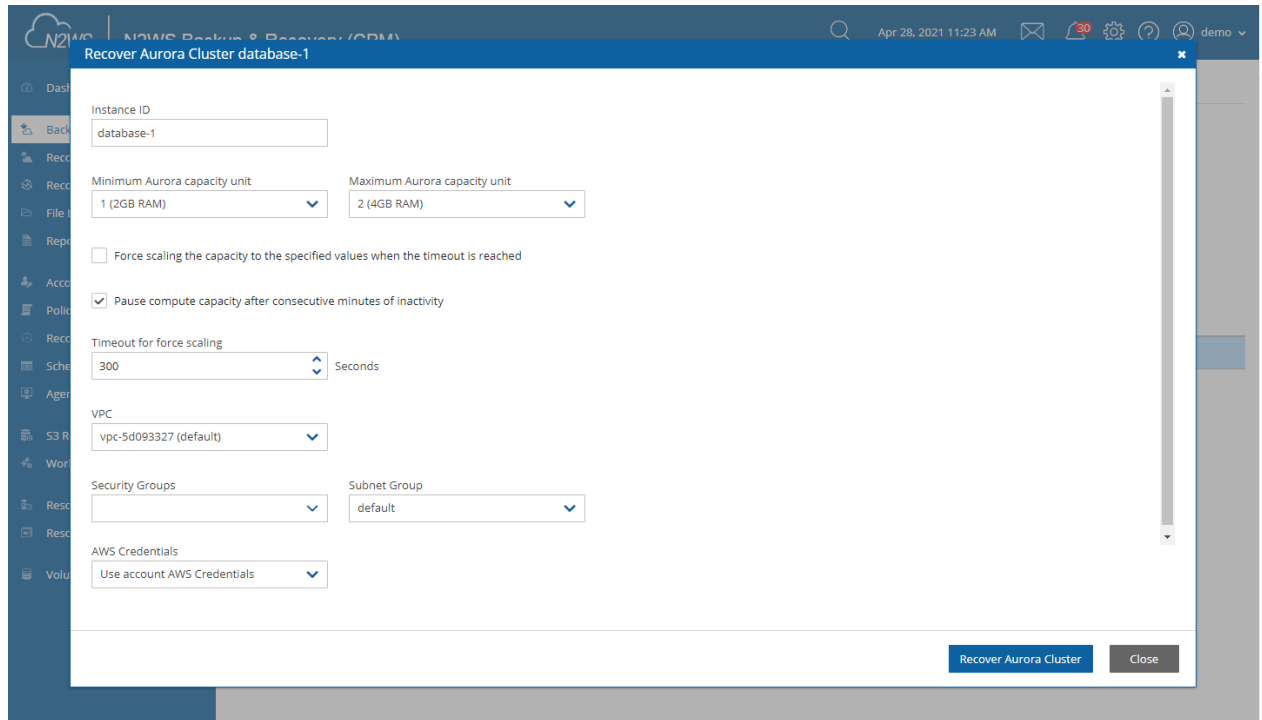


The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Backup Monitor > RDS-serverless-Aurora (demo) - 04/28/2021 10:44 AM > Recover'. It features a search bar for 'Resource ID or name' and three dropdown menus for 'Restore From' (Original Account (aws-a1)), 'Restore to Account' (Same as Snapshot (aws-a1)), and 'Restore to Region' (Origin). Below this is a table titled 'Aurora Clusters' with a 'Recover' button. The table has columns for 'Original Cluster Id', 'Role', and 'Size'. One cluster is listed: 'database-1' with a 'Serverless' role and '2 Capacity Unit(s)' size.

2. In the **Aurora Clusters** tab, select the recovery target. Aurora Serverless can be identified by the value 'Serverless' in the **Role** column.
3. Select **Recover**. The Recovery Aurora Cluster screen opens.

The screenshot shows the 'Recover Aurora Cluster database-1' dialog box. It contains the following fields and options: 'Instance ID' (database-1), 'Minimum Aurora capacity unit' (1 (2GB RAM)), 'Maximum Aurora capacity unit' (2 (4GB RAM)), a checkbox for 'Force scaling the capacity to the specified values when the timeout is reached', a checkbox for 'Pause compute capacity after consecutive minutes of inactivity', 'VPC' (vpc-5d093327 (default)), 'Security Groups' (empty), 'Subnet Group' (default), and 'AWS Credentials' (Use account AWS Credentials). At the bottom right are 'Recover Aurora Cluster' and 'Close' buttons.

4. Change the default field values as needed. See section 10.6 for **Instance ID** and **Subnet Group**.
5. If you select **Force scaling the capacity to the specified values when the timeout is reached** or **Pause compute capacity after consecutive minutes of inactivity**, the **Timeout for force scaling** list appears. Change the timeout seconds as needed.



6. Select **Recover Aurora Cluster** when finished.

## 10.8 Redshift Cluster Recovery

When a backup to recover includes snapshots of Redshift clusters, the **Redshift Clusters** tab opens. All Redshift clusters in the current backup are listed. You can change the following options:

- **Recover** – Clear **Recover** to not recover the current cluster.
- **Zone** – The AZ of the cluster. By default, it will be the zone of the backed-up cluster, but this can be changed.

**Note:** Currently, recovering a cluster into a VPC subnet is not supported by N2WS. You can always recover from the snapshot using AWS Management Console.

- **Cluster ID** – The default will be the ID of the original cluster. If the original cluster still exists, the recovery operation will fail. To recover a new cluster, type a new ID.
- **Cluster Snapshot ID** – Displays the snapshot ID.
- **Node Type** and **Nodes** – For information only. Changing these fields is not supported by AWS.
- **Port** – The port of the cluster. The default is the port of the original backed-up cluster.
- **Subnet Group** – Whether to launch the cluster in a VPC subnet or not and to which subnet group. The default will be the value from the original backed-up cluster. You can recover a cluster from outside a VPC to a VPC subnet group, but the other way around is not supported.
- **AWS Credentials** - You can choose to use different AWS credentials and enter your keys.



## 10.9 DynamoDB Table Recovery

When a backup to recover includes DynamoDB Table backups, the **DynamoDB Tables** tab opens.

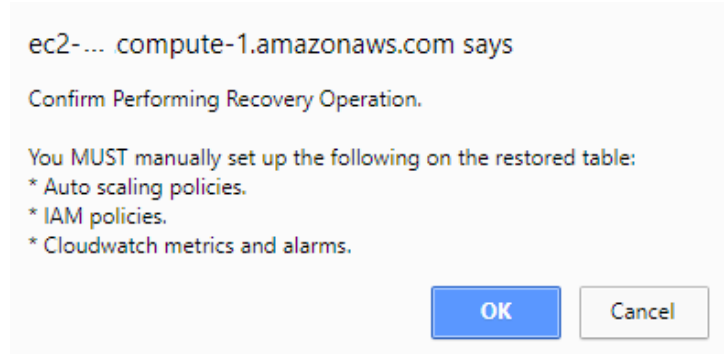
**Note:** If you reach the limit of the number of tables that can be recovered at one time, you will need to wait until they have completed before starting the recovery of additional tables.

All DynamoDB tables in the current backup are listed. You can change the following options:

- **Recover** – Clear **Recover** to not recover a table.
- **Region** – The Region where the table will be recovered, which is the same region as the backup.
- **Table Name** – The default will be the Name of the original table. However, if the original table still exists, the recovery operation will fail. To recover to a new table, type a new Name.
- **Backup Name** – Displays the name of the backup.
- **AWS Credentials** - You can choose to use different AWS credentials and enter your keys.

During backup, N2WS retains the DynamoDB tags at the table level and the Time To Live (TTL) metadata and enables these attributes on recovery.


During the recovery process, a confirmation message appears with a reminder to recreate the following settings on the restored DynamoDB tables *MANUALLY*: Auto Scaling policies, IAM policies, CloudWatch metrics, and alarms.



## 10.10 EFS Recovery

When a backup includes EFS backups, the **Recover EFS** tab is available.

**Note:** The AWS role “**AWSBackupDefaultServiceRole**” is required for recovery.

1. In the **Backup Monitor** screen, select an EFS backup. To search backups, you can enter either the EFS name or AWS ID in the search box, select **By Elastic File System** in the list, and then select the **Search**  icon.



Backup Monitor

Cloud: my By Elastic File System All Policies All Accounts

All Backup Statuses Show: 20 records/page

<input checked="" type="checkbox"/>	Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle:
<input checked="" type="checkbox"/>	Jun 14, 2021 2:31 PM	Jun 14, 2021 2:31 PM	backup-my-efs	a1	Successful		

1 of 1 items selected

2. Select **Recover**.
3. In the Target EFS list, select the target to restore to to:
  - **New** - Recover to a separate EFS
  - **Original** - Recover to the same EFS
4. In cases where EFS DR was performed, select the **Restore to Region**.

**Note:** Regular recoveries to original and new EFSs are supported. For DR, only recovery to a *new* EFS is supported.

Backup Monitor > efs - 06/09/2020 3:41 PM > Recover

Search by Resource  
Resource ID or name

Restore From: Original Account (a1)  
Restore to Account: Same as Snapshot (a1)  
Restore to Region: US East (Ohio) **DR region**

**Recovery only to new EFS is available**

Elastic File Systems

<input checked="" type="checkbox"/>	Region	Original EFS ID	Target EFS	Performance	IAM Role	Encryption
<input checked="" type="checkbox"/>	us-east-2	My-EFS-NV (fs-9eda4a1d)	New	General Purpose	AWSBackupDefaultServiceRole	Not Encrypted

AWS Credentials: Use account AWS Credentials

**Note:** To not miss matching an EFS vault name in the target region during a snapshot backup or a copy, in the AWS console, go to **AWS Backup > Backup vaults** and select the region you would like to backup or copy EFS snapshots to. This action is to be performed only *once* before running an EFS backup or DR.

5. Select **Recover Volumes**.

For file-level recovery, see section 13.3.



### To view the progress of the recovery:

1. In N2WS, select the **Recovery Monitor** tab.
2. To view details of the recovery process, select the recovery record, and select **Log**.  
Select **Refresh** as needed.

**Note:** Regular recoveries to original and new EFSs are supported. For DR, only recovery to a new EFS is supported.

## 10.11 FSx Recovery

In the **Backup Monitor**, select an FSx backup for the recovery. Select **Recover**. The **FSx File Systems** tab will show the Original FSx Name, ID, Region, and File System Type.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Backup Monitor > fsx - 10/25/2020 3:52 PM > Recover'. It features a search bar 'Search by Resource' with a dropdown 'Resource ID or name'. Below this is a table titled 'FSx File Systems' with a 'Recover' button. The table has columns: Original FSx Name, Original FSx ID, Region, and File System Type. A single row is visible with the following data: fsx--n-virginia, fs-083362023b7894fb3, US East (N. Virginia), and LUSTRE. Below the table is a section for 'AWS Credentials' with a dropdown menu set to 'Use account AWS Credentials'.

Original FSx Name	Original FSx ID	Region	File System Type
fsx--n-virginia	fs-083362023b7894fb3	US East (N. Virginia)	LUSTRE

Select an FSx and then select **Recover**. Parameters are shown depending on whether they are relevant for the type of FSx.



All of the following parameters are optional except for the password of Win-SMAD, where the original password is the default.

Parameter	FSx Types	Comment
Target VPC	All	AWS Subnet ID of selected VPC
Security Group	All	AWS Security Group IDs of selected VPC
Subnet ID	Win-AD, Win-SMAD	Preferred Subnet ID
Active Directory ID	Win-AD	
Domain Name	Win-SMAD	
IP Addresses	Win-SMAD	
User Name	Win-SMAD	
Password	Win-SMAD	Mandatory



## 11 Disaster Recovery (DR)

N2WS's DR (Disaster Recovery) solution allows you to recover your data and servers in case of a disaster. DR will help you recover your data for whatever reason your system was taken out of service. N2WS flexibility allows users to copy their backup snapshots to multiple AWS regions as well as to various AWS accounts, combining cross-account and cross-region options. What does that mean in a cloud environment like EC2? Every EC2 region is divided into AZs which use separate infrastructure (power, networking, etc.). Because N2WS uses EBS snapshots you will be able to recover your EC2 servers to other AZs. N2WS's DR is based on AWS's ability to copy EBS snapshots between regions and allows you the extended ability to recover instances and EBS volumes in other regions. You may need this ability if there is a full-scale outage in a whole region. But it can also be used to migrate instances and data between regions and is not limited to DR. If you use N2WS to take RDS snapshots, those snapshots will also be copied and will be available in other regions.

- **DynamoDB Tables** - DR for DynamoDB tables is currently not supported by AWS.
- **Redshift Clusters** - Currently N2WS does not support DR of Redshift clusters. If you enable DR on a policy containing Redshift clusters, they will be ignored at the DR stage. You can enable copying Redshift snapshots between regions automatically by enabling cross-region snapshots using the EC2 console.

### 11.1 Configuring DR

After defining a policy, select the **DR** tab.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title "N2WS Backup & Recovery (CPM)", a search icon, the date "Oct 25, 2020 10:43 PM", and various system icons. A left sidebar contains a menu with items like Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies (selected), Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled "Policies > P1" and shows a status bar with "Last updated: Oct 25, 2020 2:12 PM", "Last recovery: Never", and "Last DR recovery: Never". Below this is a tabbed interface with tabs for "Policy Details", "Backup Targets", "More Options", "DR" (selected), and "Lifecycle Management (Snapshot / S3 / Glacier)". The "DR" tab contains the following settings: "Enable DR" is checked; "DR Frequency (backups)" is set to 1; "DR Timeout (hours)" is set to 24; "Target Regions" is a dropdown menu labeled "Choose Region"; and "Cross Account DR Backup Enabled" is an unchecked checkbox. At the bottom right of the interface are buttons for "Previous", "Next", "Save", and "Cancel".





In the DR Options screen, configure the following and then select **Save**.

- **Enable DR** – Select to display additional fields.
- **DR Frequency (backups)** – Frequency of performing DR in terms of backups. On each backup, the default is to copy snapshots of all supported backups to other regions. To reduce costs, you may want to reduce the frequency. See section 11.4 below for considerations in planning DR.
- **DR Timeout (hours)** – How long N2WS waits for the DR process on the policy to complete. DR copies data between regions over a WAN (Wide Area Network) which can take a long time. N2WS will wait on the copy processes to make sure they are completed successfully. If the entire DR process is not completed in a certain timeframe, N2WS assumes the process is hanging and will declare it as failed. Twenty-four hours is the default and should be enough time for a few 1 TiB EBS volumes to copy. Depending on the snapshot, however, you may want to increase or decrease the time.
- **Target Regions** – List of regions of region or regions that you want to copy the snapshots of the policy to.

To configure Cross-Account backup, see section 12.1.

## 11.2 About the DR Process

Things to know about the DR process:

- N2WS's DR process runs in the background.
- It starts when the backup process is finished. N2WS determines then if DR should run and kicks off the process. In the **Backup Monitor**, you will see the 'In Progress' status.

Start Time	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle
Oct 25, 2020 2:12 PM		P1	ACCOUNT-1	In Progress		
Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P3	ACCOUNT-3	Successful		Store
Oct 25, 2020 11:03 AM	Oct 25, 2020 11:14 AM	P2	ACCOUNT-1	Successful	Completed	
Oct 25, 2020 11:03 AM	Oct 25, 2020 11:13 AM	P1	ACCOUNT-1	Successful		
Oct 25, 2020 11:03 AM	Oct 25, 2020 11:04 AM	CPMDATA	ACCOUNT-1	Successful		
Oct 24, 2020 2:43 PM	Oct 24, 2020 2:44 PM	P3	ACCOUNT-3	Successful		Delete
Oct 24, 2020 1:37 PM	Oct 24, 2020 1:39 PM	P2	ACCOUNT-1	Successful	Completed	
Oct 24, 2020 1:37 PM	Oct 24, 2020 1:49 PM	P1	ACCOUNT-1	Successful		
Oct 24, 2020 1:37 PM	Oct 24, 2020 1:37 PM	CPMDATA	ACCOUNT-1	Successful		
Oct 22, 2020 8:22 AM	Oct 22, 2020 8:24 AM	P2	ACCOUNT-1	Successful	Completed	
Oct 22, 2020 8:21 AM	Oct 22, 2020 8:22 AM	P1	ACCOUNT-1	Successful		

- N2WS will wait until all copy operations are completed successfully before declaring the DR status as **Completed** as the actual copying of snapshots can take time.
- As opposed to the backup process that allows only one backup of a policy to run at one time, DR processes are completely independent. This means that if you have an hourly



backup and it runs DR each time, if DR takes more than an hour to complete, the DR of the next backup will begin before the first one has completed.

- Although N2WS can handle many DR processes in parallel, AWS limits the number of copy operations that can run in parallel in any given region to avoid congestion. See section 11.4.2.
- N2WS will keep all information of the original snapshots and the copied snapshots and will know how to recover instances and volumes in all relevant regions.
- The automatic retention process that deletes old snapshots will also clean up the old snapshots in other regions. When a regular backup is outside the retention window and its snapshots are deleted, so are the DR snapshots that were copied to other regions.

## 11.3 DR and Mixed-region Policies

N2WS supports backup objects from multiple regions in one policy. In most cases, it would probably not be the best practice, but sometimes it is useful. When you choose a target region for DR, DR will copy all the backup objects from the policy which are not already in this region to that region. For example, if you back up an instance in Virginia and an instance in North California, and you choose N. California as a target region, only the snapshots of the Virginia regions will be copied to California. So, you can potentially implement a mutual DR policy: choose Virginia and N. California as target regions and the Virginia instance will be copied to N. California and vice versa. This can come in handy if there is a problem or an outage in one of these regions. You can always recover the instance in the other region.

### 11.3.1 DR of EFS

**Note:** Disaster Recovery is supported for EFS to a new EFS *only*. DR to an original EFS is not supported.

- If the source and target regions are the same for DR, no action is required as the target region will default to the source.
- If the target region is different than the source, the target region must have a backup vault with the same name as the source and must be specified using a tag before the DR begins.
  - For the "Default" vault, if this is the initial time copying a snapshot to the DR region, go to the **AWS Backup** console and activate the vault by selecting **Backup vaults**.
  - For a non-default custom vault, a vault with the same name needs to be created in the DR region. For example, if the source region's vault name is "Test", the DR region also must include a vault with the name "Test".

#### To set a custom vault name for cross-region EFS DR:

Before the DR, add a tag to the resource with the key '**cpm\_dr\_backup\_vault**' and the value of the custom backup vault ARN:

Key='cpm\_dr\_backup\_vault:REGION', Value='BACKUP\_VAULT\_ARN'

Add a key for each target region that is different from the source.

**Note:** Cross-account DR for EFS is currently not supported.



## 11.4 Planning your DR Solution

### 11.4.1 Time and Financial Considerations

There are some fundamental differences between local backup and DR to other regions. It is important to understand the differences and their implications when planning your DR solution. The differences between storing EBS snapshots locally and copying them to other regions are:

- Copying between regions is transferring data over a WAN. It means that it will be much slower than moving data locally. A data transfer from the U.S to Australia or Japan will take considerably more time than a local copy.
- AWS will charge you for the data transfer between regions. This can affect your AWS costs, and the prices are different depending on the source region of the transfer. For example, in March 2013, transferring data out of U.S regions will cost 0.02 USD/GiB and can climb up to 0.16 USD/GiB out of the South America region.

As an extreme example: You have an instance with 4 x TiB EBS volumes attached to it. The volumes are 75% full. There is an average of 3% daily change in data for all the volumes. This brings the total size of the daily snapshots to around 100 GiB. Locally you take 4 backups a day. In terms of cost and time, it will not make much of a difference if you take one backup a day or four, which is true also for copying snapshots, since that operation is incremental as well. Now you want a DR solution for this instance. Copying it every time will copy around 100 GiB a day. You need to calculate the price of transferring 100 GiB a day and storing them at the remote region on top of the local region.

### 11.4.2 Timing your DR processes

You want to define your recovery objectives both in local backup and DR according to your business needs. However, you do have to take costs and feasibility into consideration. In many cases, it is ok to say: For local recovery, I want frequent backups, four times a day, but for DR recovery it is enough for me to have a daily copy of my data. Or, maybe it is enough to have DR every two days. There are two ways to define such a policy using N2WS:

- In the definition of your policy, select the frequency in **DR Frequency (backups)**. If the policy runs four times a day, configure DR to run once every four backups. The DR status of all the rest will be **Skipped**.
- Or, define a special policy for the DR process. If you have a **sqlserver1** policy, define another one and name it something like **sqlserver1\_dr**. Define all targets and options the same as the first policy, but choose a schedule relevant for DR. Then define DR for the second policy. Locally it will not add any significant cost since it is all incremental, but you will get DR only once a day.

### 11.4.3 Performing DR on the N2WS Server (The cpmdata Policy)

To perform DR recovery, you will need your N2WS server up and running. If the original server is alive, then you can perform recovery on it across regions. You want to prepare for the case where the N2WS server itself is down. You may want to copy your N2WS database across regions as well. Generally, it is not a bad idea to place your N2WS server in a different region than your other production data. N2WS has no problem working across regions and even if you



want to perform recovery because of a malfunction in only one of the AZs in your region, if the N2WS server happens to be in that zone, it will not be available.

To make it easy and safe to back up the N2WS server database, there is a special policy named `cpmdata`. Although N2WS supports managing multiple AWS accounts, the only account that can back up the N2WS server is the one that owns it, i.e. the account used to create it. Define a new policy and name it `cpmdata` (case insensitive), and it will automatically create a policy that backs up the CPM data volume.


**Note:** Application consistency is disabled by default for the `cpmdata` policy. When enabled, N2WS will run application-consistent scripts. See section 4.2.1.

Not all options are available with the `cpmdata` policy, but you can control Scheduling, Number of generations, and DR settings.

When setting these options, remember that at the time of recovery you will need the most recent copy of this database, since older ones may point to snapshots that no longer exist and not have newer ones yet. Even if you want to recover an instance from a week ago, you should always use the latest backup of the `cpmdata` policy.

## 11.5 DR Recovery

DR recovery is similar to regular recovery with a few differences:

- When you select  **Recover** for a backup that includes DR (DR is in **Completed** state), you get the same Recovery Panel screen with the addition of a drop-down list.
- The DR Region default is **Origin**, which will recover all the objects from the original backup. It will perform the same recovery as a policy with no DR.
- When choosing one of the target regions, it will display the objects and will recover them in the selected region.

**Recommendation:** N2W Software strongly recommends that you perform recovery drills occasionally to be sure your recovery scenario works. It is not recommended to try it for the first time when your servers are down. Each policy on the policy screen shows the last time recovery was performed on it. Use the last recovery time data to track recovery drills.

### 11.5.1 DR Instance Recovery

Volume recovery is the same in any region. For instance recovery, there are a few things that need consideration. An EC2 instance is typically related to other EC2 objects:

- Image ID (AMI)
- Key Pair
- Security Groups
- Kernel ID
- Ramdisk ID

These objects exist in the region of the original instance, but they do not mean anything in the target region. To launch the instance successfully, you will need to replace these original objects with ones from the target region:



- **Image ID (AMI)** - If you intend to recover the instance from a root device snapshot, you will not need a new image ID. If not (as in all cases with Windows and instance store-based instances), you will need to type a new image ID. If you use AMIs you prepared, you should also prepare them at your target regions and make their IDs handy when you need to recover. If needed, AMI Assistant can help you find a matching image. See section 10.3.4.
- **Key Pair** - You should have a key pair created with AWS Management Console ready so you will not need to create it when you perform a recovery.
- **Security Groups** - In a regular recovery, N2WS will remember the security groups of the original instance and use them as default. In DR recovery, N2WS cannot choose for you. You need to choose at least one, or the instance recovery screen will display an error. Security groups are objects you own, and you can easily create them in AWS Management Console. You should have them ready so you will not need to create them when you perform recovery.
- **Kernel ID** - Linux instances need a kernel ID. If you are launching the instance from an image, you can leave this field empty, N2WS will use the kernel ID specified in the AMI. If you are recovering the instance from a root device snapshot, you need to find a matching kernel ID in the target region. If you do not do so, a default kernel will be used, and although the recovery operation will succeed and the instance will show as running in AWS Management Console, it will most likely not work. AMI Assistant can help you find a matching image in the target region. See section 10.3.4. When you find such an AMI, copy and paste its kernel ID from the AMI Assistant window.
- **RAMDisk ID** - Many instances do not need a RAM disk at all and this field can be left empty. If you need it, you can use AMI Assistant the same way you do for Kernel ID. If you're not sure, use the AMI Assistant or start a local recovery and see if there is a value in the RAMDisk ID field.

Note: DR of instances from Africa (Cape Town) and Asia Pacific (Hong Kong) might fail when using an **Assuming Account**.

### 11.5.2 Setting a Tag with an AMI ID for Cross-Account DR Recovery

N2WS can add a tag with an AMI ID to a resource during backup. The tag will hold the AMI ID that is expected to be present on the AWS account in case of recovery to a different AWS account.

**Example of tag format that will be used only on the region/account combination specified:**

Key = 'cpm\_dr\_recover\_ami:REGION:ACCOUNT'; Value = 'ami-XXXXX'

In this case, the region and account are optional.

**Example of tag format for a tag that will be used on any region/account combination:**

Key = 'cpm\_dr\_recover\_ami'; Value = 'ami-XXXXX'

When this tag is found and there is no other proper option for instance recovery, N2WS then uses this AMI if the recovery region and account fits.



**Note:** The AMI with an ID that is provided in the value of the tag is expected to be available on the other AWS account while recovering the instance.

### 11.5.3 DR of Encrypted Volumes, AMIs and RDS Instances

N2WS supports DR of encrypted EBS volumes. If you are using AWS KMS keys for encryption:

- N2WS will seek a KMS key in the target region, which has the same alias.
- The AWS ID of the DR account should be added to the 'Other AWS accounts' section on a Backup account.

#### To configure your cross-region DR:

Create a matching-alias key in the source and in the remote region for N2WS to use automatically in the DR copy process:

- If a matching key is not found in the target region, the DR process will fail.
- If the key uses the default encryption, then it will be copied to the other region with the default encryption key as well.
- N2WS supports copy of AMIs with encrypted volumes with the same logic it uses for volumes.
- N2WS supports cross-region DR of encrypted RDS databases, except for the Asia Pacific (Hong Kong) region.

#### To add the AWS ID of the DR Account to the 'Other AWS accounts' section of KMS on a Backup account:

1. Log on to your Backup AWS account and navigate to the KMS console.
2. Select your Customer managed keys.
3. Go to the 'Other AWS accounts' section.
4. Select **Add other AWS accounts**.
5. In the box, enter the AWS account ID of the DR account.

**Other AWS accounts** X

Specify the AWS accounts that can use this key. Administrators of the accounts you specify are responsible for managing the permissions that allow their IAM users and roles to use this key. [Learn more](#)

arn:aws:iam::25[REDACTED]07:root Remove

Add another AWS account

Cancel Save changes

**Note:** To let N2WS see keys and aliases, add these two permissions to the IAM policy that N2WS is using: **kms:ListKeys**, **kms:ListAliases**.



**To support the usage of a custom encryption key for DR, do the following in AWS:**

1. In the account where the custom key resides:
  - a. Go to KMS and browse to the key you wish to share.
  - b. Go to Other AWS accounts at the bottom of the page and select Add other AWS accounts.
  - c. Add the Id of the DR account you wish to share the key with.
2. Go to the volume you wish to copy to the DR account and/or region and add the following tag:
  - a. The tag's "key" = cpm\_dr\_encryption\_key
  - b. The tag's "value" = The full arn of the encryption key you shared in step #1, for example, arn:aws:kms:us-east-1:123456789101:key/2eaadfb1-b630-4aef-9d90-2d0fb2061e05
  - c. If you perform cross-region DR, you will need to have a key for each region as AWS does not allow sharing encryption keys across regions. The tag's "key" should include the region where the key is. For example, an Ohio key tag will be key = cpm\_dr\_encryption\_key:us-east-2, value = arn:aws:kms:us-east-1:123456789101:key/2eaadfb1-b630-4aef-9d90-2d0fb2061e05

**Note:** To recover an EFS with a non-default KMS, in AWS KMS, in the **Key user** field, select **Add** and choose **"AWSBackupDefaultServiceRole"**.

## 11.5.4 A Complete Disaster Recovery Scenario

Let's assume a real disaster recovery scenario: The region of your operation is completely down. It means that you do not have your instances or EBS volumes, and you do not have your N2WS Server, as it is down with all the rest of your instances. Here is Disaster Recovery step by step:

1. In the AWS Management Console:
  - a. Find the latest snapshot of your cpmdata policy by filtering snapshots with the string cpmdata. N2WS always adds the policy name to any snapshot's description.
  - b. Sort by Started in descending order and it will be the first one on the list.
  - c. Create a volume from this snapshot by right-selecting it and choosing Create Volume from Snapshot. You can give the new volume a name so it will be easy to find later.
2. Launch a new N2WS Server at the target region. You can use the [Your Software](#) page to launch the AWS Marketplace AMI. Wait until you see the instance in **running** state.
3. As with the regular configuration of an N2WS server:
  - a. Connect to the newly created instance using HTTPS.
  - b. Approve the SSL certificate exception. Assuming the original instance still exists, N2WS will come up in recovery mode, which means that the new server will perform recovery and not backup.
  - c. If you are running the BYOL edition and need an activation key, most likely you do not have a valid key at the time, and you do not want to wait until you can acquire one from N2W Software. You can quickly register at N2WS Free Edition. In step 2 of the registration, use your own username, and type any password. In step 3, choose the volume you just created for the CPM data volume. Afterward, complete the configuration.





4. With a working N2WS server, you can perform any recovery you need at the target (current) region:
  - a. Select the backup you want to recover.
  - b. Select Recover.
  - c. Choose the target region from the drop-down list.

**Note:** If your new server allows backup (it can happen if you registered to a different edition or if the original one is not accessible), it can start to perform backups. If that is not what you want, it is best to disable all policies before you start the recovery process.

- d. You can recover all the backed-up objects that are available in the region.

## 11.6 DR Monitoring and Troubleshooting

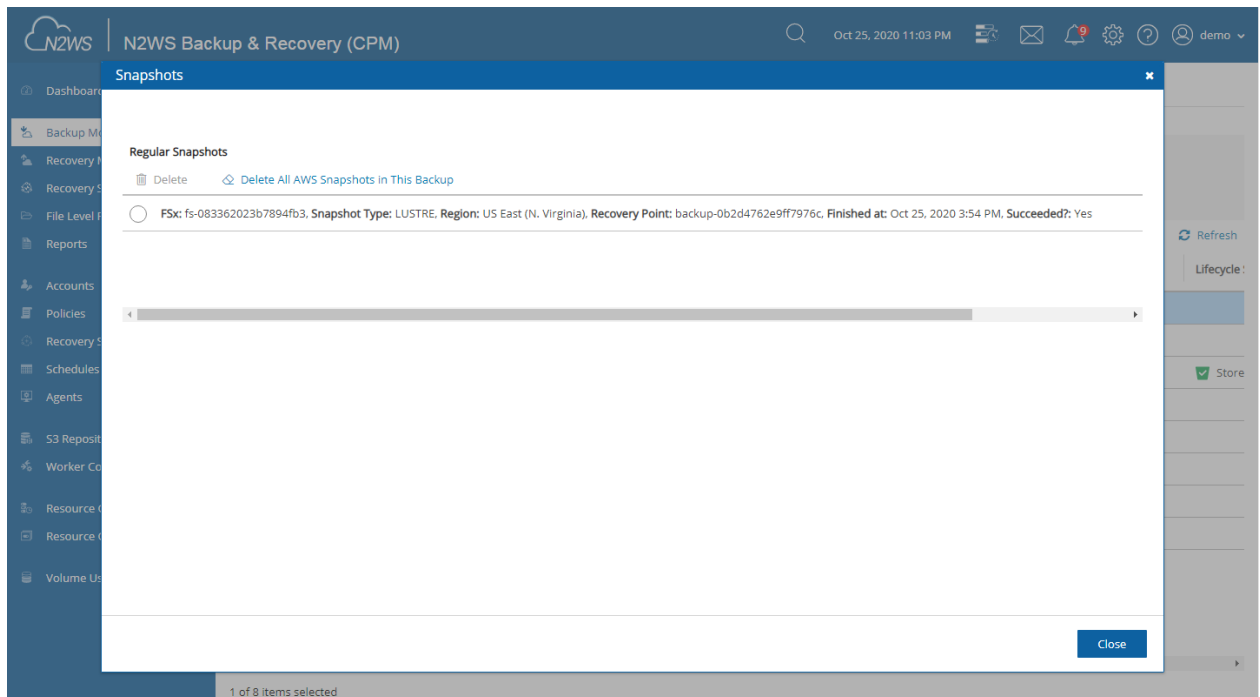
DR is a straightforward process. If DR fails, it probably means that either a copy operation failed, which is not common, or that the process timed-out. You can track DR's progress in the **Recovery Monitor** **Log** screen where every stage and operation during DR is recorded:

The screenshot shows the N2WS Recovery Log interface. The table contains the following data:

Time	Level	Message
10/25/2020 10:54:50 PM	Info	Started recovery of fsx (fs-083362023b7894fb3)
10/25/2020 10:54:55 PM	Info	FSx: fs-0508d1c57ad136e9e, Lifecycle=CREATING
10/25/2020 11:00:00 PM	Info	FSx: fs-0508d1c57ad136e9e, Lifecycle=AVAILABLE
10/25/2020 11:00:00 PM	Info	Succeeded recovering FSx fs-0508d1c57ad136e9e (original: fsx (fs-083362023b7894fb3))
10/25/2020 11:00:00 PM	Info	Recovery completed successfully

You can also view DR snapshot IDs and statuses in the **View Snapshots** screen of the **Backup Monitor**:





Every DR snapshot is displayed with region information and the IDs of both the original and the copied snapshots. In the **Snapshots** list, you can choose to [Delete All AWS Snapshots in This Backup](#).

If DR fails, you will not be able to use DR recovery. However, some of the snapshots may exist and be recoverable. You can see them in the snapshots screen and, if needed, you can recover from them manually.

If DR keeps failing because of timeouts, you may need to increase the timeout value for the relevant policy. The default of 24 hours should be enough, but there may be a case with a very large amount of data, that may take longer.

Reminder: You can only copy a limited number of snapshots to a given region at one time. Currently, the number is 5. If the limit is reached, N2WS will wait for copy operations to finish before it continues with more of them which can affect the time it takes to complete the DR process.



## 12 Cross-Account DR, Backup and Recovery

Available only in Standard, Advanced, and Enterprise Editions, N2WS's cross-account functionality allows you to automatically copy snapshots between AWS accounts as part of the DR module. With cross-region DR, you can copy snapshots between regions as well as between accounts and any combination of both. In addition, you can recover resources (e.g. EC2 instances) to a different AWS account even if you did not copy the snapshots to that account. This cross-account functionality is important for security reasons.

The ability to copy snapshots between regions can prove crucial if your AWS credentials have been compromised and there is a risk of deletion of your production data as well as your snapshot data. N2WS utilizes the **snapshot share** option in AWS to enable copying them across accounts. Cross-account functionality is currently supported only for EC2 instances, EBS volumes and RDS instances, including Aurora.

Cross-account functionality is enabled for encrypted EBS volumes and instances with encrypted EBS volumes, and RDS databases.

**Note:** Cross-region DR is not supported for RDS databases in the Asia Pacific (Hong Kong) region.

- Users will need to share the encrypted key used for the encryption of the volumes or RDS instance to the other account as N2WS will not do it.
- In addition, N2WS expects to find a key in the target account with the same alias as the original key (or just uses the default key).

For information on sharing encryption keys between different accounts, see

<https://support.n2ws.com/portal/kb/articles/cpm-supports-custom-encryption-keys-for-dr>

If a matching encryption key is not found with an alias or with custom tags, the behavior of the backup depends on the setting in the **Encryption Key Detection** list in the **Security** tab of the **General Settings** screen:

- **Use Default Key** – If the encryption key is not matched, the default encryption key is used.
- **Strict** – DR encryption key must match, either with an alias or a custom tag.
- **Use Default Key & Alert** – Use the default key and send an alert.

N2WS can support a DR scheme where a special AWS account is used only for snapshot data. This account's credentials are not shared with anyone and used only to copy snapshots. The IAM credentials used in N2WS can have limited permissions that do not allow snapshot deletion.

N2WS will tag outdated snapshots instead of actually deleting them, allowing an authorized user to delete them separately using the EC2 console or a script. The tag '**cpm\_deleted**' will have a value of '**CPM deleted this snapshot (<time-of-deletion>)**'. Also, you may choose to keep the snapshots only in the vault account and not in their original account. This will allow you to save storage costs and utilize the cross-recovery capability to recover resources from the vault account back to the original one.



## 12.1 Configuring Cross-Account Backup

Once you have created an account with the **Account Type** DR, you can configure cross-account DR from the **DR** tab of a policy.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation links: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies (selected), Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Policies > P3'. It shows a status bar with 'Last updated: Oct 25, 2020 11:43 AM', 'Last recovery: Never', and 'Last DR recovery: Never'. A warning message states: 'Cannot store snapshots in S3 if 'Keep Original Snapshots' in 'Cross-Account DR Backup Enabled' is unchecked'. Below this, the 'DR' tab is selected, showing configuration options: 'Enable DR' (checked), 'DR Frequency (backups)' (1), 'DR Timeout (hours)' (24), 'Target Regions' (Choose Region), 'Cross Account DR Backup Enabled' (checked), 'To Account' (assume\_role), and 'DR Account Target Regions' (empty). At the bottom right are buttons for 'Previous', 'Next', 'Save', and 'Cancel'.

Cross-account fields will be available only if your N2WS is licensed for cross-account functionality. See the [pricing and registration page](#) on our website to see which N2WS editions include cross-account backup & recovery.

Once you select **Cross-Account DR Backup Enabled**, other fields become visible:

- **To Account** – Which account to copy the snapshots to. This account needs to have been defined as a **DR Account Type** in the **Accounts** screen.
- **DR Account Target Regions** – Which region or regions you want to copy the snapshots of the policy to. To include all of the Target Regions selected for backup, select **Original** in the list. Select additional regions as needed.
- **Keep Original Snapshots** – Enabled by default, the original snapshot from the source region will be kept. If disabled, once the snapshot is copied to the DR account, it will be deleted from the source region.

**Note:** **Keep Original Snapshots** *must* be enabled for Copy to S3 for Cross-Account DR Backup.

## 12.2 Cross-Account DR and Clean-Up

N2WS performs clean-up on backup policies and deletes backups and snapshots that are out of the retention window, according to the policy's definition. By default, N2WS will clean up snapshots copied to other accounts as well. However, if you do not wish for N2WS to clean up,



because you want to provide IAM credentials that are limited and cannot delete data, you have that option. If you defined the DR account with **Allow Deleting Snapshots** set as False, N2WS will not try to delete snapshots in the DR account. It will rather flag a snapshot for subsequent deletion by adding a tag to the snapshot called **cpm\_deleted**. The tag value will contain the time when the snapshot was flagged for deletion by N2WS.

When using this option, occasionally make sure that these snapshots are actually deleted. You can either run a script on a schedule, with proper permissions or make it delete all snapshots with the tag **cpm\_deleted**. Or, using the EC2 console, filter snapshots by the tag name and delete them.

## 12.3 Cross-Account with Cross-Region

If you configure the backup policy to copy snapshots across accounts as well as across regions, be aware of how the increased number of copies might affect your AWS costs.

Cross-account with cross-region DR with AMIs is supported.

## 12.4 Cross-Account Recovery

If you have cross-account functionality enabled in your N2WS license, and even if you actually configured N2WS to copy snapshots between accounts, you can recover across accounts. This is already mentioned in Recovery section 10. You need to choose which account to recover the resource (EC2 instance, EBS volume, or RDS database) to.

**Note:** Only account type **DR** may be the target of a cross-account recovery.

When copying snapshots between accounts and not keeping the original snapshots, you will also have the option to restore the instance/volume to the original account. N2WS will utilize the AWS **share snapshot** option to enable recovering resources across accounts.

**Note:** There is an AWS limitation for restoring encrypted RDS snapshots from a DR AWS account. Directly restoring a cross-account DR copy of encrypted RDS snapshots is not supported. As a workaround, you can either restore directly to the DR AWS account, or the snapshot data can be copied back to the original AWS account, and then the restore can work as intended from there.





## 13 File-level Recovery





N2WS supports file-level recovery. N2WS does backup on the volume and instance level and specializes in the instant recovery of volumes and complete instances. However, in many cases, a user may want to access specific files and folders rather than recovering an entire volume.

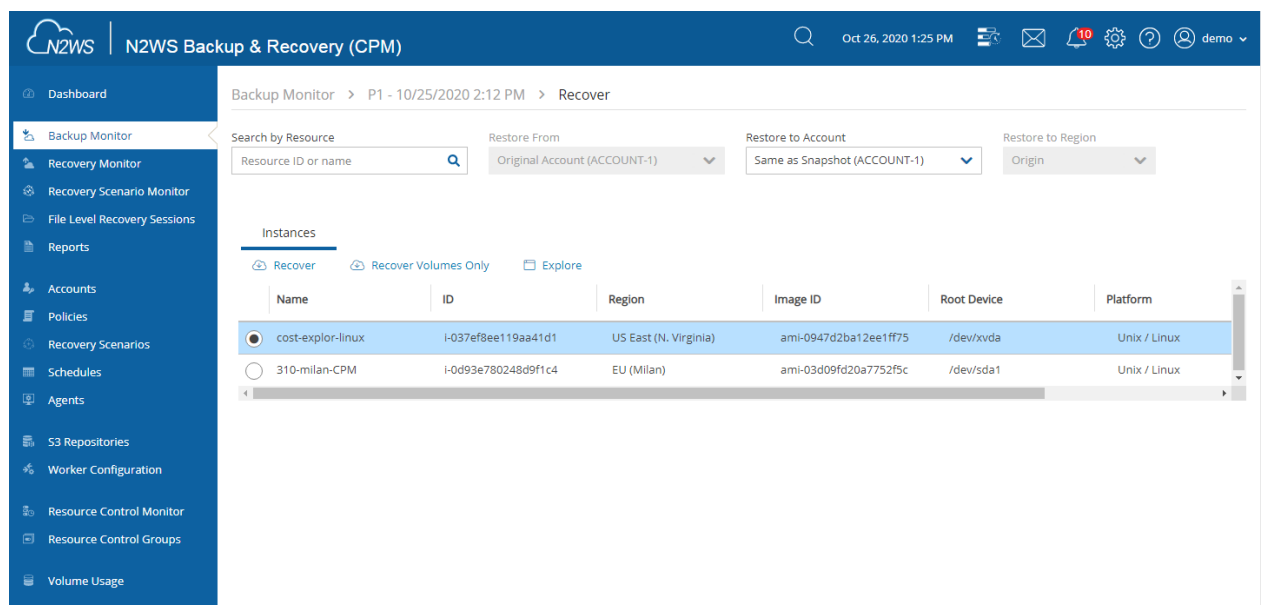
N2WS also provides the ability to locate the same item across a chain of consecutive snapshots during a single recovery session.

**Note:** AWS allows item-level recovery for individual files and folders from EFS. After reviewing this section, see the sections below for target-specific considerations.

In previous versions of N2WS, you could recover a volume, attach it to an instance, mount it, and then access the data from within that instance. After completing the restore, assuming the volume is no longer needed, the user needed to unmount, detach and delete the volume. N2WS now automates this entire process.

**Note:** To  **Explore** the directory tree structure and select files or directories for recovery, the disk on the target backup must have an OS. If there is no OS on the disk,  **Explore** will not work and a File Level Recovery Sessions will not open.

In the **Backup Monitor**, select an instance or volume backup and then select  **Recover**. In the Recover screen, select  **Explore** in the **Instances** or **Independent Volumes** tab. When selecting  **Recover Volumes Only**,  **Explore** is available in the **Volume Recovery** screen.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title "N2WS Backup & Recovery (CPM)", a search icon, the date "Oct 26, 2020 1:25 PM", and several utility icons. The left sidebar contains a list of navigation items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled "Backup Monitor > P1 - 10/25/2020 2:12 PM > Recover". It features a search bar labeled "Search by Resource" with a placeholder "Resource ID or name" and a search icon. To the right of the search bar are three dropdown menus: "Restore From" (set to "Original Account (ACCOUNT-1)"), "Restore to Account" (set to "Same as Snapshot (ACCOUNT-1)"), and "Restore to Region" (set to "Origin"). Below these is a tabbed interface with three tabs: "Instances" (selected), "Recover Volumes Only", and "Explore". Under the "Instances" tab, there is a table with the following columns: Name, ID, Region, Image ID, Root Device, and Platform. The table contains two rows: one for "cost-explor-linux" with ID "i-037ef8ee119aa41d1" in "US East (N. Virginia)" region, and another for "310-milan-CPM" with ID "i-0d93e780248d9f1c4" in "EU (Milan)" region. The first row is selected.

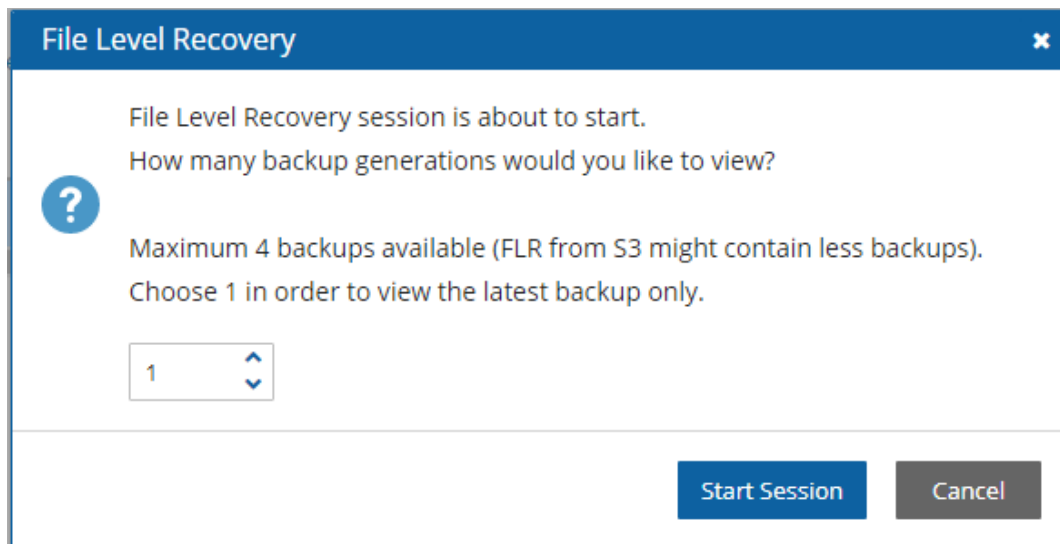
Name	ID	Region	Image ID	Root Device	Platform
cost-explor-linux	i-037ef8ee119aa41d1	US East (N. Virginia)	ami-0947d2ba12ee1ff75	/dev/xvda	Unix / Linux
310-milan-CPM	i-0d93e780248d9f1c4	EU (Milan)	ami-03d09fd20a7752f5c	/dev/sda1	Unix / Linux



If there is more than 1 backup available to view, the File Level Recovery dialog opens showing the number of backups.

**Note:** For Windows instances with dynamic disks partitioned using the master boot record (MBR) style, **Explore** only supports a single generation of snapshots. When more than 1 generation is selected for browsing, the dynamic disks will *not* be presented to the browser.

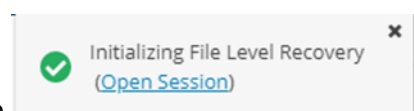
1. To view an instance across a chain of snapshots, select the number of available backups to view.
2. To view the latest backup only, leave the value at the default of 1.
3. Select **Start Session**.



**Note:**

- Only the number of available snapshots is presented, regardless of the number of generations.
- There is a limit of 72 volumes in a **File Recovery Session**.

N2WS will open the Initializing File Level Recovery message




Select **Open Session** for an **Explorer**-like view of the entire instance or a specific volume, folders, or files. Loading the session may take a few seconds. If the Initializing File Level Recovery message closes before you can select **Open Session**, in the left pane, select the **File Level Recovery Sessions** tab, select the active session, and then select **Explore**.

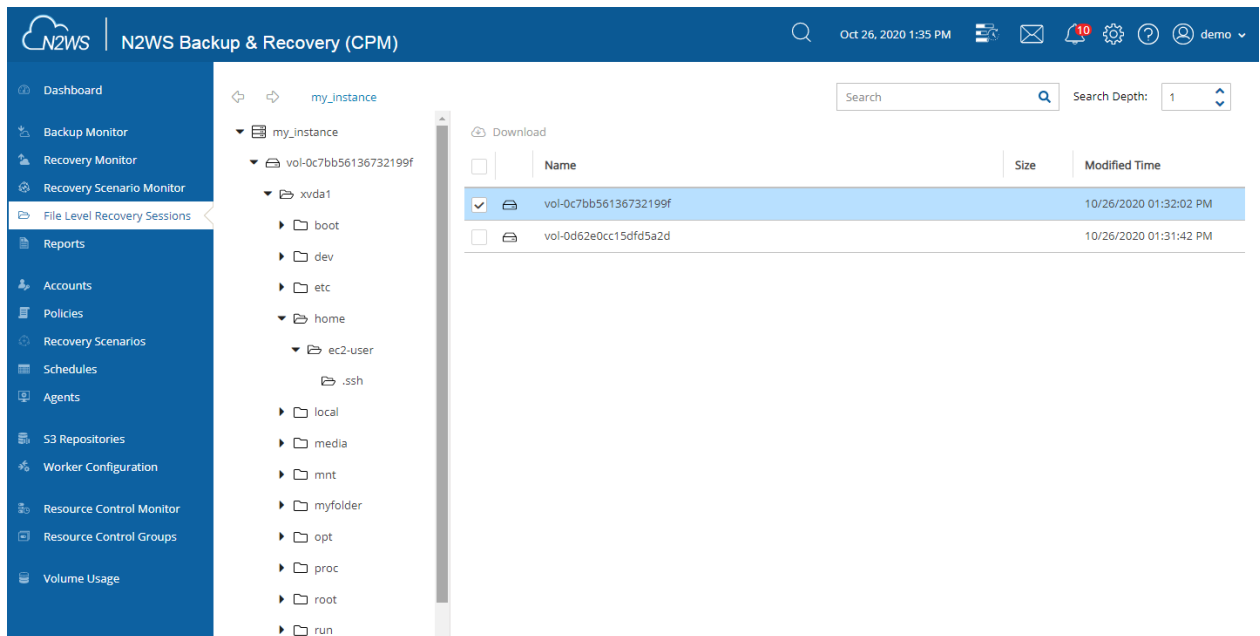
You will be able to browse, search for files, and download files and folders. Use the left and right arrows in the left corner to move between folders.

**Note:** Files in an **Explore** volume may actually be soft links (symbolic links) to other files. Trying to access this type of file may result in an error. However, the file is



accessible via its real path. For example, `root/folder2/file2` is a soft link to `root/folder1/file1`, where `/root/folder1/file1` is the real path.

Select any file or folder and then select  **Download**. Folders are downloaded as uncompressed zip files.



To perform these operations, N2WS needs to be able to use AWS credentials belonging to the N2WS server instance account, with sufficient permissions to create and attach volumes. By default, N2WS will use the same credentials used to initially configure the instance, but they can be modified using the **General Settings** screen.

File-level recovery requires N2WS to recover volumes in the background and attach them to a ‘worker’ launched for the operation. The worker will be launched in the same account and region as the snapshots being explored, using a pre-defined worker configuration. See section 22 to configure a ‘worker’ instance in the region that the snapshots exist.

**Note:** The worker will communicate with the N2WS server over both HTTPS and SSH. Verify that your configuration allows such communication.

After you complete the recovery operation, select **Close** for all the resources to be cleaned up and to save costs. Even if you just close the tab, N2WS will detect the redundant resources and clean them up, but it is recommended that you use **Close**. Sessions can be closed from the **File Level Recovery Sessions** tab also.

## 13.1 Limitations

There are a few limitations:

- File-level recovery is supported only for file system types Ext2, Ext3, Ext4, NTFS, XFS, Btrfs.

**Note:** If several XFS volumes have the same UUID, they cannot be mounted.



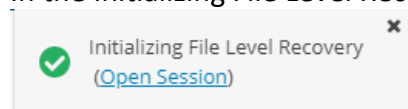
- **Explore** works only on the supported file systems listed above. Attempting to **Explore** a volume of a non-supported file system will fail.
- **Explore** works only on simple volumes and Logical Volume Management (LVM). LVM is supported with file-level restore on Linux, as well as for Windows dynamic disks. Additionally, disks defined with Microsoft Storage Spaces are not supported.
- To **Explore** snapshots taken in a different region than where the N2WS server is, it is required to configure a '**worker**' instance in the region that the snapshots exist. See section 22.

## 13.2 File Level Recovery from S3

1. In the **Backup Monitor**, select a backup **Stored in S3** and then select **Recover**. The **Recover** screen opens.
2. Select **Recover Volumes Only** or **Recover Volumes** to list the available volumes.

Original Volume ID	Type	Capacity (GiB)	IOPS	Encrypted	Device
vol-0d62e0cc15df5a2d	General Purpose SSD	88	264	No	/dev/sdb
vol-0c7bb56136732199f	General Purpose SSD	77	231	No	/dev/xvda
vol-005b9dce242ff5a08	General Purpose SSD	22	100	Yes	/dev/sdc

3. Select a volume and then select **Explore Volumes**.
4. In the Initializing File Level Recovery message, select **Open Session**.



Loading the session may take a few seconds. If the Initializing File Level Recovery message closes before you can select **Open Session**, in the left pane, select the **File Level Recovery Sessions** tab, select the active session, and then select **Explore**.

5. In the File Level Recovery Session window, navigate to the desired folder. See section 13.
6. Select the folders or snapshots to recover and select **Download**.
7. To close an active session, in the **File Level Recovery Sessions** tab, select the active session and then select **Close**.







## 13.3 File-Level Recovery from EFS

You can restore up to 5 items in your EFS to the files and directories in the source file system.

To restore EFS at the item level:

1. In the **Backup Monitor**, select a snapshot, and then select  **Recover**.
2. In the **EFS Restore Type** column, select **File/Directory Restore**.
3. At the left, select the right arrow (>) to open the item recovery path input box.
4. In the **Paths for Files/Directories to Recover** box, enter a forward slash (/) and the name of the path. See further limitations on the pathname in the Warning box below.
5. Select  **New** to add up to 5 recovery paths.



**Note:** When defining a recovery path:

- AWS Backup restores a specific file or directory. You must specify the path relative to the mount point. For example, if the file system is mounted to `/user/home/myname/efs` and the file path is `user/home/myname/efs/file1`, enter `/file1`.
- A forward slash (/) is required at the beginning of the path.
- Paths should be unique. If not, the 'This path already exists' error message will appear.
- Paths are case sensitive.
- Wildcards and regex strings are not supported.



## 14 Tag-based Backup Management

Cloud and specifically AWS, is an environment based largely on automation. Since all the functionality is available via an API, scripts can be used to deploy and manage applications, servers, and complete environments. There are very popular tools available to help with configuring and deploying these environments, like Chef and Puppet.

N2WS allows configuring backup using automation tools by utilizing AWS tags. By tagging a resource (EC2 instance, EBS volume, EFS, DynamoDB, RDS instance, Aurora Cluster or Redshift cluster), N2WS can be notified of what to do with this resource, and there is no need to use the UI. To tag Aurora clusters, tag one of the cluster's DB instances, and N2WS will pick it up and back up the entire cluster.

Since tagging is a basic functionality of AWS, it can be easily performed via the API and scripts.

N2WS supports both the '**cpm backup**' tag (see section 14.1) and custom tags (see section 14.2).

**Note:** For information on using tags with Resource Control, see section 15.5.

### 14.1 The "cpm backup" Tag

To automate backup management for a resource, you can add a tag to that resource named **cpm backup** (lower case with a space). N2WS will identify this tag and parse its content. In this tag you will be able to specify whether to:

- Ignore the resource and remove it from all backup policies.
- Add the resource to a policy or list of policies.
- Create a new policy, based on an existing one (template), and then add the resource to it.

**Note:** The policy name on the 'cpm backup' tag is case sensitive and should be aligned with the policy name create on CPM.

If an AWS resource has 2 AWS tags with the same tag name, differing only by the case of the letters (upper, lower), then N2WS will back up just one tag. The tag name will be in the format of the first tag N2WS scans, and the tag value *may* be from the second tag. Check that tag names are in the same case.

Following is a summary table of all **cpm backup** tag values:

Purpose	cpm backup Tag Value	Examples
Add resource to existing backup policy. See 14.1.1.	<i>policy1</i>	<i>policy1 policy2 policy3</i>
Create policy from a template. See 14.1.2.	<i>new_policy1:existing_policy1</i>	



Purpose	cpm backup Tag Value		Examples
Set backup options for EC2 instances. See 14.1.3.	<b>only-snaps</b> (create AMIs without reboot) <b>initial-ami</b> <b>only-amis</b> <b>only-amis-reboot</b> (create AMIs with reboot) <b>app-aware</b> (Windows instance backup agent is same as snapshot and AMI options) <b>app-aware-vss</b> (Enable application consistent with VSS) <b>app-aware-script</b> (Enable application consistent without VSS)		<i>policy1#only-snaps</i> <i>new_policy:existing_policy#only-amis</i> <i>policy1#initial-ami#app-aware</i>
Set backup options for EFS instances. N2WS will override EFS configuration with tag values. See 14.1.4.	<b>key</b>	<b>value</b>	<i>policy1+vault=Default+exp_opt=D+exp_opt_val=1</i>
	<b>vault</b> <b>role_arn</b> <b>cold_opt</b>  <b>cold_opt_val</b> <b>exp_opt</b>  <b>exp_opt_val</b>	Default (example) ARN of role Lifecycle transition: N, D, W, M, Y Integer for D,W,M,Y only When resource expires: P (Policy Gen), N, D, W, M, Y Integer for D, W, M, Y only	
Remove resource from all policies. See 14.1.5.	<b>no-backup</b>		
Exclude volumes from backup. See 14.1.6.	<i>policy1#exclude</i> Note: Tagged instances are excluded from the <b>Exclude volumes</b> option in <b>General Settings</b> for <b>Tag Scan</b> . Tagged instances are only excluded with the ' <b>#exclude</b> ' tag.		<i>policy1#exclude</i> <i>policy2#exclude</i>

### 14.1.1 Adding to a Policy or Policies

To add a resource (e.g. an EC2 instance) to an existing backup policy, all you need to do is to create the tag for this resource and specify the policy name (e.g. **policy1**):

tag key: **cpm backup**, tag value: **policy1**

To add the resource to multiple policies all you need to do is to add a list of policy names, separated by spaces:

**policy1 policy2 policy3**

**Note:** You can add an RDS target using the tag scan, but the resource will be added *without* the connection parameters. After the tag scan, you will need to configure the Connection Details in the policy manually. See section 21.4.2.



### 14.1.2 Creating a Policy from a Template

To create a new policy and to add the resource to it, add a new policy name with a name of an existing policy which will serve as a template (separated by semicolon):

tag value: **new\_policy1:existing\_policy1**

You can also add multiple policy name pairs to create additional policies or create a policy (or policies) and to add the resource to an existing policy or policies.

When a new policy is created out of a template, it will take the following properties from it:

- Number of generations
- Schedules
- DR configuration
- Script/agent configuration
- Retry configuration

It will not inherit any backup targets, so you can use a real working policy as a template or an empty one.

#### For Script definitions:

If backup scripts are defined for the template policy, the new one will keep that definition but will not initially have any actual scripts. You are responsible to create those scripts. Since the N2WS server is accessible via SSH you can automate script creation. In any case, since scripts are required, the backups will have a failure status and will send alerts, so you will not forget about the need to create new scripts.

#### For Windows instances with a backup agent configured:

If that was the configuration of the original policy, the new instance (assuming it is a Windows instance) will also be assigned as the policy agent. However, since it does not have an authentication key, and since the agent needs to be installed and configured on the instance, the backups will have a failure status. Setting the new authentication key and installing the agent needs to be made manually.

**Auto Target Removal** for the new policy will always be set to **yes and alert**, regardless of the setting of the template policy. The basic assumption is that a policy created by a tag will automatically remove resources that do not exist anymore, which is the equivalent as if their tag was deleted.

### 14.1.3 Setting Backup Options for EC2 Instances

When adding an instance to a policy, or creating a new policy from template, you may make a few decisions about the instance:

- To create snapshots only for this instance.
- To create snapshots with an initial AMI.
- To schedule AMI creation only.

If this option is not set, N2WS will assume the default:

- Snapshots only for Linux.
- Snapshots with initial AMI for Windows instances by adding a backup option after the policy name. The backup option can be one of the following values:



- **only-snaps**
- **initial-ami**
- **only-amis**
- **only-amis-reboot**

For example, with existing policy: `policy1#only-snaps`.

Or, for a new policy based on template and setting AMI creation:

```
my_new_policy:existing_policy#only-amis
```

Note: The **only-amis** option will create AMIs without rebooting them. The option **only-amis-reboot** will create AMIs with reboot.

For a Windows instance, you can also define backup with **app-aware**, i.e. a backup agent. It is used the same as the snapshots and AMI options.

- When adding the **app-aware** option, the agent is set to the default: VSS is enabled and backup scripts are disabled.
  - **app-aware-vss** - Enable application consistent with VSS.
  - **app-aware-script** - Enable application consistent without VSS.
- Additional configurations need to be made manually, and not with the tag.

You can also combine the backup options: `policy1#initial-ami#app-aware`.

#### 14.1.4 Setting Backup Options for EFS Instances

EFS can be configured by creating the **cpm backup** tag with the following values. In this case, N2WS will override the EFS configuration with the tag values:

Key	Value
vault	Vault. Example: Default
role_arn	ARN of role. Example: arn:aws:iam::040885004714:role/service- role/AWSBackupDefaultServiceRole
cold_opt	Lifecycle transition: N – Never                                  M – Months D – Days                                      Y - Years W – Weeks
cold_opt_value	Integer for D, W, M, Y only
exp_opt	When does resource expire: P – Policy Generations                  W- Weeks N – Never                                      M – Months D – Days                                      Y - Years
exp_opt_val	Integer for D, W, M, Y only

### Example:

```
cpm backup my policy+vault=Default+exp opt=D+exp opt val=1
```

N2WS will back up EFS to the default vault, and set its expiration date to 1 day.

**Note:** The max length for the **cpm backup** value is limited to 256 characters.



### 14.1.5 Tagging a Resource to be Removed from All Policies

By creating the **cpm backup** tag with the value **no-backup** (lower case), you can tell N2WS to ignore the resource and remove this resource from all policies. Also, see section 14.1.

### 14.1.6 Excluding Volumes from Backup

N2WS can exclude a volume from an instance that is backed up on policy using the **cpm backup** tag with **#exclude** added to the end of the policy name value.

- Add a tag to an instance that you want to back up:  
Key = **cpm backup**; Value = policy\_name1 policy\_name2

**Add/Edit Tags** [X]

Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	
CPM Silent Configuration	succeeded	[X] Show Column
Name	Glacier	[X] Hide Column
cpm backup	p1 p2	[X] Show Column

Create Tag Cancel Save

- Add a tag to volumes that you would like to exclude from being backed up:  
Key = **cpm backup**; Value = policy\_name1#exclude policy\_name2#exclude

**Add/Edit Tags** [X]

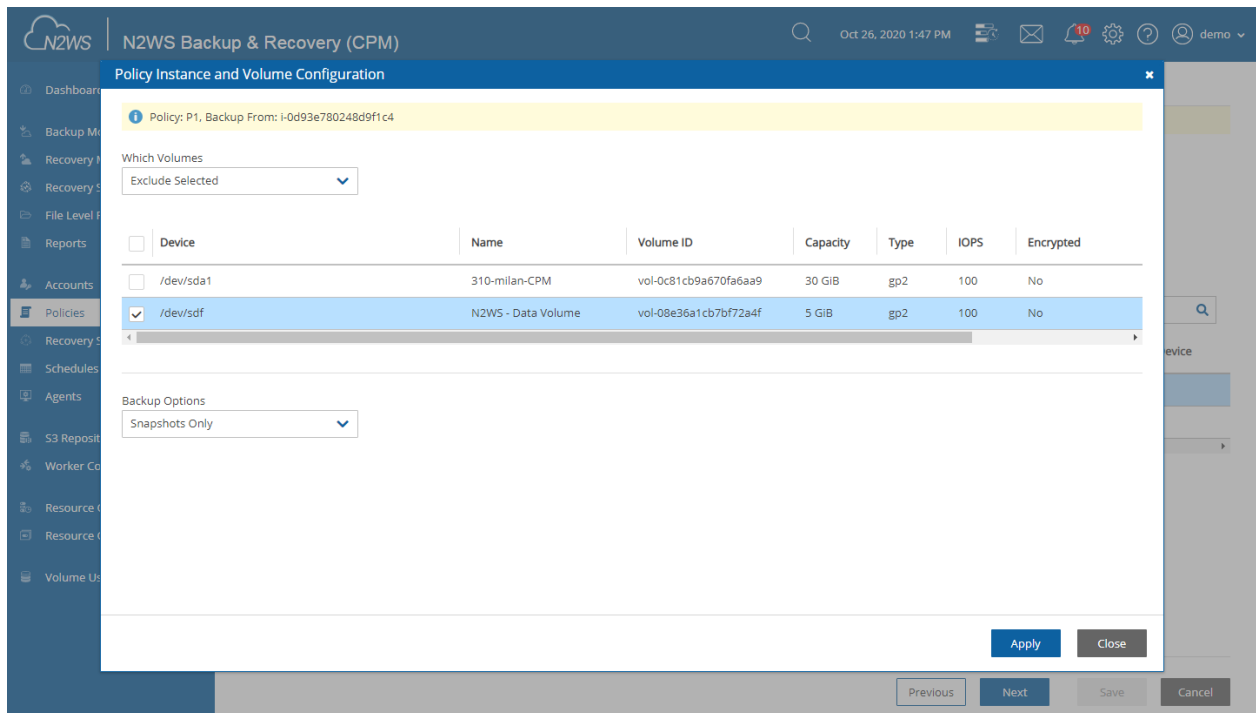
Apply tags to your resources to help organize and identify them.

A tag consists of a case-sensitive key-value pair. For example, you could define a tag with key = Name and value = Webserver. [Learn more](#) about tagging your Amazon EC2 resources.

Key	Value	
Name	CPM Cloud Protection Man	[X] Hide Column
cpm backup	p1#exclude p2#exclude	[X] Show Column

Create Tag Cancel Save

For example, if instance1 has 3 volumes and has a **cpm backup** tag with the value policy1, adding the **cpm backup** tag with value policy1#exclude to a volume will remove it from the policy. The instance with the excluded volume(s) will be added automatically as a backup target to the policy, after running **Scan Tag**.



**Note:** Tagged instances are not included in the **Exclude volumes** option in the **Tag Scan** tab of **General Settings** and are excluded from backup only when tagged with **#exclude** for the policy.

## 14.2 Custom Tags

Custom Tags allow N2WS users to easily backup resources using any tag of their choice.

- You can define any number of Custom Tags on a Policy definition.
- Custom tags take precedence over **cpm backup** tags if both exist on a server.
- Define Custom Tags with the Names and Values to match the Tags of AWS Resources to add to the Policy.
- If a user-defined Custom Tag exists on an AWS resource, the resource will be automatically added to the Policy during the **Tag Scan** process. See section 14.3.
- It is possible to match an AWS Resource Tag with an N2WS Tag Name or Value defined as a Prefix. For example, if the Tag Name 'Department' is defined as a Prefix, the following AWS resources that have a Tag Name starting with 'Department' will be added to the policy: 'Department A', 'Departments', and Department\_3'.

**Notes:**

- Custom Tags are case-sensitive.
- If the **cpm backup** tag is used on a resource with **no-backup**, Custom Tags will be ignored and the resource will not be backed up.

To see which resources were added to backup, open the Tag Scan log (**Show Log**) and look for a Custom Tags match.





### To create Custom Tags:

1. In the **Policies** tab, select a policy.
2. Select the **More Options** tab.
3. Turn on the **Custom Tags** toggle.
4. Select **+ New**.

5. Define the **Tag Name** and **Tag Value**.
6. If the Name and/or Value is a prefix, select **Name is Prefix**.

## 14.3 Tag Scanning

Tag scanning can only be controlled by the admin/root user. When the scan is running, it will do so for all the users in the system but will only scan AWS accounts that have **Scan Resources** enabled. This setting is disabled by default. N2WS will automatically scan resources in all AWS regions.

1. In the **General Settings** tab, select the **Tag Scan** tab.
2. Select **Scan Resources**.
3. In the **Tag Scan interval** list, set the interval in hours for automatic scans.
4. To override the exclusion of volumes specified in the UI and to exclude instances tagged with **#exclude** for the policy, select **Exclude volumes**. See section 9.6.
5. Select **Save**.
6. To initiate a tag scan immediately, select **Scan Now**.

7. To view the Last Scan, select **Show Log**.



**Note:** Even if scanning is disabled, selecting **Scan Now** will initiate a scan.

If you do want automated scans to run, keep scanning enabled and set the interval in hours between scans using the **General Settings** screen. You will also need to enable **Scan Resources** for the relevant N2WS Accounts. See section 3.1.2.

## 14.4 Pitfalls and Troubleshooting

The following topics should help guide you when developing tags.

### 14.4.1 Pitfalls

There are potential issues you should try to avoid when managing your backup via tags:

- The first is not to create contradictions between the tags content and manual configuration. If you tag a resource and it is added to a policy, and later you remove it from the policy manually, it may come back at the next tag scan. N2WS tries to warn you from such mistakes.
- Policy name changes can also affect tag scanning. If you rename a policy, the policy name in the tag can be wrong. When renaming a policy, correct any relevant tag values.
- When you open a policy that was created by a tag scan to edit it, you will see a message at the top of the dialog window: “\* This policy was automatically added by tag scan”.

**Note:** Even if all the backup targets are removed, N2WS will not delete any policy on its own, since deletion of a policy will also delete all its data. If you have a daily summary configured (section 17.5), policies without backup targets will be listed.

- If the same AWS account is added as multiple accounts in N2WS, the same tags can be scanned multiple times, and the behavior can become unpredictable. N2W Software generally discourages this practice. It is better to define an account once, and then allow delegates (section 18.4) access to it. If you added the same AWS account multiple times (even for different users), make sure only one of the accounts in N2WS has **Scan Resources** enabled in N2WS.

### 14.4.2 Troubleshooting

Sometimes you need to understand what happened during a tag scan, especially if the tag scan did not behave as expected, such as a policy was not created. In the **General Settings** screen, you can view the log of the last tag scan and see what happened during this scan, as well as any other problems, such as a problem parsing the tag value, that were encountered. Also, if the daily summary is enabled, new scan results from the last day will be listed in the summary.

#### Ensure tag format is correct:

Tips for ensuring correct tag formats are:

- When listing multiple policy names, make sure they are separated by spaces.
- When creating new policy, verify using a colon ‘:’ and not a semi-colon ‘;’. The syntax is `new_policy1:existing_policy1`.



- Use a valid name for the new policy or it will not be created. An error message will be added to scan log.
- Use correct names for existing/template policies.
- Resource scanning order is NOT defined, so use policy names as existing/template only if you are sure that it exists in N2WS – defined manually or scanned previously.



## 15 Resource Control


Resource Control allows users to stop and start Instances and RDS Databases for each Account during the course of a week. It also allows users to stop the resources at a designated time in the future.

**Note:** RDS Aurora Clusters are *not* supported by Resource Control.

- A Group is the controlling entity for the stopping and starting of selected resources. Resource Control allows for stopping on one day of a week and starting on another day of the same week. Once an Off/On schedule is configured for a Group, N2WS will automatically stop and start the selected resource targets.
- Resources that are eligible and enabled for hibernation in AWS will be hibernated regardless of whether their current operation is On or Off if their controlling Resource Control Group is enabled for hibernation. Hibernated instances are restarted by an On operation.
- See [AWS hibernation prerequisites](#) in the [User Guide for Linux Instances](#).
- For enabling hibernation in N2WS, see the Hibernation description in section 15.1.
- The stopping and starting of targets identified for each Group are independent of the backup schedule for an Account's policy.
- It is possible to turn off operations for a long period of time even though the Group was never turned on.
- Ad hoc Off and On operations are available in addition to the Resource Control schedule.
- Off/On operations are not allowed for Groups with a **Status** of 'disabled'.

**Recommendation:** N2WS recommends that you not execute a stop or start operation on critical servers.

Following are Resource Control tabs in the left panel of the N2WS user interface:

- **Resource Control Monitor** – Lists the current operational status of Groups under Resource Control. The  **Log** lists the details of the most recent operation for a Group.



N2WS Backup & Recovery (CPM)

Resource Control Monitor

Search resource control operations

All Groups All Accounts All Operation Statuses 20 records/page

Log Delete Refresh

<input type="checkbox"/>	Start Time	Finish Time	Group	Account	Status
<input type="checkbox"/>	Oct 26, 2020 11:00 AM	Oct 26, 2020 11:00 AM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 25, 2020 11:00 PM	Oct 25, 2020 11:00 PM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 25, 2020 11:00 AM	Oct 25, 2020 11:01 AM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 25, 2020 12:00 AM	Oct 25, 2020 12:00 AM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 24, 2020 12:00 PM	Oct 24, 2020 12:00 PM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 24, 2020 12:00 AM	Oct 24, 2020 12:00 AM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 23, 2020 12:00 PM	Oct 23, 2020 12:01 PM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 23, 2020 12:00 AM	Oct 23, 2020 12:00 AM	rcg1	ACCOUNT-1	✓ Su
<input type="checkbox"/>	Oct 22, 2020 12:00 PM	Oct 22, 2020 12:00 PM	rcg1	ACCOUNT-1	✓ Su

0 of 9 items selected

- **Resource Control Groups** – Use the **Groups** tab to add and configure a Group: the account, the days and off/on times, which Resource Targets are subject to the Group control, and other features. You can also delete a group and activate **Turn On Now** / **Turn Off Now** controls.

N2WS Backup & Recovery (CPM)

Resource Control Groups

Search resource control groups

All Accounts 20 records/page

+ New Edit Turn On Now Turn Off Now Delete Refresh Savings Data from AWS Refresh

<input type="checkbox"/>	Name	Account	Timeout (minutes)	Enabled	Cost \$
<input type="checkbox"/>	rcg1	ACCOUNT-1	30	Yes	\$ 4.18

0 of 1 items selected

After configuring a group, you can add resources in the **Operation Targets** tab. See section 15.2.



N2WS Backup & Recovery (CPM)

Resource Control Groups > rcg1

Last Update: Oct 25, 2020 12:27 PM

Group Details | Operation Targets | Schedules

Add Backup Targets

- Instances
- RDS Databases
- Instances

Remove

Search resources

Name	Instance	Region	Status	AMI ID	Root Device
yotam	i-0c55cdac1c53d3c2c	us-east-1	stopped	ami-01009d26d7971950b	ebs

0 of 1 items selected

Previous Next Save Cancel

## 15.1 Adding a Resource Control Group

In the **Resource Control Groups** tab, select **+ New** and complete the **Group Details** screen fields:

N2WS Backup & Recovery (CPM)

Resource Control Groups > New Resource Control Group

Group Details | Operation Targets | Schedules

Name

User demo + New Account ACCOUNT-1 + New

☒ Enabled

Operation Mode Turn On/Off

Auto Target Removal No

Timeout (minutes) 30

☐ Hibernate (if possible) [Check Hibernation Limitations](#)

Next Save Cancel

- **Name** –Only alphanumeric characters and the underscore allowed (no spaces).

**Note:** A Group may belong to *only* one Account.



- **Account** – Owner of the Group. Users are configured for a maximum number of Resource Control entities. See section 18.
- **Enabled** – Whether the Group is enabled to run.

Note: Off/On operations are not allowed for Groups that are Disabled.

- **Operation Mode** – Two options for controlling operation:
  - **Turn On/Off** – Turn Group on and off according to schedule.
  - **Turn Off Only** – Turn off for an undefined long period of time without having to ever have the Group turned on.
- **Auto Target Removal** – Whether a target resource is automatically removed from the Group if the resource no longer exists in AWS.
- **Timeout (in minutes)** - How long will the operation wait in minutes until finished. Default is 30 minutes. Failure from exceeding the timeout does not necessarily mean that the operation of stopping or starting the resource has failed. The Log will show the run status for each resource.
- **Hibernate (if possible)** – Whether eligible instances will be hibernated. If enabled, only instances within the Group's target resources that are eligible for hibernation by AWS will be hibernated. See Note on limitations below.

Note: If an enabled Group contains mixed types of instances, only some of which are eligible for hibernation, then the Off operation will 'hibernate' only the eligible instances, while the remaining instances will 'stop'.

Note: Select the ["Check Hibernation Limitations"](#) link to view current AWS limitations on hibernating instances. During instance creation in AWS, hibernation would have been enabled and encryption configured. If the resource is eligible and the Group is enabled, instances that are 'stopped' move to 'hibernation' state.

- **Description** – Optional description of the Resource Control Group function.

After adding a Group, select **Next** at the bottom of the screen or select the **Operation Targets** tab and configure the **Operation Targets** (section 15.2) and the **Off/On Times** (section 15.3).

## 15.2 Adding Resource Targets to a Group

Instances and RDS Databases may be added to the Group.

Note: A Resource Target (Instance or RDS Database) may belong to *only* one Group.

- Eligible resources within a Group enabled for hibernation that has been stopped have a **Status** of 'stopped-hibernation'.
- The **Status** column shows whether a target is 'running' or 'stopped'.

Select the **Operation Targets** tab. In the **Add Backup Targets** menu, select a resource type to add to the Group.

Note: It is important to not configure a critical server as part of a Group.



1. If you selected **Instances**, the **Add Instances** screen opens. The following instance types are omitted from **Add Instances** and not allowed to be part of a Group:

- CPM
- Instance-Store type
- Worker - See section 22.

Resource Control Groups > New Resource Control Group

**Add Instances**

US East (N. Virginia) Search resources Refresh

<input type="checkbox"/>	Name	Instance	Status	AMI ID
<input type="checkbox"/>	DD-LS-RELEASE-32	i-0ace588af37254d8b	stopped	ami-0626796a06737431
<input type="checkbox"/>	My-Proxy	i-0ab3d1abffe770f3d	stopped	ami-0df5c14f8c57da13b
<input checked="" type="checkbox"/>	RE-LOGIN-PAGE-32-rc	i-0b5f94abfad3c44cf	running	ami-085c2b00a2c1da7e
<input type="checkbox"/>	copy-to-GOV	i-0082636e9b5f72f68	running	ami-0817d428a6fb6864
<input type="checkbox"/>	cost-explor-linux	i-037ef8ee119aa41d1	running	ami-0947d2ba12ee1ff75
<input type="checkbox"/>	dev-32-DD-18-10	i-06ce81d350dd2f50	running	ami-0dbd8cf51e1a95c12
<input type="checkbox"/>	release-32-DD-take2-18-10	i-05h6h9518e9a4d000	stopped	ami-018a0de67f6b6b5h

1 of 7 items selected

Add selected Close

Previous Next Save Cancel

2. If you selected RDS Databases, the following screen opens:

Resource Control Groups > New Resource Control Group

**Add RDS Databases**

IMPORTANT: You can't take snapshots of stopped RDS instances

US East (N. Virginia) Search resources Refresh

<input type="checkbox"/>	DB Instance	Status	Multi AZ	Class	Storage (GiB)	Type
--------------------------	-------------	--------	----------	-------	---------------	------

Add selected Close

Previous Next Save Cancel

**Note:** If an RDS database is stopped, a regularly scheduled backup will fail.





3. Check the **Status** column to determine whether a resource is eligible for adding to the Group.
4. Select one or more resources, and then select **Add Selected**. Selected resources are removed from the table.
5. Continue until you are finished and select **Close** to return to the **Operations Targets** screen.
6. Select **Save** to save the **Operation Targets** selections.

## 15.3 Configuring Off/On Scheduler

Scheduling overlapping off and on time ranges is invalid. For example:

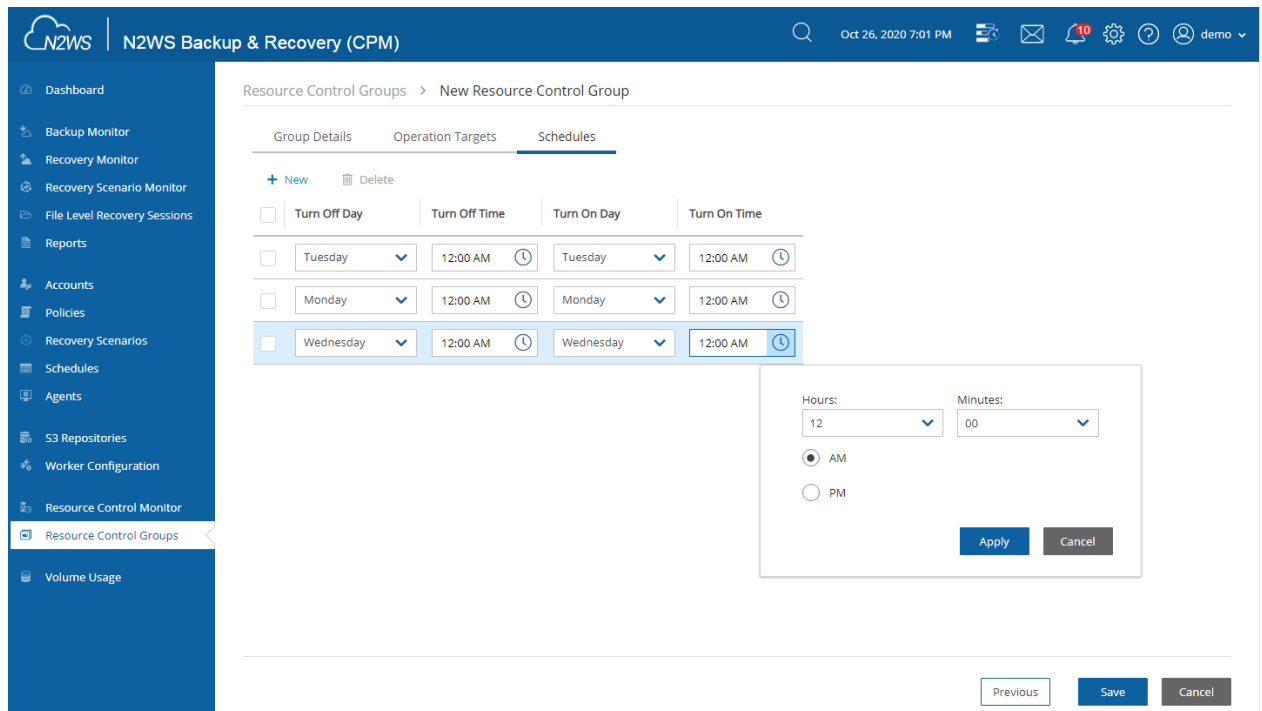
- A resource is turned off at 20:00 on Wednesday and turned on at 23:00 the same day.
- Then, an attempt to schedule the same resource to be turned off on Wednesday at 9:00 and turned off at 22:00 on Wednesday will result in an invalid input error.

1. Select **Next** to advance to the **Schedules** tab for the group.
2. Select **+ New** to open a default time range row ready for your changes.

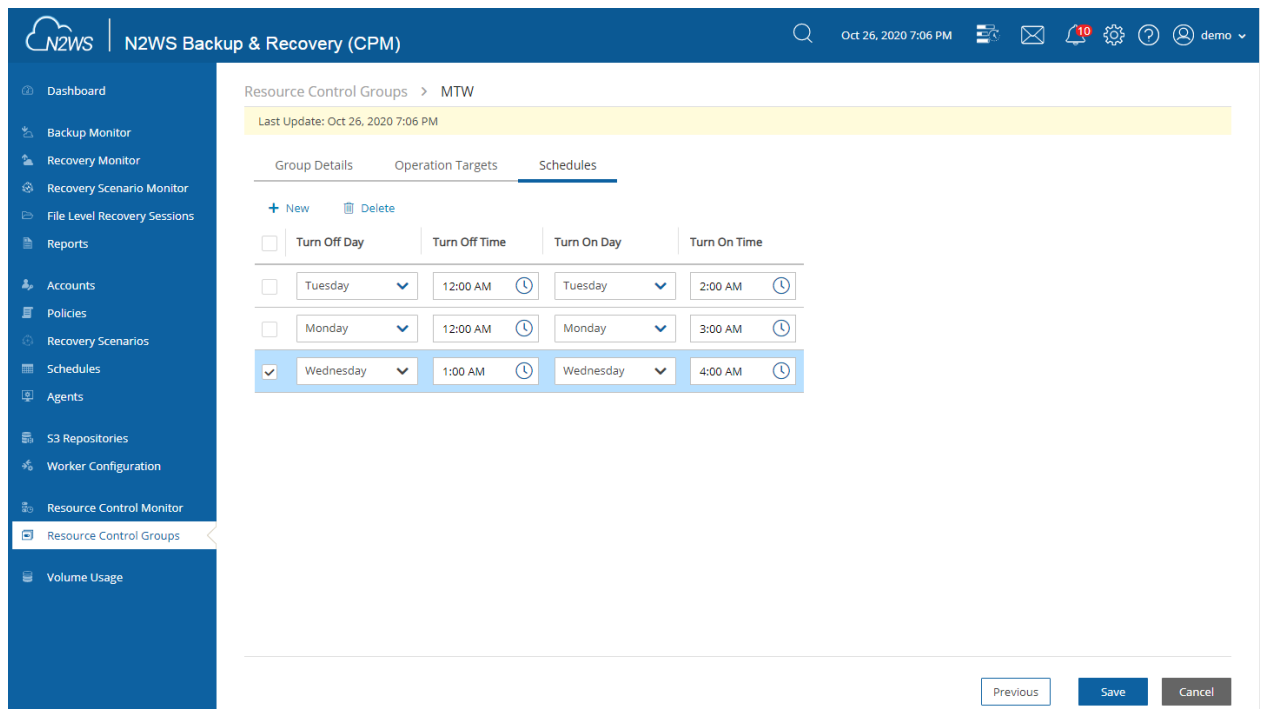
The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with items like Dashboard, Backup Monitor, Recovery Monitor, etc. The main area is titled 'Resource Control Groups > New Resource Control Group'. It has three tabs: 'Group Details', 'Operation Targets', and 'Schedules'. The 'Schedules' tab is active, showing a table with columns: Turn Off Day, Turn Off Time, Turn On Day, and Turn On Time. There are two rows in the table. The first row has 'Tuesday' for both days and '12:00 AM' for both times. The second row has 'Monday' for both days and '12:00 AM' for both times. The 'Monday' dropdown is highlighted. At the bottom right are 'Previous', 'Save', and 'Cancel' buttons.

3. In the time range row, select the **Turn Off Day** and **Time** and the **Turn On Day** and **Time** values from the drop-down lists, choosing **AM** or **PM** as required. After each time selection, select **Apply**.

**Note:** There must be 60 minutes between each operation in order for them to work.



4. Select **+ New** to open another time range row.
5. When finished creating the time ranges, select the required time range rows, and then select **Save**.



## 15.4 Overriding a Resource Control Schedule

After creating the Group, you can initiate a stop or start action outside of the scheduled times by selecting the **▶ Turn On Now** or **□ Turn OFF Now** in the **Resource Control Groups** tab.



Resource Control Groups

<input type="checkbox"/>	Name	Account	Timeout (minutes)	Enabled	Cost Si
<input checked="" type="checkbox"/>	MTW	ACCOUNT-1	30	Yes	N/A
<input type="checkbox"/>	rcg1	ACCOUNT-1	30	Yes	\$ 4.18

1 of 2 items selected

## 15.5 Using Scan Tags with Resource Control

Scan tags for Resource Control can be used to:

- Create a new Group based on an existing Group's configuration.
- Add a resource to a Group.
- Remove a tagged or untagged resource from a Group.

The tag format is Key: `cpm_resource_control` with one of the following values:

- Value: `<group-name>` or `<group-name>:<based-on-group>`
  - If the value in `<group-name>` equals 'g1', the resource will be added to the g1 group.
  - The template `<group-name>:<based-on-group>` means, in the case of g1:g2:
    - If g1 exists, add the resource to g1.
    - Otherwise, create a new group g1 based on group g2, and add the resource to it.
- Value: **no-resource-control** - Remove the resource instance or RDS database from the Group whether it is tagged or not.
- Value: `<no value>` - Remove the tagged resource instance or RDS database from the Group.

## 15.6 Resource Control Reporting

Resource Control provides individual logs of off and on operations and a summary report of all operations.

The individual log contains timestamps for each step within the operation, from firing to completion, and is downloadable as a CSV file. To view individual logs, in the **Resource Control Monitor** tab, select a group and then select **Log**.

Time	Level	Message
02/28/2020 2:00:00 AM	✓ Info	Turn Off operation was fired by schedule
02/28/2020 2:00:01 AM	✓ Info	Turn Off operation of instance i-077441dd85a72e6d5 started successfully
02/28/2020 2:00:01 AM	✓ Info	Turn Off operation of instance i-0d6abf533c3049e61 started successfully
02/28/2020 2:00:46 AM	✓ Info	Turn Off operation of instance i-0d6abf533c3049e61 completed successfully.
02/28/2020 2:01:02 AM	✓ Info	Turn Off operation of instance i-077441dd85a72e6d5 completed successfully.
02/28/2020 2:01:02 AM	✓ Info	Turn Off Operation Finished successfully on all Instances/RDS.

To download the individual log, select [Download Log](#).

resource\_control\_log\_g\_2020-01-13\_04-57-41 - Excel

FileHomeInsertPage LayoutFormulasDataReviewViewHelpTell me what you

A1

X✓fx

Log Time

	A	B	C
1	Log Time	Log Type	Log
2	1/13/2020 4:57	Info	Turn Off operation was fired by schedule: Immediate/ASAP
3	1/13/2020 4:57	Info	Turn Off operation of instance i-063cfd80cab17e715 started successfully
4	1/13/2020 4:57	Info	Turn Off operation of instance i-0bdcb2c7b69b0f90 started successfully
5	1/13/2020 4:57	Info	Turn Off operation of instance i-092d5a3314bb2295b started successfully
6	1/13/2020 4:57	Info	Turn Off operation of instance i-0a7382f080e25b858 started successfully

**To generate the summary log:**

1. Select the **Reports** tab in the left panel.
2. Select the **Immediate Report Generation** tab and then select **Resource Control Operations** in the **Report Type** list.
3. Complete the filter and time range boxes.
4. Select **Generate Report**. The report is automatically downloaded as a CSV file.

The Resource Control Operations Report contains information for all saved operations for all accounts. For each operation it contains:

- **Resource Control Operation ID** – A sequential number for each operation.



- **User** – User generating the report.
- **Account** – The N2WS owner of the Resource Control Group.
- **AWS Account Number** – The AWS account number of the owner of the resources.
- **Resource Control Group** – The N2WS Resource Control Group name.
- **Status** – Operation status.
- **Start Time** – Start date and time.
- **End Time** – End date and time.
- **Marked for Deletion** – Whether the resource is marked for deletion.



## 16 Security Concerns and Best Practices

Security is one of the main issues and barriers in decisions regarding moving business applications and data to the cloud. The basic question is whether the cloud is as secure as keeping your critical applications and data in your own data center. There is probably no one simple answer to this question, as it depends on many factors.

Prominent cloud service providers like Amazon Web Services, are investing a huge amount of resources so people and organizations can answer ‘yes’ to the question in the previous paragraph. AWS has introduced many features to enhance the security of its cloud. Examples are elaborate authentication and authorization schemes, secure APIs, security groups, IAM, Virtual Private Cloud (VPC), and more.

N2WS strives to be as secure as the cloud it is in. It has many features that provide you with a secure solution.

### 16.1 N2WS Server

N2WS Server’s security features are:

- Since you are the one who launches the N2WS server instance, it belongs to your AWS account. It is protected by security groups you control and define. It can also run in a VPC.
- All the metadata N2WS stores are stored in an EBS volume belonging to your AWS account. It can only be created, deleted, attached, or detached from within your account.
- You can only communicate with the N2WS server using HTTPS or SSH, both secure protocols, which means that all communication to and from N2WS is encrypted. Also, when connecting to AWS endpoints, N2WS will verify that the SSL server-side certificates are valid.
- Every N2WS has a unique self-signed SSL certificate. It is also possible to use your own SSL certificate.
- AWS account secret keys are saved in an encrypted format in N2WS’s database.
- N2WS supports using different AWS credentials for backup and recovery.
- N2WS Server supports IAM Roles. If the N2WS Server instance is assigned an adequate IAM role at launch time, you can use cross-account IAM roles to “assume” roles from the main IAM role of the N2WS instance account to all of the other AWS accounts you manage and not type AWS credentials at all.
- To manage N2WS, you need to authenticate using a username and password.
- N2WS allows creating multiple users to separately manage the backup of different AWS accounts, except in the Free Edition.

### 16.2 Best Security Practices for N2WS

Implementing all or some of the following best practices depends on your company’s needs and regulations. Some of the practices may make the day-to-day work with N2WS a bit cumbersome, so it is your decision whether to implement them or not.



### 16.2.1 Avoid using AWS Credentials

By using the N2WS Server instance IAM role and cross-account IAM role, you can manage multiple AWS accounts without using AWS credentials (access and secret keys) at all. This is the most secure way to manage multiple AWS accounts and the one recommended by AWS.

### 16.2.2 Credential Rotation

Assuming you have to use AWS credentials, you should follow AWS practices. It is recommended that you rotate account credentials from time to time. See <http://docs.amazonwebservices.com/AWSSecurityCredentials/1.0/AboutAWSCredentials.html#CredentialRotation>

After changing credentials in AWS, you need to update them in N2WS. Select on the account name in the **Accounts** management screen and modify the access and secret keys.

### 16.2.3 Passwords

Create a strong password for the N2WS server and make sure no one can access it. Change passwords from time to time. N2WS does not enforce any password rules. It is the user's responsibility to create strong passwords.

### 16.2.4 Security Groups

Since the N2WS server is an instance in your account, you can define and configure its security groups. Even though N2WS is a secure product, you can block access from unauthorized addresses:

- You need HTTPS access (original 443 port or your customized port) from:
  - Any machine which will need to open the management application
  - Machines that have N2WS Thin Backup Agent installed on them. See section 6.1.
- You will also need to allow SSH access to create and maintain backup scripts.
- Blocking anyone else will make N2WS server invisible to the world and therefore completely bullet-proof.

**Note:** The only problem with this approach is that any time you will try to add new backup agents or connect to the management console or SSH from a different IP, you will need to change the settings of the security groups.

## 16.3 Using IAM

N2WS keeps your AWS credentials safe. However, it is preferable to use IAM roles and not use credentials at all. Additionally, N2WS will not accept root user credentials. To minimize risk, try:

- To provide credentials that are potentially less dangerous if they are compromised, or
- To set IAM roles, which will save you the need of typing in credentials at all.

You can create IAM users/roles and use them in N2WS to:

1. Create a user/role using IAM.
2. Attach a user policy to it.
3. Use the policy generator to give the user custom permissions.



**Warning:** Using IAM User credentials is not recommended as they are less secure than using IAM roles.

An IAM role can also be used in the N2WS Server (for the account the N2WS Server was launched in) and for instances running N2WS Agent to perform the configuration stage as well as normal operations by combining some of the policies. You can attach more than one IAM policy to any IAM user or role.

The permissions that the IAM policy must have depend on what you want to policy to do. For more information about IAM, see IAM documentation:

<http://aws.amazon.com/documentation/iam/>

### 16.3.1 N2WS Server Configuration Process

AWS credentials in the N2WS configuration process are only used for configuring the new server. However, if you want to use IAM credentials for the N2WS configuration process, or to use the IAM role associated with the N2WS Server instance, its IAM policy should enable N2WS to:

- View volumes instances, tags, and security groups
- Create EBS volumes
- Attach EBS volumes to instances
- Create tags

Generally, if you want to use IAM role with the N2WS Server instance, you will need the following policy and the policies for N2WS Server's normal operations, as described in the next section.

#### Minimal IAM Policy for N2WS Configuration:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:AttachVolume",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeTags",
        "ec2:DescribeVolumeAttribute",
        "ec2:DescribeVolumeStatus",
        "ec2:DescribeVolumes"
      ],
      "Sid": "Stmt1374233119000",
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}
```






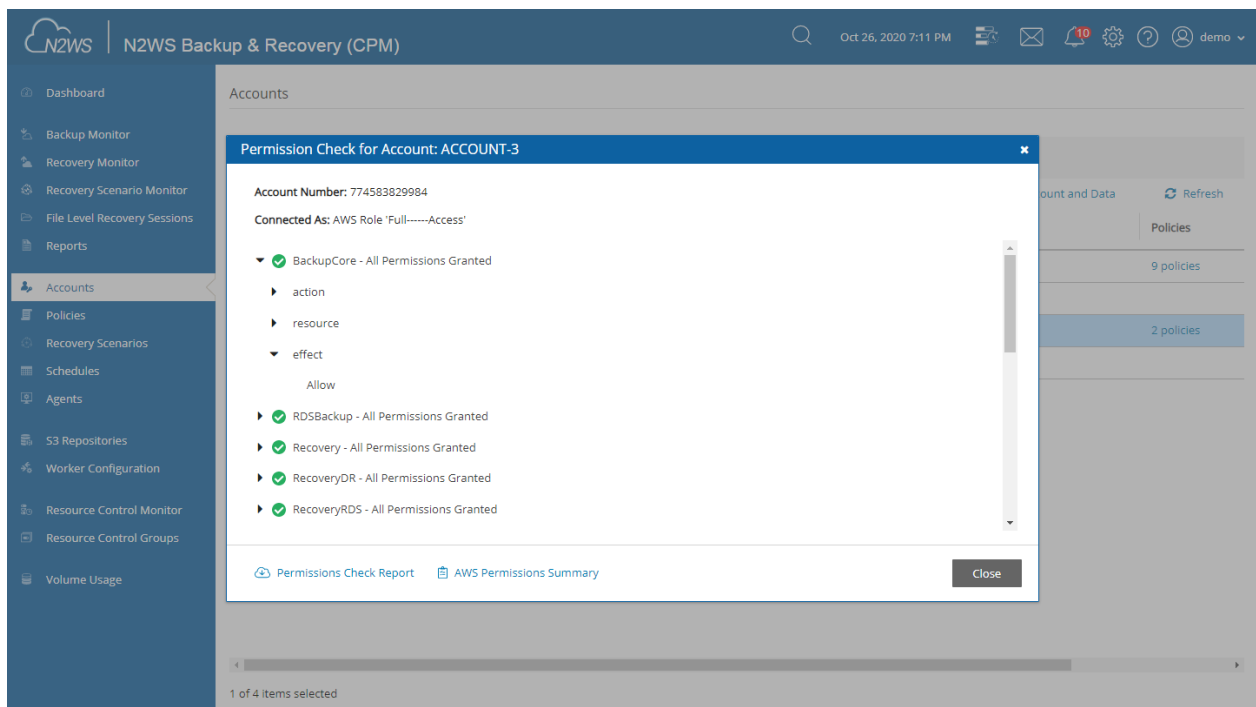
### 16.3.2 N2WS Server IAM Settings

You can use the N2WS Server's IAM role to manage backups of the same AWS account. If you manage multiple AWS accounts, you will still either need to create cross-account roles or enter the credentials for other accounts. If you want to use an IAM user for an account managed by N2WS Server (or the IAM role), you need to decide whether you want to support backup only or recovery as well. There is a substantial difference:

- For backup, you only need to manipulate snapshots.
- For recovery, you will need to create volumes, create instances, and create RDS databases. Plus, you will need to attach and detach volumes and even delete volumes. If your credentials fall into the wrong hands, recovery credentials can be more harmful.
- If you use a backup-only IAM user or role, then you will need to enter ad hoc credentials when you perform a recovery operation.
- Generally, if you want to use the IAM role with the N2WS Server instance, you will need a certain policy, or policies, for N2WS Server's normal operations. For details, see the N2W Software Knowledge Base article on minimal IAM policies at <https://support.n2ws.com/portal/kb/articles/what-are-the-required-minimal-aws-permissions-roles-for-cpm-operation>



**Warning:** Using IAM User credentials is not recommended as they are less secure than using IAM roles.

You can check on the permissions required for AWS services and resources, such as backup, RDS, and DynamoDB, and compare them to the policies which cover the requirements. In the **Accounts** tab, select an account and then select  **Check AWS Permissions**. To expand a line, select its down arrow ▼.



The screenshot displays the N2WS Backup & Recovery (CPM) web interface. The left sidebar contains a navigation menu with options like Dashboard, Backup Monitor, Recovery Monitor, and Accounts. The main content area shows the 'Accounts' tab with a list of accounts. A modal dialog titled 'Permission Check for Account: ACCOUNT-3' is open, showing the account number 774583829984 and the connected role 'Full-----Access'. The dialog lists several permissions that are granted, including BackupCore, RDSBackup, Recovery, RecoveryDR, and RecoveryRDS. At the bottom of the dialog, there are links for 'Permissions Check Report' and 'AWS Permissions Summary', and a 'Close' button.



- To download a CVS report, select  **Permissions Check Report**.
- To download a JSON file, select  **AWS Permissions Summary**.

### 16.3.3 Configure N2WS's IAM Role with CloudFormation

CloudFormation is an AWS service that allows you to treat a collection of AWS resources as one logical unit. CloudFormation provides a common language for you to describe and provision all the infrastructure resources in your cloud environment, across all regions and accounts in an automated and secure manner.

The IAM role will automatically contain the required permissions for N2WS operations. See section 20.




## 17 Alerts, Announcements, Notifications and Reporting


N2WS manages the backup operations of your EC2 servers and Azure VMs. To notify you when something is wrong and to integrate with your other cloud operations, N2WS allows sending alerts, notifications and even raw reporting data. And when something is not wrong, N2WS can send you an announcement of interest, such as a new feature or money-saving promotion. So, if you have a network operations center (NOC), are using external monitoring tools or just want an email to be sent to the system administrator whenever a failure occurs, N2WS has an answer for that.

Report types include:

- Audit
- AWS Backups
- AWS Protected Resources
- AWS Resource Control Operations
- AWS Snapshots
- AWS Resources Summary (PDF) of regular, DR, and S3 Backups, Volume Usage Percentage, and other metrics
- AWS Usage
- AWS Unprotected Resources (Scheduled Report only)
- Azure Backups
- Azure Protected Resources
- Azure Snapshots
- Azure Resources Summary (PDF) of backups, DR, S3 Backups, Volume Usage percentage, and other metrics.

### 17.1 Alerts

Alerts are notifications about issues in your N2WS backup solution. Whenever a policy fails, in backup or DR, an alert is issued so you will know this policy is not functioning properly. If there are current alerts, **Alerts**  in the toolbar has a number to show you how many there are.

Select **Alerts**  to open the Alerts list.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with items like Dashboard, Backup Monitor, Recovery Monitor, etc. The main area displays the Backup Monitor. An 'Alerts' dialog box is open, showing a list of alerts. The dialog has a 'Delete' button and a 'Delete All' button. The list of alerts includes columns for a checkbox, timestamp, instance name, status, category, and details. The alerts are as follows:

Checkbox	Timestamp	Instance	Status	Category	Details
<input type="checkbox"/>	Oct 27, 2020 11:41 AM	demo	Error	Tag Scan	Backup Tag scan - Policy 'vol' doe 05f8b1aa3ea873271]
<input type="checkbox"/>	Oct 27, 2020 12:41 AM	demo	Warning	volume usage limit exceeded	aws_instance_id : None, aws_volu threshold:
<input type="checkbox"/>	Oct 26, 2020 11:48 PM	demo	Warning	Data Lifecycle Management - S3 Copy	Copy to S3 completed: 1 snapsho
<input type="checkbox"/>	Oct 26, 2020 9:21 PM	demo	Warning	Reports	Scheduled_report: BCKUP, No ver
<input type="checkbox"/>	Oct 24, 2020 12:45 PM	demo	Info	Data Lifecycle Management - S3 Repository	S3 snapshots deleted successfully

At the bottom of the dialog, it says '0 of 8 items selected' and there is a 'Close' button.

Later, when the policy succeeds, the alert is turned off or deleted, so you will know that the issue is resolved. Alerts can be issued for failures in backup and DR, as well as general system issues like license expiration, for relevant installations.

Depending on the resolution of the output device, a list of Alerts is automatically shown under the Dashboard. The Dashboard list shows the same information except for an abbreviated message and is grouped by functional categories, such as Backup and Resource Control.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu. The main area displays the Dashboard. The dashboard has several sections:

- Backups (Last 24 Hours)**: A circular gauge showing 3 successful backups.
- DR (Last 24 Hours)**: A circular gauge showing 1 successful DR event.
- S3 Backups (Last 24 Hours)**: A circular gauge showing 1 successful S3 backup.
- Volume Usage Percent**: A circular gauge showing 4 volumes above 50% usage.
- Alerts**: A section showing a message: 'There are some volumes above/below threshold (2)'.

On the right side of the dashboard, there is a sidebar with various metrics and links:

- Accounts: 3
- Policies: 4
- Protected Resources: 4
- Managed Snapshots: 6
- Cost Savings: \$ 4.18
- Cost Explorer: \$ 0.00

You can manage the number of Alerts shown by selecting alerts to remove in the toolbar Alerts list and then selecting **Delete**.

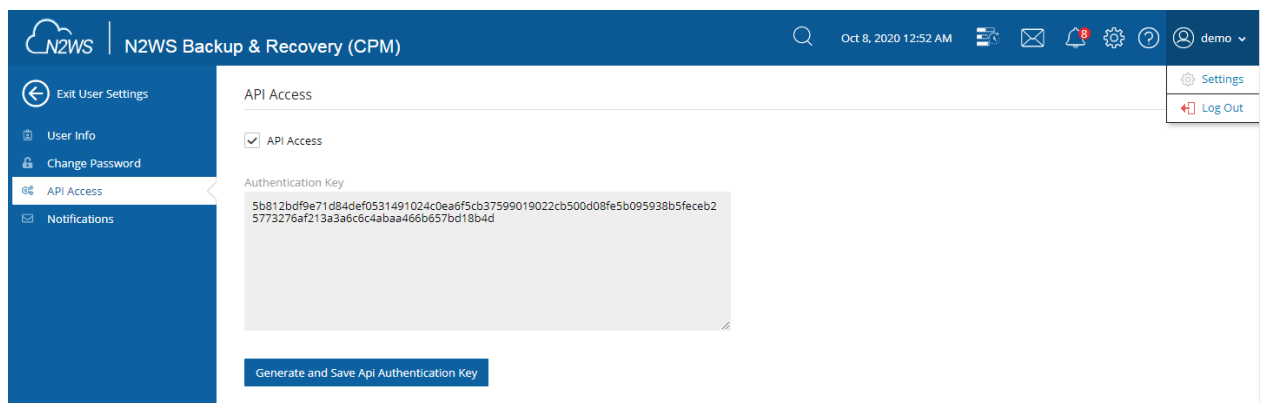


## 17.2 Pull Alerts

If you wish to integrate N2WS with 3<sup>rd</sup> party monitoring solutions, N2WS allows API access to pull alerts out of N2WS. A monitoring solution can call this API to check if N2WS has alerts. When calling this API, the caller receives the current alerts in JSON format. The call is an HTTPS call, and if you configured the N2WS server to use an alternate port (not 443), you will need to use that port for this API call as well. N2WS requires an authentication key from the caller. Every N2WS user can define such a key to get the relevant alerts. The root user can also get relevant alerts from other managed users, but not from independent users.

### To configure an API call:

1. In the toolbar, select **Settings** in the **User** menu.
2. In the **User Settings** panel, select the **API Access** tab.



3. To enable access and generate an Authentication Key:
  - a. Select API Access.
  - b. To generate a new Authentication Key and invalidate the current, select Generate API Authentication Key.
  - c. Select Save.
4. After enabling and setting the key, you can use the API call to get all alerts:  
`https://{host}}/api/alerts`

### A simple example of Python is:

```
d:\tmp>python
Python 2.7.2 (default, Jun 12 2011, 15:08:59) [MSC v.1500 32 bit (Intel)]
on win32
Type "help", "copyright", "credits" or "license" for more information.
>>> import urllib2, json
>>> server_address = 'ec2-54-228-126-14.compute-1.amazonaws.com'
>>> server_port = 443
>>> authkey =
'afb488681baf0132fe190315e87731f883a7dac548c08cf58ba0baddc7006132a
a74f99ab07eff736477dca86b460a4b1a7bfe826e16fdbbc'
>>> url = 'https://%s:%d/agentapi/get_cpm_alerts/' % (server_address,
server_port)
>>> url
```



```
'https://ec2-54-228-126-14.compute-
1.amazonaws.com:443/agentapi/get_cpm_alerts/'

>>> request = urllib2.Request (url)
>>> request.add_header("Authorization", authkey)
>>> handle = urllib2.urlopen (request)
>>> answer = json.load (handle)
>>> handle.close ()
>>> answer

[{'category': u'Backup', u'message_body': u'Policy win_server (user:
root, account: main) - backup that started at 07/20/2013 09:00:00 AM
failed. Last successful backup was at 07/20/2013 08:00:00 AM',
u'severity': u'E', u'title': u'Policy win_server Backup Failure',
u'alert_time': u'2013-07-20 06:00:03', u'policy': {u'name':
u'win_server'}}], {'category': u'Backup', u'message_body': u'Policy
web_servers (user: root, account: main) - backup that started at
07/20/2013 09:20:03 AM failed. Last successful backup was at 07/20/2013
08:30:00 AM', u'severity': u'E', u'title': u'Policy web_servers Backup
Failure', u'alert_time': u'2013-07-20 06:22:12', u'policy': {u'name':
u'web_servers'}}}]

>>>
```

The JSON response is a list of alert objects, each containing the following fields:

- category
- title
- message\_body
- alert\_time (time of the last failure)
- policy
- severity

## 17.3 Using SNS

N2WS can also push alerts to notify you of any malfunction or issue via SNS. To use it, your account needs to have SNS enabled. SNS can send push requests via email, HTTP/S, SQS, and depending on location, SMS.

With SNS you create a topic, and for each topic, there can be multiple subscribers and multiple protocols. Every time a notification is published to a topic, all subscribers get notified. For more information about SNS, see <https://aws.amazon.com/sns/>.

N2WS can create the SNS topic for you and subscribe to the user email defined in the configuration phase. To add subscribers, go to the SNS Dashboard in the AWS Management console), add a recipient, and choose a protocol (SMS, HTTP, etc.), A link to this console is in the N2WS notifications screen.

For the small volume of SNS messages N2WS uses, there is usually no cost or it is negligible. For SNS pricing see <https://aws.amazon.com/sns/pricing/>.



### 17.3.1 Configuring SNS

To configure users for SNS:

1. In the toolbar, select **Settings** in the **User** menu
2. Select the **Notifications** tab in the **User Settings** panel.
3. For each of the boxes, select a value from its list.
4. Depending on the type of credentials selected in the **Authenticate using** box, you may be prompted with additional boxes:
  - **CPM Instance IAM Role** – Requires no additional selections.
  - **Account** – Select the Account name or add a new Account by selecting **+ New**.
  - **IAM User Credentials** – Enter the **AWS Access** and **Secret** keys.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date and time 'Oct 26, 2020 7:20 PM', and several utility icons. A left sidebar contains a list of settings: 'Exit User Settings', 'User Info', 'Change Password', 'API Access', and 'Notifications' (which is highlighted). The main content area is titled 'Notifications' and contains the following fields:

- SNS Region**: A dropdown menu currently showing 'US East (Ohio)'. A red informational message states: 'Alerts and daily summary topic ARN's are unique per region and need to be updated.'
- Authenticate using**: A dropdown menu currently showing 'CPM Instance IAM Role'.
- Enable Push Alerts**: A checkbox that is checked.
- Alerts Topic**: A dropdown menu currently showing 'Auto Generate New Topic'.
- Add User Email as Recipient**: A checkbox that is checked.
- Enable Daily Summary**: An unchecked checkbox.

A 'Save' button is located at the bottom right of the form.

To use SNS:

- You will need to enter AWS account credentials for the SNS service.
- There is one notifications configuration per user, but there can be multiple AWS accounts (where applicable).
- SNS credentials are not tied to any of the backed-up AWS accounts. You can choose a region, and enter credentials, which can be regular credentials, IAM user. See section 16.3. To use the N2WS Server instance's IAM role (only for the root user), type `use_iam_role` for both access and secret keys.
- If you are the root (main) user, you can choose whether to include or exclude alerts about managed users. See section 18.2.
- Root/admin users, and independent users who oversee managed users, can also configure a managed user to receive alerts directly by selecting the user in the **User** list and setting the notification properties described in sections 17.4 and 17.5.
- SNS is used both for push alerts and for sending a daily summary.



## 17.4 Push Alerts

Push alerts use SNS to send notifications about malfunctions and issues in N2WS's operation.

**To enable push alerts:**

1. In the **Notifications** tab of the **User Settings** panel, select **Enable Push Alerts**.
2. Define the **Alerts Topic** by selecting one of the following options in the list:
  - To create a new topic, select **Auto Generate New Topic**.
  - To use a current topic, select **Use Existing Topic**. Enter the name in the **Alerts Topic Name** box. Or, you can copy the topic's ARN from the **SNS** tab of the AWS Management Console (**Open SNS Management Console**).
3. To have the user also receive the alert as an email, select **Add User Email as Recipient**. The recipient will receive a message requesting subscription confirmation before receiving alerts.

## 17.5 Daily Summary

The Daily Alert Summary is a message that is sent once a day, summarizing all current alerts, and some policy warnings, in the system. It can be configured instead of, or in addition to, regular alerts. It can be useful for several reasons:

- If you are experiencing issues frequently it sometimes reduces noise to get a daily summary. Furthermore, since backup is the second line of defense, some people feel they do not need to get an instant message on every backup issue that occurs.
- Even if there are no issues, a daily summary is a reminder that everything is ok. If something happens and N2WS crashed altogether, and your monitoring solution did not report it, you will notice the Daily Summary will stop.
- The Daily Summary contains a list of policies that are disabled and policies that do not have schedules assigned to them. Although neither is an error, sometimes someone can accidentally leave a policy disabled or without a schedule and not realize that it is not working.





### To configure the Daily Summary:

1. In the **Notifications** tab of the **User Settings**, select **Enable Daily Summary**.
2. Define the **Daily Summary Topic** by selecting one of the following options in the list:
  - If you want to use the Alert topic for summaries, select **Use Existing Topic**. Enter a **Summary Topic Name**.
  - To create a new topic, select **Auto Generate New Topic**.

**Note:** There is an advantage of using a separate topic since sometimes you want different recipients: It makes sense for a system admin to get alerts by SNS and to get the daily summary by email only. The display name of the topic appears in the message and in emails, it appears as the sender name. With separate topics, it is easier to distinguish alerts.

3. To have the user also receive the summary as email, select **Add User Email as Recipient**.
4. In the **Send Daily Summary At** ⌚ list, select the hour and minutes to send the notification.
5. Select **Save**.
6. To test the notification, select **Test Daily Summary**.

## 17.6 Resources Summary PDF Report

The new downloadable Resources Summary PDF report for AWS and Azure accounts resembles the Dashboard in layout, with the exception of the Alerts section, and provides historical data for the filtered time period. The PDF includes Dashboard graphics and statistics:

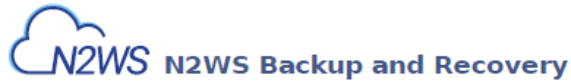
- Backups, with breakdowns for Successful, Partial, and Failed, for Backups, DR Backups, and S3 Backups
- Volume Usage Percentage, with breakdowns below, within, and above usage thresholds



- Statistics for Accounts, Policies, Protected Resources, Managed Snapshots, Cost Savings, and Cost Explorer

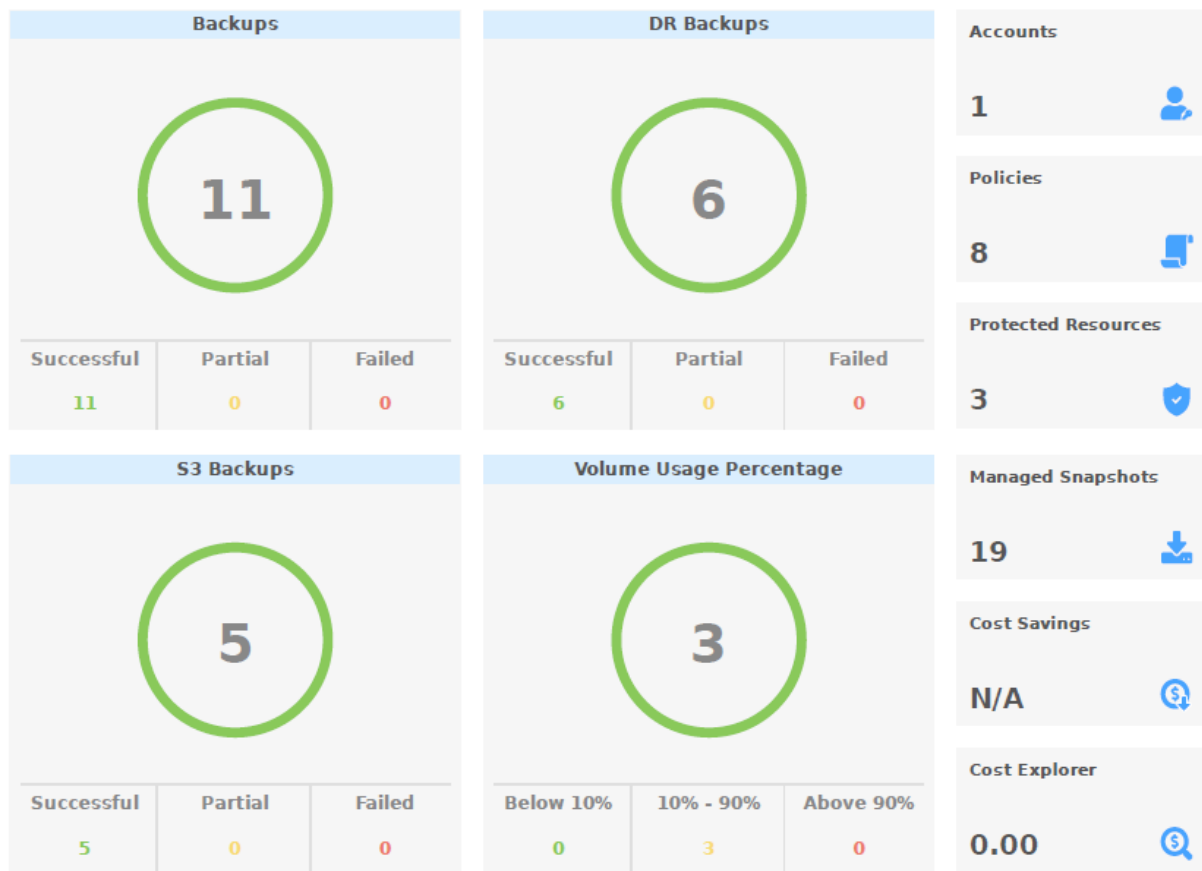
Filters are available for the Resources Summary report as follows:

- AWS – User, and time period.
- Azure – User, account, and time period.



Summary report for **all users**

Report created for **last month** period, starting **Fri, 01 Jan 06:04 2021** ending **Mon, 01 Feb 06:04 2021**



You can create the Resources Summary PDF report as follows:

- As a Scheduled Report - see section 17.10.1.
- As an Immediate Report Generation - see section 17.10.3.
- When using the REST API, see REST API/SCHEMA DOCS. Report time filters are:
  - `period_type`: 'M' | 'W' for prior Months or Weeks
  - `period_length`: number of `period_type` units

## 17.7 Raw Reporting Data

You can download two raw data reports in CSV format (Comma Separated Values) for AWS and Azure. These reports are for the logged-in user. For the root user, they will include also data of



other managed users. These reports include all the records in the database; you can filter or create graphic reports from them by loading them to a spreadsheet or reporting tool. The two reports combined give a complete picture of backups and snapshots taken by N2WS.

### To download the CSV reports:

1. In the left panel, select **Reports** and then select the **Immediate Report Generation** tab.
2. For the backup view, in the **Report Type** list, select **AWS Backups** or **Azure Backups**.

3. For the snapshot view, in the **Report Type** list, select **AWS Snapshots** or **Azure Snapshots**.
4. For details on Scheduled Reports, see section 17.10.1.
5. Select **Run Now**.

## 17.7.1 Backup View CSV Report

This report will have a record for each backup (similar to the Backup Monitor) with details for each of the backups, including backups imported to S3:

AWS	Azure	Field / Description
X	X	<b>Backup ID</b> – A unique numerical ID representing the backup
X	X	<b>Account</b> – Name of the account if the system has multiple users and the user downloading the report is root.
X		<b>AWS Account Number</b> –ID of the AWS account.
	X	<b>Azure subscription id</b> – ID of the Azure subscription.
X	X	<b>Policy</b> – Name of the policy.
X	X	<b>Status</b> – Status of the backup, the same as in the Backup Monitor.
X		<b>DR Status</b> – Status of DR, same as in the Backup Monitor.
X		<b>S3 Copy Status</b> – Status of a Copy to S3. If <b>Import</b> equals Yes, then backup was imported to S3.
X		<b>Archive Status</b> – Status of a Copy to Glacier Archive.
X	X	<b>Start Time</b> – Time the backup started.
X	X	<b>End Time</b> – Time the backup ended.
X	X	<b>Is Retry</b> – Yes if this backup was a retry after failure, otherwise no.



AWS	Azure	Field / Description
X	X	<b>Marked for Deletion</b> – Yes if this backup was marked for deletion. If yes, the backup no longer appears in the <b>Backup Monitor</b> and is not recoverable.
X	X	<b>Deleted</b> – Yes if the backup was deleted.
X		<b>Import</b> – Yes if the backup was imported to S3.

### 17.7.2 Snapshot View CSV Report

This report will have a record for each AWS EBS or RDS or **Azure VM and Disk** snapshot in the database.

AWS	Azure	Field / Description
X	X	<b>Backup ID</b> – ID of the backup the snapshot belongs to. Matches the same snapshots in the previous report
X	X	<b>Account</b> – Name of the account.
X		<b>Snapshot Account</b> – Name of snapshot account.
X		<b>Snapshot AWS Account</b> – Number of AWS snapshot account.
	X	<b>Azure Subscription ID</b> – ID of the Azure Subscription.
X	X	<b>Policy</b> – Name of the policy.
X	X	<b>Status</b> – Status, such as ‘Backup Successful’ or ‘All Snapshots Deleted’.
X		<b>Region</b> – AWS region.
	X	<b>Location</b> – Azure location.
X	X	<b>Type</b> – Type of snapshot. <ul style="list-style-type: none"> <li>For AWS: EBS, RDS, or EBS Copy, which is a DR copied snapshot.</li> <li>For Azure: VM or Disk.</li> </ul>
X		<b>Volume/DB/Cluster</b> – AWS ID of the backed-up EBS volume, RDS database, or cluster.
X		<b>Volume/DB/Cluster Name</b> – Name of backed-up volume, database, or cluster.
X		<b>Instance</b> – If this snapshot belongs to a backed-up EC2 instance, the value will be the AWS ID of that instance, otherwise it will contain the string: None
X		<b>Instance Name</b> – Name of the instance.
	X	<b>Backed Up Resource Id</b> – ID of backed up resource.
	X	<b>Backed Up Resource Name</b> – Name of backed-up resource.
	X	<b>Related VM ID</b> – ID of related VM.
	X	<b>Related VM Name</b> – Name of related VM.
X	X	<b>Snapshot ID</b> – ID of the snapshot.
X	X	<b>Succeeded</b> – Yes or No.
X	X	<b>Start Time</b> – Time the snapshot started.
X	X	<b>End Time</b> – Time the snapshot ended.
X	X	<b>Deleted At</b> – Time of deletion, or N/A, if the snapshot was not deleted yet.
X		<b>Import</b> – Yes if the snapshot was imported to S3.
Additional columns contain data for tracking changes in storage size for EBS and S3 copies:		
X		<b>Volume Size (GB)</b> – Logical size of volume, as specified during creation or resizing.
X		<b>Valid Data Size (GB)</b> – Part of the volume that is allocated and used at the time of the snapshot. From this number, you can deduce <b>volume utilization</b> .




AWS	Azure	Field / Description
X		<b>Changed Data Size (GB)</b> – If the snapshot is incremental, and CPM can locate the previous snapshot, then this is the amount of data in the current snapshot that is different from the previous snapshot, i.e. the size of the incremental snapshot. If 'Unknown', the above conditions are not met. From this number, you can deduce the <b>data change rate</b> .
	X	<b>Disk Size (GB)</b> – Size of disk.

### 17.7.3 Keeping Records After Deletion

By default, when a backup is marked for deletion, it will be deleted right away from the N2WS database, and therefore not appear in the reports. There are exceptions, such as if N2WS could not delete all the snapshots in a backup (e.g. a snapshot is included in an AMI and cannot be deleted). Sometimes you need to save records for a period of time after they were marked for deletion for compliance, such as General Certificate of Conformity (GCC). To keep records after deletion, see section 9.4.


## 17.8 AWS Usage Reports

In addition to the raw reports, you can also download AWS CSV usage reports. A usage report for a user will give the number of AWS accounts, instance and non-instance storage this user is using. This can be helpful for inter-user accounting.

1. In the left panel, select the **Reports** tab.
2. For the usage report (current user), select **AWS Usage** in the **Report Type** list and your user name in the **User** list.
3. To get the usage report (all users) for the root user, select **AWS Usage** in the **Report Type** list and **All** in the **User** list.
4. Select  **Run Now**.

## 17.9 Protected Resources and AWS Unprotected Resources Reports

The AWS and Azure protected resources reports provide information about AWS and Azure resources *with* backup protection. The unprotected resources report is available for AWS accounts only.

1. In the left panel, select the **Reports** tab.
2. For AWS accounts, select **AWS Unprotected** or **Protected Resources** in the **Report Type** list, and
3. For Azure accounts, select **Azure Protected Resources** in the **Report Type** list, and
4. For the current user, select your user name in the **User** list.
5. For the root user, to get all users, select **All** in the **User** list.
6. Select  **Run Now**.
7. When you are notified that the report has completed, check your Downloads folder.



AWS resources that are tagged with key:**cpm backup**, value:**no-backup** will be ignored. Also, see section 14.1.5.

### 17.9.1 Protected Resources

The protected resources report contains information about the AWS and Azure resources with backup policies.

- **Account / Azure Account**
- **User Name** (on all user reports)
- **Resource ID**
- **Resource Name**
- **Region (AWS) / Location (Azure)**
- **Policies / Azure Policies**
- **Schedules**
- **Resource Type (Azure)**

The protected resources report is available immediately for the current user or all users depending on the account type.

The protected resources report is also available as a Scheduled Report. See section 17.10.

### 17.9.2 AWS Unprotected Resources

The AWS unprotected resources report is available as a scheduled report *only* and contains information about AWS resources that do not have backup policies.

- Resource Type
- Name of resource
- Resource ID
- Region
- Partial
- Account
- User
- Count of number of unprotected resources per resource type.

## 17.10 Reports Page

As part of the N2W Software plan of moving toward a robust reporting module, versions 3.x.x have all Reports accessible from the **Reports** tab in the left panel.

The reports will be available in your Downloads folder. Reports are for the logged-in user. For the root user, the reports will also include the data of other managed users.

### 17.10.1 Scheduled Reports

Scheduled Reports allow you to create a schedule for each report. To receive a Scheduled Report, configure at least one recipient email address and the SES service for that email. See section **Error! Reference source not found..**

You can run reports outside of a schedule and create ad hoc reports for download:



- In the **Scheduled Reports** tab, **Run Now** generates a defined Scheduled Report and sends emails to its recipients.
- In the **Immediate Report Generation** tab, you can define a new report for immediate execution and download.

Also, see section 17.10.3.

By default, the **Reports** page opens with a list of all reports which have been scheduled. To narrow the list, use the search box, or the filters for report type, user, and schedule.

Name	Report Type	Schedules	Enabled
BCKUP	Backup	Daily_Sched	Yes


Filters are available based on the chosen Report Type. Depending on the report, you can filter the results as follows:

- **Audit** – Filter for User and records for prior days, weeks, or months.
- **AWS / Azure Backups**– Filter for User, Account, and records for prior days, weeks, or months.
- **AWS / Azure Protected Resources** – Filter for User and Account.
- **AWS Resource Control Operations**– Filter for Account and records for prior days, weeks, or months.
- **AWS / Azure Snapshots** - Filter for Account and records for prior days, weeks, or months.
- **AWS Resources Summary (PDF)** – Filter for User and historical data for prior weeks or months. Information contained is the same as in the Dashboard except that it is historical. Alerts are not included.
- **Azure Resources Summary (PDF)** – Filter for User, Account, and historical data for prior weeks or months. Information contained is the same as in the Dashboard except that it is historical. Alerts are not included.



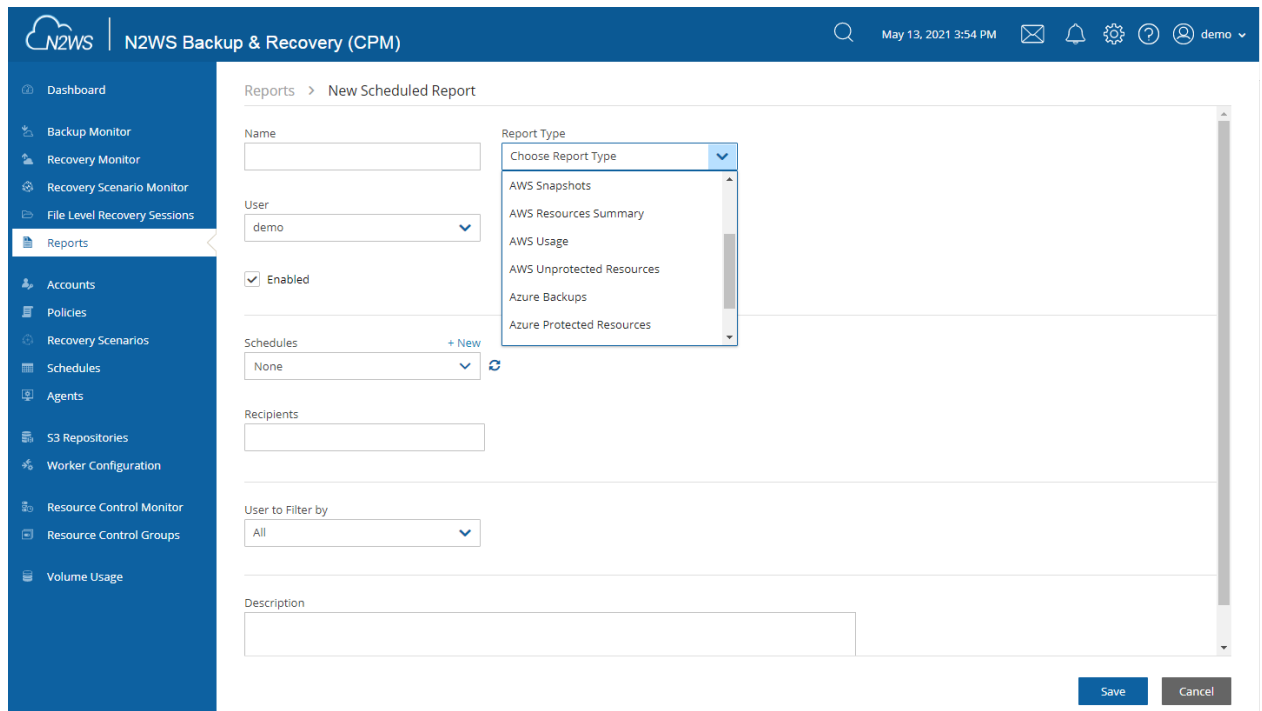
- **AWS Usage** – Filter by User and records for prior days, weeks, or months. Select **Detailed** or **Anonymized**.
- **AWS Unprotected Resources** – Filter by User and Account.

## 17.10.2 Defining a Scheduled Report

Reports are run according to their defined schedule and immediately using  **Run Now**. Schedules reports must include at least one email recipient.

**To create a scheduled report:**

1. Select the **Scheduled Reports** tab and then  **New**.



2. Enter a name for the new report and choose the **Report Type**.
3. By default, the report is enabled. To disable the Schedule Report, clear **Enabled**.
4. In the **Schedules** list, select one or more schedules. To create or edit a schedule, see section 4.1.1.

**Note:** You can create a Scheduled Report without a schedule and edit the report later after creating the schedule.

5. In the **Recipients** box, enter the email address of recipients, separated by a semi-colon (;).
6. Select from the filters presented for the **Report Type**.
  - a. If **Include Records From Last** boxes appear, you can select the number (first list) of Days, Weeks, or Months (last list) to include in the report. The default is all available records.
7. In the **Description** box, enter an optional informative description.
8. Select **Save**.

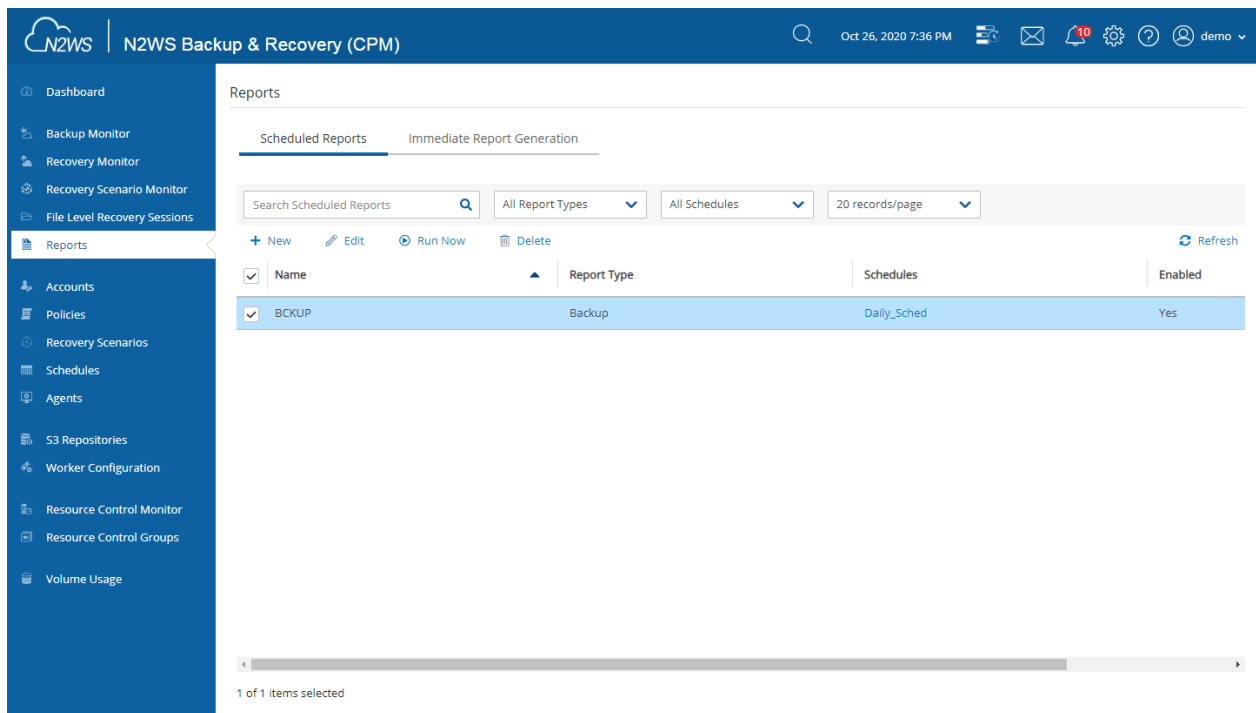




### 17.10.3 Running Reports Outside Their Schedule

To run a **Scheduled Report** and send emails to its recipients immediately:

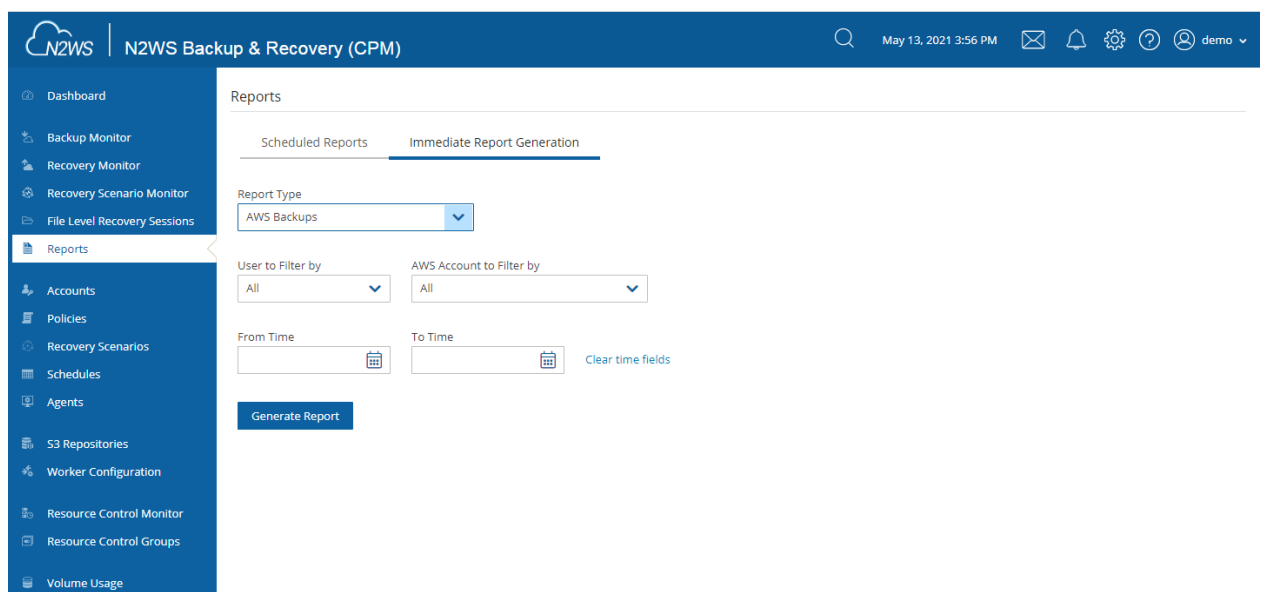
In the **Scheduled Reports** tab, select the report in the list and then select  **Run Now**.




The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports (selected), Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Reports' and has two tabs: 'Scheduled Reports' (active) and 'Immediate Report Generation'. Below the tabs, there is a search bar for 'Search Scheduled Reports', a dropdown for 'All Report Types', a dropdown for 'All Schedules', and a dropdown for '20 records/page'. Below these are buttons for '+ New', 'Edit', 'Run Now' (highlighted), and 'Delete'. A table lists the reports with columns: Name, Report Type, Schedules, and Enabled. The table contains one entry: 'BCKUP' with Report Type 'Backup', Schedules 'Daily\_Sched', and Enabled 'Yes'. A 'Refresh' button is in the top right of the table. At the bottom, it says '1 of 1 items selected'.

To define a new report and download it immediately:

1. Select the **Immediate Report Generation** tab.
2. Select a **Report Type** and one or more filters depending on the **Type** selected, as listed above in section 17.10.1.



The screenshot shows the N2WS Backup & Recovery (CPM) interface with the 'Immediate Report Generation' tab selected. The left sidebar is the same as in the previous screenshot. The main content area is titled 'Reports' and has two tabs: 'Scheduled Reports' and 'Immediate Report Generation' (active). Below the tabs, there is a 'Report Type' dropdown menu with 'AWS Backups' selected. Below this are two dropdown menus: 'User to Filter by' (set to 'All') and 'AWS Account to Filter by' (set to 'All'). Below these are two date/time pickers: 'From Time' and 'To Time', both with calendar icons. A 'Clear time fields' link is next to the 'To Time' picker. A 'Generate Report' button is at the bottom.

3. To filter the report data by date and time, select **Calendar**  and choose the **From** and **To** date and time values. Select **Apply** after each definition.



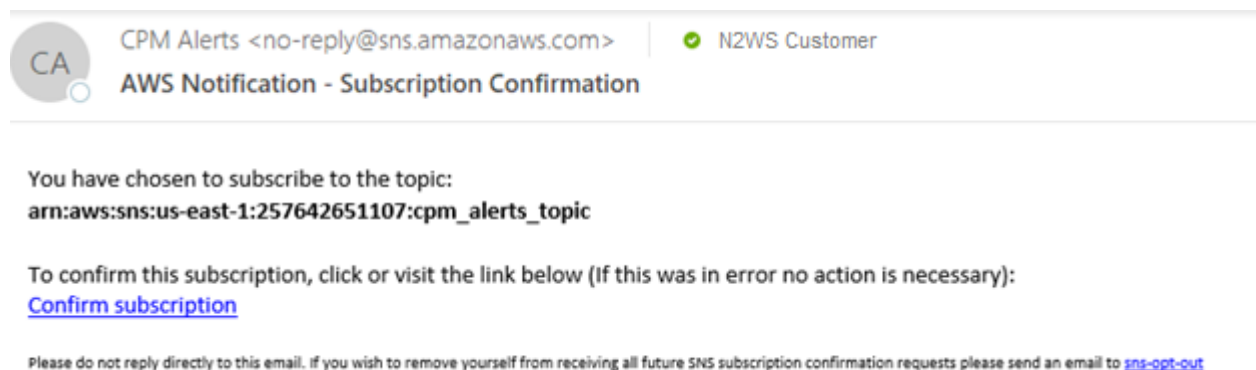
4. Select **Generate Report**. The output will be downloaded by your browser.

## 17.11 Examples of AWS Alerts

AWS uses SNS to provide a number of N2WS alert services by subscription.

### 17.11.1 Subscription Confirmation Alert

After subscribing to CPM Alerts in AWS, you will receive an email with a confirmation link:



Select the **Confirm subscription** link. You will receive a subscription confirmation email:



Simple Notification Service

### Subscription confirmed!



You have subscribed n2ws\_cust@compa.com to the topic:  
**cpm\_alerts\_topic**.

Your subscription's id is:  
arn:aws:sns:us-east-1:257642651107:cpm\_alerts\_topic:e58b8543-39ef-4d05-8ab8-c98936e7d4f1

If it was not your intention to subscribe, [click here to unsubscribe](#).

## 17.11.2 Daily Summary Alert

Following is an example of a CPM Daily Summary where all AWS functions were OK:

 CPM Alerts <no-reply@sns.amazonaws.com> |  N2WS Customer  
CPM Daily Summary - All OK

CPM Daily Summary - All OK for user demo (and managed users)

Reporting CPM Server: N2W Internal (i-0df161304d594b53f) - CPM Server (fa516eb8-8d27-4c6e-8204-ea2b9bf799c5):

Policies with no schedules:  
policy1 (user: demo)  
cpmdata (user: demo)



--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
[https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:726541571499:cpm\\_alerts\\_topic:865ee71d-88b9-4056-974f-c](https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:726541571499:cpm_alerts_topic:865ee71d-88b9-4056-974f-c)

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>

## 17.11.3 Unprotected Resources Alert

Following is an example of an alert that the unprotected resources report is available:

 CPM Alerts <no-reply@sns.amazonaws.com> |  N2WS Customer  
Unprotected Resources

CPM Server - CPM Server (da91c303-84e8-4e20-a69e-5daa699dc7e0):  
The unprotected resources report creation is complete.

--

If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:  
[https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:257642651107:cpm\\_alerts\\_topic:e58b8543-39ef-4d05-8ab8-c98936e7d4f1](https://sns.us-east-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-east-1:257642651107:cpm_alerts_topic:e58b8543-39ef-4d05-8ab8-c98936e7d4f1)

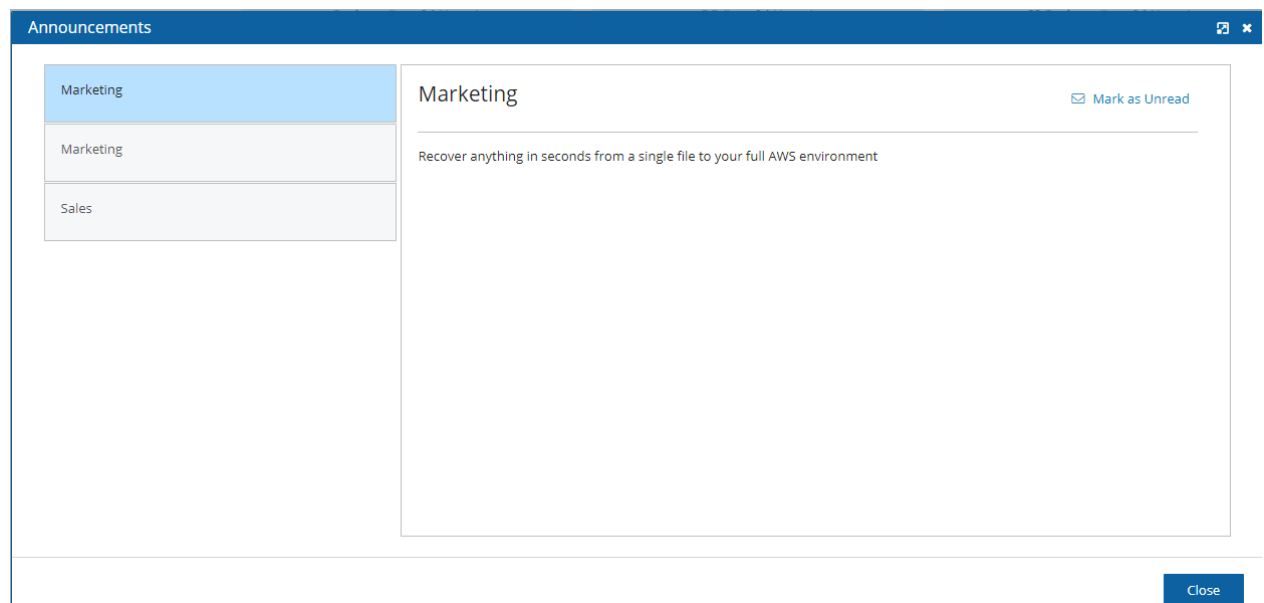
Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at <https://aws.amazon.com/support>




## 17.12 Announcements

In version 3.0.0, Announcements were introduced as a method for N2WS to communicate directly to users about non-operational topics, such as promotions and other sales-related information.


In the toolbar, the **Announcements** icon  shows the number of unread announcements waiting in the user's mailbox. In the **Announcements** inbox panel, select an announcement to open.

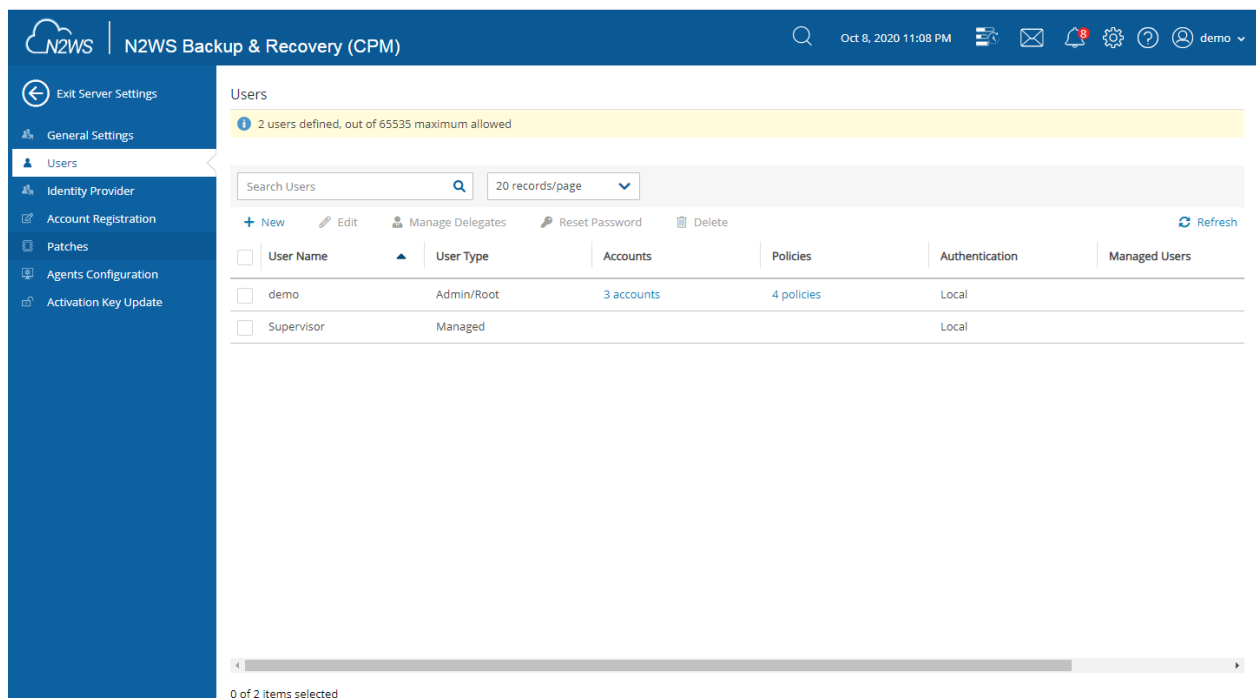


After selecting an announcement, you can reset the message status by selecting  **Mark as Unread** in the upper right corner of the message.



## 18 N2WS User Management

N2WS is built for a multi-user environment. At the configuration stage, you define a user that is the root user. The root user can create additional users (depending on the edition of N2WS you are subscribed to). Additional users are helpful if you are a managed service provider, in need of managing multiple customers from one N2WS server or if you have different users or departments in your organization, each managing their own AWS resources. For instance, you may have a QA department, a Development Department, and an IT department, each with their own AWS accounts. Select  **Server Settings > Users**.



The screenshot shows the N2WS web interface for user management. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date 'Oct 8, 2020 11:08 PM', and various system icons. The left sidebar contains a list of settings: 'Exit Server Settings', 'General Settings', 'Users' (selected), 'Identity Provider', 'Account Registration', 'Patches', 'Agents Configuration', and 'Activation Key Update'. The main content area is titled 'Users' and displays a message: '2 users defined, out of 65535 maximum allowed'. Below this is a search bar and a table of users. The table has columns for 'User Name', 'User Type', 'Accounts', 'Policies', 'Authentication', and 'Managed Users'. Two users are listed: 'demo' (Admin/Root) and 'Supervisor' (Managed). At the bottom, it shows '0 of 2 items selected'.

User Name	User Type	Accounts	Policies	Authentication	Managed Users
demo	Admin/Root	3 accounts	4 policies	Local	
Supervisor	Managed			Local	

The following are the types of users you can define. Delegate users are defined after users are created.

- Independent
- Managed

### 18.1 Independent Users

Independent users are completely separate users. The root user can create such a user, reset its password, and delete it with all its data, but it does not manage this user's policies and resources. Independent users can:

- Log-in to N2WS
- Create their own accounts
- Manage their backup
- Manage policies and resources of managed users that were assigned to them



Independent users can have Managed users assigned to them by the root/admin in the **Users** management screen. An Independent user can log on, manage the backup environment of their assigned Managed users, and receive alerts and notifications on their behalf.

## 18.2 Managed Users

Managed Users are users who can log on and manage their backup environment, or the root/admin user or independent user can do it for them. The root user can perform all operations for managed users: add, remove and edit accounts, manage backup policies, view backups, and perform recovery. Furthermore, the root user, or independent user, can receive alerts and notifications on behalf of managed users. The root/admin user can also configure notifications for any managed user and independent users can configure notifications for their managed users (section 17.3.1.) To create a managed user, select **+ New** and choose **Managed** as the **User Type**. If the root user does not want managed users to log in at all, they should not receive any credentials.

Managed users may be managed by Independent users. See section 18.1.


## 18.3 User Definitions

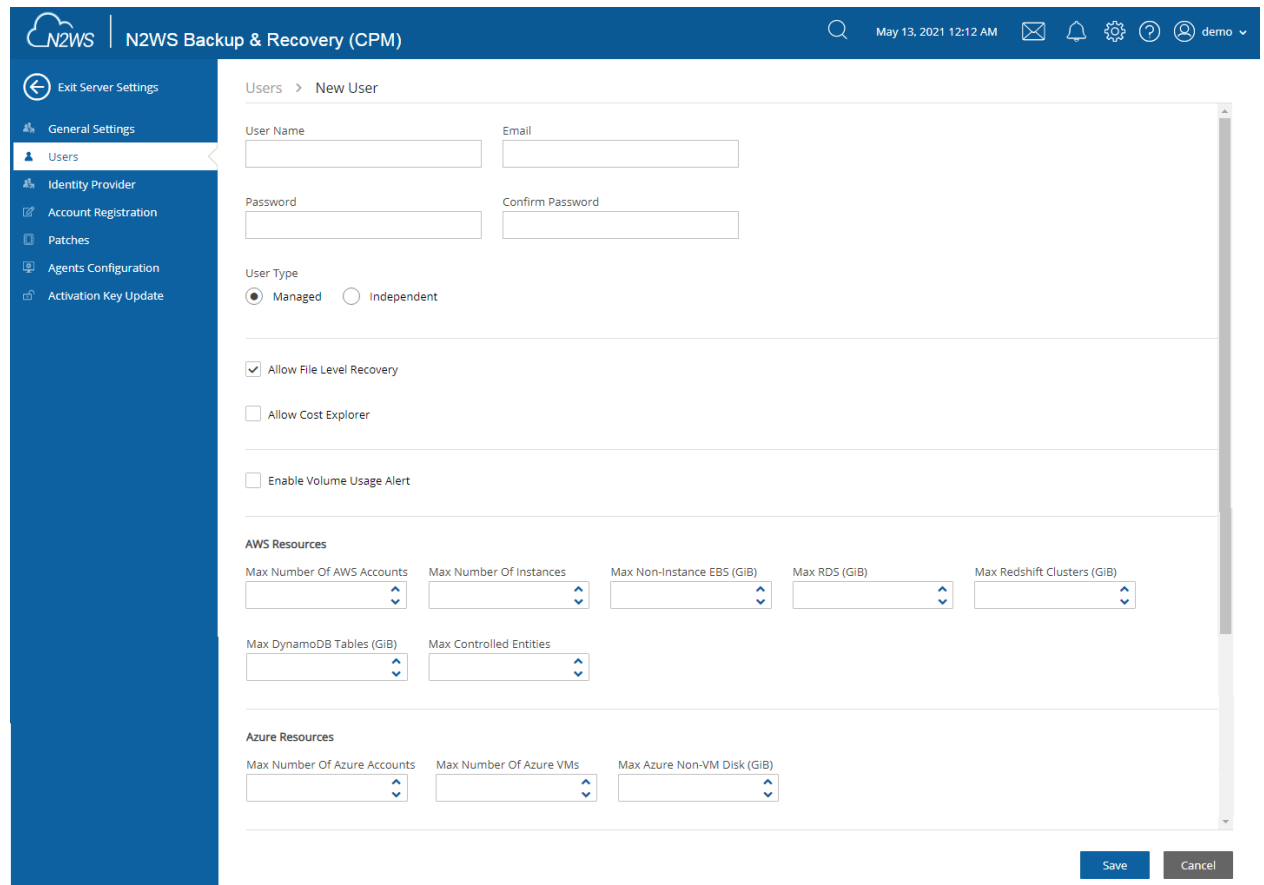
When editing a user, the root user can modify email, password, type of user, and resource limitations.

**Note:** The user name cannot be modified once a user is created.

**Note:** Users who are created in N2WS via IdP integration (section 19) cannot be edited, only deleted.

### To define users:

1. If you are the root or admin user, in the toolbar, select  **Server Settings**.
2. In the left panel, select the **Users** tab. The **Users** screen opens.
3. Select **+ New**.



4. In the **User name**, **Email**, and **Password** boxes, type the relevant information.
5. Select the **User Type** option. For type details, see sections 18.1 and 18.2.
6. If the user can recover at the file level, select **Allow File Level Recovery**.
7. To enable Cost Explorer calculations:
  - Verify that Cost Explorer is enabled for CPM. See section 25.
  - Select **Allow Cost Explorer**. The default is to deny the calculations.
  - In AWS, allow the CPM Cost Explorer feature. See section 25.1.1.
  - For information about Cost Explorer, see section 25.
8. In the **Max Number of Accounts**, **Max Number of Instances**, **Max Non-instance EBS (GiB)**, **Max RDS (GiB)**, **Max Redshift Clusters**, **Max DynamoDB Tables (GiB)**, and **Max Controlled Entities** boxes, select the value for the respective resource limitation from its list.  
 The value for **Max Controlled Entities** is the maximum number of allowed instances and RDS database resources.
9. For Users that will have Azure accounts, in the Azure Resources section, select the value for the respective resource limitations for **Max Number of Azure Account**, **Max Number of Azure VMs**, and **Max Azure Non-VM Disk (GiB)**.

**Note:** If the resource limitation fields are left empty, there is no limitation on resources, except the system level limitations that are derived from the licensed N2WS edition used.




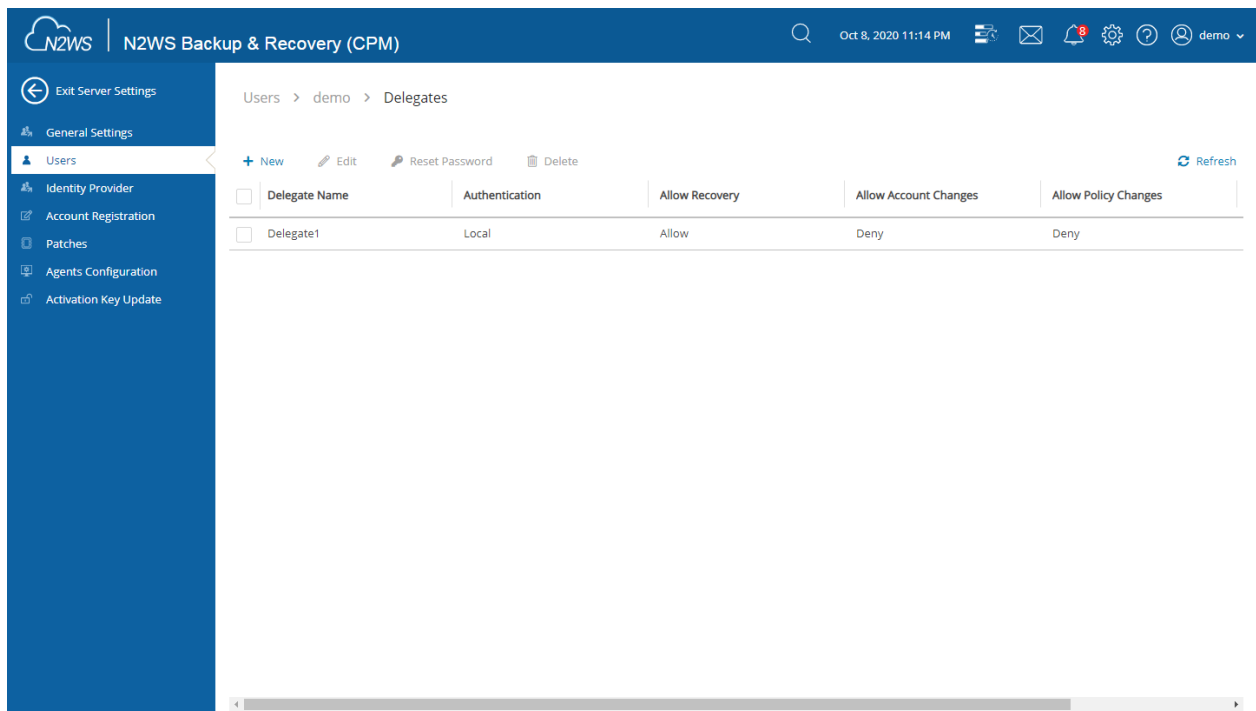
## 18.4 Delegates

Delegates are a special kind of user, which is managed via a separate screen. Delegates are similar to IAM users in AWS:

- They have credentials used to log on and access another user's environment.
- The access is given with specific permissions.

**Warning:** Using IAM User credentials is not recommended as they are less secure than using IAM roles.

For each user, whether it is the root user, an independent user, or a managed user, the  **Manage Delegates** command in the **Users** list screen that opens the Delegates screen for that user. Selecting an existing entry in the Delegates column also opens the Delegates screen for that user.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a menu with options: Exit Server Settings, General Settings, Users (selected), Identity Provider, Account Registration, Patches, Agents Configuration, and Activation Key Update. The main content area is titled 'Users > demo > Delegates'. It features a table with columns: Delegate Name, Authentication, Allow Recovery, Allow Account Changes, and Allow Policy Changes. The table contains one entry: Delegate1, Local, Allow, Deny, Deny. Above the table are buttons for + New, Edit, Reset Password, and Delete. A Refresh button is in the top right corner. The top navigation bar shows the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date 'Oct 8, 2020 11:14 PM', and user profile information.

You can add as many delegates as needed for each user and also edit any delegate's settings:

### To add a delegate:

**Note:** Once a user is defined as a delegate, the name cannot be changed.

1. Select a user.
2. Select  **Manage Delegates** and then select **+ New**.





3. In the **Delegate Name** box, type the name of the new delegate.
4. Enter a valid **Email** and set the **Password**.
5. Permissions are denied by default. To allow permissions, select the relevant ones for this delegate:
  - **Perform Recovery** – Can perform recovery operations.
  - **Change Accounts** – Can add and remove AWS accounts as well as edit accounts and modify credentials.
  - **Change Backup** - Can change policies: adding, removing, and editing policies and schedules, as well as adding and removing backup targets.
  - **Change Settings and S3 Repositories** – Root delegates can change Notifications, Users and General Settings, and S3 Repositories.

**Note:** By default, the delegate will only have permissions to view the settings and environment and to monitor backups.

Allowing all permissions will allow the non-root delegate the permissions of the original user except for notification settings.

When in **Edit** mode, the root user can reset passwords for delegates.

## 18.5 Usage Reports

The root user can also use the user management screen to download CSV usage reports for each user, which can be used for accounting and billing. The usage report will state how many accounts this user is managing, and for each account, how many instances and non-instance storage is backed up.

Reporting is now available for daily tracking of resources that were configured as a backup target on each policy. The **Reports** tab contains two levels of detail for Usage Reports. Users can



download the following Usage Reports, both of which are filterable by user and timeframe. The report can be created as a **Scheduled Report** or for **Immediate Report Generation**. In each case, select **Detailed** for usage per account or **Anonymized** for aggregated account usage per user. See sections 17.8 and 17.10.2.

**Note:** Data saved to the reports is compliant with the EU's General Data Protection Regulation (GDPR).

## 18.6 Audit Reports

N2WS will record every operation initiated by users and delegates. This is important when the admin needs to track who performed an operation and when. By default, audit logs are kept for 30 days. The root user can:

- Modify the audit log retention value in the **Cleanup** tab of the **General Settings** screen. See section 9.4.
- Download audit reports for specific users or delegates. See section 17.10.

Included in the audit reports are:

- A timestamp
- The event type
- A description of the exact operation.
- In the report of all users, the user with delegate information, if any


## 18.7 Email Configuration

N2WS uses the following email services to effortlessly distribute reports.

- Amazon Simple Email Service (AWS SES) is a cloud-based email sending service required for AWS accounts.
- Simple Mail Transport Protocol (SMTP) is an internet standard communication protocol for non-AWS accounts.

**Note:** Currently, the only regions that are available for the SES service are Asia Pacific (Mumbai), Asia Pacific (Sydney), EU (Frankfurt), EU (Ireland), US East (N. Virginia), US West (Oregon).

**To allow N2WS to configure the email parameters:**

1. In the toolbar, select  **Server Settings > General Settings**.
2. Select the **Email Configuration** tab.
3. Select **Enable Email Configuration**.
4. In the **Email Method** list, select **AWS SES** or **SMTP** for other accounts.
5. If you selected **AWS SES**, complete the following parameters:
  - **Sender Email Address** – The 'From' e-mail address.
  - **Verify Email Address** – Select to verify address.



- **SES Region** – Select the region for the SES service.
- **Authentication Method** – Select a method and supply additional information if prompted:
  - **IAM User Credentials** – Enter AWS Access Key ID and Secret Access Key.
  - **CPM Instance IAM Role** – Additional information is not needed.
  - **Account** – In the **Account** list, select one of the CPM accounts defined in the **Accounts** tab.

The screenshot shows the 'Email Configuration' tab in the 'General Settings' section of the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation links: Exit Server Settings, General Settings, Users, Identity Provider, Account Registration, Patches, Agents Configuration, and Activation Key Update. The main content area has tabs for CPM Server, Proxy, Security, Capture VPC, Tag Scan, Cleanup, Email Configuration (selected), and Cost Explorer. Under 'Email Configuration', there is a checkbox for 'Enable Email Configuration' which is checked. Below it is a dropdown for 'Email Method' set to 'AWS SES'. A text field for 'Sender Email Address' is present, followed by a checked checkbox for 'Verify Email Address'. Further down is a dropdown for 'SES Region' set to 'US East (N. Virginia)' and another dropdown for 'Authentication Method' set to 'CPM Instance IAM Role'. A link for 'Open SES Management Console' is at the bottom. A 'Save' button is in the bottom right corner.

6. If you selected **SMTP**, complete the following:

Note: SMTP requires a dedicated proxy server that supports SMTP sockets.

- **Sender Email Address** – The 'From' e-mail address.
- **Password**

Note: A non-ASCII password results in an exception on update.

- **SMTP Server Address**
- **SMTP Port** – Default is 587.
- **SMTP Connection Method** – Select **STARTTLS** or **TLS**.
- **Network Access** – Select **via Socket Proxy**.
- **SOCKS Version** – Select **SOCKS4** or **SOCKS5**.
- **Proxy Address** and **Proxy Port**
- **Proxy Username** and **Password**



## General Settings

CPM Server	Proxy	Security	Capture VPC	Tag Scan	Cleanup	<b>Email Configuration</b>	Cost Explorer
							Volume Usage Percent
Email Method SMTP							
Sender Email Address				Password			
SMTP Server Address		SMTP Port		SMTP Connection Method			
		587		STARTTLS			
⚠ SMTP requires a dedicated proxy server which supports SMTP sockets							
Network Access via Socket Proxy							
SOCKS Version SOCKS5							
Proxy Address		Proxy Port					
		1080					
Proxy Username		Password					

Save

7. When finished, select **Save** to confirm the parameters.

Amazon will respond with an Email Address Verification Request for the region to the defined address. The Amazon verification e-mail contains directions for completing the verification process, including the amount of time the confirmation link is valid.

Currently, the Scheduled Reports are sent using the defined email identity if the reports are run with **Schedules** or the **Run Now** option.



## 19 N2WS IdP Integration

N2WS supports users configured locally (local users) and users configured using the organization's federated identity provider (IdP).

- Local users are created and managed using the N2WS User Management capabilities described above.
- IdP users are users whose credentials are received from the organization's IdP. N2WS can be configured to allow users in the organization's IdP system to log in to N2WS using their IdP credentials. Integration with IdP systems is performed using the SAML 2.0 protocol.
- N2WS supports:
  - Active Directory (AD) 2012 and 2016. If using SAML 2.0, AD 2019 also supported.
  - Azure Active Directory-based Single Sign-On (SSO)
  - IDP vendors who support SAML 2.0

**Note:** The N2WS root user can only login through the local user account even when N2WS is configured to work with IdP.

Configuring N2WS to work with IdP consists of the following:

- Configuring the IdP to work with N2WS
- Configuring N2WS to work with the IdP
- Configuring N2WS Groups in N2WS
- Configuring N2WS Groups and Users in IdP

### 19.1 Configuring IdPs to Work with N2WS

N2WS supports the SAML 2.0 protocol for integration with IdP systems. N2W Software qualifies only certain IdP systems internally, but any SAML 2.0 compliant IdP system should be able to work smoothly with N2WS.

#### 19.1.1 Prerequisites to IdP Integration with N2WS

Before configuring N2WS to work with an IdP system, it is required that N2WS be configured in the IdP system as a new application. Consult the IdP system's documentation on how to configure a new application.


**Note:** When configuring N2WS as a new IdP application, verify that:

- The default Name **ID** format used in SAML requests is set to **Unspecified**, or modify the default N2WS configuration as per section on N2WS configuration below.
- The X509 certificate Secure hash algorithm is set to SHA-256.
- The following URL values are used:

**Note:** <N2WS-ADDRESS> is either the DNS name or the IP address of the N2WS Server.



- **Entity ID** - `https://<N2WS-ADDRESS>/remote_auth/metadata`
- **Sign in response** - `https://<N2WS-ADDRESS>/remote_auth/complete_login/`
- **Sign out response** - `https://<N2WS-ADDRESS>/remote_auth/complete_logout/`


As part of configuring N2WS as a new IdP application, the IdP system will request a file containing the N2WS x509 certificate. The certificate file can be obtained from the N2WS **Settings** screen in the **Identity Provider** tab. In the **Settings** tab, select  **Download CPM's Certificate** and choose a location to save the file. See section 19.1.2.

If configuring N2WS to work with Microsoft Active Directory/AD FS, refer to section 19.4.1.

### 19.1.2 Configuring N2WS for IdP Integration

If configuring N2WS for integration with Microsoft Active Directory/AD FS, refer to section 19.5.

**To configure N2WS to work with the organization's IdP:**

1. In the N2WS toolbar, select  **Server Settings**.
2. In the left panel, select the **Identity Provider** tab and then select the **Settings** tab.
3. Select **Identity Provider**. The configuration parameters appear.

4. Complete the following:
  - **CPM IP or DNS** – The IP Address or DNS name of the N2WS server.

**Note:** N2WS accepts either the IP address or DNS name in many fields. However, some IdPs require that N2WS be configured using the format used when configuring N2WS as an application in the IdP system. If the IdP uses DNS names, use DNS names in N2WS, and if the IdP uses IP address, use IP addresses in N2WS



- **Entity ID** – The Identity Provider Identifier’s URI provided by the IdP system. Consult the IdP system’s documentation.
  - **Sign In URL** – The authentication request target is the URL, provided by the IdP system, to which N2WS will redirect users after entering their IdP credentials. Consult the IdP system’s documentation.
  - **Sign Out URL** – The logout request target is the URL, provided by the IdP system, to which N2WS will redirect users once they logout of N2WS. Consult the IdP system’s documentation.
  - **NameID format** – The format of the SAML **NameID** element.
  - **X509 Certificate** – Select **Choose file** to upload the IdP’s X509 certificate. Consult the IdP system’s documentation about obtaining their x509 certificate.
5. Optionally, you can **Download CPM’s Certificate** and **Metadata**.
  6. Once all the parameters have been entered, select **Save** and then select **Test Connection** to test the connection between N2WS and the IdP.

## 19.2 Configuring Groups and Group Permissions on the N2WS Side

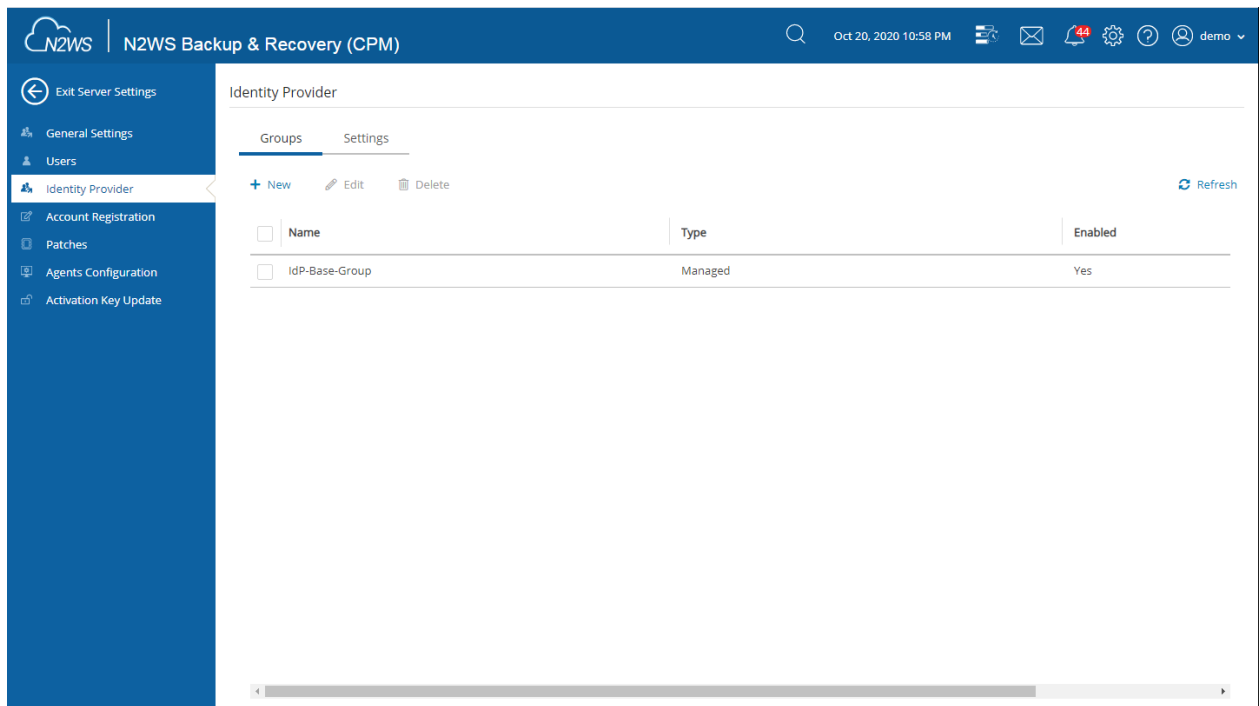
Groups and the permissions assigned to groups are configured in N2WS. When an IdP user logs into N2WS, the information about the user’s group membership is received from the IdP and that group’s permissions are assigned to the user.

**Note:** Every IdP user must belong to an N2WS group. IdP users who do not belong to a group, even if they have user-specific permissions as detailed below, cannot log on to N2WS. Logon by IdP users who do not belong to a group will be failed with an appropriate error message.

**Note:** Default groups do not appear until **Identity Provider** is enabled in the **Settings** tab.

N2WS comes with pre-defined groups named with the prefix **default**:

- default\_managed\_users
- default\_independent\_users
- default\_root\_delegates
- default\_root\_delegates\_readonly



**Note:** The default groups cannot be modified or deleted. To see the permission settings assigned to the default groups, select the group name.

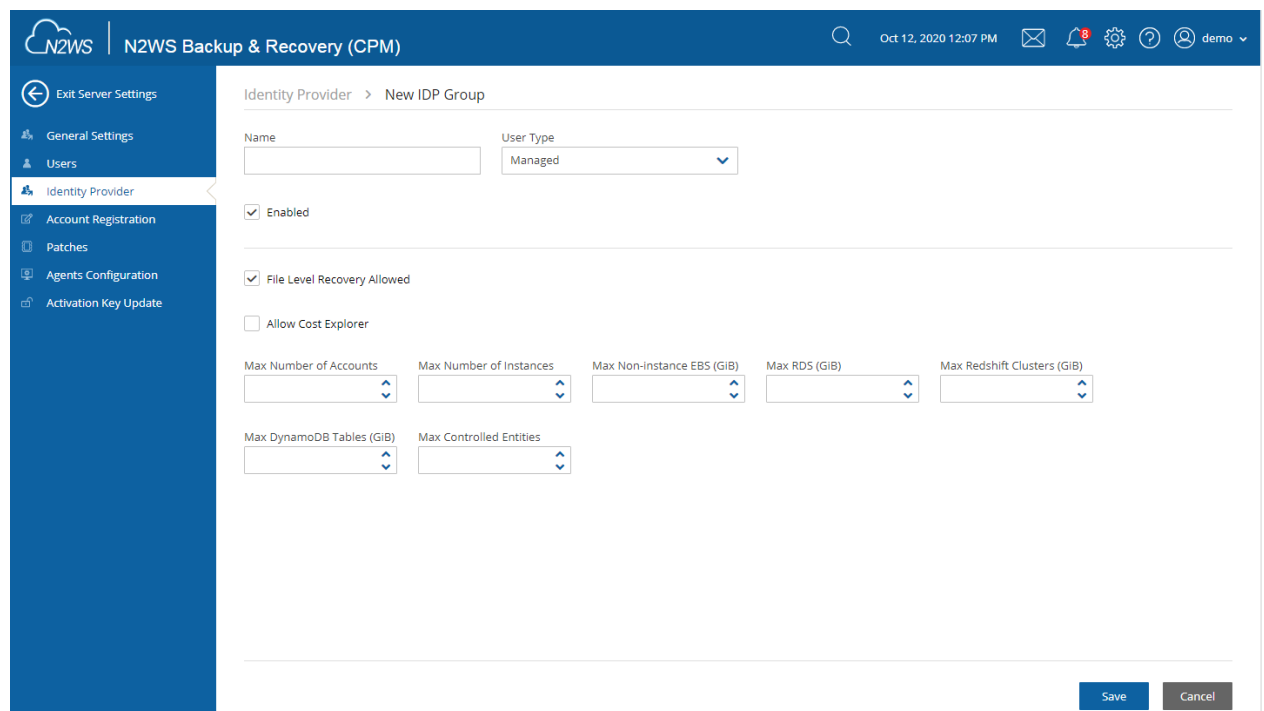
Additional groups can be created and removed easily in the **Identity Provider** tab of the N2WS **Server Settings** screen.

**To add a new group:**

**Note:** The group permission settings essentially mirror the user permissions detailed in section 18.

1. In the **Identity Provider** tab, select the **Groups** tab and then select **+ New**. The New IDP Group screen will appear.
2. Complete the fields as needed, and then select **Save**.





- **Name** – Name of the group.
  - **User Type** – For details, see section 18. Parameters depend on the **User Type** selected.
    - Managed
    - Independent
    - Delegate
  - **Enabled** – When disabled, group users will not be able to log on to N2WS.
3. For User Type **Managed**:
- **File Level Recovery Allowed**– When selected, members of the group can use the file-level recovery feature.
  - **Allow Cost Explorer** – When selected, members of the group can see cost data. For Cost Explorer information, see section 25.
  - **Max Number of Accounts** – The maximum number of AWS accounts users belonging to this group can manage.
  - **Max Number of Instances** – The maximum number of instances users belonging to this group can manage.
  - **Max Non-Instance EBS (GiB)** – The maximum number of Gigabytes of EBS storage that is not attached to EC2 instances that users belonging to this group can manage.
  - **Max RDS (GiB)** – The maximum number of Gigabytes of RDS databases that users belonging to this group can manage.
  - **Max Redshift Clusters (GiB)** – The maximum number of Gigabytes of Redshift clusters that users belonging to this group can manage.
  - **Max DynamoDB Tables (GiB)** – The maximum number of Gigabytes of DynamoDB tables that users belonging to this group can manage.
  - **Max Controlled Entities** – The maximum number of allowed entities for Resource Control.



#### 4. For User Type **Delegate**:

**Note:** When Delegate is selected, the **Original Username** to which this group is a delegate is required although the Original Username does not yet need to exist in N2WS. After creation, the Original Username cannot be modified.

- **Original Username** – User name of delegate.
- **Allow to Perform Recovery** – Whether the delegate can initiate a recovery.
- **Allow to Change Accounts** – Whether the delegate can make changes to an account.
- **Allow to Change Backup** – Whether the delegate can make changes to a backup.

## 19.3 Configuring Groups on the IdP Side

IdPs indicate a user's group membership to N2WS using IdP claims. Specifically, the IdP must configure an **Outgoing Claim Type** of `cpm_user_groups` whose value is set to all the groups the user is a member of, both N2WS related groups and non-N2WS related groups.

**Note:** Group names on the IdP side no longer need the 'cpm' prefix. In cases where the names of the group users are assigned to in the IdP is of the form `cpm_<group-name-in-N2WS>`, for example `cpm_mygroup` where `mygroup` is the name of a group that was created in N2WS, the `<group-name-in-N2WS>` part of the name must match the name of a group in N2WS. See section 19.2.

For example, to give IdP users permissions of the N2WS group `default_managed_users`:

1. The relevant users can be members of an IdP group called `cpm_default_managed_users`.
2. The IdP must have an outgoing claim called `cpm_user_groups`.
3. The value of the claim must include the names of all the user's groups in the IdP, which presumably includes `cpm_default_managed_users`.

Or

1. The relevant users can be members of an IdP group called `default_managed_users`.
2. The IdP must have an outgoing claim called `cpm_user_groups`.
3. The value of the claim should not include the names of all the user's groups in the IdP, which presumably is `default_managed_users`.

**Note:** An IdP user logging onto N2WS can belong to only one N2WS group, i.e. of all the groups listed in the `cpm_user_groups` claim, only one can be an N2WS group, such as `cmp_mygroup`. If an IdP user is a member of more than one N2WS group, the logon will fail with a message indicating the user belongs to more than one N2WS group.

### 19.3.1 Understanding N2WS User Permissions

A user logged into the N2WS system can have several types of permissions. This section discusses the different types of permissions as they are applied to N2WS IdP integration. For full



treatment of the meanings of these permissions, see section 16.3. To override N2WS group permissions on a per user basis, see section 19.3.2.

### General User Attributes

Attribute Name	Mandatory (Y/N)	Meaning	Valid Values
user_type	N	Type of user.	<ul style="list-style-type: none"><li>• Managed</li><li>• Independent</li><li>• Delegate</li></ul>
user_name	N	Username in N2WS.	Alphanumeric string
user_email	N	User's email address.	Valid email address

### Attributes for Independent and Managed Users

Attribute Name	Mandatory (Y/N)	Meaning	Valid Values
allow_file_level_recovery	N	Whether the user is allowed to use the N2WS file-level restore feature.	yes, no
max_accounts	N	The number of AWS accounts the user can manage in N2WS. Varies by N2WS license type.	Number between 1 and max licensed
max_instances	N	The number of instances the user can backup. Varies by N2WS license type.	Number between 1 and max licensed
max_independent_ebs_gib	N	Total size of EBS independent volumes being backed up in GiB (i.e. volumes not attached to a backed-up instance).	Number between 1 and max licensed
max_rds_gib	N	Total size of AWS RDS data being backed up in GiB	Number between 1 and max licensed
max_redshift_gib	N	Total size of AWS Redshift data being backed up in GiB	Number between 1 and max licensed
max_dynamodb_gib	N	Total size of AWS DynamoDB data being backed up in GiB.	Number between 1 and max licensed
max_controlled_entities	N	Total number of AWS resources under N2WS Resource Control.	Number between 1 and max licensed.



## Attributes for Delegate Users

Attribute Name	Mandatory (Y/N)	Meaning	Valid Values
original_username	Y	The name of the user for whom <b>user_name</b> is a delegate.	Alphanumeric string
allow_recovery_changes	N	Whether the user can perform N2WS restore operations.	yes, no
allow_account_changes	N	Whether the user can manage N2WS user accounts.	yes, no
allow_backup_changes	N	Whether the user can modify backup policies.	yes, no
allow_settings	N	Whether the user can modify S3 Repository settings.	yes, no

All the permissions detailed above are set for a group when the group is created in N2WS. Additionally, it is possible to assign N2WS permission at the level of individual IdP users as described in 19.3.2. When there is a conflict between a user's group permissions and a user's individual permissions, the individual permissions take precedence.

A permission string consists of **key=value** pairs, with pairs separated by a semicolon.

For convenience, below is a string of all the possible security parameters. N2WS will accept a partial list consisting of any number of these parameters in any order:

```
user_type=independent;email=yeepee@redpil.com;allow_recovery=yes;allow_account_changes=yes;allow_backup_changes=yes;allow_file_level_restore=no;max_accounts=1;max_instances=2;max_independent_ebs_gib=3;max_rds_gib=4;max_redshift_gib=5;max_dynamodb_gib=5;original_username=robi@stam
```

### 19.3.2 Overriding Group Settings at the User Level

Users get the N2WS permissions assigned to their group. However, it is possible to give specific IdP group members permissions different from their group permissions.

#### To override the group permission for a specific user:

1. The IdP administrator must first enter the new permissions in an IdP user attribute associated with the user. The attribute can be an existing attribute that will now serve this role (e.g. msDS-cloudExtensionAttribute1) or a custom attribute added to the IdP user schema specifically for this purpose.

The content of the attribute specifies the user's N2WS permissions in the **key=value** format detailed in the section above.

- Permissions specified in the user attribute will override permissions inherited from the group.



- Permission types not specified in the user attribute will be inherited from the group's permissions. For example, if the attribute contains only the value `max_accounts=1`, all other permissions will be inherited from the user's group permissions.
2. Once a user attribute has been configured with the correct permissions, an IdP claim rule with Outgoing Claim Type `cpm_user_permissions` must be created. The value of the claim must be mapped to the value of the attribute chosen above.
  3. When the user-level claim is enabled, the user will be able to log on to N2WS with permissions that are different from the group's permissions.
- If configuring Microsoft Active Directory/AD FS, refer to section 19.6 for details.

## 19.4 N2WS Login Using IdP Credentials

To use IdP credentials to log on to N2WS, select the **Sign in with: Identity Provider** option on the N2WS Logon screen.

Username:

Password:

[Sign In](#)

Or

[Sign in with Identity Provider](#)

[License Agreement](#)

Selecting **Sign in with Identity Provider** will redirect the user to the organization's IdP system using SAML.

**Note:** To log on to N2WS as root, log on with the standard user and password option.

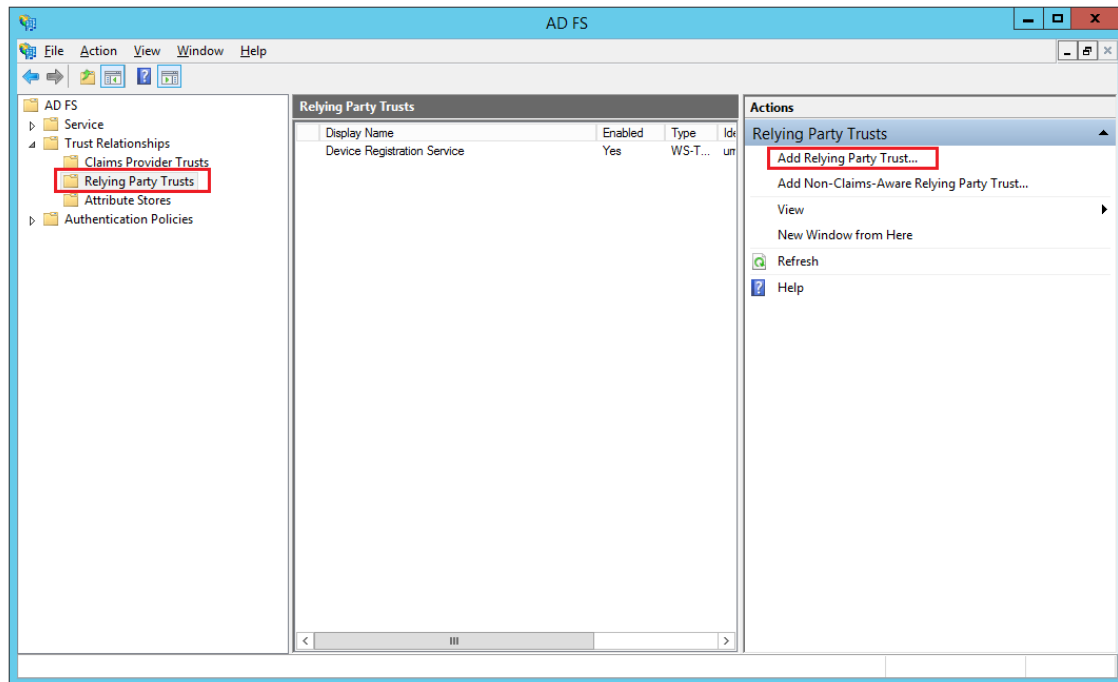
### 19.4.1 Configuring AD/AD FS for Integration with N2WS

To enable N2WS to integrate with AD/AD FS, N2WS must be added to AD FS as a **Relying Party Trust**.

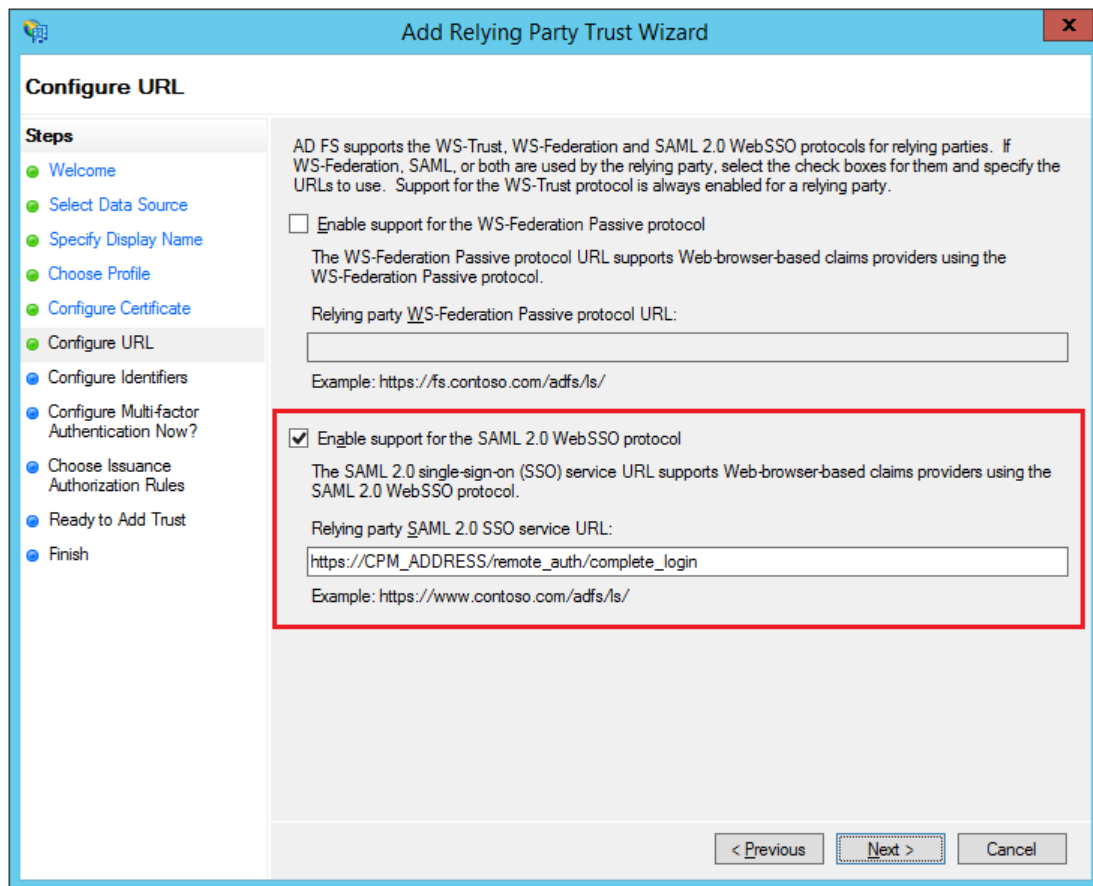
**Note:** The following AD FS screenshots are from AD 2012. The AD 2016 screens are very similar.

**To run the Add Relying Party Trust Wizard:**

1. In the left pane of the AD FS console, select **Relying Party Trusts**.
2. In the right pane, select **Add Relying Party Trust**. . . The Wizard opens.



3. Select **Start**.
4. Select the **Enter data about the relying party manually** option.
5. Select **Next**.
6. On the **Welcome** screen, type the display name for N2WS (e.g. N2WS), and then select **Next**.
7. On the **Choose Profile** screen, select the **AD FS profile** option, and then select **Next**.
8. Skip the **Configure Certificate** screen by selecting **Next**.
9. On the **Configure URL** screen:
  - a. Select Enable support for SAML 2.0 WebSSO protocol.
  - b. In the Relying Party SAML 2.0 SSO Service URL box, type `https://` followed by the N2WS DNS name or IP address, and then followed by `/remote_auth/complete_login/`.  
For example, the resulting string might look like:  
`https://ec2-123-245-789.aws.com/remote_auth/complete_login/`
10. Select **Next**.



**Add Relying Party Trust Wizard**

**Configure URL**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☐ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☒ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

https://CPM\_ADDRESS/remote\_auth/complete\_login

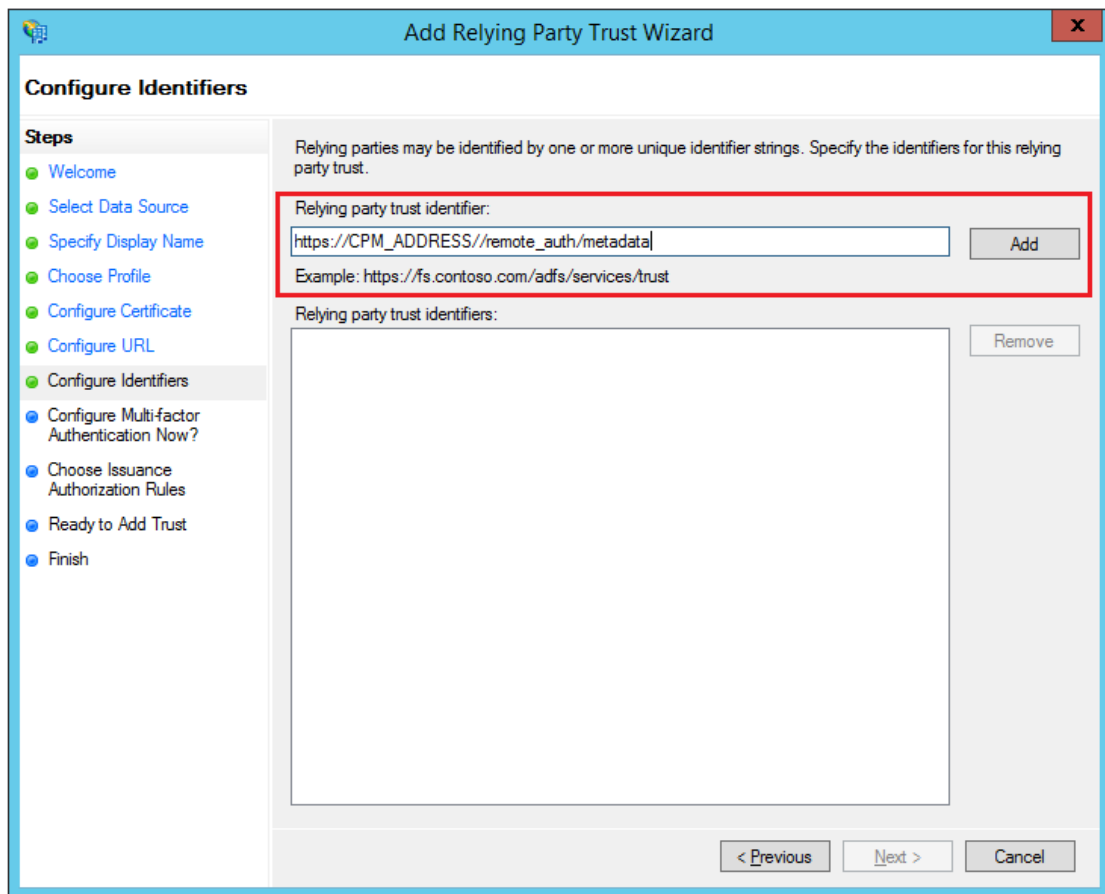
Example: https://www.contoso.com/adfs/ls/

< Previous   Next >   Cancel

11. In the **Configure Identifiers** screen, type `https://` followed by the N2WS DNS name or IP address, and then followed by `/remote_auth/metadata` in the **Relying party trust identifier** box. For example, the resulting string might look like:

`https://ec2-123-245-789.aws.com/remote_auth/metadata`

12. Select **Add** on the right.



**Add Relying Party Trust Wizard**

**Configure Identifiers**

**Steps**

- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers**
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

< Previous   Next >   Cancel

13. Select **Next**.
14. On the **Configure Multi-factor Authentication Now?** screen, select the **I do not want to configure multi-factor authentication settings for this relying party trust at this time** option, and then select **Next**.
15. On the **Issuance Authorization Rules** screen, select the **Permit all users to access this relying party** option, and then select **Next**.
16. On the **Ready to Add Trust** screen, review the setting of the **Relying party trust** configured with the Wizard. When finished, select **Next**.
17. On the **Finish** screen of the Wizard, select **Close**. There is no need to select the **Open the Edit Claim Rules dialogue for this relying party trust when the wizard closes** option.

## 19.4.2 Setting AD FS Properties

Once the Relying Party Trust has been configured, set the AD FS properties.

**To set the AD FS properties:**

1. Go back to the AD FS management console, and in the middle pane, right-select the N2WS line under **Relying Party Trust**, and then select **Properties**.
2. On the screen that opens, select the **Endpoints** tab, and then select **Add SAML....**





3. In the **Edit Endpoint** screen, select **SAML Logout** from the **Endpoint type** list.

**Edit Endpoint**

Endpoint type:  
SAML Logout

Binding:  
POST

☐ Set the trusted URL as default

Index: 0

Trusted URL:  
https://128.111.132.56/adfs/ls/?wa=wsignout1.0  
Example: https://sts.contoso.com/adfs/ls

Response URL:  
https://ec2-5-6-7-8.compute-1.amazonaws.com/remote\_auth/complete\_logout/  
Example: https://sts.contoso.com/logout

OK Cancel


4. In the **Trusted URL:** box, type the DNS name or IP address of the AD FS server followed by `/adfs/ls/?wa=wsignout1.0` (e.g. `https://adserver.mycompany.com/adfs/ls/?wa=wsignout1.0`).
5. In the **Response URL:** box, type DNS name or IP address of the N2WS server followed by `/remote_auth/complete_logout/` (e.g. `https://ec2-123-245-789.aws.com/remote_auth/complete_logout/`).
6. Select **OK**.
7. Go to the **Advanced** tab, and in the **Secure hash algorithm** list, select **SHA-256**. Select **Apply**.

### 19.4.3 Installing the N2WS Certificate

In order for N2WS to work with AD FS the X.509 certificate used by N2WS needs to be added to the AD FS **Trusted Root Certification Authorities** list. If you installed your own certificate in N2WS when you first configured N2WS (as per section 2.4.2) then your certificate may already be in your AD FS root trust. Otherwise, you will need to add it. If you used the certificate N2WS creates during installation, you will need to add that certificate into the AD FS **Trusted Root Certification Authorities**.

**To add a root certificate to the AD FS Trusted Root Certification Authorities:**

1. Go to the **Signature** tab under properties and select **Add...**
2. In the **File** box at the bottom of the screen, type the name of the file containing the N2WS x.509 certificate. This will be either:
  - a. The root certificate you installed in N2WS when it was first configured as per section 2.4.2 if not already in the AD FS Trusted Root Certification Authorities, or
  - b. The certificate N2WS created when it was first configured.

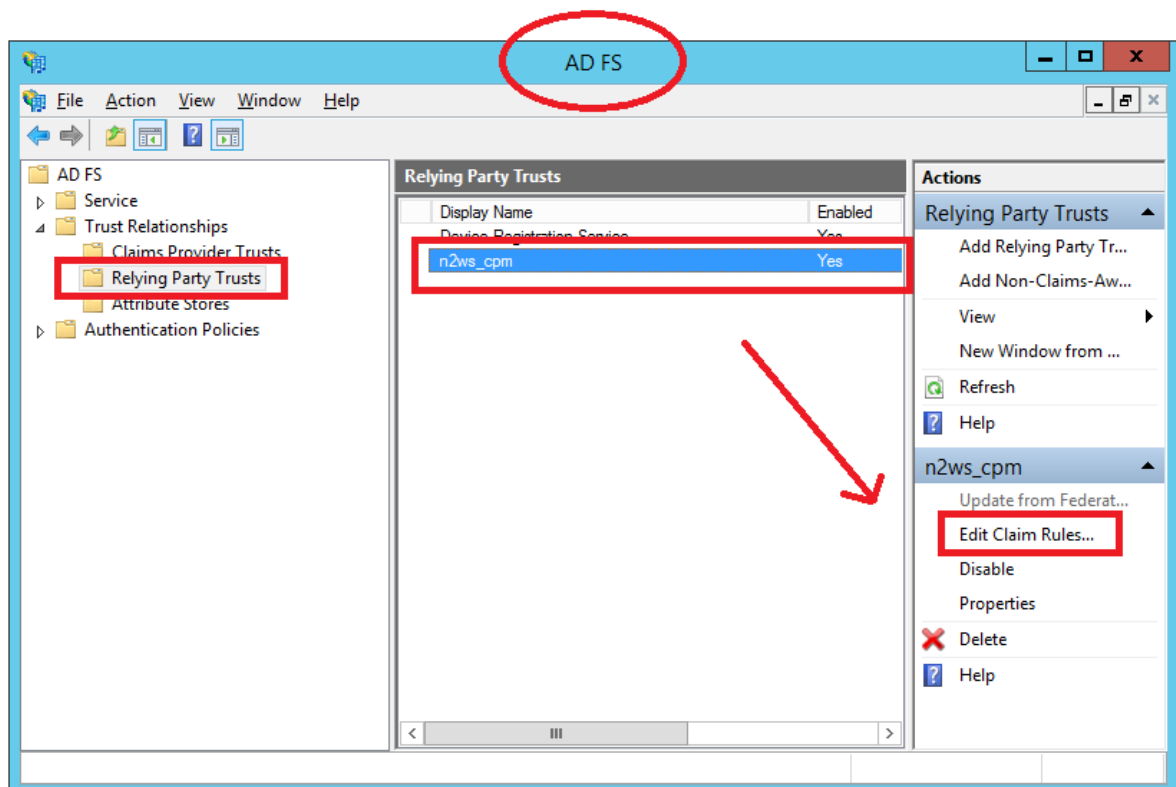
3. To obtain a copy of the certificate being used by N2WS, either the one you originally installed or the one N2WS created, select  **Download CPM's Certificate** at the bottom of the **Identity Provider** tab of the **General Settings** screen.
4. Once you have entered the name of the file, select **Open**.  
The N2WS certificate is now visible in the center pane in the **Signature** tab.
5. In the center pane of the **Signature** tab, double select the N2WS certificate.
6. Under the **General** tab, select **Install Certificate....**
7. In the **Certificate Import Wizard** screen, select the **Local Machine** option, and then select **Next**.
8. Select the **Place all certificates in the following store** option, select **Browse...**, and then select the **Trusted Root Certification Authorities** store. Select **OK**.
9. Select **Next**.
10. Select **Finish**. Then select **OK** on the pop-up screen, select **OK** on the **General** tab, and then select **OK** on the **Properties** screen.

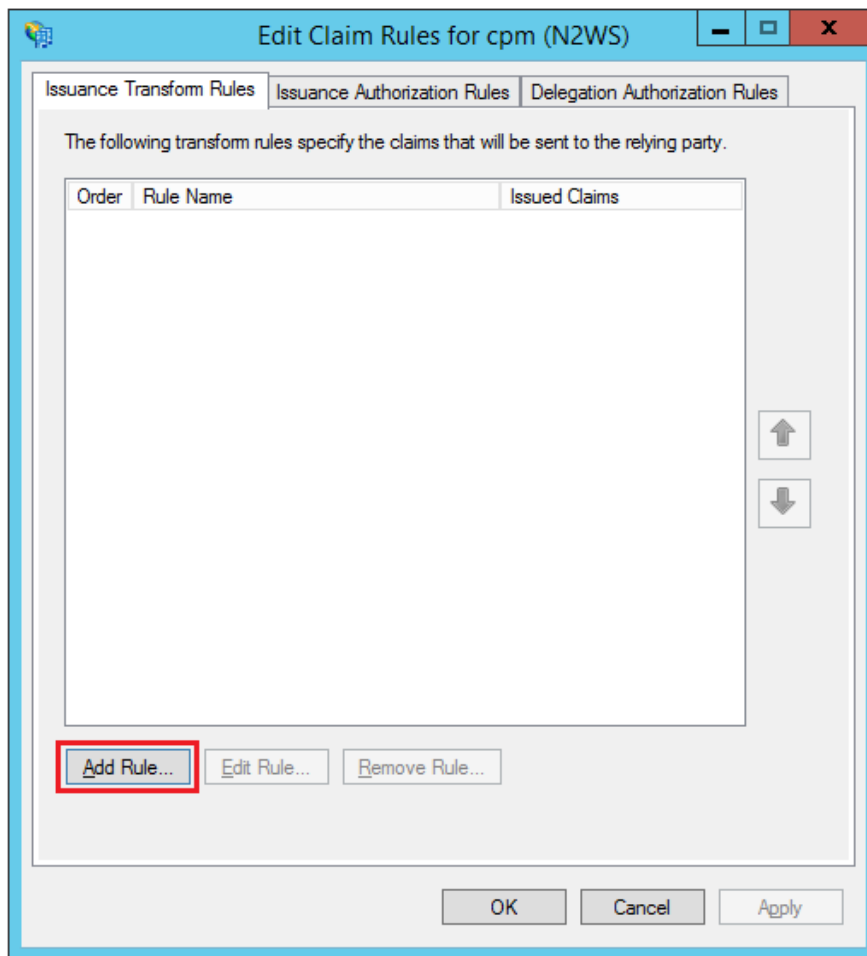
The next step is to create a Name ID claim in AD FS.

#### 19.4.4 Creating an AD FS Name ID Claim

To create an AD FS claim:

1. Open the ADFS management console. In the main page of the management console, select **Relying Party Trusts** in the left pane.
2. In the middle **Relying Party Trust** pane, select the N2WS party (e.g. N2WS).
3. In the right pane, select **Edit Claim Rules...**
4. In the **Edit Claim Rules** screen, select **Add Rule**.





5. In the **Claim rule template** list, select **Transform an Incoming Claim** and then select **Next**.
6. Complete the **Add Transform Claim Rule Wizard** screen:
  - a. In the **Claim rule name** box, type a name for the claim.
  - b. In the **Incoming claim type** list, select Windows account name.
  - c. In the **Outgoing claim type** list, select Name ID.
  - d. In the **Outgoing name ID format** list, select Unspecified.
  - e. Select the **Pass through all claim values** option.
  - f. Select OK.

Edit Rule - demo nameid
✕

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

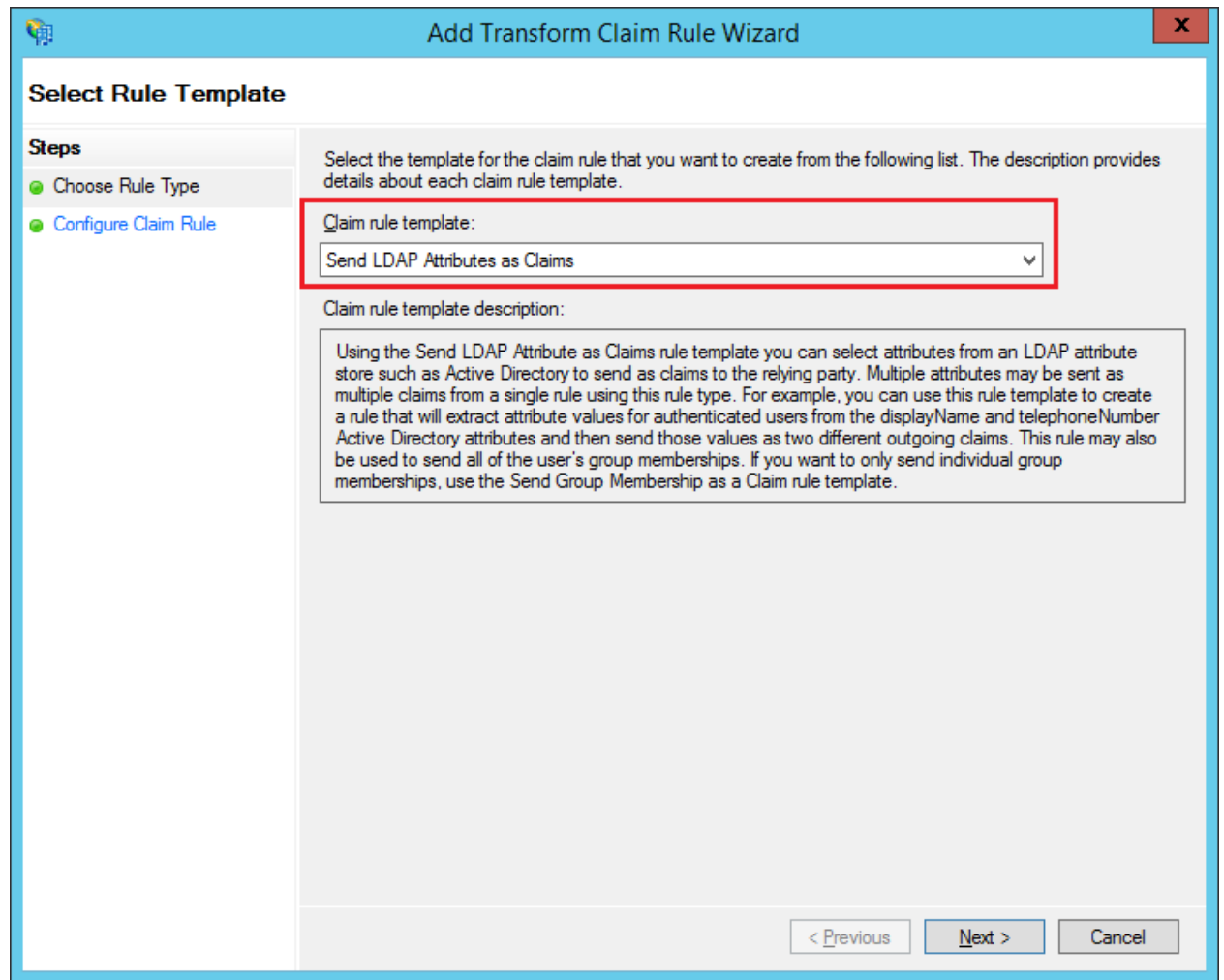
Example: fabrikam.com

The next step is to add a Token-Groups claim.

### 19.4.5 Adding a Token-Group's Claim

An ADFS Token-Groups claim must be configured so that AD FS will send N2WS the list of groups a user is a member of. To configure the Token Group's claim, perform steps 1 and 2 of the Configuring Name ID Claim process in section 19.4.4. Then continue as follows:

1. In the **Claim rule template** list, select **Send LDAP Attributes as Claims** and then select **Next**.



**Add Transform Claim Rule Wizard**

**Select Rule Template**

**Steps**

- Choose Rule Type
- Configure Claim Rule

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

< Previous   Next >   Cancel

2. In the **Claim rule name** box, type a name for the rule you are creating.
3. In the **Attribute store** list, select **Active Directory**. In the **Mapping of LDAP attributes to outgoing claim types** table:
  - a. In the left column (**LDAP Attribute**), select **Token-Groups - Unqualified Names**.
  - b. In the right column (**Outgoing Claim Type**), type 'cpm\_user\_groups'.

Edit Rule - user permissions claim
X

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	Token-Groups - Unqualified Names	cpm_user_groups
	msDS-cloudExtensionAttribute1	cpm_user_permissions
▶*		

### 19.4.6 Testing the Connection

At this point AD FS has been configured to work with N2WS. It is now possible to perform a connectivity test between N2WS and AD FS.


**To test the connection between N2WS and AD FS:**

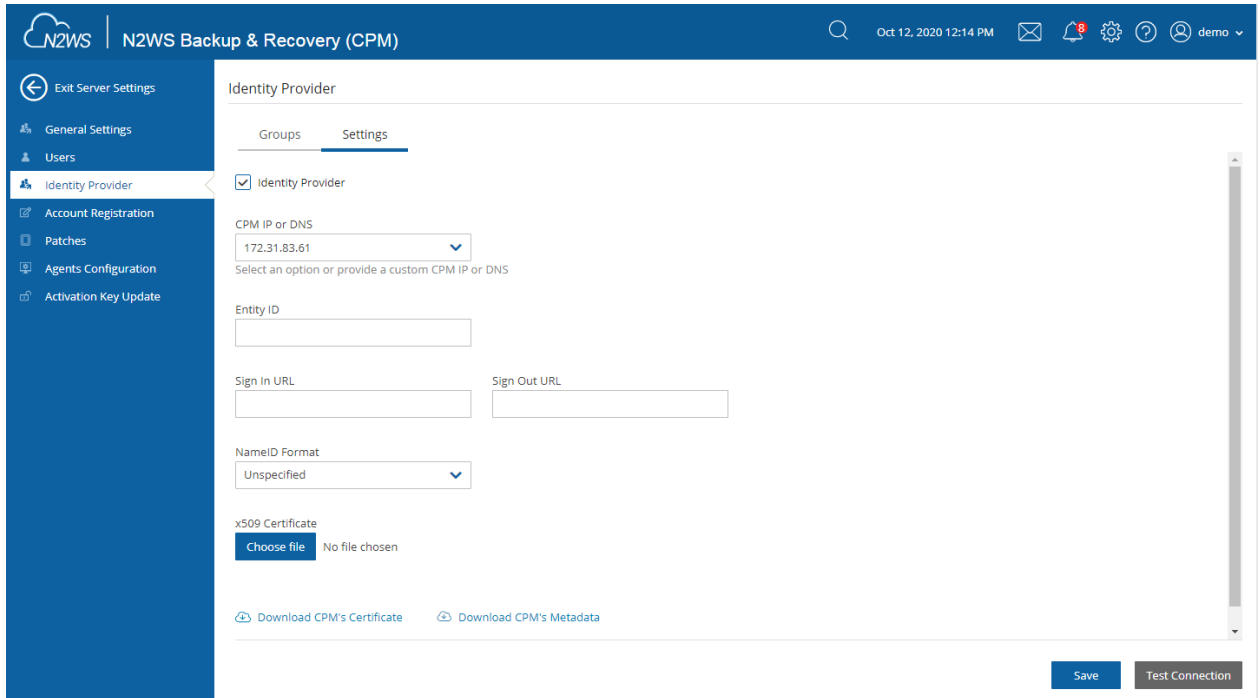
1. Go to the N2WS **General Settings** screen.
2. Select **Identity Provider**.
3. In the **Groups** tab, select an Identity Provider.
4. In the **Settings** tab, select **Test Connection**.
5. Type a valid AD username and password on the login page.
6. Select **Sign in**.



## 19.5 Configuring N2WS to Work with Active Directory / AD FS

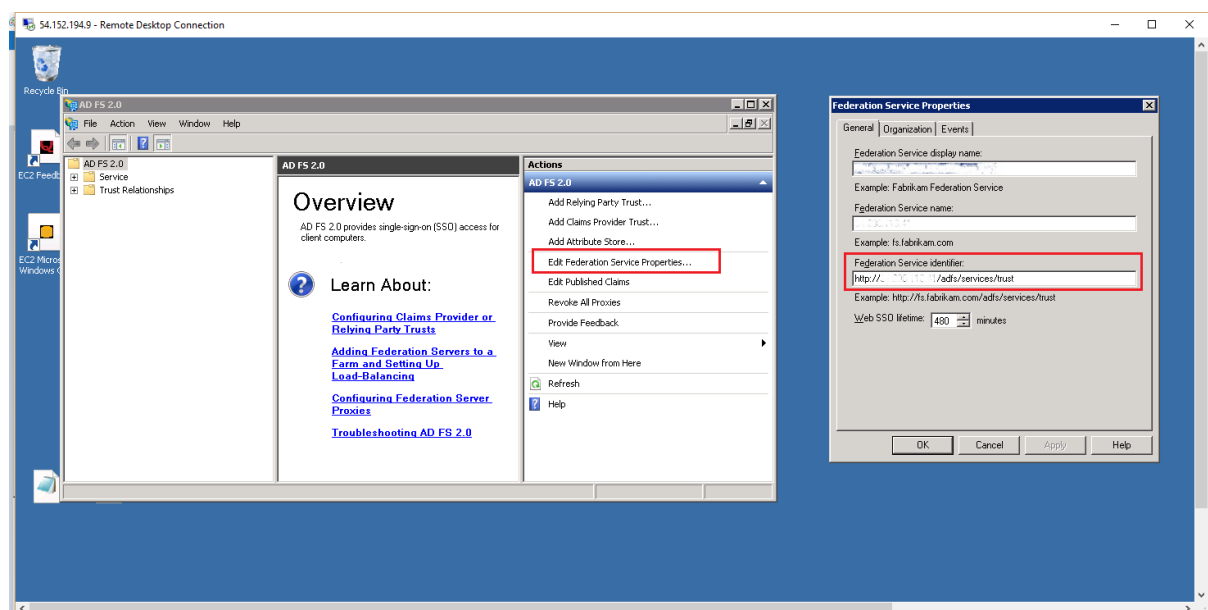
To configure N2WS to work with the organization's AD server:

1. Go to the N2WS  **Server Settings > General Settings**.
2. Select the **Identity Provider** tab.
3. In the Identity Provider list, select a **Group**.
4. To enable the group, select the **Settings** tab, and then select **Identity Provider**. Several IdP related parameters are presented.



The screenshot shows the N2WS web interface. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date 'Oct 12, 2020 12:14 PM', and several status icons. The left sidebar contains a list of settings: 'Exit Server Settings', 'General Settings', 'Users', 'Identity Provider' (selected), 'Account Registration', 'Patches', 'Agents Configuration', and 'Activation Key Update'. The main content area is titled 'Identity Provider' and has two tabs: 'Groups' and 'Settings'. The 'Settings' tab is active, showing a list of Identity Providers with 'Identity Provider' checked. Below this, there are several configuration fields: 'CPM IP or DNS' (a dropdown menu showing '172.31.83.61'), a note 'Select an option or provide a custom CPM IP or DNS', 'Entity ID' (a text input field), 'Sign In URL' and 'Sign Out URL' (text input fields), 'NameID Format' (a dropdown menu showing 'Unspecified'), and 'x509 Certificate' (a 'Choose file' button with 'No file chosen' text). At the bottom of the settings area are links for 'Download CPM's Certificate' and 'Download CPM's Metadata'. At the very bottom right of the interface are 'Save' and 'Test Connection' buttons.

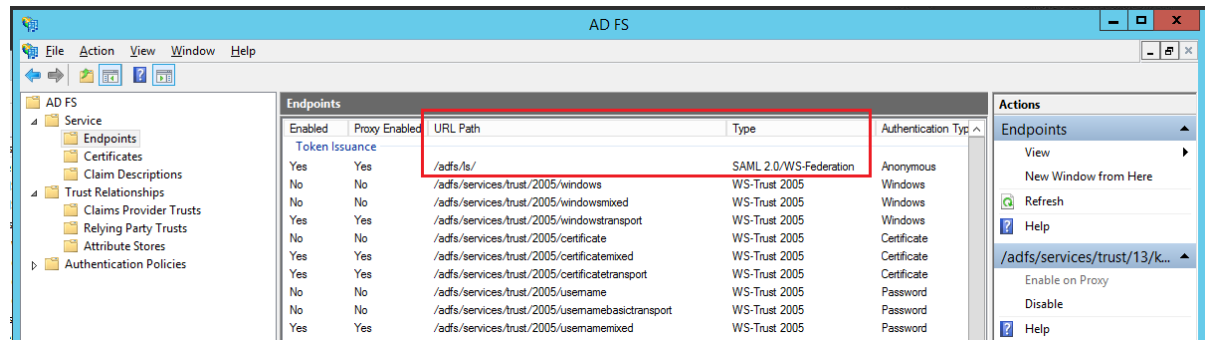
5. In the **Entity ID** box, type the AD FS **Federation Service Identifier**, as configured in AD FS. See below how to locate this parameter in AD FS.



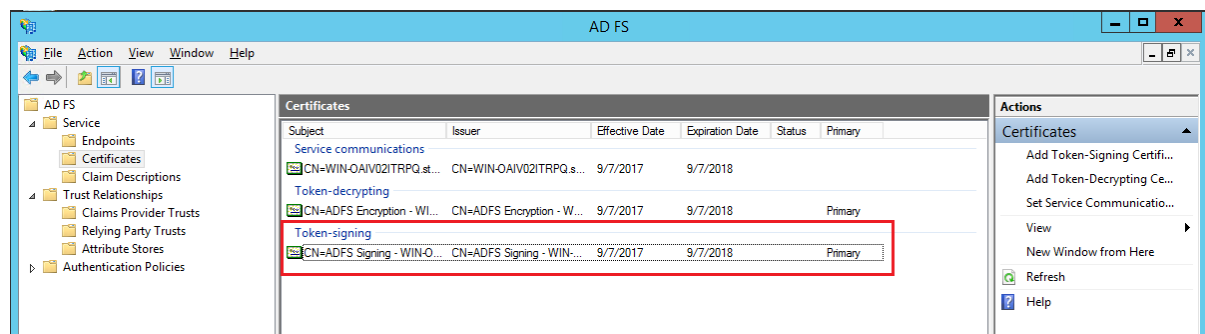


6. In the **Sign in URL** box, type the URL to which N2WS will redirect users for entering their AD credentials.

This parameter is configured as part of AD FS. The AD FS server's DNS name, or IP address, must be prepended to the URL Path listed in AD FS. See below to locate this information in AD FS.



7. In the **NameID Format** list, select the format of the SAML **NameID** element.
8. In the **x509 cert** box, upload the X509 certificate of the AD FS server. The certificate file can be retrieved from the AD FS management console under **Service -> Certificates**, as shown below:



9. To export the IdP's certificate:
  - a. Double select the **Token signing** field to open the **Certificate** screen.
  - b. Select the Details tab and then select Copy to File . . . on the bottom right.
  - c. Select Next to continue with the Certificate Export Wizard.
  - d. Select the Base-64 Encoded X.509 (.crt) option and then select Next.
  - e. Type a name for the exported file and select Next.
  - f. Select Finish.
10. Once all the parameters for N2WS have been entered, select **Save** and then select **Test Connection** to verify the connection between N2WS and the IdP.

## 19.6 Configuring an AD FS User Claim

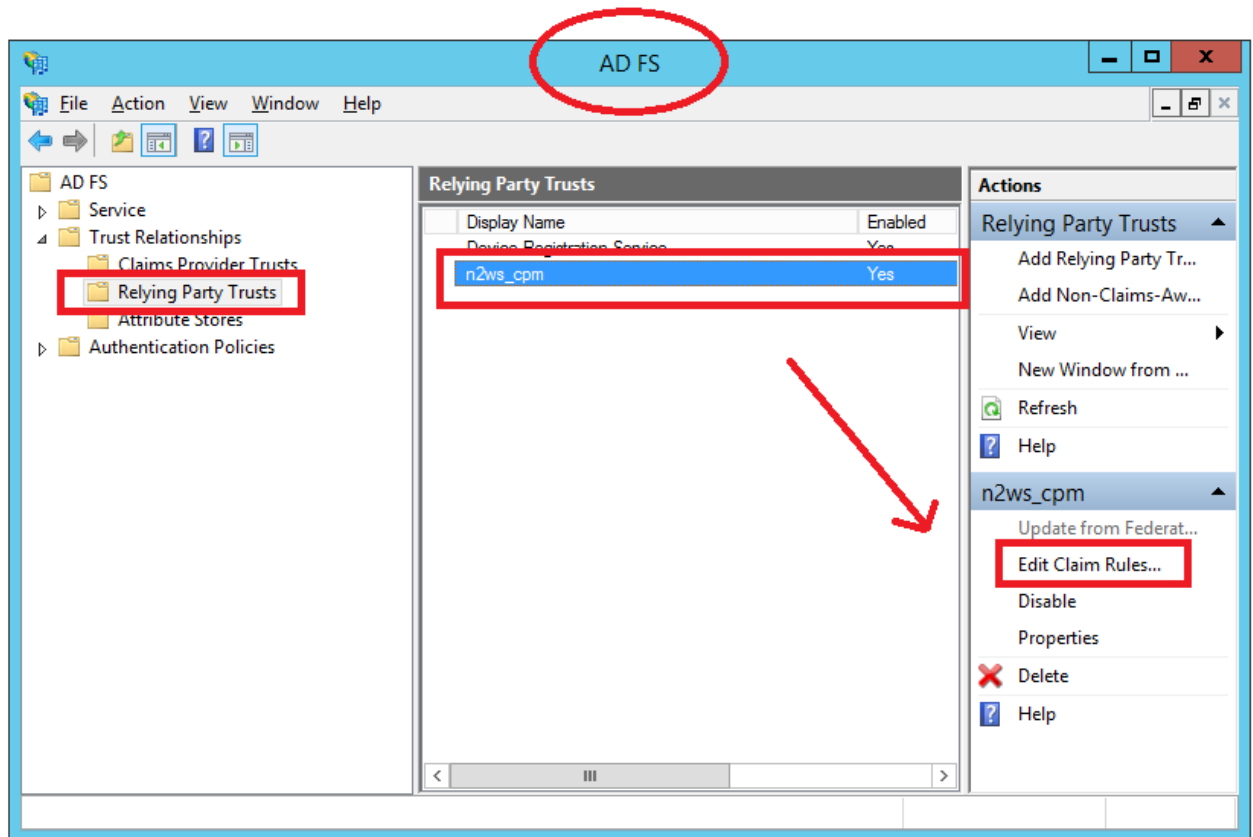
Once a user attribute has been configured with the correct permissions, an ADFS claim rule with **Outgoing Claim Type** `cpm_user_permissions` must be created before the user-level permissions can take effect.

**To create the claim rule:**

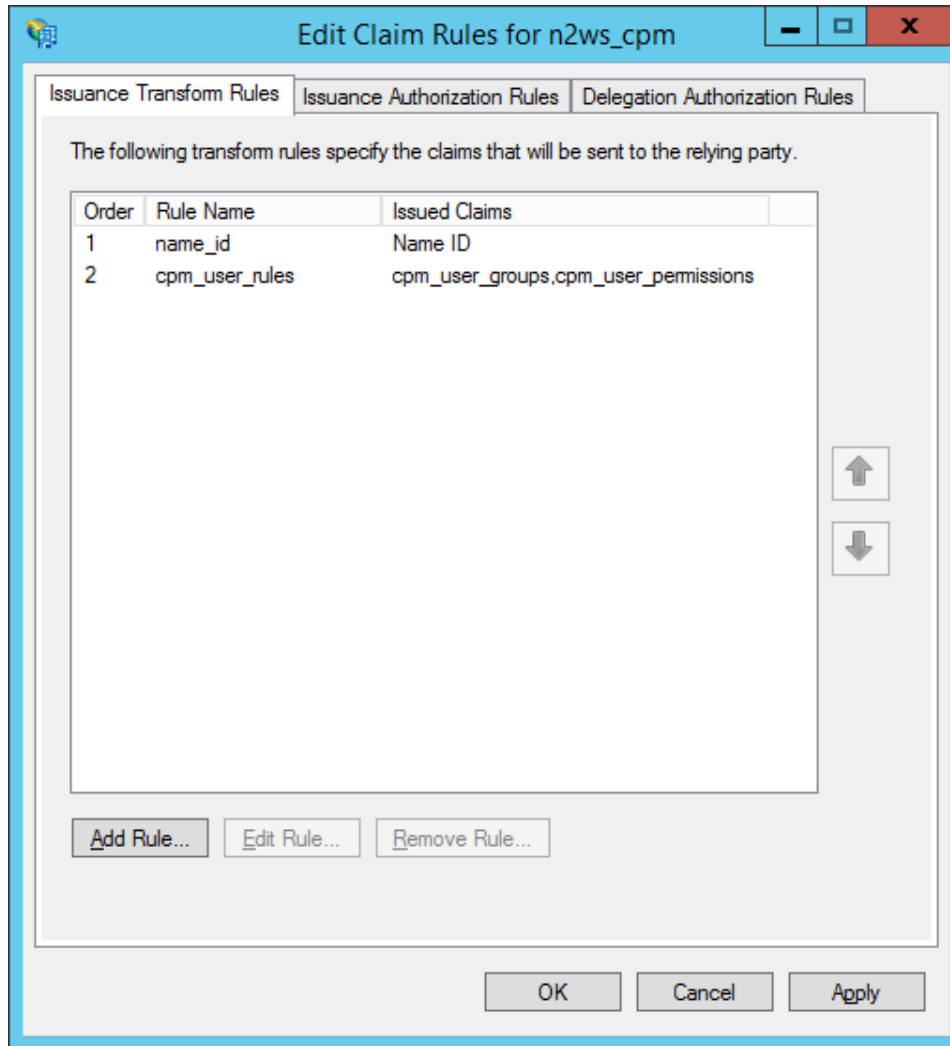
1. Open the AD FS management console.
2. In the main page of the management console, in the left pane, select **Relying Party Trusts**.



3. Select the N2WS party (e.g. N2WS) in the middle pane, and in the right pane, select **Edit Claim Rules**.



4. In the **Edit Claim Rules** screen, select **Add Rule**.

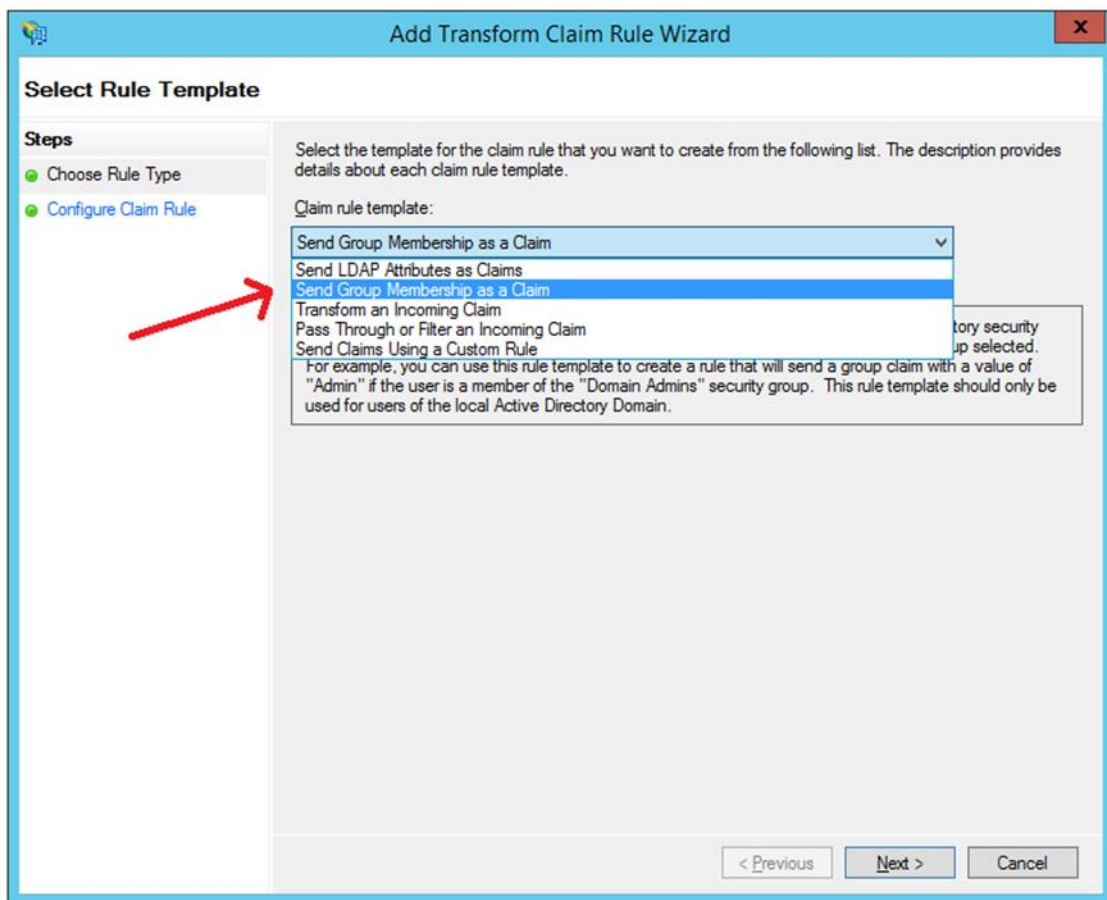


Issuance Transform Rules | Issuance Authorization Rules | Delegation Authorization Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	name_id	Name ID
2	cpm_user_rules	cpm_user_groups, cpm_user_permissions

5. In the **Add Transform Claim Rule Wizard** screen, select **Send LDAP Attributes as Claims** in the **Claim rule template** list, and then select **Next**.



6. The **Claim Rule Wizard** opens the **Edit Rule** screen. Complete as follows:
  - a. In the **Claim rule name** box, type a name for the rule you are creating.
  - b. In the **Attribute store** list, select **Active Directory**.
  - c. In the **Mapping of LDAP attributes to outgoing claim types** table:
    - i. In the left column (**LDAP Attribute**), type the name of the user attribute containing the user permissions (e.g. `msDS-cloudExtensionAttribute1`).
    - ii. In the right column (**Outgoing Claim Type**), type `cpm_user_permissions`.

Edit Rule - user permissions claim
✕

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Rule template: Send LDAP Attributes as Claims

Attribute store:

Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)		Outgoing Claim Type (Select or type to add more)
	Token-Groups - Unqualified Names ▼		cpm_user_groups ▼
	msDS-cloudExtensionAttribute1 ▼		cpm_user_permissions ▼
▶*	▼		▼

7. Select **OK** to create the rule.

Once the user-level claim is enabled, the user will be able to log on to N2WS with permissions that are different from the group's permissions.

## 19.7 Configuring Azure AD and N2WS IdP Settings

This section shows how to configure Microsoft Azure Active Directory and N2WS IdP settings to communicate and enable logging.

### 19.7.1 Azure AD Configuration

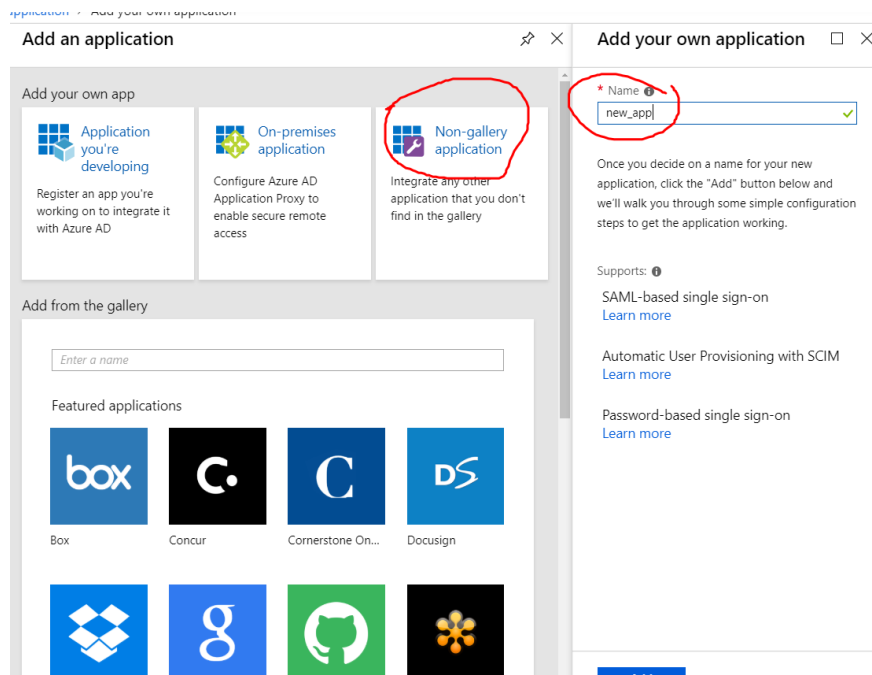
After logging in to Azure, go to **Azure Active Directory** in the left menu.

1. Start creating a new user (or use the existing user), group, and application in the **Create** menu on the right.

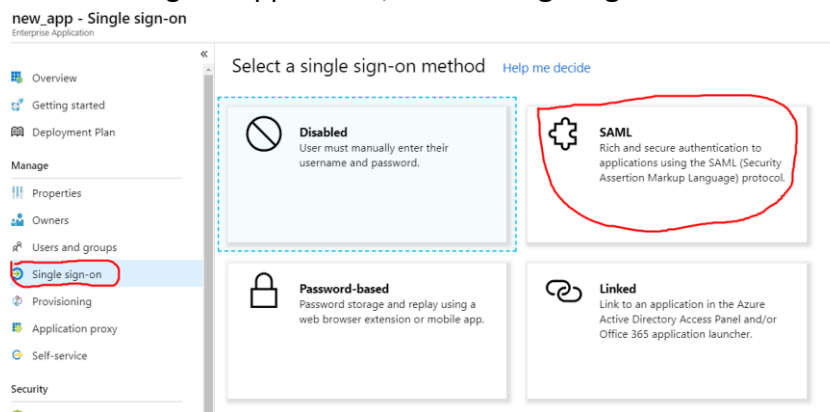


## 2. Create the group and assign a user:

## 3. Create a new application and choose **Non-gallery application**. Name the application.

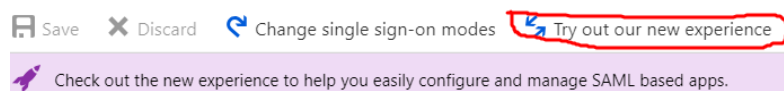


4. After naming the application, choose **Single sign-on** and **SAML**.



5. In the single sign-on setting, enter **Identifier** and **Reply URL** using your own N2WS IP or URL.

**Note:** There is a link at the top to change the appearance of this settings page.



#### 1. How to configure cpm\_dev with Azure AD

We highly recommend reviewing the following document to reduce configuration errors. [How to configure single sign-on between Azure AD and cpm\\_dev.](#)

#### 2. cpm\_dev Domain and URLs

Values for the fields below are provided by cpm\_dev. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by cpm\_dev. [Upload metadata file.](#)

\* Identifier (Entity ID) ⓘ

\* Reply URL (Assertion Consumer Service URL) ⓘ

☐ Show advanced URL settings



6. Ensure that the other attributes match. Download the certificate.

3. User Attributes [Learn more](#)

Edit the user information sent in the SAML token when user signs in to cpm\_dev.

User Identifier user.mail

☐ View and edit all other user attributes

4. SAML Signing Certificate [Learn more](#)

Manage the certificate used by Azure AD to sign SAML tokens issued to cpm\_dev.

App Federation Metadata Url

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	11/5/2021	7DE298DA6C856D891D49F495E3634CFC92F9D200	<a href="#">Certificate (Base64)</a> <a href="#">Certificate (Raw)</a> <a href="#">Metadata XML</a>

[Create new certificate](#)

☒ Show advanced certificate signing settings [Learn more](#)

Signing Option Sign SAML assertion

Signing Algorithm SHA-256

\* Notification Email dannyaram@gmail.com

7. Save the new application.

8. In the main menu, go to **Users and groups** and select **+ Add user**.

**new\_app - Users and groups**  
Enterprise Application

Overview  
Getting started  
Deployment Plan

Manage

Properties  
Owners  
**Users and groups**

**+ Add user** Edit Remove Update Credentials Columns

The application will appear on the access panel for assigned users. Set 'visible to users?' to no

First 100 shown, to search all users & groups, enter a display name.

DISPLAY NAME	OBJECT TYPE
No application assignments found	

9. Select **Users and groups** and then select the group you created.



Home > n2ws > Enterprise applications - All applications > new\_app - Users and groups > Add Assignment > Users and groups

### Add Assignment

Users and groups  
None Selected

Select Role  
User

### Users and groups

Select member or invite an external user

Search by name or email address

- CP cpm\_azure\_grp
- DA dannyaram@gmail.com
- GR grp\_name

Selected members:

- GR grp\_name [Remove](#)

[Assign](#) [Select](#)

10. In your new application, choose **Single sign-on** and edit the **User Attributes & Claims**.

Home > n2ws > Enterprise applications - All applications > new\_app - Single sign-on > SAML-based sign-on

### new\_app - SAML-based sign-on

Enterprise Application

Change single sign-on mode Switch to the old experience


Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback.

Reply URL (Assertion Consumer Service URL)	ote_auth/metadata
Sign on URL	https://ec2-34-230-163-111.compute-1.amazonaws.com/rem
Relay State	ote_auth/complete_login/
	Optional
	Optional

2

### User Attributes & Claims

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname



11. Choose to edit the **Name identifier** attribute and change the value to `user.mail`.



## User Attributes & Claims



[+ Add new claim](#)

Name identifier value: **user.userprincipalname**



CLAIM NAME	VALUE	
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

### Manage user claims

\* Name:

Namespace:

Choose name identifier format

Source: ☒ Attribute ☐ Transformation

\* Source attribute:

## 12. Add 2 new attributes.

### User Attributes & Claims

[+ Add new claim](#)

Name identifier value: **user.mail**

CLAIM NAME	VALUE
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.mail
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname

- `name: cpm_user_groups`  
`value: user_type=default;`  
`user_email=cpm@gmail.com;allow_file_level_recovery=default;`



```
max_accounts=default;max_instances=default;max_independent_ebs_gi  
b=default;max_rds_gib=default;max_redshift_gib=default;
```

- Change the parameters to meet N2WS needs:

name: cpm\_user\_groups

value: cpm\_<group-name>

Manage user claims

Name

cpm\_user\_permissions

✓

Namespace

Enter a namespace URI

Source

☒ Attribute ☐ Transformation

Source attribute

"user\_type=default; user\_email=cpm@gmail.com;allow\_file\_level\_re..."

Save

Complete

Successfully saved SSO SAML user claims

User Attributes & Claims

+ Add new claim

Name identifier value: user.mail

CLAIM NAME

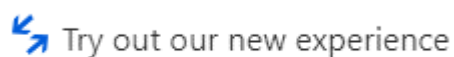
VALUE

cpm_user_groups	"cpm_azure_grp"	...
cpm_user_permissions	"user_type=default; user_email=cpm@gmail.c..."	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	user.givenname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	user.userprincipalname	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	user.mail	...
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	user.surname	...

## 19.7.2 N2WS IdP Configuration

To view the Azure AD settings for use in N2WS configuration:

1. While still in the Azure AD settings, go to single sign-on and switch to the new view:





2. Scroll down to section 4. These parameters will be used to configure the N2WS IdP settings.

**4** Set up new\_app

You'll need to configure the application to link with Azure AD.

Login URL	<code>https://login.microsoftonline.com/9e45459f-b668-4...</code>	
Azure AD Identifier	<code>https://sts.windows.net/9e45459f-b668-4300-9292-...</code>	
Logout URL	<code>https://login.microsoftonline.com/common/wsfe...</code>	

[View step-by-step instructions](#)

### To configure the N2WS Azure AD IdP settings:

1. In the N2WS UI, go to **Server Settings > Identity Provider**.
2. Select the provider, and select **Edit**.
3. In the **Settings** tab, complete the following:

- **Entity ID** - Copy Azure AD Identifier.
  - **Sign In URL** - Copy Login URL.
  - **Sign Out URL** – Copy Logout URL.
  - **NameID format** - Select **Unspecified**.
  - **x509 cert** - Upload the certificate downloaded in section 2.
4. Add a new group with the name of the group you added in the Azure Active Directory, without the **cpm** prefix. Select the **Groups** tab and then select **+ New** and add a name for the group.



N2WS | N2WS Backup & Recovery (CPM)

Oct 27, 2020 12:37 PM

Exit Server Settings

General Settings

Users

Identity Provider

Account Registration

Patches

Agents Configuration

Activation Key Update

Identity Provider

Groups Settings

+ New Edit Delete Refresh

<input type="checkbox"/>	Name	Type	Enabled
<input type="checkbox"/>	IdPBase	Managed	Yes

5. Select **Save**.
6. Return to the **Settings** tab and select **Test Connection**.



## 20 Configuring 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 CPM Edition to install:
    - Free Trial & BYOL
    - Advanced
    - Free
    - Standard
    - Enterprise


The screenshot shows the product page for N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition. The page includes the N2WS logo, a description of the product, and a list of features. The 'Highlights' section lists the following:

- 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

The page also shows a 'Typical Total Price' of \$0.042/hr and a 'Continue to Subscribe' button.

4. Select **Continue to Subscribe**. 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 **Continue to Configuration**.



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**  

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**. Select the relevant **Software Version** and **Region** and then select **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 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  
**BYOL**  
running on t3.medium  
\$0/hr

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



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

[< Product Detail](#) [Subscribe](#) [Configure](#) [Launch](#)

### Launch this software

Review your configuration and choose how you wish to launch the software.

#### Configuration Details

Fulfillment Option	Cloud Protection Manager Free Trial & BYOL (CFT) N2WS Backup & Recovery (CPM) Free Trial & BYOL Edition <i>running on t3.medium</i>
Software Version	3.0.0
Region	US East (N. Virginia)

[Usage Instructions](#)

#### Choose Action

Launch CloudFormation

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

Launch

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

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

Cancel **Next**

- Under **Prepare template**, select **Template is ready**.
- Under **Template source**, choose **Amazon S3 URL**. Select the default Amazon S3 URL and then 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

cpm-30

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

t3.medium

**Networking and Security Configuration**

Key Pair  
Name of an existing EC2 KeyPair

my-key-pair

VPC  
The VPC in which you want to Launch N2WS

vpc-1a4e8062 (172.31.0.0/16)

Subnet  
SubnetId in VPC

subnet-ac09d0e7 (172.31.16.0/20)

Inbound Access CIDR  
CIDR for Security Groups source IP

0.0.0.0/0

Cancel Previous **Next**

10. Complete the **Stack name** and **Parameters** sections.

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>

11. Select **Next**. The **Configure stack options** page opens.

228





CloudFormation > Stacks > Create stack

Step 1  
Specify template

Step 2  
Specify stack details

Step 3  
**Configure stack options**

Step 4  
Review

### Configure stack options

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

Name: CPM-3.0 Remove

Add tag

**Permissions**  
Choose an IAM role to explicitly define how CloudFormation can create, modify, or delete resources in the stack. If you don't choose a role, CloudFormation uses permissions based on your user credentials. [Learn more](#)

**IAM role - optional**  
Choose the IAM role for CloudFormation to use for all operations performed on the stack.

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

CloudFormation > Stacks > cpm-30

Stacks (8) Filter by stack name Active View nested 1

cpm-30 2020-01-26 19:34:21 UTC+0200 CREATE\_COMPLETE

cmp-27-cf 2019-10-15 11:11:22 UTC+0300 CREATE\_COMPLETE

cpm-30

Delete Update Stack actions Create stack

Stack info Events Resources Outputs Parameters Template Change sets

Events (1)

Search events

Timestamp	Logical ID	Status	Status reason
2020-01-26 19:34:21 UTC+0200	cpm-30	CREATE_IN_PROGRESS	User initiated

**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](#)

☒ I acknowledge that AWS CloudFormation might create IAM resources.

Cancel Previous Create change set Create stack

13. Select **I acknowledge that AWS CloudFormation might create IAM resources**, and then select **Create stack**. The **CloudFormation Stacks** page opens.

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

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

**Note:** Configure CPM with CloudFormation will fail where the requested Instance type is not supported in the requested Availability Zone. Retry your request, but do not specify an Availability Zone or choose us-east-1a, us-east-1b, us-east-1c, us-east-1d, or us-east-1f.

16. Continue configuring N2WS as in section 2.



## 21 Managing Snapshots with Lifecycle Policies

In addition to creating and managing EBS snapshots, N2WS can store backups in Simple Storage Service (S3) and S3 Glacier, allowing you to lower backup costs when storing backups for a prolonged amount of time. N2WS allows you to create a lifecycle policy, where older snapshots are automatically moved from high-cost to low-cost storage tiers. A typical lifecycle policy would consist of the following sequence:

1. Store daily EBS snapshots for 30 days.
2. Store one out of seven (weekly) snapshots in S3 for 3 months.
3. Finally, store a monthly snapshot in S3 Glacier for 7 years, as required by regulations.

**Note:** Storing snapshots in S3 is not supported for periods of less than 1 week.

Configuring a lifecycle management policy in N2WS consists of the following sequence:

1. Defining how many EBS snapshots to keep.
2. Enabling and configuring Backup to S3.
3. Enabling and configuring Archive to S3 Glacier.

For detailed S3 storage class information, refer to <https://aws.amazon.com/s3/storage-classes>.

### 21.1 Using S3 with N2WS

Using the N2WS **Copy to S3** feature, you can:

- Define multiple folders, known as repositories, within a single S3 bucket
- Define the frequency with which N2WS backups are moved to a Repository in S3, similar to DR backup. For example, copy every third generation of an N2WS backup to S3.
- Define backup retention based on time and/or number of generations per Policy.
- N2WS stores backups in S3 as block-level incremental backups.

**Note:** Only one S3 operation is allowed for a policy at a time – Copy, Recovery, Archive, or retention Cleanup.

- For instance, an S3 Copy or S3 Recovery is not allowed when the S3 backup retention Cleanup is executing. If a new backup is created while a copy of a previous backup is still running, the new backup will not be copied to S3.
- Likewise, only one Archive or Cleanup operation can run for a policy at a time, so if a new backup is created while another backup is being archived, or while cleanup is running for the policy, no Archive or Cleanup will be performed for the policy following the completion of the copy operation.
- If the S3 Cleanup process is running at the time of an S3 Copy or Recovery, you can abort the Cleanup process to allow the Copy or Recovery process to continue. See section [21.5.3](#).



**Important:** AWS Encryption at the bucket-level *must* be *enabled*.

Strongly Recommended:

- S3 buckets used by **Copy to S3** should *not* be used by other applications.
- Versioning at the bucket level should be *disabled*.

Notes: Before continuing, consider the following:

- Copy to S3 currently supports only backups of Windows and Linux instances, and RDS. DynamoDB, etc. are not supported.
- Independent volumes will be supported in a future release.
- Most N2WS operations related to the S3 repository (e.g. writing objects to S3, clean up, restoring, etc.) are performed by launching N2WS worker instances in AWS. The worker instances are terminated when their tasks are completed.

### 21.1.1 Limitations

Only the copy of instance and RDS backups is supported.

- Copy to S3 is supported for weekly and monthly backup frequencies *only*. Daily backup copies to S3 are *not* supported.
- Copy is not supported for other AWS resources that N2WS supports, such as Aurora.
- Snapshots consisting of 'AMI-only' cannot be copied to an S3 repository.
- Due to AWS service restrictions in some regions, the root volume of instances purchased from Amazon Marketplace, such as instances with product code, may be excluded from Copy to S3. The data volumes of such instances, if they exist, will be copied.
- Backup records that were copied to S3 cannot be moved to Freezer.
- Users cannot delete specific snapshots from an S3 repository. S3 snapshots are deleted according to the retention policy. In addition, users can delete all S3 snapshots of a specific policy, account, or an entire repository. See below.
- A separate N2WS server, for example, one with a different "CPM Cloud Protection Manager Data" volume, cannot reconnect to an existing S3 repository.
- To use the Copy to S3 functionality the "cpmdata" policy must be enabled. See *N2WS User Guide* for details on enabling the "cpmdata" policy.
- Only a single S3 operation is possible on a policy at any given time. Additional executions of Copy to S3 backups will not occur if the previous execution is still running. Restore from S3 is always possible unless the backup itself is being cleaned up.
- AWS accounts have a default limit to the number of instances that can be launched. Copy to S3 launches extra instances as part of its operation and may fail if the AWS quota is reached. See *N2WS User Guide* for details.
- Copy and Restore of volumes to/from regions different from where the S3 bucket resides may incur long delays and additional bandwidth charges.
- Instance names may not contain slashes (/) or backslashes (\) or the copy will fail.



### 21.1.2 Cost Considerations

N2W Software has the following recommendations to N2WS customers for help lowering transfer and storage costs:

- Lowering transfer fees:
  - When an 'N2WSWorker' instance is using a public IP (or NAT/IGW within a VPC) to access an S3 bucket within the same region/account, it results in network transfer fees.
  - Using a VPC endpoint instead will enable instances to use their private IP to communicate with resources of other services within the AWS network, such as S3, without the cost of network transfer fees.
  - For further information on how to configure N2WS with a VPC endpoint, see section 26.

### 21.1.3 Overview of S3 and N2WS

The Copy to S3 feature is similar in many ways to the N2WS Disaster Recovery (DR) feature. When Copy to S3 is enabled for a policy, copying EBS snapshot data to S3 begins at the completion of the EBS backup, similar to the way DR works. Copy to S3 can be used simultaneously with DR feature.

### 21.1.4 Workflow for Using S3 with N2WS

1. Define an S3 Repository.
2. Define a Policy with a Schedule, as usual.
3. Configure the policy to include **Copy to S3** by selecting the **Lifecycle Management (Snapshot/S3/Glacier)** tab. Turn on the **Backup to S3** toggle and complete the parameters.
4. If you are going to back up and restore S3 instances and volumes across accounts and regions, prepare a Worker Configuration using the **Worker Configuration** tab. See section 22.
5. Use the **Backup Monitor** and **Recovery Monitor**, with some additional controls, to manage S3 snapshots as usual.

### 21.1.5 Workflow for Copying RDS to S3

1. In AWS, create an Export Role. See section 21.4.1.
2. Define an S3 Repository. See section 21.2.1.
3. In N2WS, add required permissions to user. See section 21.4.2.
4. Define a Policy with a Schedule, as usual, and enable **Export RDS**. See section 21.4.2.
5. Prepare a Worker Configuration using the **Worker Configuration** tab. See section 22.

## 21.2 The S3 Repository

The `cpmdata` policy must exist before configuring an S3 Repository.

### 21.2.1 Configuring an S3 Repository

There can be multiple repositories in a single AWS S3 bucket.

1. In N2WS, select the **S3 Repositories** tab.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories (highlighted), Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'S3 Repositories' and features a search bar, a dropdown for 'All Accounts', and a '20 records/page' selector. Below these is a table with columns: Name, Account, AWS Region, AWS S3 Bucket, and Policies. A single repository is listed with the name 'S3', account 'ACCOUNT-1', region 'us-east-1', and bucket 'cf-templates-5n0rtok60zb7-us-e...'. At the bottom, it indicates '0 of 1 items selected'.

2. Select **+ New**.

The screenshot shows the 'New S3 Repository' form in the N2WS Backup & Recovery (CPM) interface. The form includes fields for Name, Description, User (set to 'demo'), Account (set to 'ACCOUNT-1 (Backup)'), AWS Region (set to 'US East (N. Virginia)'), and S3 Bucket Name (set to 'avner-test-123'). At the bottom right, there are 'Save' and 'Cancel' buttons.

3. In the **New S3 Repository** screen, complete the following information:

- **Name** - Type a unique name for the new repository, which will also be used as a folder name in the AWS bucket. Only alphanumeric characters and the underscore are allowed.
- **Description** - Optional brief description of the contents of the repository.
- **User** – Select the user in the list.
- **Account** - Select the account that has access to the S3 bucket.
- **AWS Region** - Select the region in which the S3 bucket is located.
- **S3 Bucket Name** - Type the name of the S3 bucket that exists in this region.




Note: AWS encryption must have been enabled for the bucket.

4. When complete, select **Save**.

### 21.2.2 Deleting an S3 Repository

You can delete all snapshots copied to a specific S3 repository.

Note: Deleting a repository is not possible when the repository is used by a policy. You must change any policy using the repository to a different repository before the repository can be deleted.

1. Select the **Repositories** tab and then select a repository.
2. Select  **Delete**.

## 21.3 The S3 Policy

**Important:** To keep transfer fee costs down when using Copy to S3, create an S3 endpoint in the worker's VPC.

### 21.3.1 Configuring a Policy for Backup to S3


Configuring a Policy for Copy to S3 backups includes definitions for the following:

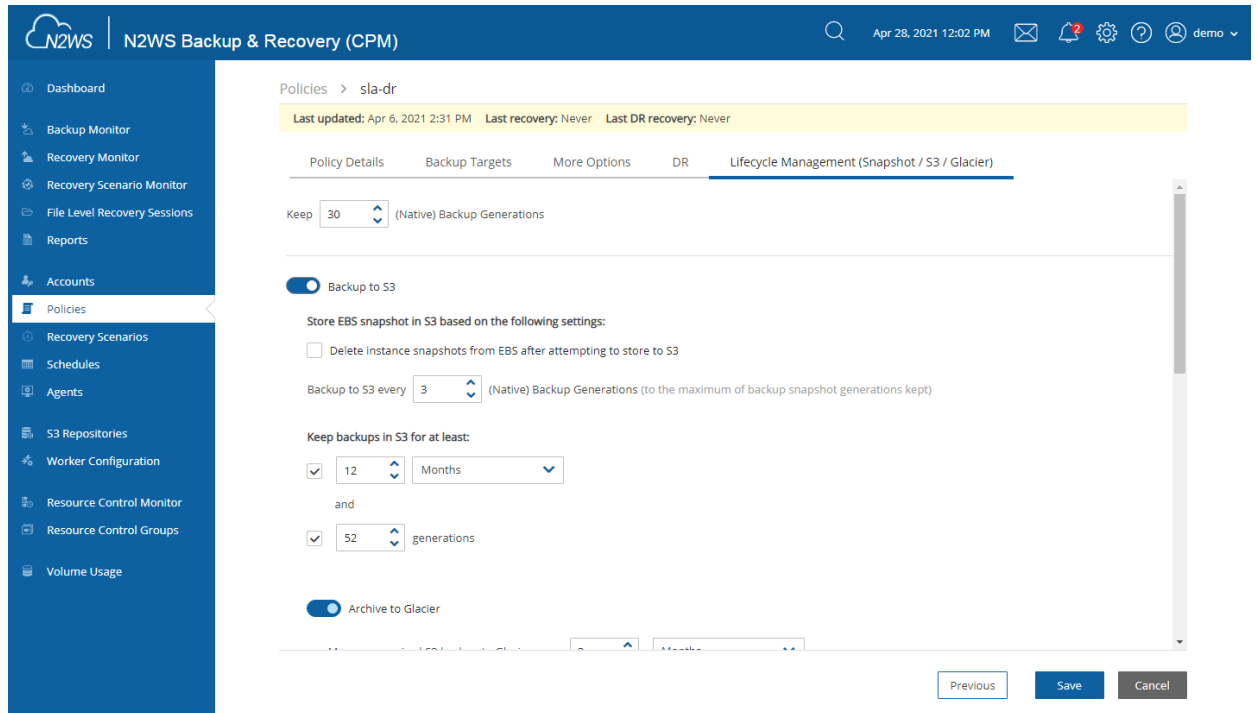
- Name of the S3 Repository defined in N2WS.
- Interval of AWS snapshots to copy.
- Snapshot retention policy. Selecting the **Delete instance snapshots from EBS after storing in S3** option minimizes the time that CPM holds any backup data in the EBS snapshots service. CPM achieves that by deleting any EBS snapshot immediately after copying it to S3.

It is possible to retain a backup based on both time and number of generations copied. If both Time Retention (**Keep backups in S3 for at least x time**) and Generation Retention (**Keep backups in S3 for at least x generations**) are enabled, both constraints must be met before old snapshots are deleted or moved to Glacier, if enabled.

For example, when the automatic cleanup runs:

- If Time Retention is enabled for 7 days and Generation Retention is disabled, S3 snapshots older than 7 days are deleted or archived. If **Run ASAP** is executed 10 times in one day, none of the snapshots would be deleted until they are more than 7 days old.
- If Generation Retention is enabled for 4 and Time Retention is disabled, the 4 most recent S3 snapshots are saved.
- If Time Retention is enabled for 7 days and Generation Retention is enabled for 4 generations, a single S3 snapshot would be deleted, or archived, after 7 days if the number of generations had reached 5.

1. In the left panel, select the **Policies** tab.
2. Select a Policy and then select  **Edit**.
3. Select the **Lifecycle Management** tab.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies (selected), Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Policies > sla-dr' and shows the 'Lifecycle Management (Snapshot / S3 / Glacier)' tab. The settings include: 'Keep' set to 30 (Native) Backup Generations; 'Backup to S3' toggle is turned on; 'Store EBS snapshot in S3 based on the following settings:' with a checkbox for 'Delete instance snapshots from EBS after attempting to store to S3' (unchecked); 'Backup to S3 every' set to 3 (Native) Backup Generations (to the maximum of backup snapshot generations kept); 'Keep backups in S3 for at least:' with a checkbox for '12 Months' (checked) and a checkbox for '52 generations' (checked); and 'Archive to Glacier' toggle is turned on. At the bottom right are 'Previous', 'Save', and 'Cancel' buttons.

4. Select the number of **(Native) Backup Generations** to keep in the list.
5. Complete the following fields:
  - **Backup to S3** – By default, Backup to S3 is disabled. Turn the toggle on to enable.
  - **Store EBS snapshots in S3 based on the following settings:**
    - **Delete instance snapshots from EBS after storing in S3** –If selected, N2WS will automatically set the **Backup to S3 every n (EBS) Backup Snapshot Generations** to 1 and will delete snapshots from EBS after performing the **Copy to S3** operation.  
 Note: When enabled, snapshots are deleted regardless of whether the **Copy to S3** operation succeeded or failed.
    - **Backup to S3 every n (EBS) Backup Snapshot Generations** – Select the maximum number of backup snapshot generations to keep. This number is automatically set to 1 if you opted to **Delete instance snapshots from EBS after storing in S3**.
6. In the **Keep backups in S3 for at least** lists, select the duration and/or number of backup generations to keep.
7. To **Archive to Glacier**, see section 21.4.
8. In the **Storage settings** section, choose the following parameters:
  - Select the **Target repository** in the S3 bucket to move the backup to, or select **+ New** to define a new repository. If you define a new repository, select **Refresh** before selecting.
  - Choose a **S3 Storage Class** that meets your needs:
    - **Standard** – (Frequent Access) - For frequent access and backups.
    - **Infrequent Access** – For data that is accessed less frequently.
    - **Intelligent Tiering** – Automatic cost optimization for S3 copy. Intelligent Tiering incorporates the Standard (Frequent Access) and Infrequent Access tiers. It monitors access patterns and moves objects that have not been accessed for 30 consecutive days to the Infrequent Access tier. If the data is subsequently accessed, it is automatically moved back to the Frequent Access tier.



Notes: Storage charges:

- S3 Infrequent Access and Intelligent Tiering have minimum storage duration charges.
- S3 Infrequent Access has a per GB retrieval fee.
- For more information about Amazon S3 Storage Classes, see <https://aws.amazon.com/s3/storage-classes/>.

9. If **Archive to Glacier** is enabled, select the **Archive Storage class**.

10. Select **Save**.

## 21.3.2 Recovering an S3 Backup

You can recover an S3 backup to the same or different regions and accounts.

If you **Recover Volumes Only**, you can:

- Select volumes and **Explore** folders and files for recovery.

**Note:** **Explore** fails on non-supported file systems. See section 13.1.

- Define Attach Behaviour
- Define the AWS Credentials for access
- Configure a Worker in the Worker Configuration tab
- Clone a VPC

If you recover an S3 **Instance**, you can specify the recovery encryption key:

- If **Use Default Volume Encryption Keys** is enabled, the recovered volumes will have the default key of each encrypted volume.
- If **Use Default Volume Encryption Keys** is disabled, all encrypted volumes will be recovered with the same key that was selected in the **Encryption Key** list.

**Note:** 'Marked for deletion' snapshots can no longer be recovered.

**Backup Monitor**

Search backups  by instance  All Policies  All Accounts  All Backup Statuses

20 records/page  Show:


me	Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle Status
2020 10:12 PM	Oct 26, 2020 10:35 PM	P3	ACCOUNT-3	✓ Successful		<input type="button" value="v"/> Storing to S3 (8%)
2020 10:12 PM	Oct 26, 2020 10:34 PM	P2	ACCOUNT-1	✓ Successful	✓ Completed	
2020 10:12 PM	Oct 26, 2020 10:36 PM	P1	ACCOUNT-1	✓ Successful		
2020 3:52 PM	Oct 25, 2020 3:54 PM	fsx	ACCOUNT-3	✓ Successful		
2020 2:12 PM	Oct 25, 2020 2:14 PM	P1	ACCOUNT-1	✓ Successful		
2020 11:03 AM	Oct 25, 2020 11:14 AM	P3	ACCOUNT-3	✓ Successful		✓ Stored in S3
2020 11:03 AM	Oct 25, 2020 11:14 AM	P2	ACCOUNT-1	✓ Successful	✓ Completed	
2020 11:03 AM	Oct 25, 2020 11:13 AM	P1	ACCOUNT-1	✓ Successful		
2020 11:03 AM	Oct 25, 2020 11:04 AM	CPMDATA	ACCOUNT-1	✓ Successful		
2020 1:37 PM	Oct 24, 2020 1:39 PM	P2	ACCOUNT-1	✓ Successful	✓ Completed	
2020 8:22 AM	Oct 22, 2020 8:24 AM	P2	ACCOUNT-1	✓ Successful	✓ Completed	

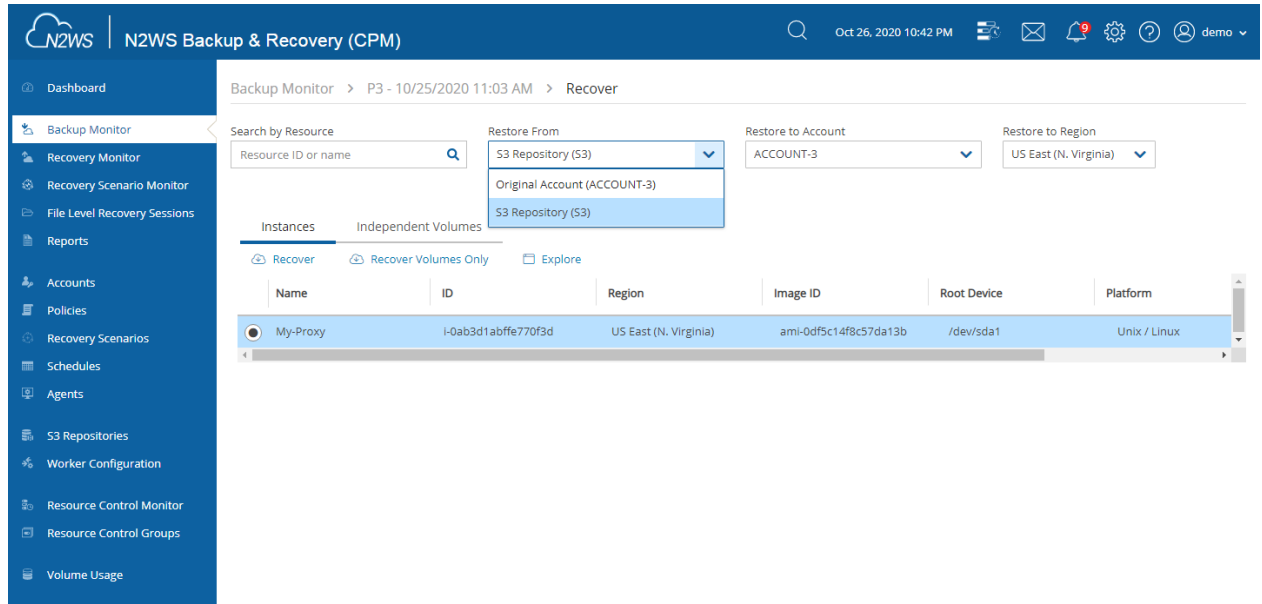
1 of 11 items selected






## To recover an S3 backup:

1. In the **Backup Monitor** tab, select a relevant backup that has a **Lifecycle Status** of '**Stored in S3**', and then select  **Recover**.
2. In the **Restore from** drop-down list of the **Recover** screen, select the name of the **S3 Repository** to recover from. If you have multiple N2WS accounts defined, you can choose a different target account to recover to.



Name	ID	Region	Image ID	Root Device	Platform
My-Proxy	i-0ab3d1abffe770f3d	US East (N. Virginia)	ami-0df5c14f8c57da13b	/dev/sda1	Unix / Linux

3. In the **Restore to Region** drop-down list, select the Region to restore the S3 copy to. The source Region of the S3 copy is displayed in the **Region** column.
4. Continue with the regular recovery procedure for the resource:
  - To recover an instance, see section 10.3.
  - To recover a volume, see section 10.4.
  - To recover folders or files, see section 13.
5. To follow the progress of the recovery, select **Open Recovery Monitor** in the 'Recovery started' message  **Recovery Started (Open Recovery Monitor)** at the top right corner, or select the **Recovery Monitor** tab.



6. To abort a recovery in progress, in the **Recovery Monitor**, select the recovery item and then select **Abort Recover from S3**.

**Note:** There may be occasions when you need to recover from S3 or retrieve S3 data while there is an active S3 archiving operation. In the **Policies** tab, select the active policy, and then select **Stop S3 / Archive Operation**.

### 21.3.3 Forcing a Single Full Copy

By default, Copy to S3 is performed incrementally for data modified since the previous snapshot was stored. However, you can force a copy of the full data for a single iteration to your S3 Repository. While configuring the **Backup Targets** for a policy with Copy to S3, select **Force a single full Copy**. See section 4.2.3.

**Note:** This option is only available for Copy to S3.

### 21.3.4 Changing the S3 Retention Rules for a Policy

You can set different retention rules in each Policy.

**To update the S3 retention rules for a policy:**

1. In the **Policies** column, select the target policy.
2. Select the **Lifecycle Management** tab.
3. Update the **Keep backups in S3 for at least** lists for time and generations, as described in section 21.3, and select **Save**.

## 21.4 The Export RDS to S3 Policy

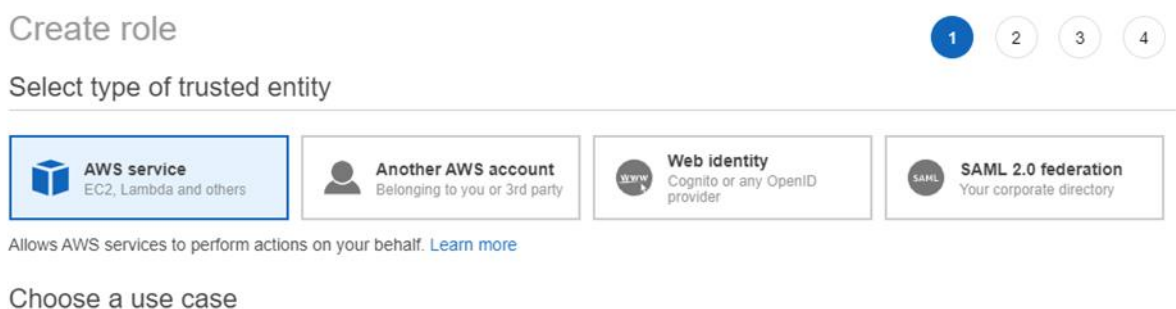
**Warning:** Export RDS to S3 is currently an experimental feature. It is strongly advised that **before** deleting any original snapshots you perform a test recovery and verification of the recovered data/schema.

### Limitations:

- Exporting RDS to S3 is currently not supported by AWS for Osaka and GOV regions.
- Default encryption keys for RDS export tasks are not supported.
- RDS Export to S3 is currently not supporting Shared CMK encryption keys.
- Cross region/account recoveries are not supported.
- Currently, only MySQL databases are supported for exporting RDS to S3.
- RDS Export to S3 is supported for databases residing in the same region where the S3 bucket is located.
- AWS export Parquet format might change some data, such as date-time.
- AWS does not support RDS export with stored procedure triggers.

### 21.4.1 Configuring an AWS Export Role

1. In AWS IAM Management Console, select Roles and then select Create role.
2. For the type of trusted entity, select AWS service.
3. In the **Create role** section, select the type of trusted entity: **AWS service**.



Create role

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 a use case

4. In the **Choose a use case** section, select **RDS**.



Or select a service to view its use cases

API Gateway	CloudWatch Events	EKS	IoT Things Graph	Redshift
AWS Backup	CodeBuild	EMR	KMS	Rekognition
AWS Chatbot	CodeDeploy	ElastiCache	Kinesis	RoboMaker
AWS Marketplace	CodeGuru	Elastic Beanstalk	Lake Formation	S3
AWS Support	CodeStar Notifications	Elastic Container Registry	Lambda	SMS
Amplify	Comprehend	Elastic Container Service	Lex	SNS
AppStream 2.0	Config	Elastic Transcoder	License Manager	SWF
AppSync	Connect	ElasticLoadBalancing	MQ	SageMaker
Application Auto Scaling	DMS	Forecast	Machine Learning	Security Hub
Application Discovery Service	Data Lifecycle Manager	GameLift	Macie	Service Catalog
Batch	Data Pipeline	Global Accelerator	Managed Blockchain	Step Functions
Braket	DataBrew	Glue	MediaConvert	Storage Gateway
Budgets	DataSync	Greengrass	Migration Hub	Systems Manager
Certificate Manager	DeepLens	GuardDuty	Network Firewall	Textract
Chime	Directory Service	Health Organizational View	OpsWorks	Transfer
CloudFormation	DynamoDB	Honeycode	Personalize	Trusted Advisor
CloudHSM	EC2	IAM Access Analyzer	Purchase Orders	VPC
CloudTrail	EC2 - Fleet	Inspector	QLDB	WorkLink
CloudWatch Alarms	EC2 Auto Scaling	IoT	RAM	WorkMail
CloudWatch Application Insights	EC2 Image Builder	IoT SiteWise	<b>RDS</b>	

- To add the role to the RDS database, in the **Select your use case** section, select **RDS – Add Role to Database**.

Select your use case

#### RDS

Allows RDS to perform operations using AWS resources on your behalf.

#### RDS - Add Role to Database

Allows you to grant RDS access to additional resources on your behalf.

#### RDS - Beta

Allows RDS to perform operations using AWS resources on your behalf in the Beta region.

#### RDS - CloudHSM

Allows RDS to manage CloudHSM resources on your behalf.

#### RDS - Directory Service

Allows RDS to manage Directory Service resources on your behalf.

#### RDS - Enhanced Monitoring

Allows RDS to manage CloudWatch Logs resources for Enhanced Monitoring on your behalf.

#### RDS - Preview

Allows RDS Preview to manage AWS resources on your behalf.

- In the Review screen, enter a name for the role and select **Create policy**.
- Create a policy, and add the following permissions to the JSON:

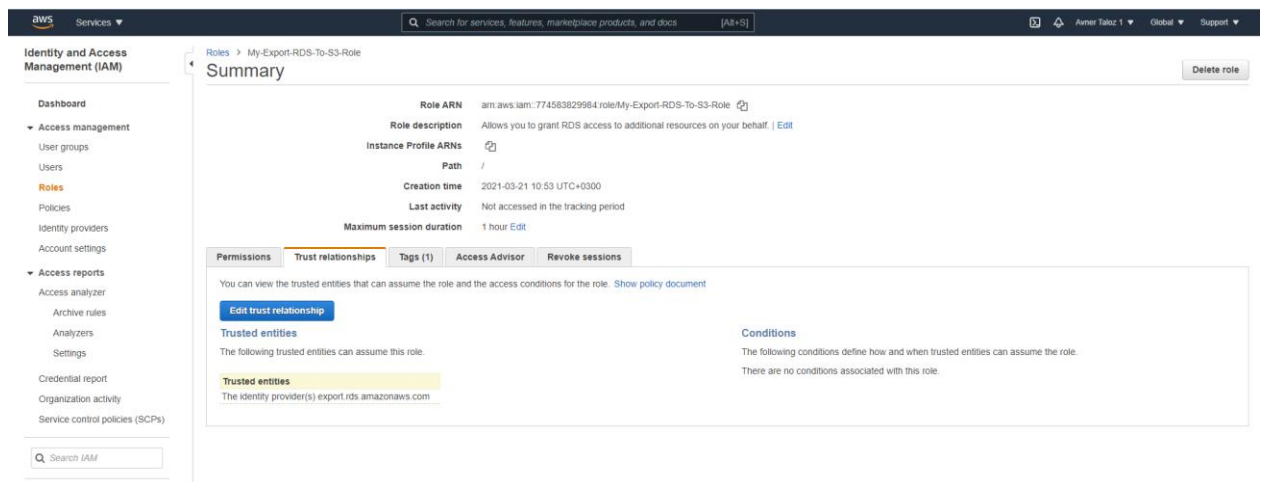
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
```

```

        "Sid": "ExportRDS",
        "Action": [
            "s3:PutObject*",
            "s3:GetObject*",
            "s3:ListBucket",
            "s3:DeleteObject*",
            "s3:GetBucketLocation"
        ],
        "Resource": [
            "*"
        ],
        "Effect": "Allow"
    }
]
}

```

8. After saving the role, in the **Trust relationships** tab:
  - a. Select **Edit trust relationship**.



The screenshot shows the AWS IAM console interface. On the left is a navigation menu with options like Dashboard, Access management, Users, Roles, Policies, etc. The main area displays the 'Summary' tab for the role 'My-Export-RDS-To-S3-Role'. Below the summary, there are tabs for 'Permissions', 'Trust relationships', 'Tags (1)', 'Access Advisor', and 'Revoke sessions'. The 'Trust relationships' tab is active, showing a list of trusted entities. A blue button labeled 'Edit trust relationship' is visible. The 'Conditions' section on the right indicates there are no conditions associated with this role.

- b. Edit the **Trust Relationship**.

**Note:** If there are multiple trust relationships, the code must be exactly as follows or the role will not appear in the **Export Role** list.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    },
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "export.rds.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}

```



```
}
```

9. To the CPM role policy, add the following required permissions under Sid “**CopyToS3**”.

- rds:StartExportTask
- rds:DescribeExportTasks
- rds:CancelExportTask

**Note:** If you want to use the CPM role as the ExportRDS role, you can use the CPM Role Minimal Permissions (<https://support.n2ws.com/portal/kb/articles/what-are-the-required-minimal-aws-permissions-roles-for-cpm-operation>) and also add the Trust Relationship.

## 21.4.2 Creating an N2WS Policy to Export RDS

1. Create a regular S3 policy as described in section 21.3.1 and select the RDS Database as the Backup Target.

**Note:**

- The RDS database security group must allow the default port 3306, or any non-default port the database is using, in the inbound rules.
- Connection parameters are required and must be valid for backup and recovery operations. If not specified, the database will not be copied to S3.

Add RDS Databases

Region:  
US East (N. Virginia)

Search resources

Refresh

<input checked="" type="checkbox"/>	DB Instance	Status	Multi AZ	Class	Storage (GiB)	Type	IOPS	Engine	Zone	Publicly Accessible
<input checked="" type="checkbox"/>	database-1	available	No	db.t2.micro	20	gp2	0	mysql	us-east-1b	No

1 of 1 items selected

Add selectedClose

2. In the **Lifecycle Management** tab:
- Turn on the **Backup to S3** toggle.
  - In the Storage settings section, select the **Target repository**.
  - In the Copy RDS to S3 section, select **Enable RDS Copy**.
  - In the **Export Role** list, select the AWS export role that you created.



- e. In the **Export KMS Key** list, select an export KMS encryption key for the role.

**Note:** The custom ARN KMS key must be on the same AWS account and region.

- f. Select **Save**.

Copy RDS to S3:

☒ Enable RDS Copy


Export Role

ExportRDSRole

Export KMS Key

Custom ARN

**Note:** Only roles that include the export RDS Trusted Service are displayed in the list.

3. In the **Backup Targets** tab, select the RDS Database and then select  **Configure**.
4. In the Policy RDS Copy to S3 Configuration screen, enter the following:
  - a. In the Database Credentials section, enter the database **User** name and **Password**.

**Note:** If the Credentials are left blank, a warning that the target will *not* be copied appears.

- b. Complete the Worker Configuration section.

**Note:**

- If the database is private, you must choose a VPC and subnet that will allow the worker to connect to the database.
- The policy can be saved *without* the complete configuration, but the copy will fail if the configuration is not completed before the policy runs.
- If the target is added using a tag scan, the **User** name, **Password**, and **Worker Configuration** must be added to the policy manually afterward.
- If the configuration is left blank, the target will *not* be copied, and a warning will appear in the backup log.

- c. Select **Apply**.



#### Policy RDS Copy To S3 Configuration

##### Database Credentials

User

admin

Password

••••••••••

##### Worker Configuration

Key Pair

nvirginia

VPC

vpc-1ce2db66 (Default)

Security Group

CPM\_SG

VPC Subnet

subnet-ef09e489 (default for us-east-1)

Network Access

Direct

Apply

Close

### 21.4.3 Recovering RDS from S3

**Note:** When recovering RDS to a different subnet group or VPC, verify that the source AZ also exists in the recovery target. If not, the recovery will fail with an invalid zone exception.

When recovering RDS from a native snapshot, using a different VPC and a subnet group that does not have a subnet in the target AZ, the recovery will also fail.

#### To recover an RDS database from S3:

1. In the **Backup Monitor**, select a backup and then select **Recover**.
2. In the Recover screen, select a database and then select **Recover**.
3. In the **Basic Options** tab, modify default values as necessary. Take into consideration any identified issues such as changing AZ, subnet, or VPC.
4. Select the **Worker Configuration** tab within the Recover screen.
5. Modify Worker values as necessary, making sure that the VPC, Security Group, and VPC Subnet values exist in the recovery target.
6. Select **Recover RDS Database**.





Recover RDS Database database-1

Basic Options Worker Configuration

Key Pair: my-key-pair VPC: vpc-5d093327 (default)

Security Group: ADV-320-CPMSecurityGroup-6QY0I3A VPC Subnet: subnet-da2181d4 (default for us-east-1)

Network Access: Direct

AWS Credentials: Use account AWS Credentials

Recover RDS Database Close

Follow the recovery process in the **Recovery Monitor**.

## 21.5 The Glacier Archive

### 21.5.1 Archiving Snapshots to S3 Glacier

Amazon S3 Glacier and S3 Glacier Deep Archive provide comprehensive security and compliance capabilities that can help meet regulatory requirements, as well as durable and extremely low-cost data archiving and long-term backup.

CPM allows customers to use the Amazon Glacier low-cost cloud storage service for data with longer retrieval times.

The CPM can now backup your data to a cold data cloud service on Amazon Glacier by moving infrequently accessed data to archival storage to save money on storage costs.

**Notes:** S3 is a better fit than AWS' Glacier storage where the customer requires regular or immediate access to data.

#### **Recommendations:**

- Use Amazon S3 if you need low latency or frequent access to your data.
- Use Amazon S3 Glacier if low storage cost is paramount, and you do not require millisecond access to your data.

### 21.5.2 Pricing

Following are some of the highlights of the Amazon pricing for Glacier:


- Amazon charges per gigabyte (GB) of data stored per month on Glacier.
- Objects that are archived to S3 Glacier and S3 Glacier Deep Archive have a minimum of 90 days and 180 days of storage, respectively.
- Objects deleted before 90 days and 180 days incur a pro-rated charge equal to the storage charge for the remaining days.

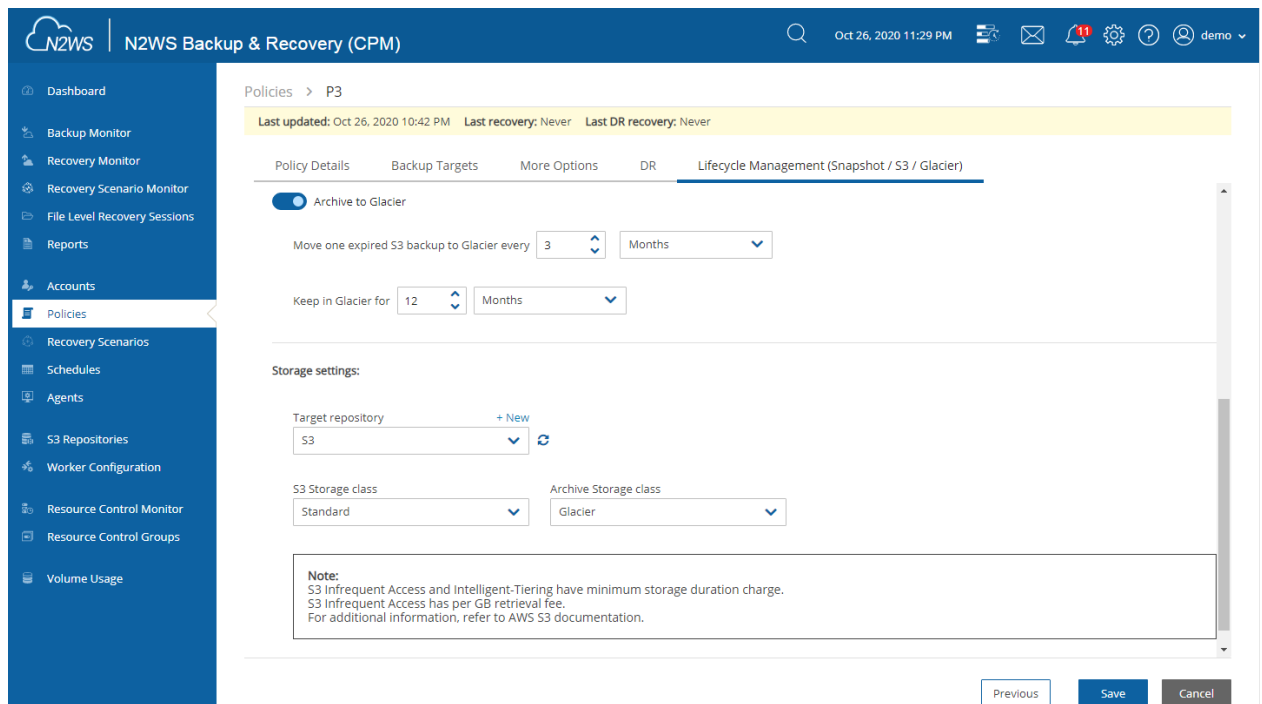


For more information about S3 Glacier pricing, refer to sections 'S3 Intelligent – Tiering' / 'S3 Standard-Infrequent Access' / 'S3 One Zone - Infrequent Access' / 'S3 Glacier' / 'S3 Glacier Deep Archive' at <https://aws.amazon.com/s3/pricing/>

### 21.5.3 Configuring a Policy to Archive to S3 Glacier

To configure archiving S3 backups to Glacier:

1. From the left panel, in the **Policies** tab, select a **Policy** and then select  **Edit**.
2. Select the **Lifecycle Management (Snapshot / S3 / Glacier)** tab. See section 21.3.
3. Follow the instructions for Backup to S3. See section 21.3.1.
4. Turn on the **Archive to Glacier** toggle.



5. Complete the following parameters:
  - **Move one expired S3 backup to Glacier every X period** – Select the frequency of archiving.
  - **Keep in Glacier for X period**– Select the duration of the archive in Glacier.

**Note:** The duration is measured from the creation of the original EBS snapshot, not the time of archiving.

6. Select the **Archive Storage class**:
  - **Glacier** - Designed for archival data that will be rarely, if ever, accessed.
  - **Deep Archive** - Solution for storing archive data that only will be accessed in rare circumstances.

### 21.5.4 Recovering Snapshots from Archive

Archived snapshots cannot be recovered directly from Glacier. The data must first be copied to S3 ('retrieved') before it can be accessed.



**Note:** The retrieving process only runs on objects that have never been retrieved. In other words, an archived snapshot can only be retrieved once.

The process of retrieving data from Archive to S3 is automatically and seamlessly managed by N2WS. However, to recover an archived snapshot, the user should specify the following parameters:


- Retrieval tier
- Days to keep

Duration and cost of Instance recovery are determined by the retrieval tier selected. Depending on the **Retrieval option** selected, the restore completes in:

- Expedited - 1-5 minutes
- Standard - 3-5 hours
- Bulk - 5-12 hours

**Note:** A typical instance backup that N2WS stores in Glacier is composed of many data objects and will probably take much longer than a few minutes.

#### To restore data from S3 Glacier:

1. Follow the steps for Recovering an S3 Backup. See section 21.3.2.
2. In the **Backup Monitor**, select a successful Glacier copy, and then select  **Recover**.
3. In the **Restore from** drop-down list, select 'Glacier'. N2WS will copy the data from Glacier to S3 and keep it for the expiration set in **Keep data in S3 for x days**.
4. In the **Restore to Region** list, select the target region.
5. Select a **Retrieval option** (Bulk, Standard, or Expedited) and then select **Retrieve**.

## 21.6 Monitoring Lifecycle Activities

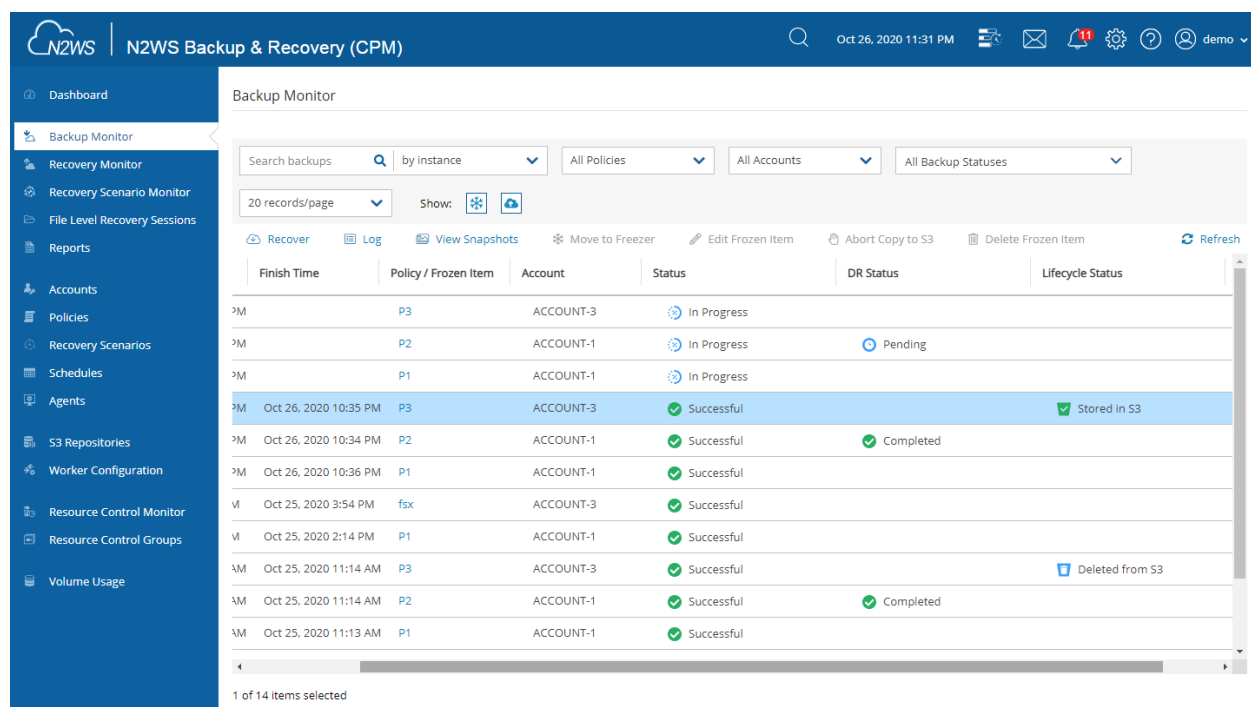
After a policy with Backup to S3 starts, you can:

- Follow its progress in the **Status** column the **Backup Monitor**.
- Abort the copy of snapshots to S3.
- Stop S3 and Archive operations.
- Delete S3 snapshots.

### 21.6.1 Viewing Status of Backups in S3 or Glacier

You can view the progress and status of S3 and archived backups in the **Backup Monitor**.

1. Select the **Backup Monitor** tab.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains navigation links: Dashboard, Backup Monitor (selected), Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main area displays the 'Backup Monitor' table with columns: Finish Time, Policy / Frozen Item, Account, Status, DR Status, and Lifecycle Status. The table shows various backup records, including those in progress, successful, and completed. The 'Lifecycle Status' column shows 'Stored in S3', 'Completed', and 'Deleted from S3'.

Finish Time	Policy / Frozen Item	Account	Status	DR Status	Lifecycle Status
PM	P3	ACCOUNT-3	In Progress		
PM	P2	ACCOUNT-1	In Progress	Pending	
PM	P1	ACCOUNT-1	In Progress		
PM Oct 26, 2020 10:35 PM	P3	ACCOUNT-3	Successful		Stored in S3
PM Oct 26, 2020 10:34 PM	P2	ACCOUNT-1	Successful	Completed	
PM Oct 26, 2020 10:36 PM	P1	ACCOUNT-1	Successful		
VI Oct 25, 2020 3:54 PM	fsx	ACCOUNT-3	Successful		
VI Oct 25, 2020 2:14 PM	P1	ACCOUNT-1	Successful		
VM Oct 25, 2020 11:14 AM	P3	ACCOUNT-3	Successful		Deleted from S3
VM Oct 25, 2020 11:14 AM	P2	ACCOUNT-1	Successful	Completed	
VM Oct 25, 2020 11:13 AM	P1	ACCOUNT-1	Successful		

2. In the **Lifecycle Status** column, the real-time status of an S3 Copy is shown. Possible lifecycle statuses include:

- Storing to S3 (n%)
- Stored in S3
- Not stored in S3 – Operation failed or was aborted by user.
- Archiving
- Archived
- Marked as archived – Some or all the snapshots of the backup were not successfully moved to Archive storage, either due to the user aborting the operation or an internal failure. However, the snapshots in the backup will be retained according to Archive retention policy, regardless of their actual storage.
- Marked for deletion – The backup was scheduled for deletion according to the retention policy and will be deleted shortly.

Note: 'Marked for deletion' snapshots can no longer be recovered.


- Deleted from S3/Archive – Snapshots were successfully deleted from either S3 or Archive.

## 21.6.2 Aborting a Copy to S3 'In Progress'

The Copy to S3 portion of a Policy backup occurs after the non-S3 backups have completed.


Note: Aborting an S3 Copy does not stop the non-S3 backup portion of the policy from completing. Only the Copy to S3 portion is stopped.

**To stop an S3 Copy in progress:**

1. In the **Backup Monitor**, select the policy.
2. When the **Lifecycle Status** is 'Storing to S3 ...', select  **Abort Copy to S3** Snapshots.





### 21.6.3 Stopping an S3 Cleanup in Progress

If an S3 retention Cleanup is 'In progress', in the **Policies** tab, select an S3 policy and then select  **Stop S3 / Archive Operations** to stop the Cleanup. See the Note in section 21 for the reasons you might want to stop the S3 Cleanup.

- Stopping S3 Cleanup does *not* stop the non-S3 cleanup portion of the policy from completing. Only the S3 cleanup portion is stopped.
- Stopping S3 Cleanup of a policy containing several instances will stop the cleanup process for a policy as follows:
  - N2WS will perform the cleanup of the current instance according to its retention policy.
  - N2WS will terminate all S3 Cleanups for the remainder of the instances in the policy.
  - N2WS will set the session status to **Aborted**.
  - N2WS user will get an 'S3 Cleanup of your policy aborted by user' notification by email.

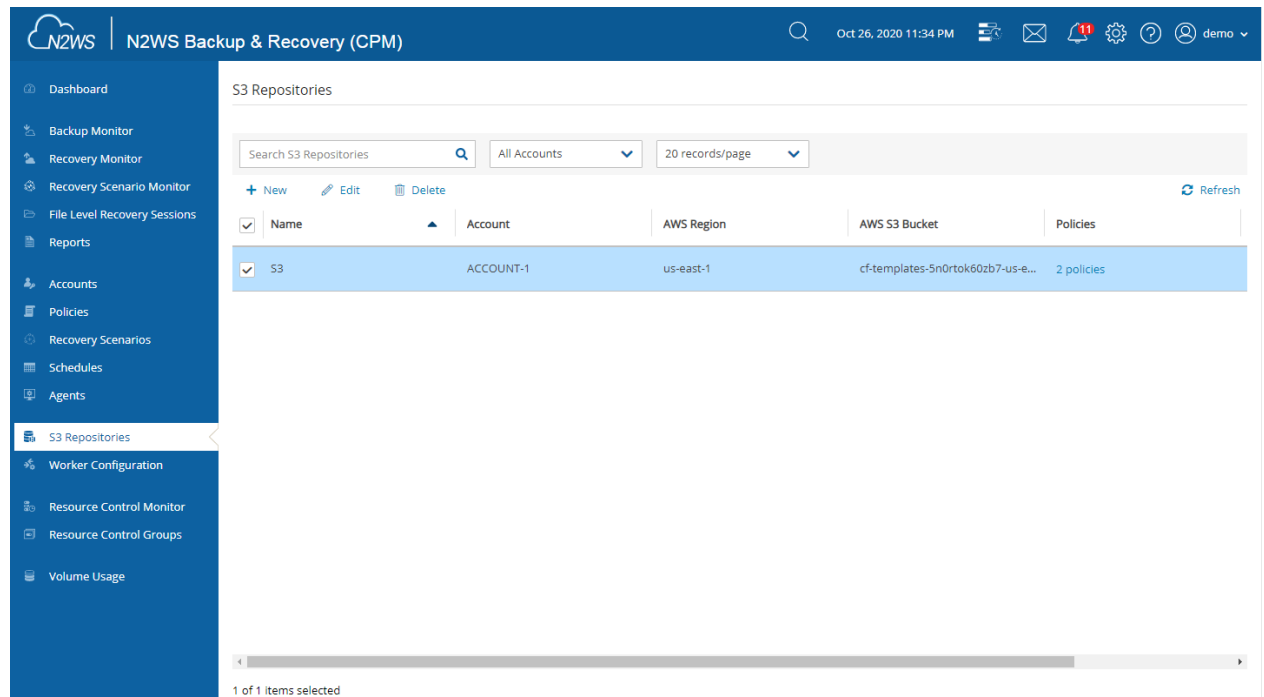
**To stop an S3 Cleanup in progress:**

1. Determine when the S3/Archiving is taking place by going to the **Backup Monitor**
2. Select the policy and then select  **Log**.
3. When the log indicates the start of the Cleanup, select  **Stop S3 /Archive Operations**.

### 21.6.4 Deleting Copy to S3 Snapshots in a Repository


**To delete only the snapshots copied to a specific S3 repository:**

1. Select the **S3 Repositories** tab.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The sidebar on the left contains navigation links: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories (selected), Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'S3 Repositories' and features a search bar, a dropdown for 'All Accounts', and a '20 records/page' dropdown. Below these are '+ New', 'Edit', and 'Delete' buttons. A table lists the repositories with columns: Name, Account, AWS Region, AWS S3 Bucket, and Policies. The first row, 'S3', is selected. At the bottom, it says '1 of 1 items selected'.

Name	Account	AWS Region	AWS S3 Bucket	Policies
S3	ACCOUNT-1	us-east-1	cf-templates-5n0rtok60zb7-us-e...	2 policies

2. Select a repository, and then select  **Delete**.



Note: When deleting Policies and **Snapshots** in the **Policies** tab or **Account and Data** in the **Accounts** tab, S3 copies are also deleted.



## 22 Configuring Workers

**Note:** Workers for recovery of RDS databases are *not* configured here but in the **Worker Configuration** tab of the RDS database Recover screen. See section 21.4.3.

When N2WS copies data to or restores data from an S3 repository, or **Explores** snapshots in a region other than that of the N2WS server, it launches a temporary ‘worker’ instance to perform the actual work, such as writing objects into S3 or exploring snapshots.

- When performing backup operations, or **Exploring** in a non-N2WS server region, the ‘worker’ instance is launched in the region and account of the target instance. The backup or **Explore** ‘worker’ instance is configured in the **Worker Configuration** tab.
- When performing restore operations, the ‘worker’ instance is launched in the region and account that the backed-up instances are to be restored to. The restore ‘worker’ instance is selected or configured according to the following criteria:
  - If a ‘worker’ for the target account/region combination was configured in the **Worker Configuration** screen, that ‘worker’ instance will be used during the restore or during the **Explore**.
  - If such a ‘worker’ does not exist for the target account/region combination, N2WS will attempt to launch one based on N2WS’s own configuration.
  - If the N2WS configuration cannot be used because the restore, or **Explore**, will be to a different account or region than N2WS’s, the user will be prompted during the restore to configure the ‘worker’.
- You can add tags to a worker for subsequent tracking in the AWS Cost Explorer.
  - To activate Cost Explorer in N2WS and AWS, see section 25.1.
  - To add worker tags, see section 22.2.

**Note:** If you plan to Copy to S3 only instances belonging to the same account and residing in the same region as that of the N2WS server, worker configuration is not required since the worker will derive its configuration from the N2WS server instance.

**Warning:** Attempts to perform S3/Glacier backup and restore operations from an account/region, or to **Explore** out of the N2WS server account/region, without a valid worker configuration will fail.

You can manage workers and their configurations as well as test their communication with the CPM, SSH, EBS API, and S3 Endpoint in the **Worker Configuration** tab (section 22.3).



Worker Configuration

Workers Configuration Worker Tags

+ New Edit Test Test Status Delete Refresh

Account	Region	Key Pair	VPC	Security Group	Subnet	Requires HTTP P
ACCOUNT-1	US East (Ohio)	ohio-new	vpc-744a811f	sg-fbd3fe9d	Any	No

## 22.1 Worker Parameters

It is necessary to define a *separate* worker configuration for *each* planned account/region combination of Copy to S3 instance snapshots, or each **Explore** region that is different from the N2WS server region.

**Important:** To keep transfer fee costs down when using Copy to S3, create an S3 endpoint in the worker's VPC.

**To configure S3 worker parameters:**

1. Select the **Worker Configuration** tab.
2. Select **+ New**.





3. In the **Account** list, select the Account that the new worker is associated with.
4. In the **Region** list, select a Region. This configuration will be applied to all workers launched in this region for this account.
5. In the **Key pair** list, select a key pair. Using the default, **Don't use key pair**, disables SSH connections to this worker.
6. In the **VPC** list, select a VPC. The selected VPC must be able to access the subnet where N2WS is running as well as the S3 endpoint.
7. In the **Security Group** list, select a security group. The selected security group must allow outgoing connections to the N2WS server and to the S3 endpoint.
8. In the **Subnet** list, select a subnet, or choose **Any** to have N2WS choose a random subnet from the selected VPC.

**Note:** If you choose '**Any**' in the **Subnet** drop-down list, N2WS will automatically choose a subnet that is in the same Availability Zone as the one you are restoring to. If you choose a specific subnet that is not in the same Availability Zone as the one you are restoring to, you will have to choose a different subnet from the **Subnet** drop-down list.

9. In the **Network Access** list, select a network access method.

**Note:** Direct network access or indirect access via an HTTP proxy is required:

- **Direct** - Select a Direct connection if no HTTP proxy is required.
- **via HTTP proxy** – If an HTTP proxy is required, select and fill in the proxy values.

10. Select **Save**.
11. Test the new worker (section 22.3).



**To edit or delete a worker configuration:**

1. In the **Worker Configuration** tab, select a worker.
2. Select **Delete** or **Edit**.

## 22.2 Worker Tags

You can add multiple tags to each account for workers for subsequent monitoring of cost and usage in the AWS Cost Explorer. When the worker is launched during Copy to S3, Recover S3, file-level recovery, or worker test, you will be able to filter for the N2WS worker tags in the **Tags** tab of the AWS **Cost Explorer**. To activate your worker tags, see section 22.2.1.

**To add worker tags:**

1. In the **Worker Configuration** tab, select a worker and then select the **Worker Tags** tab.
2. Select **+ New**, and enter the **Tag Name** and **Value**. The **Value** may be blank.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The 'Worker Configuration' section is active, and the 'Worker Tags' tab is selected. The 'User' field is set to 'demo' and the 'Account' field is set to 'ACCOUNT-1'. Below these fields, there is a table for adding tags. The table has two columns: 'Tag Key' and 'Tag Value'. A new tag is being added with the key 'AAAA' and the value 'BBBB'. The 'Save' button is visible at the bottom right.

3. Select **Save**.

### 22.2.1 Configuring AWS to Allow CPM Cost Explorer Calculations

To allow CPM Cost Explorer calculations in AWS, users must add cost allocation tags *once*.

**To activate user cost allocation tags:**

1. Log in to the AWS Management Console at <https://console.aws.amazon.com/billing/home#/> and open the Billing and Cost Management console.
2. In the navigation pane, select **Cost Allocation Tags**.
3. Choose the worker tags to activate.
4. Select **Activate**.



Note: It can take up to 24 hours for tags to activate.

For complete details, see


<http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html>.

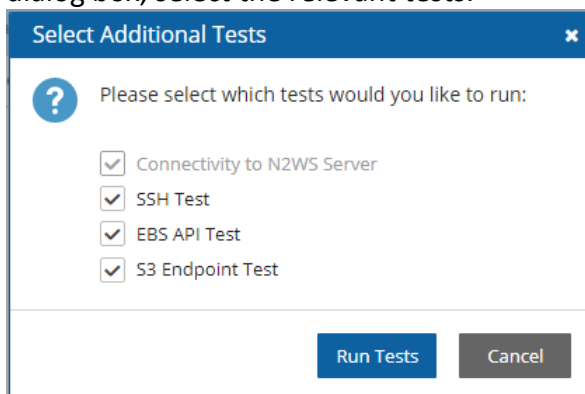
## 22.3 Testing the Configuration for a Worker




Before a worker is needed, you can test whether it successfully communicates with the N2WS server and other communication targets. Depending on the test, some, but **not all**, AWS permissions are also checked.

- Connectivity to N2WS Server (default)
- SSH Test – Connectivity to N2WS server using SSH
- EBS API Test – Test API connectivity and check AWS **ebs:ListSnapshotBlocks** permission
- S3 Endpoint Test – Test connectivity; check AWS **s3:ListAllMyBuckets** and **s3:ListBucket** permissions

To test a worker configuration:

1. Select a worker, and then select  **Test**.
2. If you want to test connections in addition to the worker, in the Select Additional Tests dialog box, select the relevant tests.



3. Select **Run Tests**. The 'Worker Configuration test is underway' message briefly appears at the top right and the  'In Progress' message appears in the **Test Status** column.
4. Check the results in the **Test Status** column: Successful or Failed.
5. If *not* 'Successful':
  - a. Select  **Test Status** to display information about the root cause.
  - b. To check settings, select  **Edit**.

Besides the requested connectivity tests, the Configuration Test Details include Account, Region, Zone, Key Pair, VPC, Security Group, and whether an HTTP Proxy was required.



Configuration Test Details	
Connectivity to worker	✓ Successful
SSH Test Status	✓ Successful
EBS API Test Status	✓ Successful
S3 Endpoint Test Status	✓ Successful
Session Start	January 13, 2021 10:37 PM
Session End	January 13, 2021 10:40 PM
Account	a
Region	US East (Ohio)
Zone	Any
Key Pair	None
VPC	vpc-744a811f
Security Group	sg-fbd3fe9d
Requires HTTP Proxv	No
Close	

To view and download the latest log, select **Test Log**.

Workers Configuration Last Test Log			Download Log	Refresh
Time	Level	Message		
12/17/2020 8:31:14 PM	✓ Info	Worker will run following internal test(s): SSH test EBS API test S3 Endpoint test		
12/17/2020 8:31:14 PM	✓ Info	launching worker for TEST in region us-west-2, zone Any		
12/17/2020 8:31:16 PM	✓ Info	worker i-0be66ad054eb0dea3 launched successfully in us-west-2c as t3.micro		
12/17/2020 8:34:45 PM	✓ Info	Worker Configuration for Account - demo-account_1, Region US West (Oregon), tested successfully with worker instance i-0be66ad054eb0dea3		
12/17/2020 8:34:47 PM	✓ Info	SSH test succeeded		
12/17/2020 8:34:49 PM	✓ Info	EBS API test succeeded		
12/17/2020 8:34:50 PM	✓ Info	S3 Endpoint test succeeded		
12/17/2020 8:34:53 PM	✓ Info	Terminating worker		
			Close	



## 23 Capturing and Cloning in VPC Environments

**Note:** VPC support is not available with the Free edition of N2WS.

### 23.1 Overview of VPC and N2WS

VPC is an AWS service that allows the definition of virtual networks in the AWS cloud. Users can define VPCs with a network range, define subnets under them, security groups, Internet Getaways, VPN connections, and more. One of the resources of the VPC service is also called 'VPC', which is the actual virtual, isolated network.

N2WS can capture the VPC settings of user environments and clone those settings back to AWS:

- In the same region and account, for example, if the original settings were lost.
- To another region and/or account, such as in DR scenarios.
- With VPC resource properties modified in template uploaded with CloudFormation, if required.

Once enabled from **General Settings**, N2WS will automatically capture VPC settings at pre-defined intervals, such as for cleanup and tag scanning. The root/admin user can enable the feature in the **Capture VPC** tab of the **General Settings** screen and set the interval of VPC captures. VPC settings are enabled at the account level, by default, same as tag scanning. Because VPC configuration metadata is small, VPC does not consume a lot of resources during storage of the capture. Metadata is captured incrementally. If nothing changed since the last capture, the metadata will not be captured again. This is the most common case in an ongoing system, where defined networks do not change frequently.

- **Regions** - N2WS will only capture VPC settings in regions that include backed-up resources. If the customer is not backing up anything in a specific region, N2WS will not try to capture the VPC settings there.
- **Retention** - N2WS will retain the VPC data as long as there are backups requiring it. If N2WS still holds backups from a year ago, the VPC version relevant for that time is still retained. Once there are no relevant backups, N2WS will delete the old VPC captured data.
- **CloudFormation** - N2WS will use the AWS CloudFormation service to clone VPCs to an AWS account. N2WS will create a CloudFormation template with the definitions for the VPC and use the template to launch a new stack and create all the VPC settings in one operation.

### 23.2 Features of Capturing and Cloning VPCs

The objective of Capture and Clone is to provide the ability to protect VPCs from disaster, by saving VPC configurations and allowing for recovery in any region.

- Backed up VPC entities include:
  - VPC resource configuration
  - Subnets - N2WS tries to match AZs with similar names and spread subnets in destinations in the same way as in source regions.
  - Security groups
  - DHCP Options Sets - Not supporting multi-name in domain server name.



- Route tables - Not supporting rules with entities that are specific to the source region.
- Network ACLs
- Internet Gateways, Egress Internet Gateways
- VPN Gateways

**Note:** The **Capture Log** in the **Capture VPC** tab of **General Settings** reports entities not captured or only partially captured.

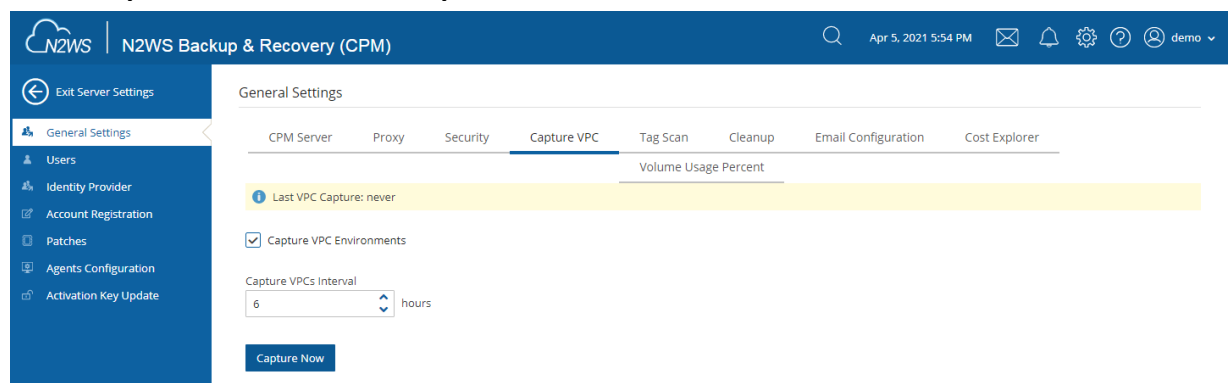
- VPC capturing:
  - Accounts are enabled for VPC capturing by default, but this setting can be disabled as needed.
  - Captures in all regions of interest.
  - N2WS will capture and save all changes made on AWS for a user's VPCs.
  - Not supported: NAT gateways, VPC peering connections, customer gateways, VPN connections, Network interfaces, Elastic IP addresses, VPC Endpoints, VPC Endpoints services, Transit Gateways
- VPC cloning:
  - Every Account that has a VPC captured in a region can clone a version of the VPC to any destination, region, and account.
  - The subnets of the cloned VPC will be located in the destination's Availability Zone with respect to their availability in the region.
  - Users can download a template of VPC resources to manually configure and load it with AWS CloudFormation.

## 23.3 Configuring VPC Capturing

The root user can:

- Enable or disable automatic VPC captures for Accounts that are VPC-enabled.
- Schedule automatic capture interval.
- Initiate an ad hoc capture by selecting **Capture Now** for all VPC-enabled Accounts, even if VPC is disabled in **General Settings**.
- View the last captured VPCs in the different regions and accounts in **Capture Log**.

1. Select  **Server Settings** > **General Settings**.
2. In the **Capture VPC** tab, select **Capture VPC Environments** to enable the feature.



3. To change the capture frequency from the default, select a new interval from the **Capture VPCs Interval** list. Valid choices are from every hour to every 24 hours.




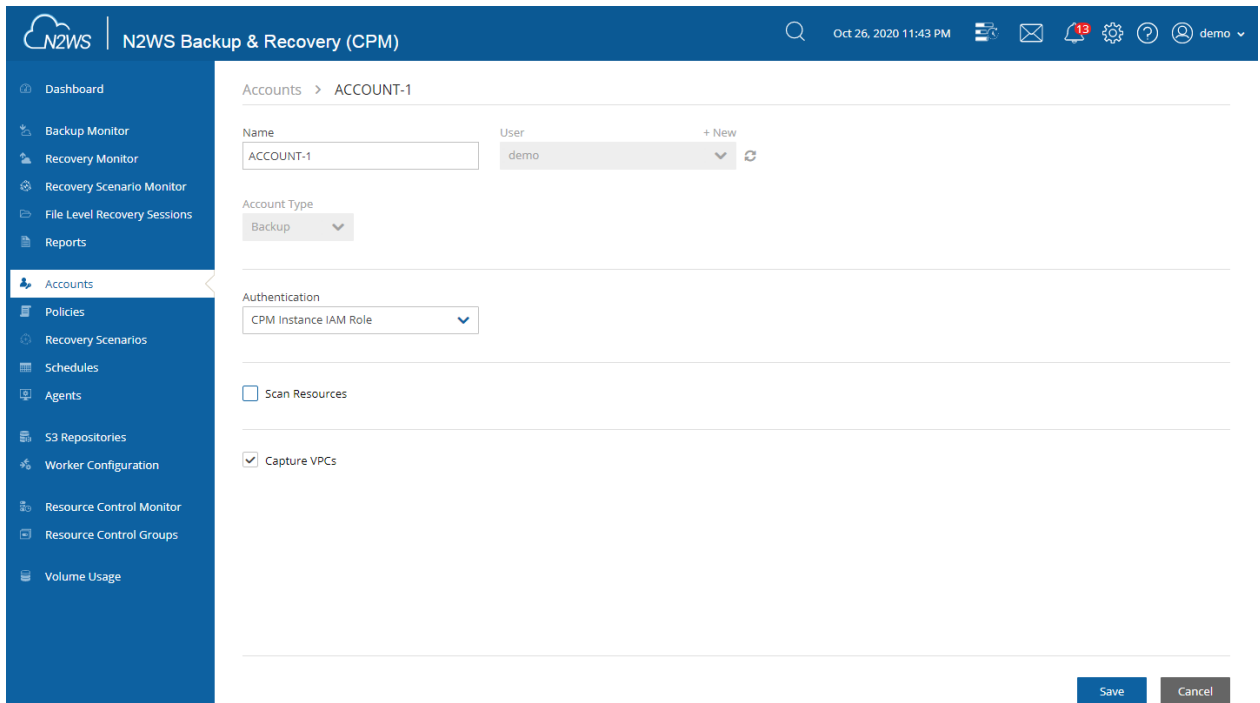
4. Select **Save** to update N2WS.
5. To initiate an immediate capture for all VPC-enabled Accounts regardless of server setting, select **Capture Now**.

## 23.4 Updating Accounts for VPC

By default, Accounts are enabled to Capture VPCs. VPCs are automatically captured for all enabled Accounts according to the interval configured in the **General Settings**. To not capture VPCs for an Account, disable the feature in the Account.

**To disable, or enable, an individual account for capturing VPCs:**

1. Select the **Accounts** tab and then select an Account.
2. Select  **Edit**.
3. Select **Capture VPCs** to enable, or clear **Capture VPCs** to disable.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts (selected), Policies, Recovery Scenarios, Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Accounts > ACCOUNT-1'. It contains the following fields: Name (ACCOUNT-1), User (demo), Account Type (Backup), Authentication (CPM Instance IAM Role), Scan Resources (unchecked), and Capture VPCs (checked). At the bottom right, there are 'Save' and 'Cancel' buttons.

4. Select **Save**.

## 23.5 Cloning VPCs

The following entities are not supported:

- Cloning CIDR block IPV6 on a subnet.
- Inbound and Outbound Endpoint rules of Security Groups.
- Inbound and Outbound rules of Security Groups that refer to a security group on a different VPC.
- Route Table rules with NAT Instance as target.
- Route Table rules with NAT Gateway as target.
- Route Table rules with Network Interface as target.
- Route Table rules with VPC peering connection as target.
- Route Table rules with status 'Black Hole'.



**Note:** A VPC-enabled account must have at least one policy with a backup target to clone VPCs.


Cloning VPCs includes the following features:

- Both cross-region and cross-account cloning are supported.
- The target clone can have a new name. The name will automatically include '(cloned)' at the end.
- During instance recovery and DR, clones may be optionally created to replicate a particular VPC environment before the actual instance recovery proceeds. The new instance will have the environment of the cloned VPC and will subsequently appear at the top of the target region and account list. A typical scenario might be to capture the VPC, clone the VPC for the first instance, and then apply the cloned VPC to additional instances in the region/account.
- Instances recovered into a cloned VPC destination environment will also have new default entities, such as the VPC's subnet definition and 1 or more security groups attached to the instance, regardless of the original default entities. Security groups can be changed during recovery.

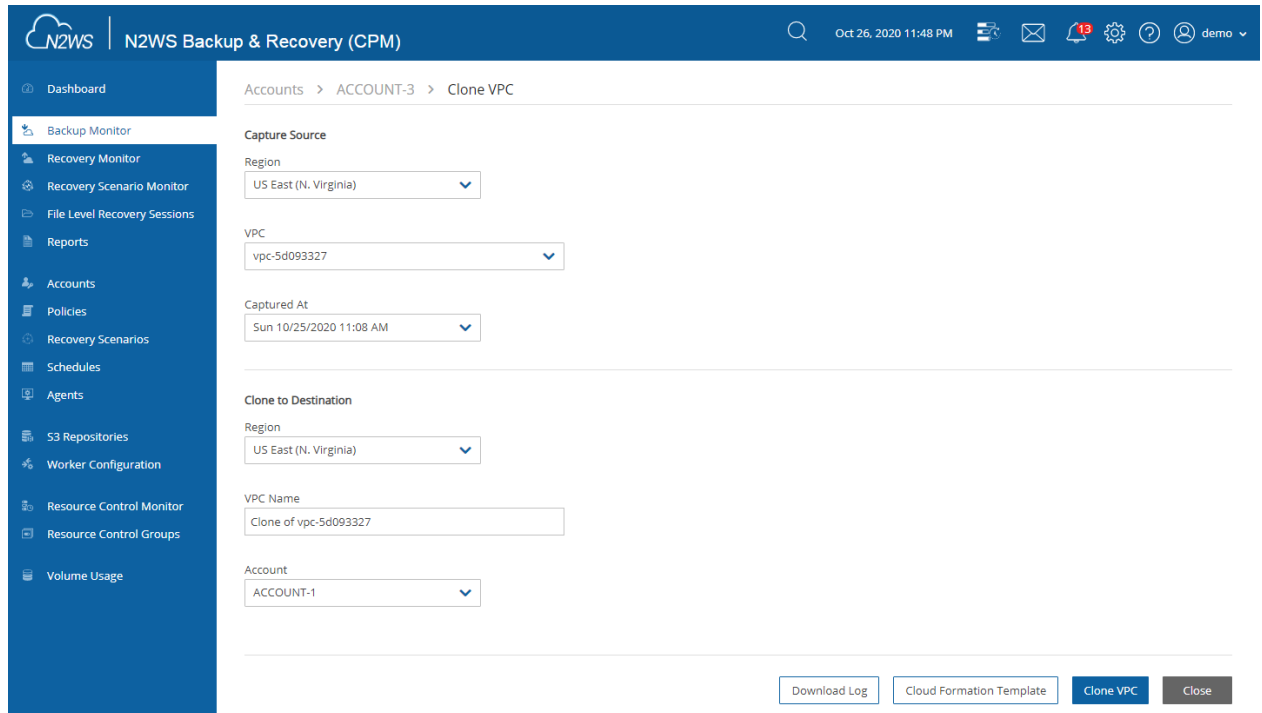
When cloning VPCs to an AWS account, N2WS generates a JSON template for use with CloudFormation.

- If the size of the CloudFormation template generated will be over 50 kB, N2WS requires the use of an existing S3 Bucket in the target destination for storing the template. **There should be an S3 bucket for each combination of accounts and regions in the destination clone.** The template file in a S3 bucket will not be removed after cloning.
- In addition to having a bucket in the target region in the presented settings, you must choose that bucket when defining where to **Upload the CF template to S3.**

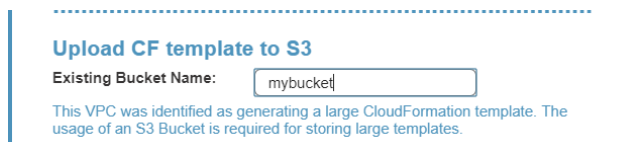
**To clone captured VPCs:**

1. Select the **Accounts** tab and then select an account.
2. Select  **Clone VPC.**





3. In the **Capture Source Region** drop-down list, select the source region of the capture to clone.
4. In the **VPC** drop-down list, select the VPC to clone.
5. In the **Captured at** drop-down list, select the date and time of the capture to clone.
6. In the **Clone to Destination Region** drop-down list, select the region to create the clone.
7. In the **VPC Name** box, a suggested name for the VPC is shown. Enter a new VPC name, if needed.
8. In the **Account** drop-down list, select the account in which to create the clone.
9. If the CF template is over 50 kB, select **CloudFormation Template** to download a JSON file with cloning information.



- a. In the Upload CF template to S3 dialog box, enter the **Existing Bucket Name** of a bucket that is located in the selected target region.
10. Select **Clone VPC**. At the end of the cloning, a status message will appear in a box:
  - VPC was Cloned. There may be an informational message that you may need to make manual changes. Check the log for further information.
11. To view the results of the clone VPC action, select **Download Log**.

When cloning VPCs with resources not supported by N2WS, you can download the CloudFormation template for the VPC, add or modify resource information, and upload the modified template to CloudFormation manually.

#### To create a clone manually with CloudFormation:

1. In the **Account Clone VPC** screen, complete the fields as described above.
2. Select **CloudFormation Template** to download the CloudFormation JSON template.



3. Modify the template, as required. See the example in section 23.5.1.
4. Manually upload the modified template with CloudFormation.

### 23.5.1 Example of CloudFormation Template

```
{'AWSTemplateFormatVersion': '2010-09-09',
  'Description': 'Template created by N2WS',
  'Resources': {'dopt4a7bcf33': {'DeletionPolicy': 'Retain',
    'Properties': {'DomainName': 'ec2.internal',
      'DomainNameServers': ['AmazonProvidedDNS']},
    'Type': 'AWS::EC2::DHCPOptions'},
    'dopt4a7bcf33vpc9d4bcbe6': {'DeletionPolicy': 'Retain',
      'Properties': {'DhcpOptionsId': {'Ref':
        'dopt4a7bcf33'},
        'VpcId': {'Ref': 'vpc9d4bcbe6'}},
      'Type': 'AWS::EC2::VPCDHCPOptionsAssociation'},
    'sgcd8af6bb': {'DeletionPolicy': 'Retain',
      'Properties': {'GroupDescription': 'default VPC security
group',
        'GroupName': 'default-0',
        'SecurityGroupEgress': [{ 'CidrIp': '0.0.0.0/0',
          'IpProtocol': '-1'}],
        'SecurityGroupIngress': [],
        'Tags': [{ 'Key': 'cpm:original:GroupId',
          'Value': 'sg-cd8af6bb'}],
        'VpcId': {'Ref': 'vpc9d4bcbe6'}},
      'Type': 'AWS::EC2::SecurityGroup'},
    'vpc9d4bcbe6': {'DeletionPolicy': 'Retain',
      'Properties': {'CidrBlock': '10.0.0.0/24',
        'EnableDnsHostnames': false,
        'EnableDnsSupport': true,
        'InstanceTenancy': 'default',
        'Tags': [{ 'Key': 'Name',
          'Value': 'Public-VPC-for-CF'},
          { 'Key': 'cpm:capturetime',
            'Value': 'Aug 22, 2018 16:15'},
          { 'Key': 'cpm:clonetime',
            'Value': 'Aug 25, 2018 21:20'},
          { 'Key': 'cpm:original:VpcId',
            'Value': 'vpc-9d4bcbe6'},
          { 'Key': 'cpm:original:region',
            'Value': 'us-east-1'}]},
      'Type': 'AWS::EC2::VPC'}}
```



## 24 Orchestrating Recovery Scenarios

### 24.1 Overview

The Recovery Scenarios feature allows N2W Software users to design an object that will automatically coordinate a sequence of recoveries for several or all backup targets of a single policy during one recovery session.


- A Recovery Scenario object is created with the saved configurations of successful backups for the particular policy.
- The user will save the recovery configuration for each selected backup target and add it to the Recovery Scenario object.
- At runtime, the user selects a successful backup record to use in the recovery.

Following are the options for executing a Recovery Scenario:

- Test the success of the Recovery Scenario configuration using the **Dry Run** command.
- Execute an ad hoc run of the Recovery Scenario using the **Run Scenario** command.
- Execute the Recovery Scenario on a schedule. The last successful backup is automatically selected as input. Assign or create a schedule in the **Recovery Scenario Details** tab.

**Note:** Backups in the Freezer are not recoverable as part of a Recovery Scenario.

### 24.2 Conditions

- During the Recovery Process:
  - All Recovery Scenario targets share the same destination account and destination region, which are set as part of the Recovery Scenario parameters.
  - Recovery Scenarios can have pre and post-scripts which will run, respectively, before recovery execution and subsequent to recovery completion.
    - In case of a pre-script failure, the Recovery Scenario will not execute.
    - In case of a Recovery Scenario failure or pre-script failure, the post-script will not run.
- Every Recovery Scenario target has a sequential **Recovery Order** value within the Recovery Scenario which determines the order in which each target is recovered.
  - Execution of a target recovery within the recovery scenario is sequenced using the target's **Recovery Order** value. The target with the lowest **Recovery Order** value runs first.
  - All recovery targets sharing the same **Recovery Order** value will run in an arbitrary sequence.
  - If the recovery of a target fails, the targets next in sequential order will not run, unless Recovery Scenario's **Continue recovering ignoring failures** parameter is enabled.
  - Testing: You can verify the Recovery Scenario input parameters, such as key pair, security groups, and VPC, by selecting  **Dry Run**. You will be prompted to select a successful backup for the **Dry Run** just as with an actual **Run Scenario**.



## 24.3 Creating a Recovery Scenario

**Note:** Be sure to execute a successful Dry Run of the Recovery Scenario before assigning a schedule.

**To add the details for a recovery scenario:**

1. Select the **Recovery Scenarios** tab.

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with the following items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios (selected), Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled "Recovery Scenarios" and includes a search bar, filters for All Accounts, All Policies, and All Schedules, and a "20 records/page" dropdown. Below these are buttons for + New, Edit, Run Scenario, Dry Run, and Delete, along with a Refresh button. A table lists the following scenarios:

Name	Policy	Account	Destination Account	Destination Region	Target Count
<input type="checkbox"/> rs-vols	P2	ACCOUNT-1	Original Account	Original Region	1 Volume
<input type="checkbox"/> rs-win	windows-vss-backup	ACCOUNT-1	Original Account	Original Region	1 Instance

At the bottom, it indicates "0 of 2 items selected".

2. Select **+ New**.


The screenshot shows the "Create Recovery Scenario" form in the N2WS Backup & Recovery (CPM) interface. The left sidebar is the same as in the previous screenshot. The main content area is titled "Recovery Scenarios > Create Recovery Scenario" and has two tabs: "Recovery Scenario Details" (selected) and "Recovery Targets". The form fields are as follows:

- Name:
- User:  + New
- Account:  + New
- Policy:  + New
- Description:
- Recovery Destination Account:
- Recovery Destination Region:
- Schedule:  + New

At the bottom right, there are "Save" and "Cancel" buttons.

3. In the **Recovery Scenario Details** tab, complete the fields as follows:



- **Name** – Enter a unique name.
- **User, Account, Policy** - Select from the lists or select **+ New**. After the addition, select  **Refresh**. Select the policy for which the Recovery Scenario is defined.
- **Recovery Destination Account** and **Recovery Destination Region** – Select from the lists.
- **Schedule** – Optionally select a schedule from the list, or select **+ New** to create a new schedule, for running the Recovery Scenario.
- **Recipients** – Enter the email addresses of users to receive notification of Recovery Scenario **Run Scenario** / **Dry Run** status.

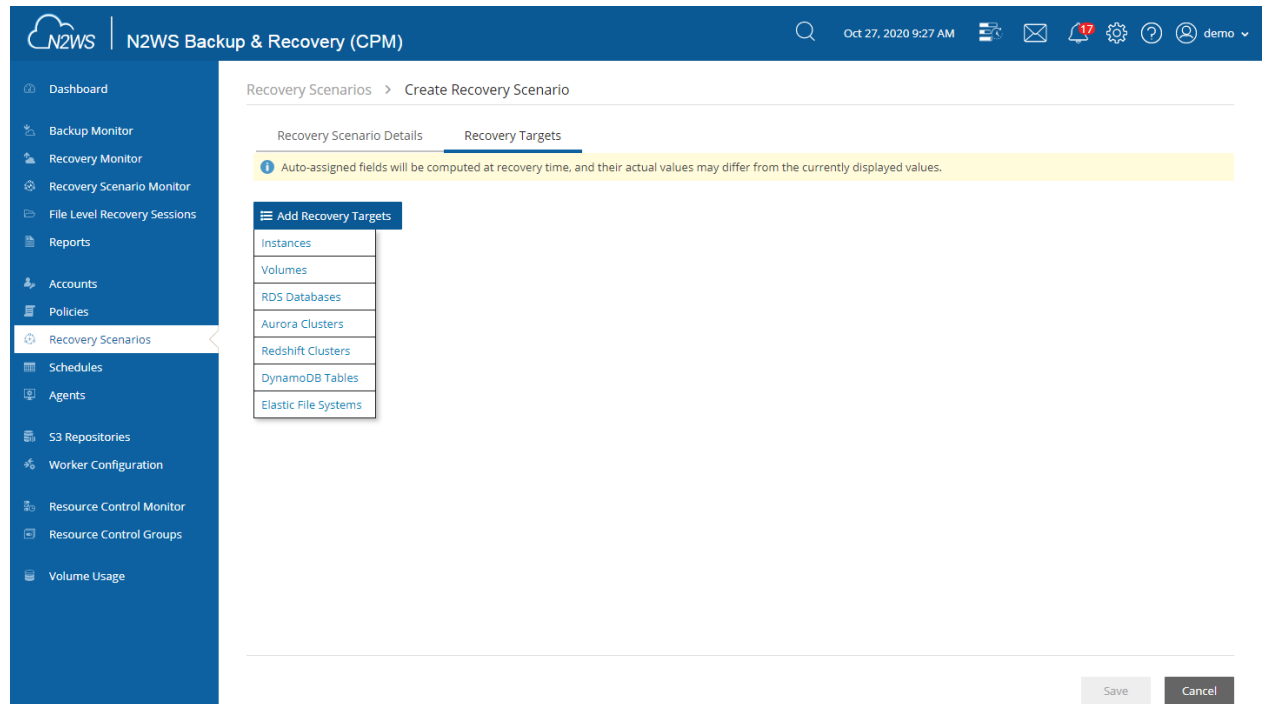
Note: If SES is disabled, emails are not sent.

- **Enable Agent Scripts** – Select if the Recovery Scenario will be run by a custom script. The default is *not* to run user scripts. See section 24.7.
  - Select **Agent Script Timeout** in seconds from the list. When the timeout is reached, N2WS will skip the script and continue with the recovery scenario.
  - **Collect Script Output** – Whether to collect script output in a log. Default is to collect.
- **Continue recovering ignoring failures** – Whether to continue the sequence of recoveries in the scenario if there is a failure. The default is to not continue the script on the failure of recovery.

4. Select **Save**.

### To add the recovery targets:

1. Select the **Recovery Targets** tab.



The screenshot shows the N2WS Backup & Recovery (CPM) interface. The top navigation bar includes the N2WS logo, the title 'N2WS Backup & Recovery (CPM)', a search icon, the date 'Oct 27, 2020 9:27 AM', and various system icons. The left sidebar contains a list of navigation items: Dashboard, Backup Monitor, Recovery Monitor, Recovery Scenario Monitor, File Level Recovery Sessions, Reports, Accounts, Policies, Recovery Scenarios (selected), Schedules, Agents, S3 Repositories, Worker Configuration, Resource Control Monitor, Resource Control Groups, and Volume Usage. The main content area is titled 'Recovery Scenarios > Create Recovery Scenario'. It has two tabs: 'Recovery Scenario Details' and 'Recovery Targets' (selected). A yellow banner at the top of the 'Recovery Targets' tab states: 'Auto-assigned fields will be computed at recovery time, and their actual values may differ from the currently displayed values.' Below this, there is a section titled 'Add Recovery Targets' with a dropdown menu showing the following options: Instances, Volumes, RDS Databases, Aurora Clusters, Redshift Clusters, DynamoDB Tables, and Elastic File Systems. At the bottom right of the dialog, there are 'Save' and 'Cancel' buttons.

2. In the **Add Recovery Targets** menu, select a resource type from the target policy to add to the scenario. Reminder: S3 Bucket Sync is not an option since it is not a backup action.




3. In the **Add** resource type screen, select one or more **Recovery Targets** for the resource type, and then select **Add selected**.

**Note:** Every Recovery Scenario target has a number identifying the sequential order of execution within the Recovery Scenario. The execution of the recovery source within the Recovery Scenario is sequenced using the target's **Recovery Order** value. The recovery of the target with the lowest value runs first.

4. To change the **Recovery Source** or **Recovery Order** for a target, select an option from its list.



**Note:** For Instance, Volume, and EFS Recovery Targets, it is important to configure the recovery details for each target. Select a recovery target and then select  **Configure**. See section 24.3.1.

When all details are complete, select **Save** in the Create Recovery Scenario screen.

### 24.3.1 Configuring an Instance Recovery Target

The Configuration screen opens with additional tabs:

- **Basic Options**
- A tab for the resource type, such as **Volumes**
- **Advanced Options**

**Note:** The configuration **Auto assigned** values may be different than the values that are shown as grayed-out. To be sure about a value, you need to assign it.

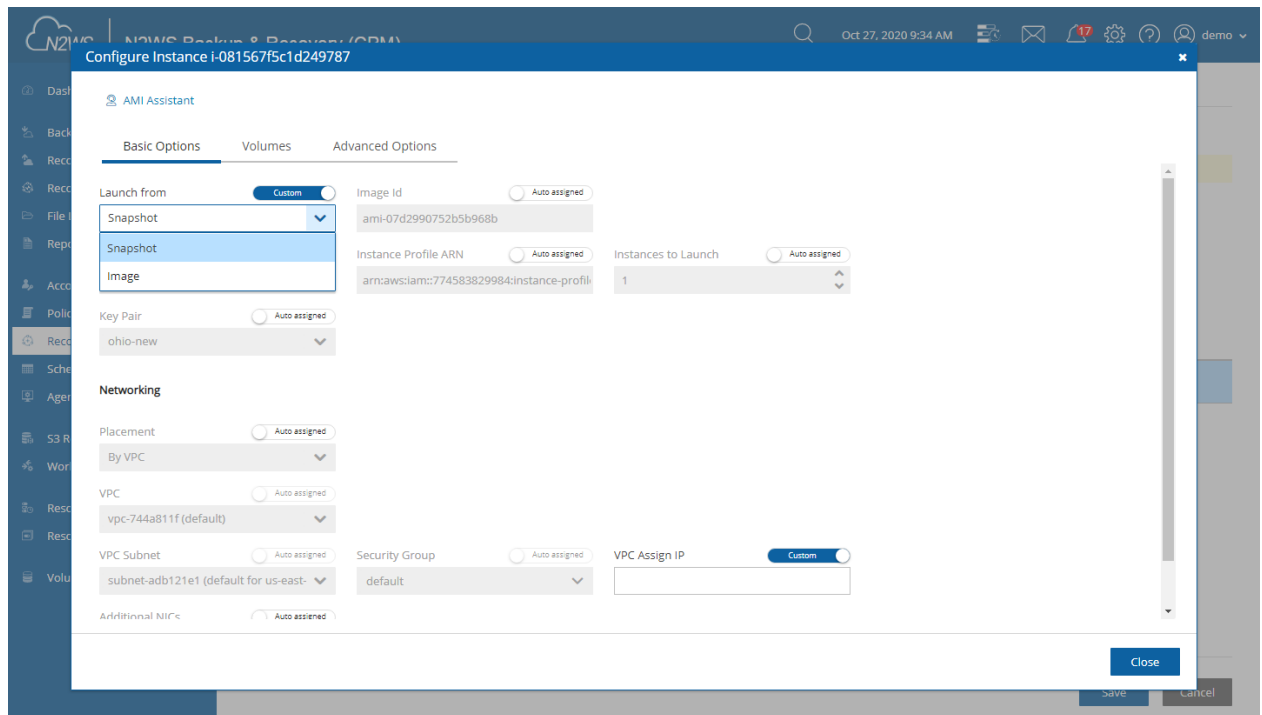
For each data item in the configuration tabs, assign the appropriate value. In each tab, you can customize a setting by turning off its **Auto assigned** toggle. Depending on the data item, you can:

- Select a different value from the **Custom** drop-down list.
- Enable or disable a feature.
- Enter a new value.

When finished with each tab, select **Close**.

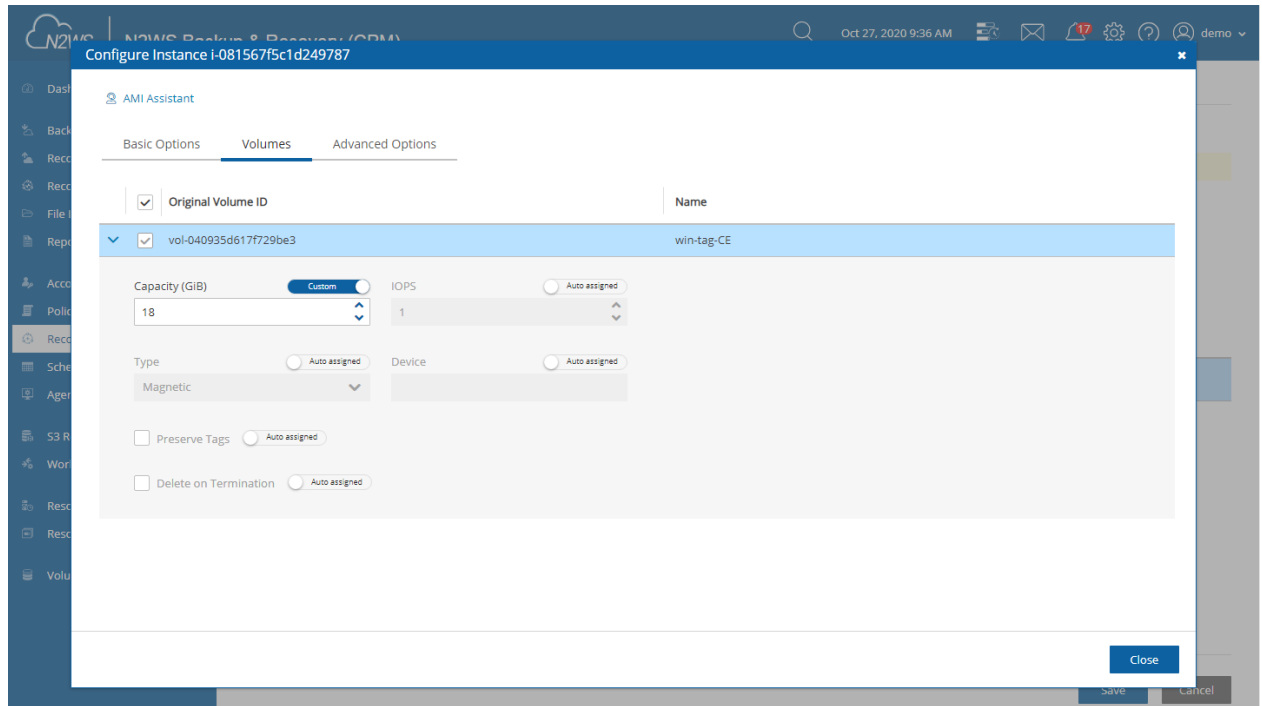
In the **Basic Options** tab, you can configure basic recovery actions, such as whether to launch from a snapshot or image, which key pair to use, and network placement.

**Note:** Since not all instance types are available in all AWS regions, recovery of an instance type to a region where the type is unsupported may fail. Where the instance type is not supported yet in an AWS region, we recommend configuring a supported **Instance Type** in the **Basic Options** parameters. See section 10.3.1.



The screenshot shows the 'Configure Instance' dialog for instance `i-081567f5c1d249787`. The 'Basic Options' tab is active. The 'Launch from' dropdown is set to 'Snapshot'. The 'Image Id' is `ami-07d2990752b5b968b`. The 'Instance Profile ARN' is `arn:aws:iam::774583829984:instance-profile`. The 'Instances to Launch' is set to 1. The 'Key Pair' is `ohio-new`. The 'Networking' section shows 'Placement' as 'By VPC', 'VPC' as `vpc-744a811f`, 'VPC Subnet' as `subnet-adb121e1`, and 'Security Group' as `default`. The 'VPC Assign IP' is set to 'Custom'.

In the **Volumes** tab, you can configure device information, such as capacity, type, and whether to preserve tags and delete on termination. To expand the configuration section for a volume, select the right arrow ➤.



The screenshot shows the 'Configure Instance' dialog for instance `i-081567f5c1d249787`, with the 'Volumes' tab active. A table lists the volumes:

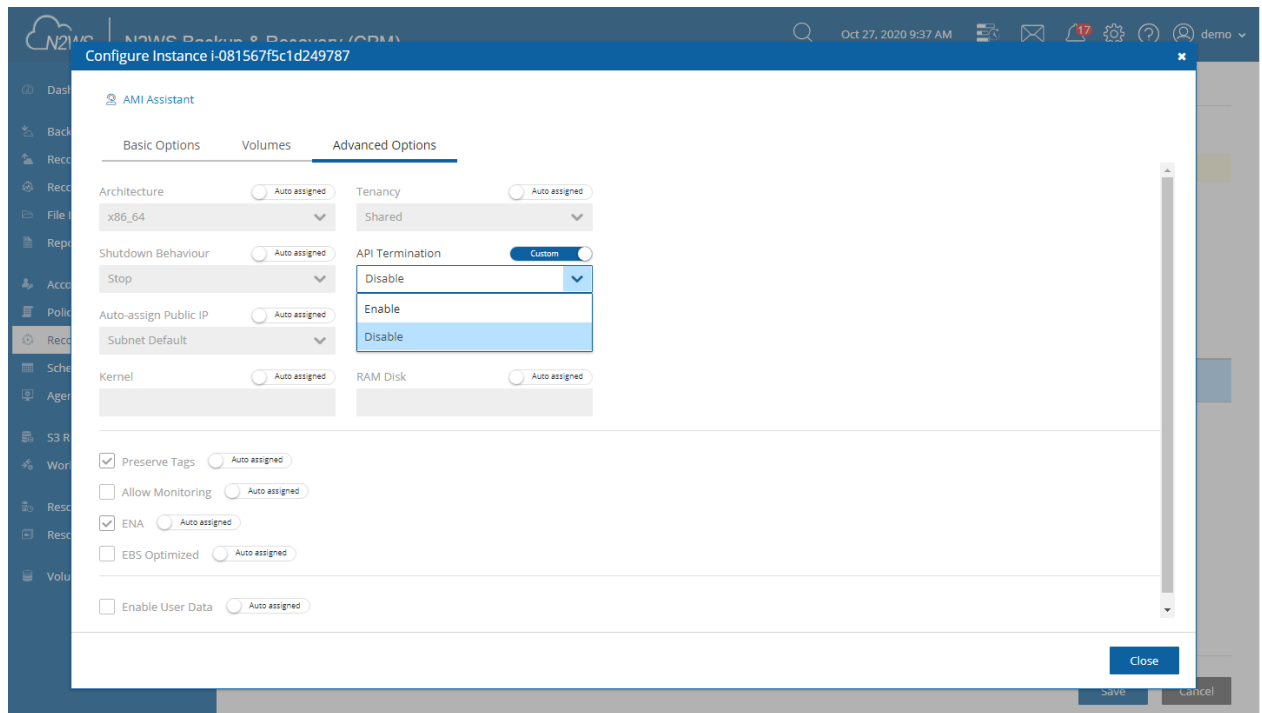
Original Volume ID	Name
vol-040935d617f729be3	win-tag-CE

The volume `vol-040935d617f729be3` is selected. The configuration for this volume is shown below:

- Capacity (GiB): 18
- IOPS: 1
- Type: Magnetic
- Device: (Auto assigned)
- Preserve Tags: (Auto assigned)
- Delete on Termination: (Auto assigned)

In the **Advanced Options** tab for an instance, you can customize recovery target features, such as architecture, shutdown behavior, whether to enable ENA and user data.






For complete details about performing an instance recovery, see section 10.3.

## 24.4 Testing a Recovery Scenario

The **Dry Run** option allows you to determine whether the input parameters, such as key pair, security groups, and VPC, are correct for the recovery.

**To test a Recovery Scenario:**

1. In the **Recovery Scenarios** tab, select a Recovery Scenario and then select  **Dry Run**.
2. In the list of successful backups, select one backup to perform the test with, and then select **Dry Run**.


Recovery Scenario - Dry Run - rs-win

Select Backup to Recover From

<input checked="" type="radio"/>	Start Time: Oct 27, 2020 12:45 AM, End Time: Oct 27, 2020 1:02 AM, Status: Successful
<input type="radio"/>	Start Time: Oct 27, 2020 12:38 AM, End Time: Oct 27, 2020 12:42 AM, Status: Successful
<input type="radio"/>	Start Time: Oct 27, 2020 12:25 AM, End Time: Oct 27, 2020 12:32 AM, Status: Successful
<input type="radio"/>	Start Time: Oct 27, 2020 12:16 AM, End Time: Oct 27, 2020 12:23 AM, Status: Successful





Dry Run
Close

- Open the **Recovery Scenario Monitor**.
- In the **Status** column for the Recovery Scenario, you will see a success message for the test:




✓ Recovery Successful
- Selecting  **Recoveries** brings you to the regular **Recovery Monitor**.

## 24.5 Managing Recovery Scenarios and Targets

To manage a Recovery Scenario object:


- In the **Recovery Scenarios** tab, select a scenario.
- Select  **Edit**,  **Delete**,  **Run Scenario**, or  **Dry Run**, as needed.

To manage targets in the scenario:

- In the Recovery **Scenarios** tab, select a scenario, and then select  **Edit**.
- To delete a target, select the **Recovery Targets** tab, select a target, and then select  **Remove from List**.
- Depending on the resource type, the action  **Configure** is available. Configure opens tabs for **Basic Options**, resource type details, and **Advanced Options**.

## 24.6 Running and Monitoring a Recovery Scenario

A Recovery Scenario can also be run on a schedule using the last successful backup. To assign or create a schedule, see section 24.3.

- In the **Recovery Scenarios** tab, select a Recovery Scenario and then select  **Run Scenario**.  
A list of backups, successful and unsuccessful, opens.

Recovery Scenario - rs-p2-vol

Select Backup to Recover From

☐ Start Time: May 27, 2020 2:17 PM, End Time: May 27, 2020 2:18 PM, Status: Successful

☒ Start Time: May 27, 2020 1:58 PM, End Time: May 27, 2020 1:58 PM, Status: Successful

☐ Start Time: May 27, 2020 1:57 PM, End Time: May 27, 2020 1:57 PM, Status: Successful

☐ Start Time: May 27, 2020 1:56 PM, End Time: May 27, 2020 1:56 PM, Status: Successful

☐ Start Time: May 27, 2020 1:53 PM, End Time: May 27, 2020 1:53 PM, Status: Successful

☐ Start Time: May 27, 2020 1:51 PM, End Time: May 27, 2020 1:51 PM, Status: Successful

☐ Start Time: May 27, 2020 1:40 PM, End Time: May 27, 2020 1:40 PM, Status: Successful

Recover
Close

2. Select one successful backup to recover from and then select **Recover**.

The started message opens in the top right corner:



3. To open the **Recovery Scenario Monitor**, select **Recovery Scenario Runs**, or select the **Recovery Scenario Monitor** tab.

N2WS | N2WS Backup & Recovery (CPM)

Oct 27, 2020 9:53 AM

Dashboard

Backup Monitor

Recovery Monitor

Recovery Scenario Monitor

File Level Recovery Sessions

Reports

Accounts

Policies

Recovery Scenarios

Schedules

Agents

S3 Repositories

Worker Configuration

Resource Control Monitor

Resource Control Groups

Volume Usage

Recovery Scenario Monitor

All Recovery Scenarios

All Accounts

All Policies

All Scenario Run Statuses

20 records/page

Log

Recoveries

Delete Record

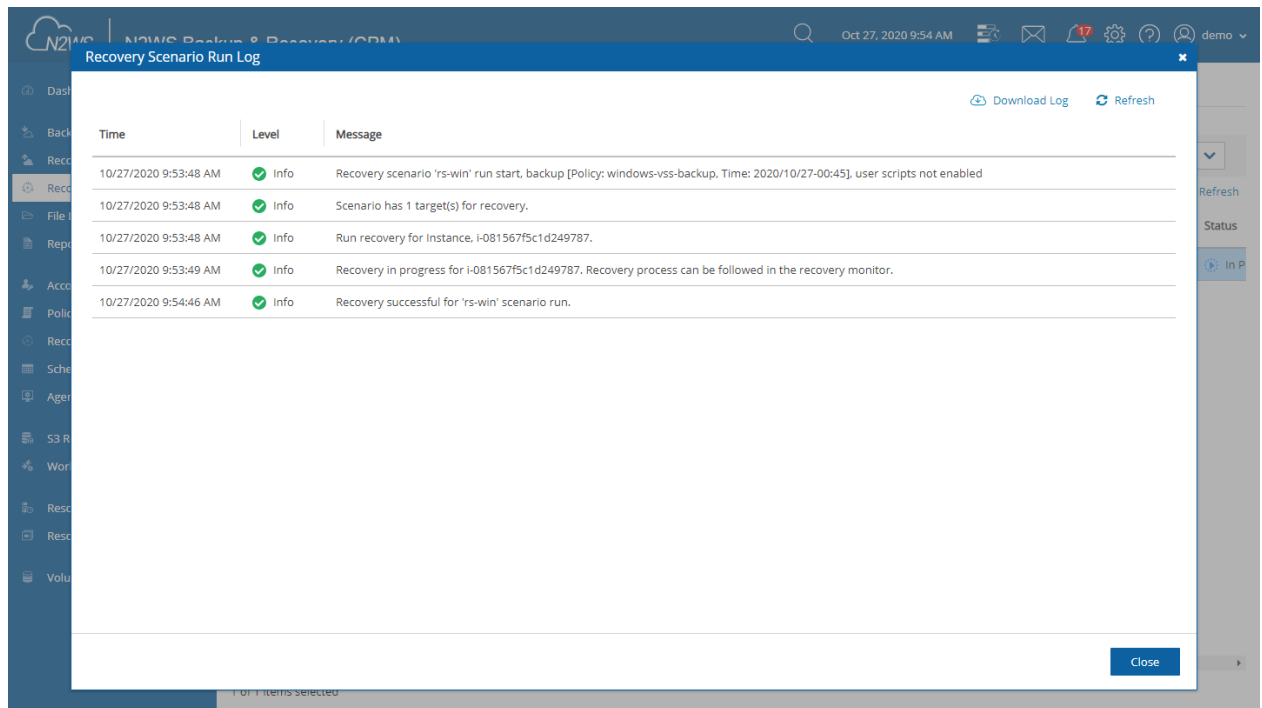
Refresh

Time	Backup Time	Recovery Scenario	Account	Policy	Status
20 9:53 AM	Oct 27, 2020 12:45 AM	rs-win	ACCOUNT-1	windows-vss-backup	In Progress

0 of 1 items selected

A **Status** of 'Recovery succeeded' with a test tube symbol next to it indicates that the recovery was a Dry Run.

4. To view details of the recovery in the Run Log, select a **Recovery Scenario** and then select **Log**.



5. To delete a run record, select a scenario, and then select **Delete Record**.

**Note:** Deleting a run record will trigger the deletion of all its target recovery records.

6. To view a live recovery, select a scenario, and then select **Recoveries**. The **Recovery Monitor** opens.

## 24.7 Recovery Scenario User Scripts

When **Enable Agent Scripts** is set in the **Recovery Scenario Details** tab, N2WS will run two scripts, one before and one after the recovery run:

- `before_<recovery-scenario-name>`
- `after_<recovery-scenario-name>`

A file extension is optional and, if added, may be for any interpreter.

**Note:** This is somewhat similar to the Linux Backup Scripts feature described in the Before Script and After Script topics, sections 6.3.1 and 6.3.2.

These scripts must be located on the N2WS server in the following folder:

- For root user: `/cpmdata/scripts/scenario`
- For non-root user: `/cpmdata/scripts/scenario/user_name`

### 24.7.1 Before Script

The **before** script passes the following parameters, in the following order:

#	Parameter	Notes
1	Scenario Id	
2	Account Id	May be <code>null</code> , if the value is NULL.
3	Policy account Id	



#	Parameter	Notes
4	Destination region	May be <code>null</code> , if the value is NULL.

### 24.7.2 After Script

The **after** script passes the same parameters as the **before** with the addition of parameters for the scenario's recovery targets:

#	Param.	Notes	
1 – 4	...	Same as <b>before_</b> parameters.	
5	Target lists	Each target is represented by the following colon-separated format: <b>RecoveryType:OriginalAwsResourceId:OriginalRegion:RecoveredAwsResourceId</b>	
	RecoveryType	A single character identifying resource type:	
		<b>I</b>	Instance
		<b>V</b>	Volume
		<b>R</b>	RDS Database
		<b>A</b>	RDS (Aurora) Cluster
		<b>C</b>	Redshift Cluster
		<b>D</b>	DynamoDB Table
		<b>E</b>	EFS
	OriginalAwsResourceId		The AWS ID of the original resource.
	OriginalRegion		The AWS region of the original resource.
	RecoveredAwsResourceId		The AWS ID of the recovered resource. If not recovered, then ' <code>null</code> '.

Following is an example of an **after\_** script for a Recovery Scenario that was defined with 2 targets: an EC2-instance and an EC2-volume. The **after\_** script passes 6 parameters, 2 of which are for the targets. In the following example, the instance recovery target was *not* recovered:

```
1
null
1
null
I:i-0a87ab83ca3fa62c2:us-east-1:null
V:vol-0197aba1f7090c513:us-east-1:vol-03336f4ed151b5d29
```



## 25 Monitoring Costs and Savings

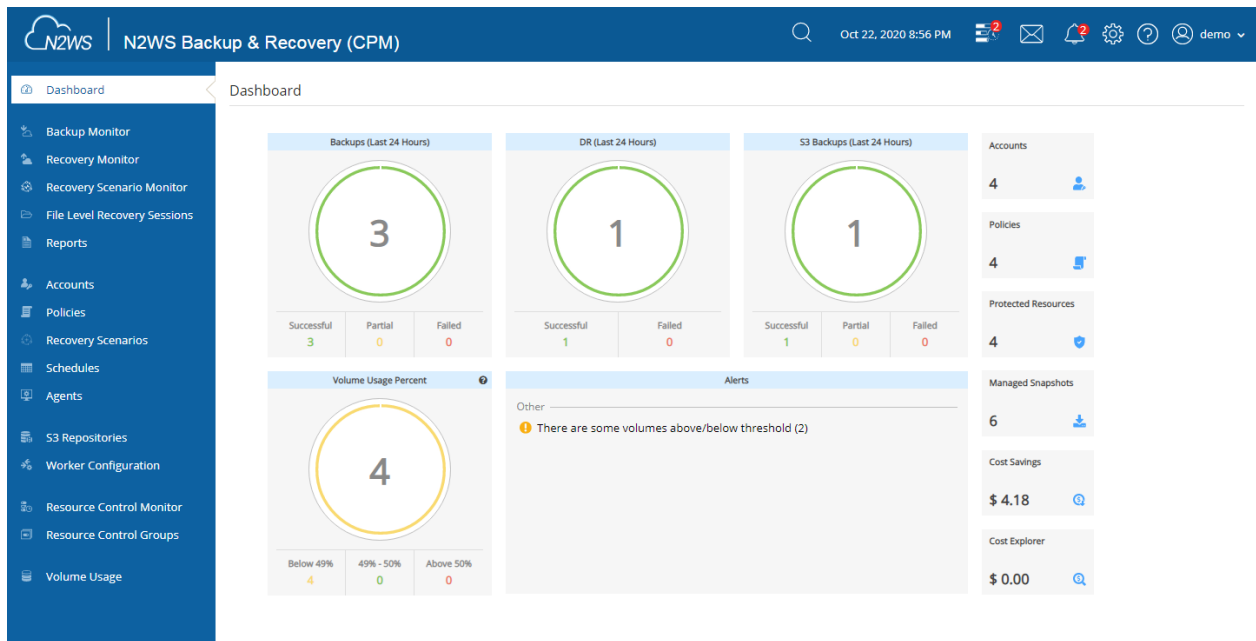
N2W Software customers have a single point of control and management over the procedure of backing up their cloud-based services and data stores. Monitoring the costs will help customers define backup plans that fit their budget and thereby avoid unexpected costs. N2WS provides the following services for monitoring costs:

- **Cost Explorer** – Cost of storage that was created by N2WS to hold short-term backup snapshots of the customer’s cloud-based assets.
  - Allows customers to monitor the costs by the backup processes generated by N2WS.
  - Allows customers to issue monthly bills per policy backups.
  - Calculations are made for the last month by default and can be set to prior periods.
  - Breakdown of costs is found in the **Costs (\$)** column of the **Policies** tab.
- **Cost Savings** – Amount of money that users can save by enabling Resource Control management.
  - Calculations are made for the next month.
  - Breakdown of savings is found in the **Cost Savings** column of the **Resource Control Groups** tab.

### Notes:

- Cost Explorer support is currently limited to the AWS resource EBS.
- N2WS uses the AWS REST API for retrieving costs for the specified policy. The Cost Explorer API allows us to programmatically query your data usage and compute the cost and usage data. It can take up to 48 hours for the cost increase to take effect.
- The costs will include both short-term and long-term backups (cross-region DR), but not snapshots that were copied onto cheaper media such as S3 and Glacier.

In the Dashboard screen, you can find both Cost Explorer and Cost Savings information in their respective tiles:



## 25.1 Enabling and Disabling Cost Explorer

**Note:** Cost Explorer is *not* available in AWS GovCloud (US).

Following are the steps necessary for using Cost Explorer:

- In AWS, activate cost allocation tags. See section 25.1.1.
- In N2WS:
  - For CPM, select **Enable Cost Explorer** in the **Cost Explorer** tab of **General Settings**.
  - For each designated user, enable **Allow Cost Explorer**. See section 18.3.

To disable Cost Explorer, it is sufficient to clear **Enable Cost Explorer** in the **Cost Explorer** tab.

### 25.1.1 Configuring AWS to Allow CPM Cost Explorer Calculations

To allow CPM Cost Explorer calculations in AWS, users must add cost allocation tags *once*.

**To activate user cost allocation tags:**

1. Log in to the AWS Management Console at <https://console.aws.amazon.com/billing/home#/>.
2. Open the **Billing and Cost Management** console.
2. In the navigation pane, choose **Cost Allocation Tags**.
3. Select the tags to activate:
  - `cpm_server_id`
  - `cpm_policy_name`
4. Choose **Activate**.

**Note:** It can take up to 24 hours for tags to activate.

See <http://docs.aws.amazon.com/awsaccountbilling/latest/aboutv2/activating-tags.html>



## 25.2 Monitoring Costs

In the **Policies** tab, you can monitor the backup costs of each policy for the last month or a different time period. The breakdown of costs per policy in dollars for the desired period appears in the **Cost (\$)** column.


Notes: Cost Explorer inclusions and exclusions:

- The cost figure includes all policies that were ever backed up by N2WS and does not filter out deleted policies. The costs for policies deleted during a cost period are still included in the cost figure for that period.
- N2WS Cost Explorer does *not* include the cost of cross-account DR snapshots.


Name	Account	Enabled	Backup Generations	Schedules	Cost (\$)
234567890	ACCOUNT-3	Yes	30		N/A
PMDATA	ACCOUNT-1	Yes	1		0.00
dd	ACCOUNT-1	Yes	30		N/A
1	ACCOUNT-1	Yes	22		0.04
2	ACCOUNT-1	Yes	33		0.04
3	ACCOUNT-3	Yes	1		0.02
ds	ACCOUNT-1	Yes	30		N/A
ol	ACCOUNT-1	Yes	30		N/A
/windows-vss-backup	ACCOUNT-1	Yes	30		N/A

If the **Allow Cost Explorer** option is not enabled for the logged in user, or if the backup was generated within the last 24 hours, the **Cost (\$)** column will show 'N/A'. To enable Cost Explorer for a user, see section 18.3.

### 25.2.1 Specifying a Different Time Period for Cost Calculations

You can monitor costs for a different time period by setting the **Cost Period** for all policies. The maximum period is one year. The current period is shown next to  **Cost Period** in the **Policies** tab below the filters.

To specify the period for cost calculations:

1. Select the **Policies** tab and then select  **Cost Period**.





Specify Time Period for Cost Calculations

☐ Last month

☒ Period:

2. Select **Period**.
3. Choose the **From** and **To** dates from the calendars, selecting **Apply** after each date.

## 25.3 Monitoring Expected Cost Savings

In the **Resource Control Groups** tab, you can monitor the expected Cost Savings for each group, based on the schedules you have set to **Turn Off** an instance or an RDS database.

**Note:** When the **Operation Mode** of a Resource Control Group is **Turn Off Only**, N2WS will show 'No-Data' in the **Cost Savings** column.

N2WS Backup & Recovery (CPM)

Resource Control Groups

Search resource control groups  All Accounts 20 records/page

+ New Edit Turn On Now Turn Off Now Delete Refetch Savings Data from AWS Refresh

<input type="checkbox"/>	Name	Account	Timeout (minutes)	Enabled	Cost Savings
<input type="checkbox"/>	MTW	ACCOUNT-1	30	Yes	N/A
<input type="checkbox"/>	rcg1	ACCOUNT-1	30	Yes	\$ 4.18

0 of 2 items selected

To update the screen with the current AWS savings, select **Refetch Savings Data from AWS**, and then select **View updated data** in the data refetched message.

Cost Savings data was refetched  
[\(View updated data\)](#)



## 26 Using N2WS with Azure

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

1. *Before* starting, configure N2WS Backup and Recovery according to [Configuring N2WS](#).
1. After the final configuration screen, prepare your Azure Subscription by adding the required permissions and custom IAM role in Azure. See section 26.1.
2. Register the CPM app in Azure. See section 26.2.
3. Create an N2WS user as usual and configure resource limitations for Azure as described in section 18.3.
4. In N2WS, add an Azure account with the custom N2WS role. See section 26.3.
5. Create an Azure policy in N2WS with Azure backup targets. See section 26.4.
6. Back up the policy. See section 26.5.
7. Recover from a backup. See section 26.6.

### 26.1 Setting Up Your Azure Subscription

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

1. For the minimal permissions for Azure, see <https://support.n2ws.com/portal/en/kb/articles/minimal-azure-permissions-roles-for-n2ws-operations>
1. Add your Subscription ID value to the “subscriptions” attribute in the minimal permissions JSON.

```
{
  "properties": {
    "roleName": "CPM",
    "description": "",
    "assignableScopes": [
      "/subscriptions/<subscriptionID>"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Compute/virtualMachines/read",
          "Microsoft.Compute/disks/read",
          "Microsoft.Compute/snapshots/write",
          "Microsoft.Network/networkInterfaces/read",
          "Microsoft.Compute/snapshots/read",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Compute/disks/write",
          "Microsoft.Compute/snapshots/delete",
          "Microsoft.Resources/subscriptions/resourceGroups/delete",
          "Microsoft.Network/virtualNetworks/read",
          "Microsoft.Network/virtualNetworks/subnets/read",
          "Microsoft.Network/networkInterfaces/write",
          "Microsoft.Network/virtualNetworks/subnets/join/action",
          "Microsoft.Network/networkInterfaces/join/action",
```

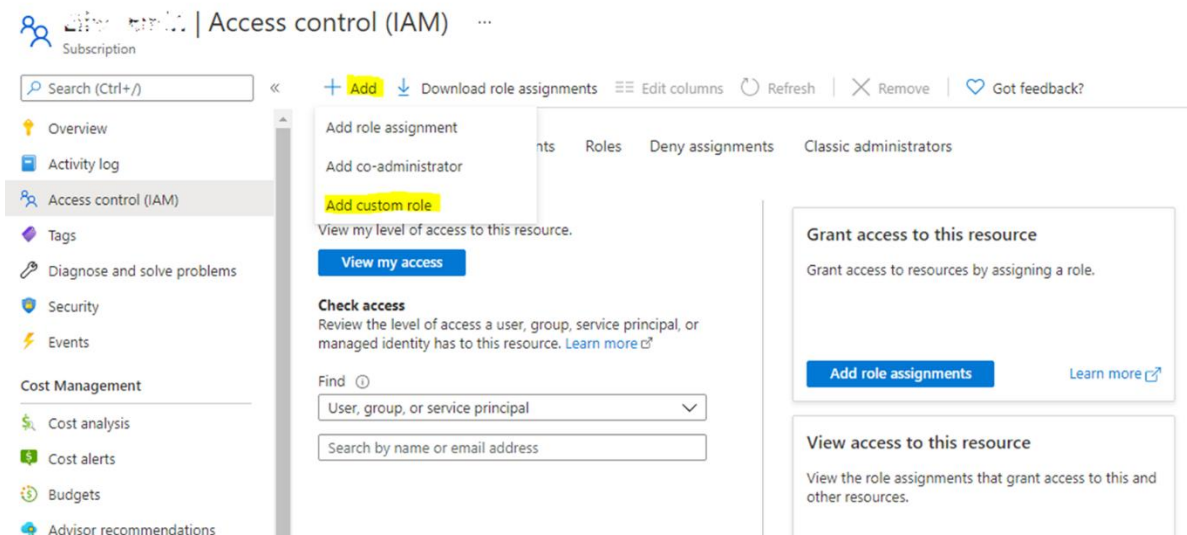


```
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/virtualMachines/powerOff/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Compute/availabilitySets/vmSizes/read"
],
"notActions": [],
"dataActions": [],
"notDataActions": []
}
]
}
}
```

2. Log on to the Azure Portal, <https://portal.azure.com>, and go to your subscription. Select a subscription that you want to use with N2WS Backup & Recovery.



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



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



## Create a custom role ...

♥ Got feedback?

Basics

Permissions

Assignable scopes

JSON

Review + create

To create a custom role for Azure resources, fill out some basic information. [Learn more](#)

\* Custom role name ⓘ  ✓

Description

Baseline permissions ⓘ ☐ Clone a role ☐ Start from scratch ☒ Start from JSON

5. Create the role with the new JSON file.

## 26.2 Registering Your Azure App

1. In the Azure portal **Dashboard** section, go to the **App registrations** service.
1. In the **Name** box, type **CPM-on-Azure** and select **Register**.

Microsoft Azure

Dashboard > App registrations >

### Register an application ...

\* Name  
The user-facing display name for this application (this can be changed later).

✓

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Default Directory only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

[Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.](#)

By proceeding, you agree to the [Microsoft Platform Policies](#)

2. Select the app.



3. Save the **Application (client ID)** and **Directory (tenant) ID** for use when adding the Azure account to N2WS.

[Dashboard](#) > [App registrations](#) >

**CPM-on-Azure** ✎ ⋮

« [Delete](#) [Endpoints](#) [Preview features](#)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Essentials

Display name : CPM-on-Azure

Application (client) ID : 5c1bdc20-daab-456d-bbe4-6f8fca44e281

Object ID : 7842a788-b1f4-4582-9d20-d34a93d9c327

Directory (tenant) ID : ff529d89-4b4d-41b3-9152-d5ef8d6e6fe2

Supported account types : My organization only

Client credentials : [Add a certificate or secret](#)

Redirect URIs : [Add a Redirect URI](#)

Application ID URI : [Add an Application ID URI](#)

Managed application in L... : CPM-on-Azure

4. Select **Add a certificate or secret**.

5. Select **+ New client secret**.

6. Complete the secret values, and save.

[Dashboard](#) > [App registrations](#) > [CPM-on-Azure](#)

**CPM-on-Azure** | **Certificates & secrets** ✎ ⋮

« [Got feedback?](#)

Overview

Quickstart

Integration assistant

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

App roles

Owners

Roles and administrators | Preview

Manifest

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	Certificate ID
No certificates have been added for this application.			

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value	Secret ID
-------------	---------	-------	-----------

## 26.3 Adding an Azure Account to N2WS

1. Log on to N2WS using the root username and password used during the N2WS configuration.

1. Select the **Accounts** tab.

2. If you have a license for Azure cloud, select **Azure account** in the **+ New** menu.

**+ New** ▼

3. Complete the New Azure Account screen using the App registration view information in the Azure portal as needed.

281



N2WS Backup & Recovery (CPM)

Accounts > New Azure Account

Name:

User:  + New

Directory (tenant) ID:

Application (client) ID:

Client Secret:

☐ Scan Resources

Save Cancel

- **Name** - Copy from your App registration name.
  - In the **User** list, select your username or select **+ New** to add a user.
  - **Directory (tenant) ID** – Copy from your App registration.
  - **Application (client) ID** – Copy from your App registration.
  - **Client Secret** – Copy from your App registration Certificates & secrets in the App Registration view, or set a new secret.
4. Select **Scan Resources** to include the current account in tag scans performed by the system. The scan will cover all VMs and disks in all locations.
  5. Select **Save**. The new account appears in the Accounts list as an Azure Cloud account.

N2WS Backup & Recovery (CPM)

Accounts

Cloud:  Search Accounts 20 records/page

+ New Edit Clone VPC Check AWS Permissions Generate Secured DR Report Delete Delete Account and Data Refresh

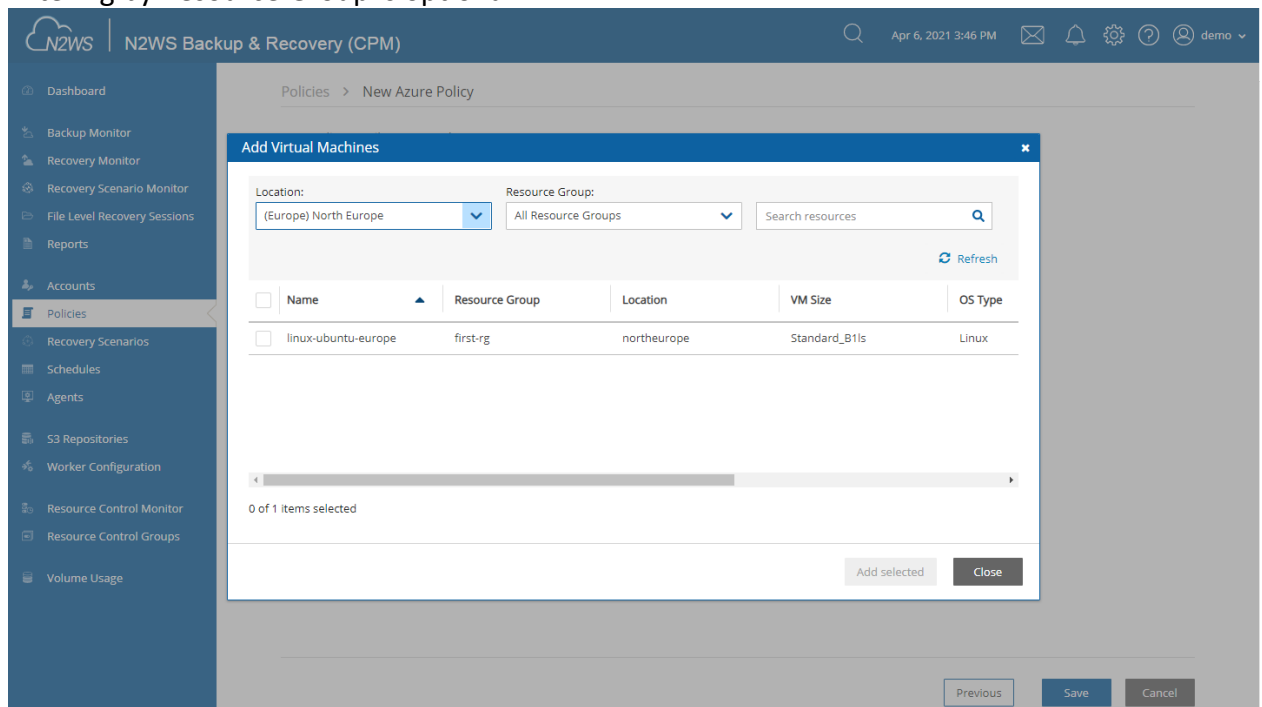
<input type="checkbox"/>	Name	Cloud	Account Type	Authentication	Policy
<input type="checkbox"/>	azure-account	Azure	Backup	4e7e937e-1e69-4324-a435-376dab9ec1d0	p2-azu

0 of 2 items selected

## 26.4 Creating an Azure Policy

To backup resources in Azure, create an N2WS Azure policy.

1. In N2WS, select the **Policies** tab.
1. In the **+ New** list, select **Azure policy**.
2. In the New Azure Policy screen, complete the fields:
  - **Name** – Enter a name for the policy.
  - **User** – Select from the list, or select **+ New** to add a new user. See section 18.
  - **Account** – Select from the list, or select **+ New** to add an account. See section 26.2.
  - **Enabled** – Clear to disable the policy.
  - **Subscription** – Select from the list.
  - **Schedules** – Optionally, select one or more schedules from the list, or select **+ New** to add a schedule. See section 4.1.1.
  - **Auto Target Removal** – Select **Yes** to automatically remove a non-existing target from the policy.
3. Select the **Backup Targets** tab.
4. In the **Add Backup Targets** menu, select the targets to backup, Disks and/or Virtual Machines. The Add Virtual Machines / Disks screen opens.
5. When selecting Virtual Machines, it is *required* to filter by the **Location** of the target resources using the list in the upper left corner *before* selecting the individual targets. Filtering by Resource Group is optional.



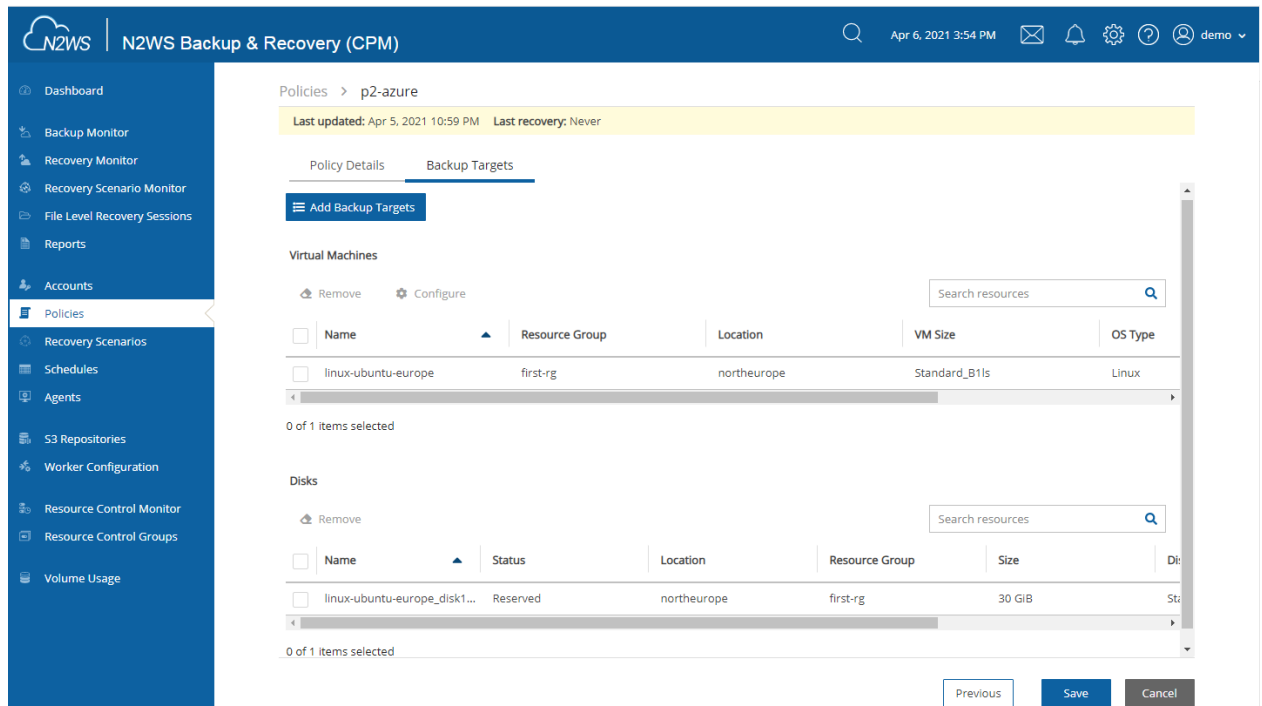
The screenshot shows the N2WS Backup & Recovery (CPM) interface. The 'Policies' tab is selected in the left navigation menu. The 'New Azure Policy' screen is open, and the 'Add Virtual Machines' dialog box is displayed. The dialog box has the following fields and content:

- Location:** (Europe) North Europe
- Resource Group:** All Resource Groups
- Search resources:** [Search bar]
- Refresh:** [Refresh button]
- Table:**

Name	Resource Group	Location	VM Size	OS Type
linux-ubuntu-europe	first-rg	northeurope	Standard_B1ls	Linux
- Selection:** 0 of 1 items selected
- Buttons:** Add selected, Close

The background interface shows the 'Policies' tab selected, and the 'Add selected' button is highlighted.

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



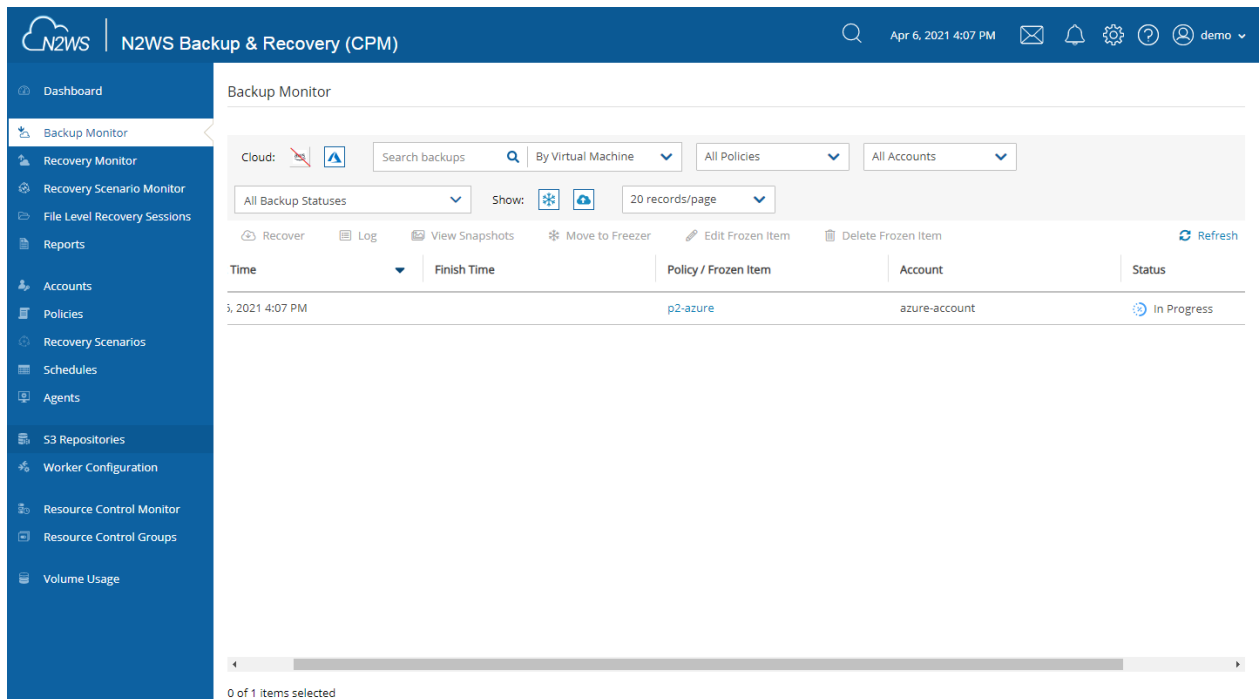
7. To determine which disks for each Virtual Machine target to backup, select **Configure**. In the **Which Disks** list of the Policy Virtual Machine and Disk Configuration screen, select the disks to include or exclude in the backup.
8. When finished, in the **Backup Targets** tab, select **Save**.

## 26.5 Backing Up an Azure Policy

If the policy has a schedule, the policy will backup automatically according to the schedule. To run a policy as soon as possible, select the policy and select **Run ASAP** in the **Policies** view. To view the policy progress and backups, select **Backup Monitor**.

- The backup progress is shown in the **Status** column.
- Use the Cloud buttons to display the Azure policies.





## 26.6 Recovering from an Azure Backup

**Note:** Only one VM is recoverable during a recovery operation.

After creating a backup, you can recover it from the **Backup Monitor**.

In the VM recovery Basic Options, there are Azure options for replicating data to additional locations in order to protect against potential data loss and data unavailability:

- **Availability Zone** – A redundant data center (different building, different servers, different power, etc.), within a geographical area that is **managed by Azure**.
- **Availability Set** – A redundant data center (different building, different servers, different power, etc.) that can be launched and fully configured by the customer and **managed by the customer**.
- **No Redundancy Infrastructure Required** – By selecting this option, the customer can choose not to replicate its data to an additional (redundant) location in another zone or set. By choosing this option, the customer would save some money, but in rare cases (usually 11 9s of durability and 99.9% of availability), the customer can experience some degree of data loss and availability.

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

- To add an additional layer of encryption during the recovery process, see <https://docs.microsoft.com/en-us/azure/virtual-machines/disks-enable-customer-managed-keys-portal>.
- Disk encryption settings can be changed only when the disk is unattached or the owner VM is deallocated.



## 26.6.1 Recovering a VM and Disks

To recover a VM and/or attached disks:

The screenshot shows the N2WS Backup & Recovery (CPM) interface. The left sidebar contains a navigation menu with options like Dashboard, Backup Monitor, Recovery Monitor, etc. The main area is titled 'Backup Monitor' and shows a list of backup records. The selected backup is highlighted in blue.

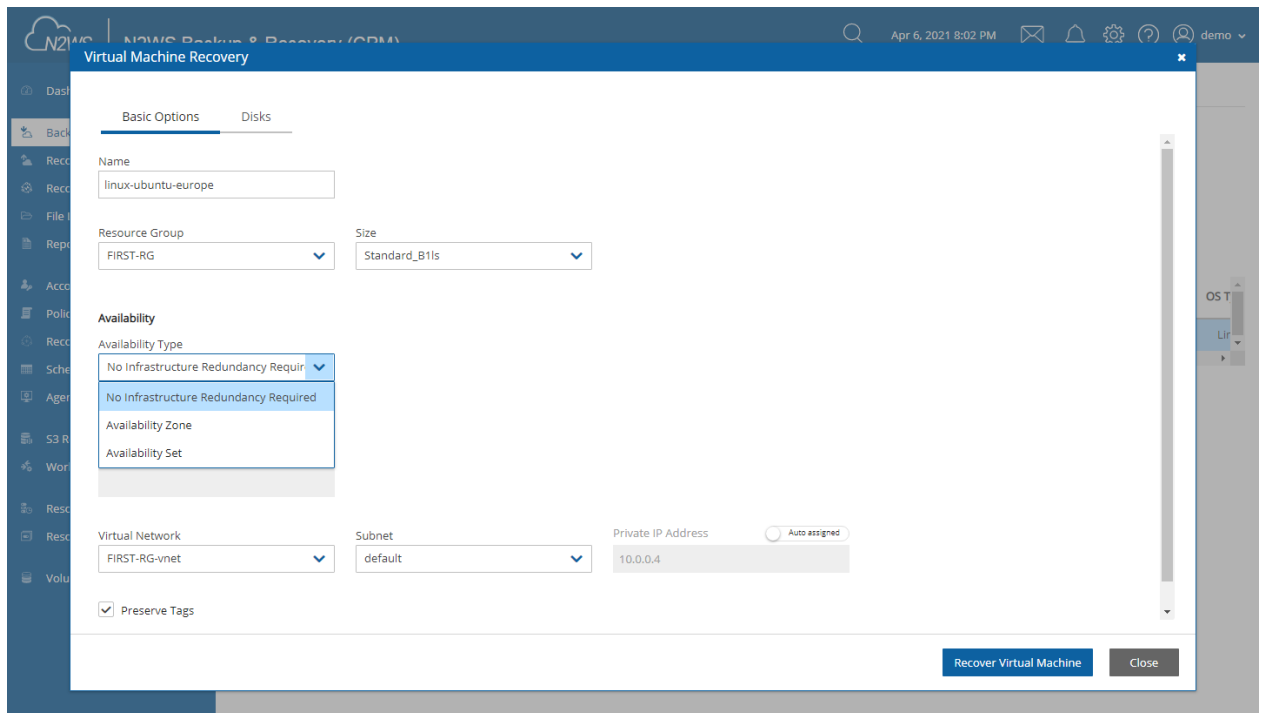
	Start Time	Finish Time	Policy / Frozen Item	Account	Status
<input type="checkbox"/>	Apr 6, 2021 7:51 PM	Apr 6, 2021 7:52 PM	p3-zure-disk	azure-account	✓ Success
<input type="checkbox"/>	Apr 6, 2021 7:05 PM	Apr 6, 2021 7:05 PM	p2-azure	azure-account	✓ Success
<input type="checkbox"/>	Apr 6, 2021 6:54 PM	Apr 6, 2021 6:54 PM	p2-azure	azure-account	✓ Success
<input checked="" type="checkbox"/>	Apr 6, 2021 4:07 PM	Apr 6, 2021 4:07 PM	p2-azure	azure-account	✓ Success



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

The screenshot shows the N2WS Backup & Recovery (CPM) interface, specifically the 'Recover' page. The left sidebar is the same as the previous screenshot. The main area is titled 'Recover' and shows a list of Virtual Machines. The selected VM is highlighted in blue.

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

1. To recover a VM, with or without its attached disks, select the VM snapshot that you want to recover from and then select **Recover**.
  - a. In the **Virtual Machines** tab of the Recover screen, select 1 VM and then select **Recover**. The **Basic Options** tab opens.

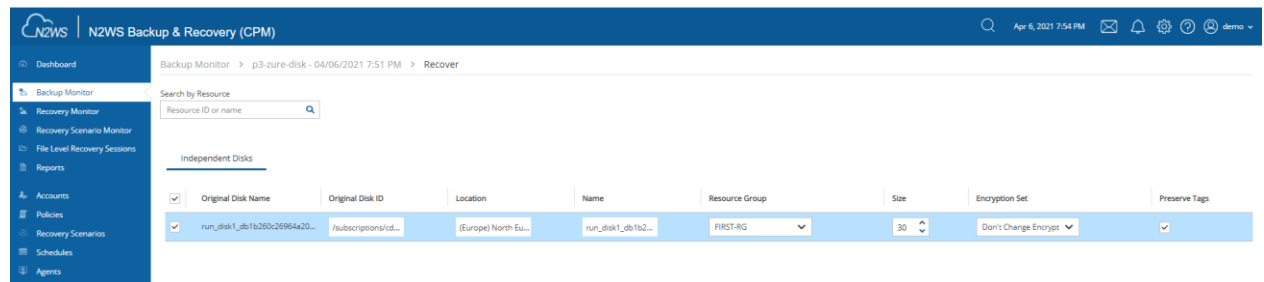


- b. In the **Availability Type** list, select one of the following:
  - **No Infrastructure Redundancy Required** – Select to not replicate data at a redundant location in another zone or set.
  - **Availability Zone** – Select a zone in the **Availability Zone** list.
  - **Availability Set** – Select a set in the **Availability Set** list.
- c. In the **Private IP Address** box, assign an available IP address or switch the **Custom** toggle key to **Auto assigned**.
- d. In the **Disks** tab, enter a new **Name** for each disk. Similar names will cause the recovery to fail.
- e. Select **Recover Virtual Machine**.
2. To recover only Disks attached to the VM, select  **Recover Disks Only**.
  - a. In the **Disks** tab, enter a new **Name** for each disk. Similar names will cause the recovery to fail.
  - b. See Note in section 26.6 about changing the Encryption Set for certain disks.
  - c. Change other settings as needed.
  - d. Select **Recover Disk**.
3. To view the recovery progress, select **Recovery Monitor**. Use the **Cloud** buttons to display the Azure () recoveries.

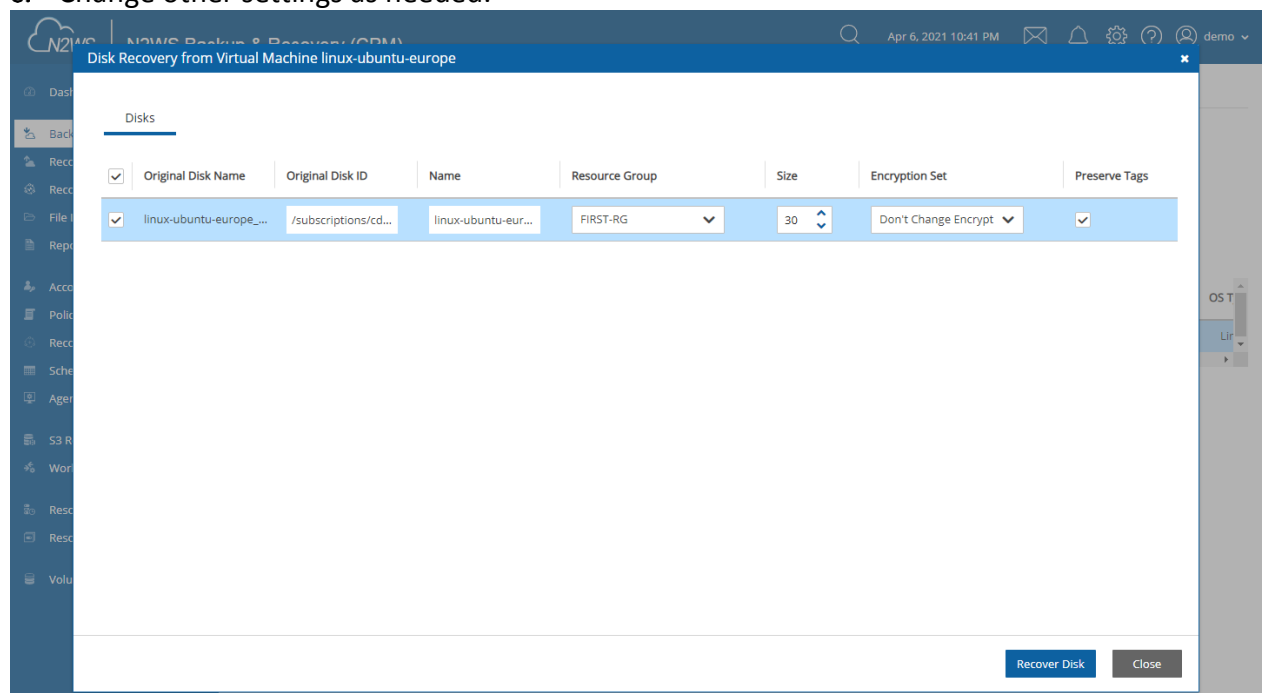
## 26.6.2 Recovering Independent Disks

To recover from backups with independent disks:

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



1. In the **Independent Disks** tab:
  - a. Enter a new Name for each disk to recover as similar names will cause failure.
  - b. See Note in section 26.6 about changing the Encryption Set for certain disks.
  - c. Change other settings as needed.



- d. Select **Recover Disk**.
2. To view the recovery progress, select **Recovery Monitor**. Use the **Cloud** buttons to display the Azure () recoveries.



## Appendix A – Recommended Configuration for Copy to S3

When ‘worker’ instances are using a public IP, NAT, or IGW within a VPC to access S3 buckets within the same region/account, it results in network transfer fees:

<https://www.linkedin.com/pulse/keep-s3-traffic-private-your-vpc-aws-travis-haag/>

<https://medium.com/nubego/how-to-save-money-with-aws-vpc-endpoints-9bac8ae1319c>

If the bucket is in another region or in another account, the transport charges will be incurred anyway.

Using VPC endpoint enables instances to use their private IP to communicate with resources in other services, such as S3, **within the AWS network without incurring network transfer fees.**

**To create a subnet associated with a route table that will direct connections to S3 in the same region as the VPC endpoint:**

1. In AWS, create a subnet within VPC of the region.

Subnets > Create subnet

### Create subnet

Specify your subnet's IP address block in CIDR format, for example, 10.0.0.0/24. IPv4 block sizes must be between a /16 netmask and /28 netmask, and can be the same size as your VPC. An IPv6 CIDR block must be a /64 CIDR block.

Name tag

VPC\*

VPC CIDRs	CIDR	Status	Status Reason

Availability Zone

IPv6 CIDR block\*

\* Required

After successful creation, the successful creation message appears.

Subnets > Create subnet

### Create subnet

✓ The following Subnet was created:

Subnet ID: subnet-0443a50753f104657

Close

The subnet is automatically associated with the default route table.

2. Create a new route table.

Create Route Table

A route table specifies how packets are forwarded between the subnets within your VPC, the Internet, and your VPN connection.

Name tag

VPC

vpc-23bcf65a

Cancel

Yes, Create

- Change the subnet association by associating the previously created subnet with this route table.
- Create a VPC endpoint for S3 in the region and associate it with the previously created route table.

Endpoints > Create Endpoint

Create Endpoint

A VPC endpoint allows you to securely connect your VPC to another service.

An interface endpoint is powered by PrivateLink, and uses an elastic network interface (ENI) as an entry point for traffic destined to the service.

A gateway endpoint serves as a target for a route in your route table for traffic destined for the service.

Service category

AWS services

Find service by name

Your AWS Marketplace services

Service Name

Select a service

Filter by attributes

1 to 23 of 23

Service Name	Owner	Type
com.amazonaws.us-east-1.cloudformation	amazon	Interface
com.amazonaws.us-east-1.cloudtrail	amazon	Interface
com.amazonaws.us-east-1.codebuild	amazon	Interface
com.amazonaws.us-east-1.codebuild-fips	amazon	Interface
com.amazonaws.us-east-1.config	amazon	Interface
com.amazonaws.us-east-1.dynamodb	amazon	Gateway
com.amazonaws.us-east-1.ec2	amazon	Interface
com.amazonaws.us-east-1.ec2messages	amazon	Interface
com.amazonaws.us-east-1.elasticloadbalancing	amazon	Interface
com.amazonaws.us-east-1.events	amazon	Interface
com.amazonaws.us-east-1.execute-api	amazon	Interface
com.amazonaws.us-east-1.kinesis-streams	amazon	Interface
com.amazonaws.us-east-1.kms	amazon	Interface
com.amazonaws.us-east-1.logs	amazon	Interface
com.amazonaws.us-east-1.monitoring	amazon	Interface
com.amazonaws.us-east-1.s3	amazon	Gateway

VPC\*

vpc-23bcf65a

- Choose a region.
- Then choose the previously defined route table.

com.amazonaws.us-east-1.monitoring

com.amazonaws.us-east-1.s3

amazon

Gateway

The permissions to access the bucket will be defined by the IAM policies attached to the roles of N2WS.



## 7. Grant Full Access.

**Policy\*** ☒ Full Access - Allow access by any user or service within the VPC using credentials from any AWS accounts to any resources in this AWS service. All policies - IAM user policies, VPC endpoint policies, and AWS service-specific policies (e.g. Amazon S3 bucket policies, any S3 ACL policies) - must grant the necessary permissions for access to succeed.

☐ Custom

Use the policy creation tool to generate a policy, then paste the generated policy below:

```
{
  "Statement": [
    {
      "Action": "*",
      "Effect": "Allow",
      "Resource": "*",
      "Principal": "*"
    }
  ]
}
```

The route table of the subnet now looks like the following:

**Subnet:** subnet-0443a50753f104657

Description Flow Logs **Route Table** Network ACL Tags

[Edit route table association](#)

**Route Table:** rtb-0effb8e6161f10a54 | test-routetable

<< < 1 to 2 of 2 > >>

Destination	Target
172.31.0.0/16	local
pl-63a5400a	vpce-052c72253680333a0

8. If N2WS is in a different account/region/VPC, add to the route table an Internet Gateway so the 'worker' can communicate with N2WS.
  - a. Add the following rule:

0.0.0.0/0	igw-f7172591	Active	No
-----------	--------------	--------	----

The route table will look like:

**rtb-0effb8e6161f10a54 | test-routetable**

Summary **Routes** Subnet Associations Route Propagation Tags

[Edit](#) Save Successful

View: All rules

Destination	Target	Status	Propagated
172.31.0.0/16	local	Active	No
0.0.0.0/0	igw-f7172591	Active	No
pl-63a5400a (com.amazonaws.us-east-1.s3)	vpce-052c72253680333a0	Active	No



In this configuration, the connection to S3 will be routed to the VPC endpoint. See example below:

#### Example: An Endpoint Route in a Route Table

In this scenario, you have an existing route in your route table for all internet traffic (0.0.0.0/0) that points to an internet gateway. Any traffic from the subnet that's destined for another AWS service uses the internet gateway.

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-1a2b3c4d

You create an endpoint to a supported AWS service, and associate your route table with the endpoint. An endpoint route is automatically added to the route table, with a destination of p1-1a2b3c4d (assume this represents the service to which you've created the endpoint). Now, any traffic from the subnet that's destined for that AWS service in the same region goes to the endpoint, and does not go to the internet gateway. All other internet traffic goes to your internet gateway, including traffic that's destined for other services, and destined for the AWS service in other regions.

Destination	Target
10.0.0.0/16	Local
0.0.0.0/0	igw-1a2b3c4d
p1-1a2b3c4d	vpce-11bb22cc

#### Example: Adjusting Your Route Tables for Endpoints

In this scenario, you have configured your route table to enable instances in your subnet to communicate with Amazon S3 buckets through an internet gateway. You've added a route with 54.123.165.0/24 as a destination (assume this is an IP address range currently within Amazon S3), and the internet gateway as the target. You then create an endpoint, and associate this route table with the endpoint. An endpoint route is automatically added to the route table. You then use the `describe-prefix-lists` command to view the IP address range for Amazon S3. The range is 54.123.160.0/19, which is less specific than the range that's pointing to your internet gateway. This means that any traffic destined for the 54.123.165.0/24 IP address range continues to use the internet gateway, and does not use the endpoint (for as long as this remains the public IP address range for Amazon S3).

Destination	Target
10.0.0.0/16	Local
54.123.165.0/24	igw-1a2b3c4d
p1-1a2b3c4d	vpce-11bb22cc

To ensure that all traffic destined for Amazon S3 in the same region is routed via the endpoint, you must adjust the routes in your route table. To do this, you can delete the route to the internet gateway. Now, all traffic to Amazon S3 in the same region uses the endpoint, and the subnet that's associated with your route table is a private subnet.

9. In N2WS, select the **Worker Configuration** tab.
  - a. Select **+ New**.
  - b. Configure the worker to use this subnet in the specific region and the VPC where it is defined.





N2WS

N2WS Backup & Recovery (CPM)

Oct 27, 2020 12:01 PM

9

demo

Dashboard

Backup Monitor

Recovery Monitor

Recovery Scenario Monitor

File Level Recovery Sessions

Reports

Accounts

Policies

Recovery Scenarios

Schedules

Agents

S3 Repositories

Worker Configuration

Resource Control Monitor

Resource Control Groups

Volume Usage

Worker Configuration > New Worker Configuration

User

+ New

demo

Account

+ New

ACCOUNT-1 (Backup)

Region

Choose

Key pair

VPC

Security Group

Subnet

Network Access

Direct

Save

Cancel

**Note:** For additional information about setting up VPC Gateway Endpoints, see <https://docs.aws.amazon.com/vpc/latest/userguide/vpce-gateway.html>




## Appendix B – Agents Configuration Format

N2WS allows configuring remote and local agents from the UI. See section 6.1.2.

- The configuration in the text box needs to be in 'INI' format.
- According to the section header, N2WS will pass the key-value pairs to the appropriate agents.
- Each agent writes the set of key-value pairs it receives for a section to its configuration file and restarts to reload the configuration.

### To configure agents:

1. Select  **Server Settings > Agents Configuration**.
2. Write the configuration in the text box with the section header followed by its key-pair, as shown below.
3. Select **Publish**.

The following sample rules show how to configure relevant agents:

- Pass configuration to **all remote agents of a given policy**.  
The following will pass the key-value 'max\_seconds\_to\_wait\_for\_vss=100' to all remote agents that belong to the policy by the name 'p1':  

```
[policy_p1]
max_seconds_to_wait_for_vss=100
```
- Pass configuration to a **specific remote agent**.  
The following will pass the key-value 'max\_seconds\_to\_wait\_for\_vss=100' to the remote agent whose AWS instance ID is 'agent\_id':  

```
[agent_agent_id]
max_seconds_to_wait_for_vss=100
```
- Pass configuration to **all remote agents**.  
The following will pass the key-value 'max\_seconds\_to\_wait\_for\_policy=600' to all remote agents:  

```
[all_remote_agents]
max_seconds_to_wait_for_policy=600
```
- Pass configuration to a **local agent**.  
The following will pass the key-value 'max\_seconds\_to\_wait\_for\_policy=600' to the local agent:  

```
[local_agent]
max_seconds_to_wait_for_policy=600
```

One or more instances of all of the above can be pasted together to the text box in the **Agent Configuration** screen. On **Publish**, N2WS iterates over all sections and passes the relevant configuration to each agent.



## Appendix C – Time Zones

The following example is the CPMCONFIG `time_zone` parameter for Israel:

```
CPMCONFIG
[SERVER]
user=demo
password=1
volume_option=new
time_zone=Asia/Jerusalem
```

### To obtain the list of time zones or to set the time zone:

1. SSH into the CPM instance using the logon `cpmuser` and the instance's private key.
2. To obtain a list of all time zones, type:

```
sudo cpm-set-timezone
```

3. To set the time zone, type:

```
sudo cpm-set-timezone <new-time-zone>
```

For example, to set the time zone to 'New York', type:

```
sudo cpm-set-timezone America/New_York
```



## Appendix D – Datadog Integration Support

N2WS Backup and Recovery Instance is now supporting the monitoring of backups, DR, copy to S3, alerts, and more by Datadog. Datadog is a monitoring service for cloud-scale applications, providing monitoring of servers, databases, tools, and services, through a SaaS-based data analytics platform. Datadog will allow CPM users to monitor and analyse the N2WS Backup and Recovery Dashboard metrics.

This section includes instructions for:

- Activating Datadog
- Monitoring N2WS with Web Proxy

### D.1 Activating Datadog and Monitoring N2WS

You can load a ready-made Datadog template to monitor N2WS with the Datadog client at <https://support.n2ws.com/portal/en/kb/articles/datadog-templates>. Or, you can use the following procedure:

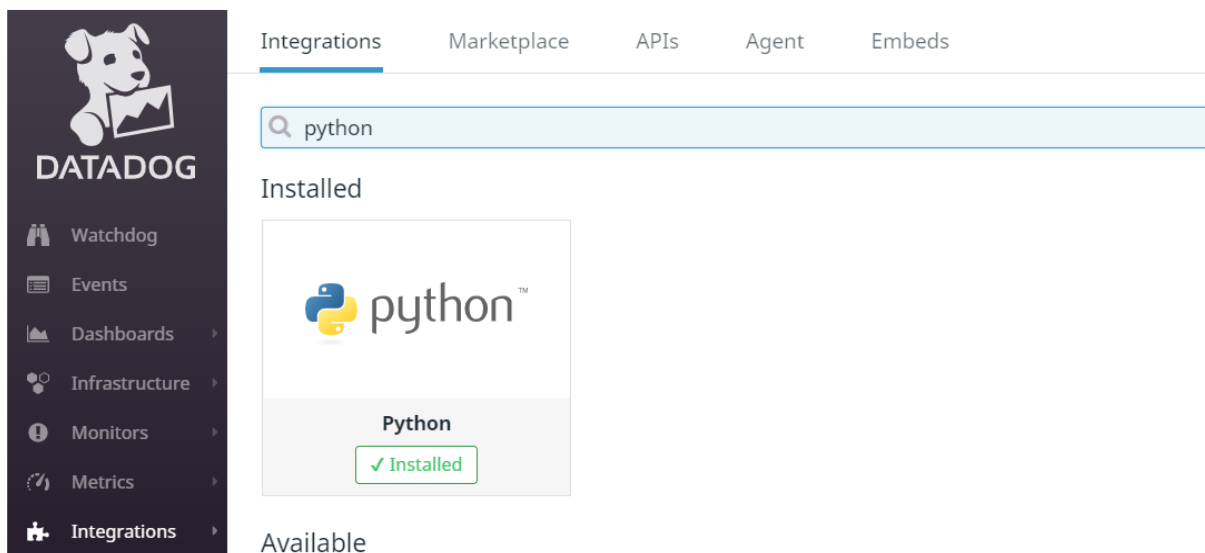
**To activate the service and to monitor your N2WS instance:**

#### 1. Setup Datadog Account

Visit Datadog at <https://www.datadoghq.com/pricing/> and setup an account that fits your scale.

#### 2. Install Python Integration

- a. Login to Datadog and go to **Integrations > Integrations**.
- b. Search for 'Python' and install it:



#### 3. Enable Datadog support on N2WS Instance

- a. Connect to your N2WS Backup and Recovery Instance with SSH Client.
- b. Type `sudo su`.
- c. Add the following lines to `/cpmdata/conf/cpmserver.cfg`:  

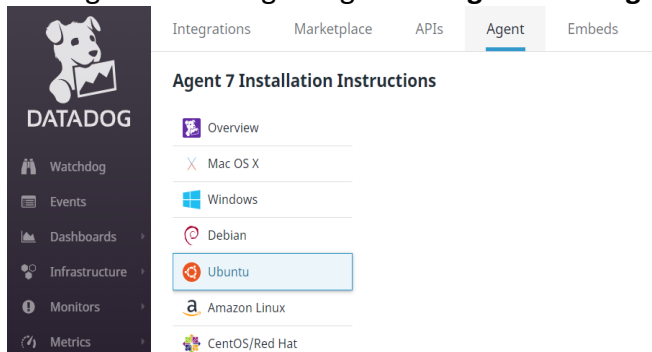
```
[external_monitoring]
enabled=True
```



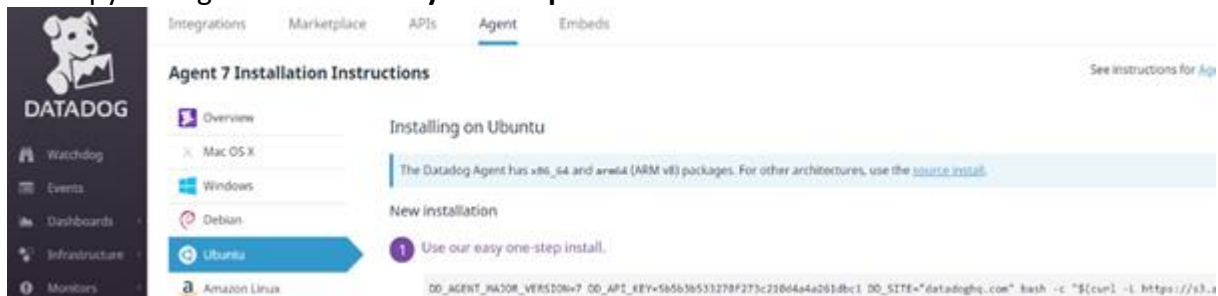
d. Run `service apache2 restart`

#### 4. Install Datadog Agent on N2WS Instance

a. Login to Datadog and go to **Integrations > Agent > Ubuntu**:



b. Copy the Agent 'Use our easy one-step install' command line



c. Connect to your N2WS Backup and Recovery Instance with SSH Client, type `sudo su` and run the agent Install command.

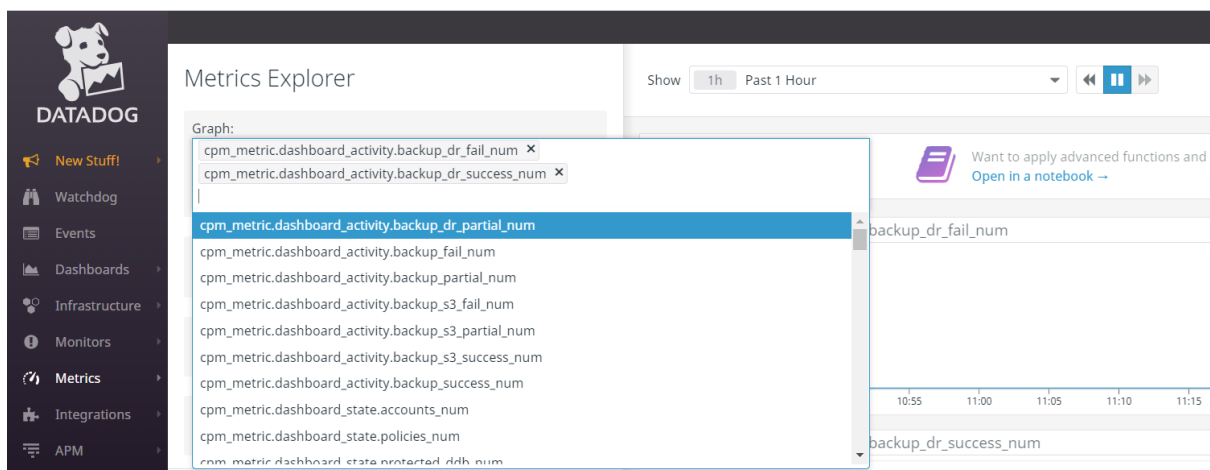
d. Restart the Datadog Agent:

```
sudo service datadog-agent restart
```

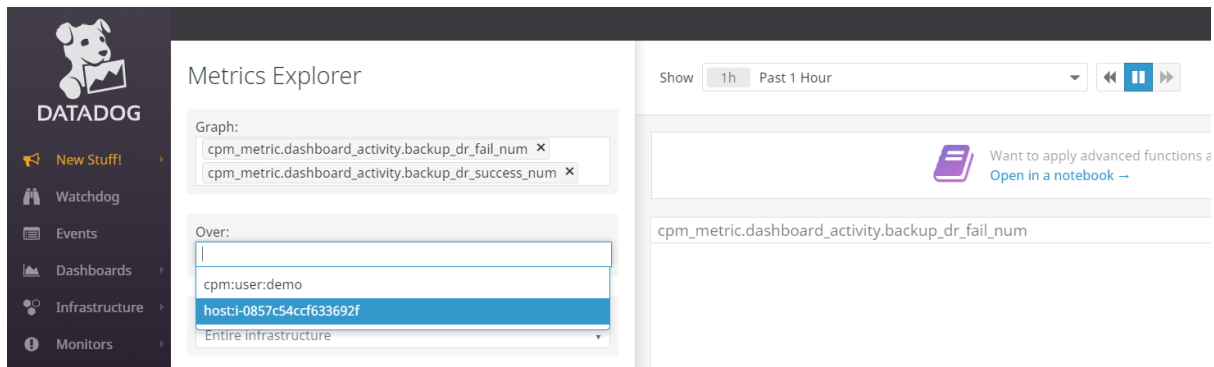
#### 5. Setup Datadog Dashboard metrics

a. Log in to Datadog and go to **Metrics > Explorer**.

In the **Graph** list, select your metrics. All N2WS metrics begin with **cpm\_** followed by <metric-name>.



b. In the **Over** list, select data. You can either select a specific user or the entire N2WS instance. All N2WS user data begins with **cpm:user:** followed by <user-name>.



6. **Configure your Datadog Dashboard by using the N2WS template or creating your own dashboards, and choose the data to monitor.**

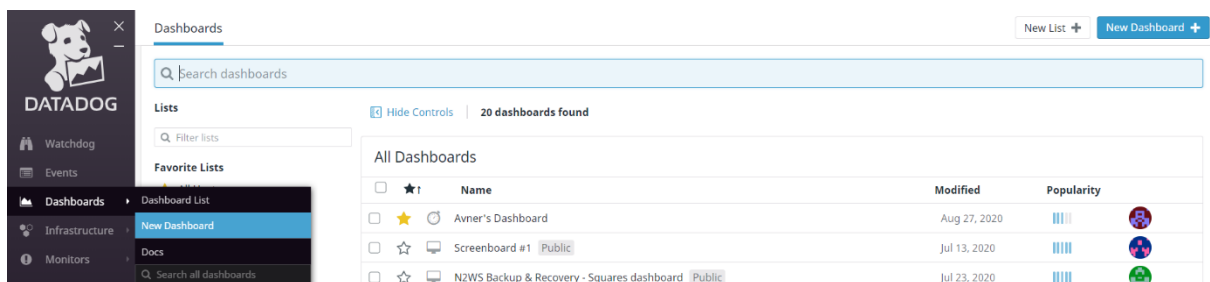
a. To use the N2WS template:

- i. In Datadog Integrations at <https://app.datadoghq.com/account/settings#integrations>, search for the '**N2WS**' tile and install it. You will get a number of types of dashboards for your account, such as:  
'N2WSBackup&Recovery-Graphicalversion'  
'N2WSBackup&Recovery-Graphicalversion-areas'  
'N2WSBackup&Recovery-Squaresdashboard'

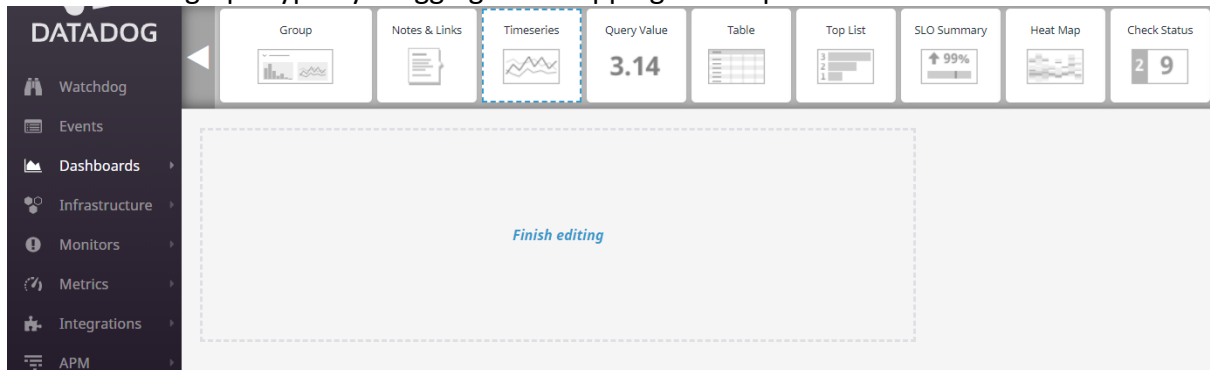
- ii. Alternatively, you can **import JSON templates from N2WS** at <https://support.n2ws.com/portal/en/kb/articles/datadog-templates>

You can modify the dashboard after creating it.

b. To create a Datadog dashboard:



i. Add a graph type by dragging and dropping its template to the dashboard:



ii. Edit the graph for the data to be monitored:



## 1 Select your visualization

Timeseries Query Value Table Heat Map Scatter Plot Distribution Top List Change Host Map

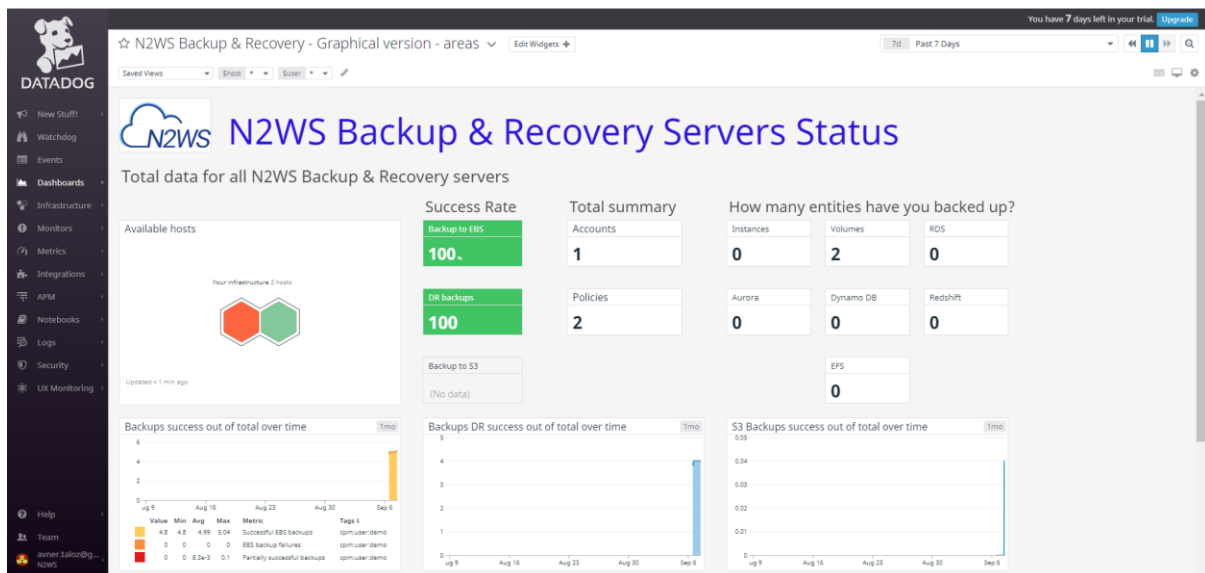
## 2 Graph your data

Edit JSON Share Custom Links

Metric ▼ cpm\_metric.dashboard\_activity.b... from (everywhere) avg by (everything) +  
Display: Lines ▼ Color: Classic ▼ Style: Solid ▼ Stroke: Normal ▼  
Graph additional: [Metrics](#) | [Log Events](#) | [Analyzed Spans](#) | [Live Processes](#) | [Network Traffic](#) | [RUM Events](#)

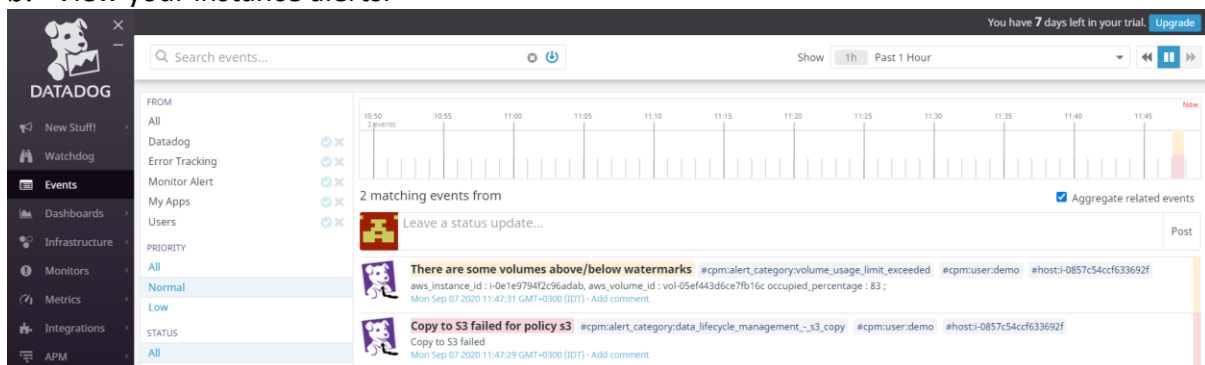
iii. Save the graph settings.

Note: Datadog updates N2WS metrics hourly.



## 7. View N2WS Alerts on Datadog Events

- Log in to Datadog and go to **Events**.
- View your instance alerts:





## D.2 Monitoring N2WS with Web Proxy

If you have restricted outbound traffic, you can proxy all Datadog Agent traffic through different hosts.

1. Connect to your N2WS Backup and Recovery Instance with SSH Client:

```
cd /etc/datadog-agent
```

2. Enable **proxy:** section on `datadog.yaml`.
3. Add your proxy IP, port, username, and password:  

```
https: "http://your-proxy-IP:your-proxy-port"  
http: "http://your-proxy-IP:your-proxy-port"
```
4. Validate **datadog.yaml** on <https://yamlchecker.com/>.

Example:

```
proxy:  
  https: http://54.159.14.45:3128  
  http: http://54.159.145.45:3128
```

For additional proxy configuration options, see <https://docs.datadoghq.com/agent/proxy/>





## Appendix E – Splunk Integration Support

N2WS Backup and Recovery Instance is now supporting the monitoring of backups, DR, copy to S3, alerts, and more by Splunk. The N2WS add-on features:

- Ability to define data input from N2WS via a Technology Add-on (TA)
- Ability to monitor resources and instances
- An N2WS app with 2 dashboards for displaying operational insights:
  - N2WS activity monitor - Information about the data
  - N2WS Alerts

### Limitations:

- No support for Microsoft Azure
- No support for multiple CPMs
- Supported with Splunk Enterprise only

Integration consists of installing Splunk and configuring the TA for N2WS.

### E.1 Configure N2WS Server for Splunk

To configure the N2WS server:

1. Edit the N2WS configuration file as follows:

```
>> su cpmuser
>> vi /cpmdata/conf/cpmserver.cfg
[external_monitoring]
enabled=True
```
2. Restart apache:

```
>> sudo service apache2 restart
```
3. To check the status of the Splunk integration, go to **Help > About** and verify that **‘External monitoring (Datadog / Splunk) enabled’** is **Yes**.

### E.2 Installation on Splunk

Splunk can work with a proxy for reaching N2WS APIs.


**Note:** Verify that you have the correct app installation files:

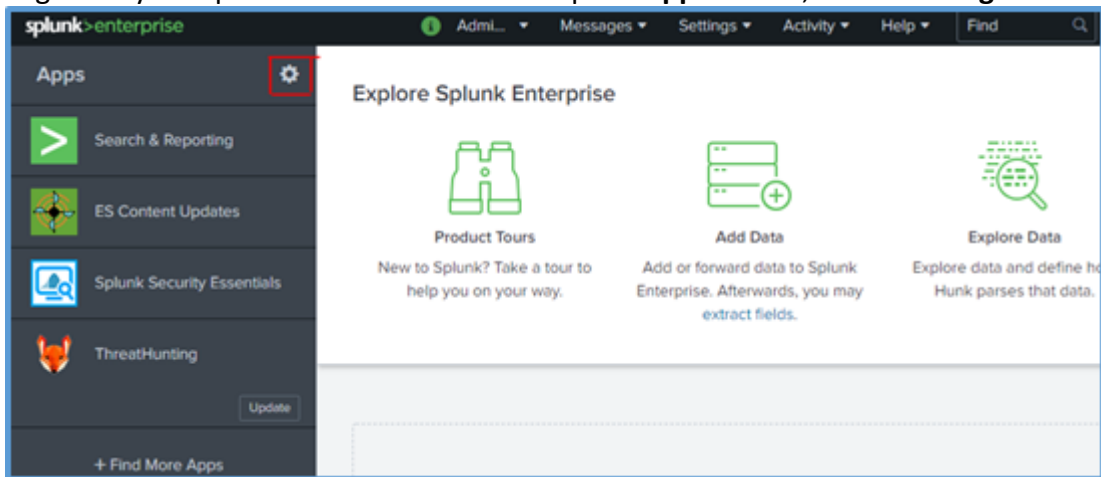
- N2WS\_app\_for\_splunk.spl
- ta\_N2WS\_for\_splunk.spl

Both files can be downloaded from the Splunk MarketPlace.

**To install:**

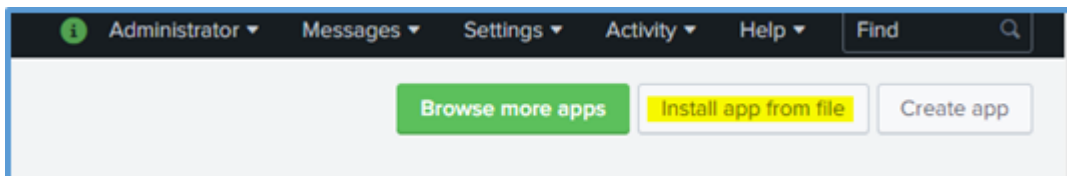


1. Log on to your Splunk Web and in the Enterprise **Apps** screen, select **Settings** .

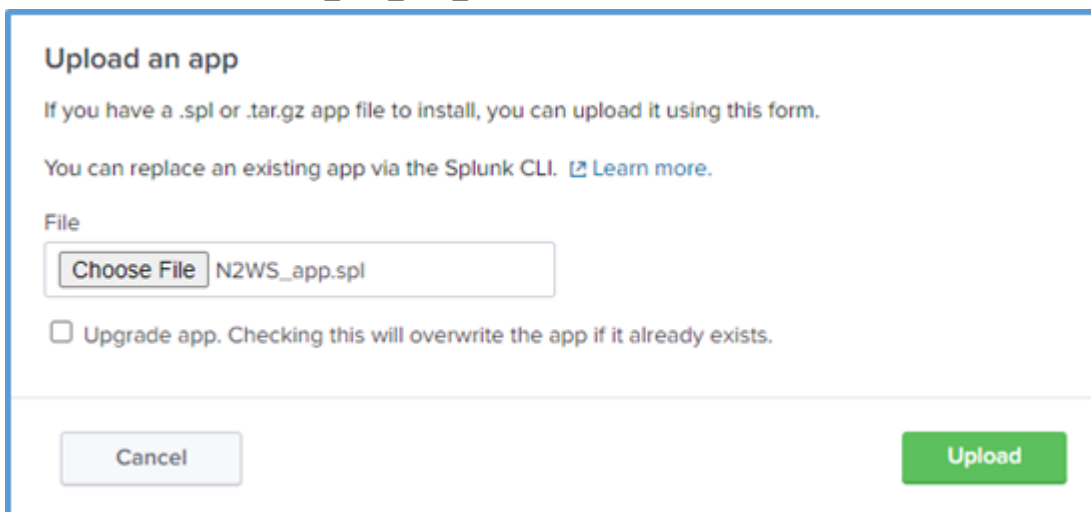


The **Manage Apps** page opens.

2. In the upper right, select **Install app from file**.



3. For an initial installation:
  - a. Browse for the `N2WS_app_for_splunk.spl` file. Select **Upload**.



- b. Browse for `ta_N2WS_for_splunk.spl`. Select **Upload**.

4. For updates, browse for the current file and select **Upgrade app**.

Installation of Splunk is fully documented at

<https://docs.splunk.com/Documentation/Splunk/8.1.1/Installation/InstallonLinux>

## E.3 Configuration of TA for N2WS

Two configurations are required:

- TA of the REST API



- Data inputs from N2WS for Alerts and Dashboard information

#### To configure the TA:

1. Go to **splunk > App N2WS Add-on > Configuration**.
2. If needed, select the **Proxy** tab, complete the settings, and select **Save**.

The screenshot shows the 'Proxy' tab in the configuration interface. It includes an 'Enable' checkbox, a 'Proxy Type' dropdown menu set to 'http', and input fields for 'Host', 'Port', 'Username', and 'Password'. There is also a 'Remote DNS resolution' checkbox and a green 'Save' button at the bottom.

3. In the **Logging** tab, select the TA Log level: DEBUG, INFO, WARNING, ERROR, CRITICAL.
4. In the **Add-on Settings** tab, set the **API Url** of the target server and the **API Key**. You can copy and paste the **API Url** and **API Key**, or both can be left empty for the customer to fill in.
  - The **API Url** is the address of your N2WS server.
  - You can generate an API Key in N2WS at **User > Settings > API Access**.

The screenshot shows the 'Add-on Settings' tab in the configuration interface. It features input fields for 'API Url \*' (containing 'https://54.152.135.121/api') and 'API Key \*' (containing a long alphanumeric string). A green 'Save' button is located at the bottom.

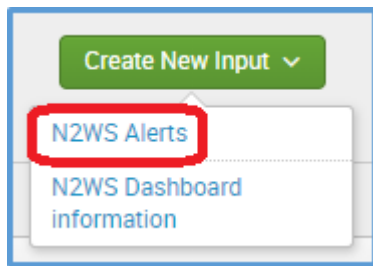
5. Select **Save**.

#### To configure data inputs:

Note: Both **Dashboard** and **Alerts** inputs should be defined.



1. In the App menu, select **Inputs**.
2. In the **Create New Input** menu, select **N2WS Dashboard** information or **N2WS Alerts**.



3. Enter the relevant data input information:

- **Name** – Unique name of the input.
- **Interval** - Time interval for fetching the data from N2WS in seconds. 300 is recommended.
- **Index** - The Splunk index (silo) to store the data in:
  - For Alerts, **n2ws\_alerts**
  - For Dashboard information, **n2ws\_di**
- **Last alert ID** – Leave blank.

4. Select **Update**.

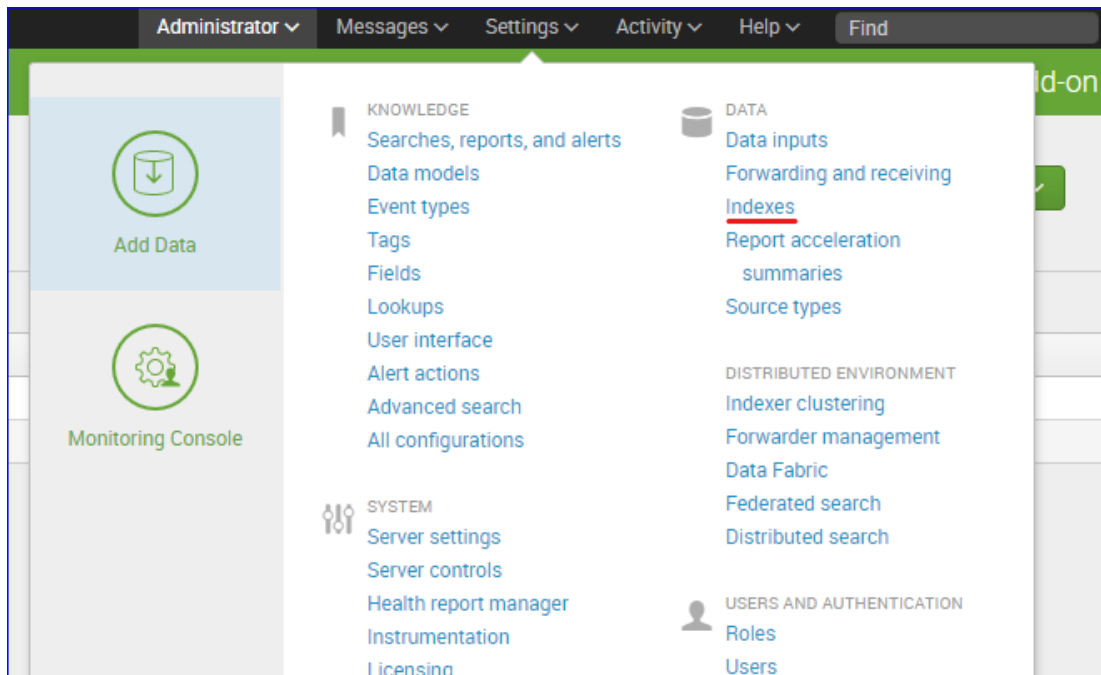
When finished, the Inputs should look like this:

Inputs Configuration Search				
Inputs				
Manage your data inputs				
2 Inputs		Services : All		filter
i	Name	Interval	Index	Status
>	n2ws_alert	60	n2ws_alerts	Enabled
>	n2ws_di	60	n2ws_di	Enabled

To manage the Inputs, in the **Actions** column, select from the **Action** menu: **Edit**, **Delete**, **Disable**, or **Clone**.

**To configure default data indexes:**

1. Select **Settings** on the upper right corner and then select **Indexes**.



- Verify that the following indexes exist under the N2WS app. If not, select **New Index** to add indexes of the CPM information:

- **N2ws\_alerts**
- **n2ws\_di**

Name	Actions	Type	App
n2ws_alerts	Edit Delete Disable	Events	N2WS_app_for_splunk
n2ws_di	Edit Delete Disable	Events	N2WS_app_for_splunk

- In the file system, copy `macros.conf` from the default folder to the local folder. For example,  
Source: `C:\Program Files\Splunk\etc\apps\N2WS_app_for_splunk\default`  
Target: `C:\Program Files\Splunk\etc\apps\N2WS_app_for_splunk\local`
- Edit the `macros.conf` file under 'local' and change the default index to the new indexes that were created.

```

1 #####
2 # Base Macros
3 #####
4
5 [n2ws_di_index]
6 definition = index="n2ws_di" sourcetype="n2ws:di"
7
8 [n2ws_alerts_index]
9 definition = index="n2ws_alerts" sourcetype="n2ws:alerts"

```

- Restart the **Splunkd** service from Windows Services.

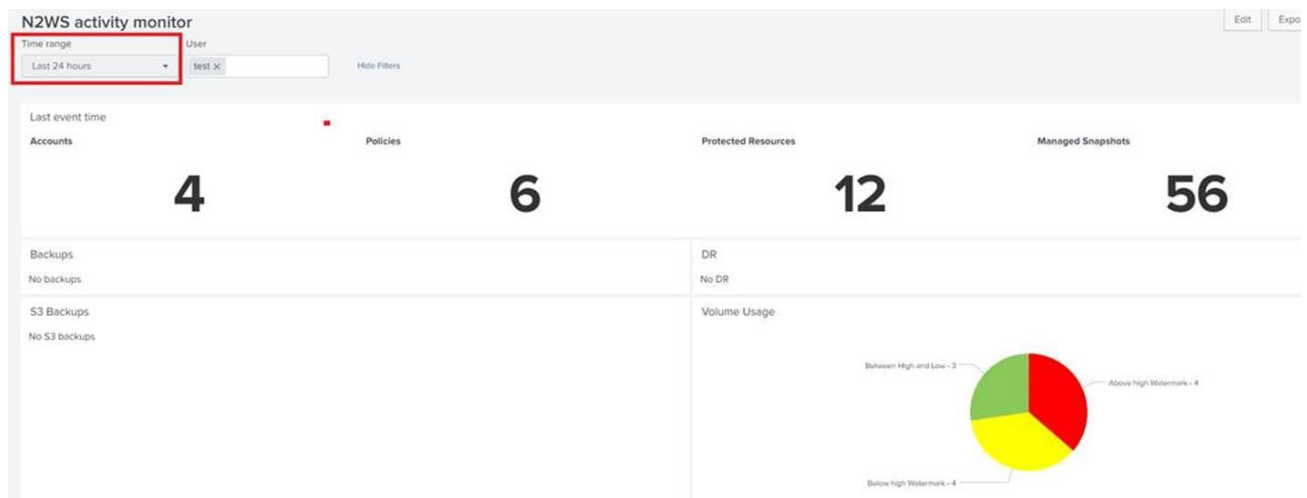


## E.4 Viewing Dashboards

Go to Splunk **Apps** and find **N2WS app for splunk**. The N2WS app contains tabs for N2WS activity monitor and N2WS Alerts. **Edit** and **Export** options are available in the upper right corner of each dashboard.

### E.4.1 N2WS activity monitor

- Filter for Time Range (defaults to last 24 hours) and Users, including root and delegates.
- Displays All Accounts, Policies, Protected Resources, Managed Snapshots, Backups DR, S3 Backups, Volume Usage, and other requested data.



For Protected Resources and Managed Snapshots, select the displayed number to drill down and view a table of the resources and the number of items for each resource type for the selected users, or managed snapshots, count of each type, and a total.

### E.4.2 N2WS Alerts

The Alerts dashboard includes filters for:

- Time range - Last 24 hours (default)
- User - All (default) or username
- Severity - All or Info or Warning
- Category - All or Tag Scan, volume usage limit exceeded



splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Search N2WS activity monitor N2WS Alerts Others N2WS Alerts N2WS app for splunk

### N2WS Alerts

Time range: Last 24 hours User: All x Severity: All x Category: All x Hide Filters

Time	User	Severity	Category	Message
2020-12-21T12:31:48Z	root	Warning	volume usage limit exceeded	aws_instance_id : i-009b92e9e8cdd12a6, aws_volume_id : vol-0993e221bbfda34e0 occupied_percentage : 0 percent exceeding Low threshold; aws_instance_id : None, aws_volume_id : vol-01d52d677432859d1 occupied_percentage : 7 percent exceeding Low threshold;
2020-12-21T11:00:52Z	root	Warning	volume usage limit exceeded	aws_instance_id : i-0603b7730c2ce5ef2, aws_volume_id : vol-04861011dc5cc8fd3 occupied_percentage : 100 percent exceeding High threshold;
2020-12-21T10:06:12Z	root	Info	Tag Scan	Backup Tag scan - Policy 'pol_custom_tag' doesn't exist/attached to account IAM_root 635216694456. Tagged Volumes: [vol-0abebc7b0574c070d]
2020-12-21T10:06:12Z	root	Info	Tag Scan	Backup Tag scan - Can't create new policy Pol3. Source policy pol2 doesn't exist
2020-12-21T10:06:12Z	root	Info	Tag Scan	Backup Tag scan - Policy 'pol111' doesn't exist/attached to account IAM_root 635216694456. Tagged Volumes: [vol-06130a9b557bdc79a, vol-0a901f0b8235d5dfb]

The list defaults to descending sort order. Select any column to change sort order.

- Time - Date, time, event ID
- User
- Severity
- Category
- Message