Noovolari Smart Back Documentation v1.0

Getting Started

In this page

Noovolari Smart Backup in few words

Noovolari Smart Backup is the smartest backup-as-a-service tool for managing backups and disaster-recovery of your AWS infrastructures.

From Noovolari smart web console it's easy to centralize the control of all your AWS resources, even in if spread across multiple AWS accounts and regions.

Noovolari allows you to backup multiple instances, full application stacks or even a whole AWS infrastructure with no downtime.

Moreover, Noovolari Smart backup ensures data integrity and full recoverability of your applications and OS thanks to its application-aware processing.

Register a new account

You can register a new account on Noovolari.com platform by providing a valid email address (verification required) and by creating a secure password.

Sign in link

Click on “Don’t have an account? Sign up” link at the bottom of the login screen; Provide a valid email address and a secure password; Click “create account” button, check your email and confirm your account.

Your account has been successfully created! Please, read carefully our “Terms of services” and “Private Policy” pages.

Sign in – Login with Google

Select “Login with Google” and choose the google account you want to use.

You are now logged in!

Login

You can easily login by filling the form with your email address and your secure password or by choosing “login with google”.

Forgot your password?

Recover it by clicking on “Forgot password” link. Provide the email address associated to your Noovolari account and check your email to recover your password.

First login

If you are new on Noovolari Platform, you first need to register a new Cloud Account.

Choose your Cloud provider and click “next”.

Quick Start

Register a new Cloud account

In this page

AWS – Automatic Registration

To proceed with an automatic registration:

provide an account name for the account you are creating and your AWS account number*. Then click “next”.

Provide admin access key and admin secret key**.

Select “attach existing policy”, choose “administrator access”, click on “Review” and then click on “create user”. From this view, you can visualize Access key value and secret key value; you are now able to copy them to the Noovolari account registration page. Click “register”. The registration of your Noovolari account is completed.

(Note: after the creation of your account on Noovolari Platform is completed, the user created on AWS and all the credentials associated to it can be deleted. We don’t store your credentials at any time).

*AWS account number is a numeric 12-Digit long value associated to your AWS account. To get it, login to your AWS console and check “my account” section from the dropdown menu placed on the right top of the screen.

**Admin access key is an alphanumeric value placed in the IAM section of your AWS account. From IAM section, click on “user” link on the left side of the screen. Click on “add user” button and insert a name. In “access type” field, choose “programmatic access” and click “next”.

AWS – Manual registration (CLI)

If you want to register your account manually using CLI, click on “switch to manual mode” during the registration process and select “Command Line Interface”. Open your terminal and follow the step-by-step guide on Noovolari registration page.
Please, verify that your console is properly configured according to AWS CLI guidelines.

1. Save the Assume Role policy locally to a file with this command. This policy contains the actions that Noovolari Smart Backup can perform in behalf of your Account.

```
echo '{"Version": "2012-10-17","Statement": [ {"Effect": "Allow","Action": [
"ec2:DescribeSnapshots", "ec2:CreateSnapshot", "ec2:DeleteSnapshot",
"ec2:ModifySnapshotAttribute", "ec2:DescribeInstances", "ec2:RunInstances",
"ec2:StartInstances", "ec2:StopInstances", "ec2:DescribeVolumes",
"ec2:CreateVolume", "ec2:DeleteVolume", "ec2:AttachVolume", "ec2:DetachVolume",
"ec2:RegisterImage", "ec2:DeregisterImage", "ec2:CreateTags", "ec2:DescribeRegions"
],"Resource": [ "*" ]}, {"Effect": "Allow","Action": [ "rds:DescribeSourceRegions",
"rds:CreateDBSnapshot", "rds:DescribeDBSnapshots", "rds:DeleteDBSnapshot",
"rds:CreateDBInstance", "rds:ModifyDBInstance", "rds:DescribeDBInstances",
"rds:DescribeDBParameters", "rds:DescribeReservedDBInstances",
"rds:RestoreDBInstanceFromDBSnapshot", "rds:DeleteDBInstance" ],"Resource": [ "*"
]}, {"Effect": "Allow","Action": [ "rds:CreateDBClusterSnapshot",
"rds:DeleteDBClusterSnapshot", "rds:DescribeDBClusterSnapshots",
"rds:DescribeDBClusters", "rds:RestoreDBClusterFromSnapshot", "rds:DeleteDBCluster",
"rds:ModifyDBCluster" ],"Resource": [ "*" ]}, {"Effect": "Allow","Action": [
"iam:GetRole", "iam:GetRolePolicy", "iam:DeleteRole", "iam:DeleteRolePolicy"
],"Resource": [ "arn:aws:iam::*:role/noovolari-smartbackup-role-[redacted]' ]} ]}' >>
nsb-assume.json
```

2. Save the Trust Relationship locally. This policy allows Noovolari smart Backup to assume the previous Role.

```
echo '{"Version": "2012-10-17","Statement": [ {"Effect": "Allow","Principal":
{"AWS": "[redacted]"},"Action":
"sts:AssumeRole","Condition": {"StringEquals": {"sts:ExternalId":
"[redacted]"}}} ]}' >> nsb-trust.json
```

3. Create the Assume Role based on the saved file in step 1. Be assured to have the CLI properly configured with a role suitable for IAM operations.

```
aws iam create-role --role-name noovolari-smartbackup-role-[redacted] --assume-role-
policy-document file://nsb-assume.json
```

4. Create the Trusted Relationship based on the file saved in step 2.

```
aws iam put-role-policy --role-name noovolari-smartbackup-role-[redacted] --policy-name
Noovolari-SmartBackup-Access --policy-document file://nsb-trust.json
```

5. (Optional) Clean the saved files.

```
rm nsb-assume.json && rm nsb-trust.json
```

AWS – Manual registration (IAM)

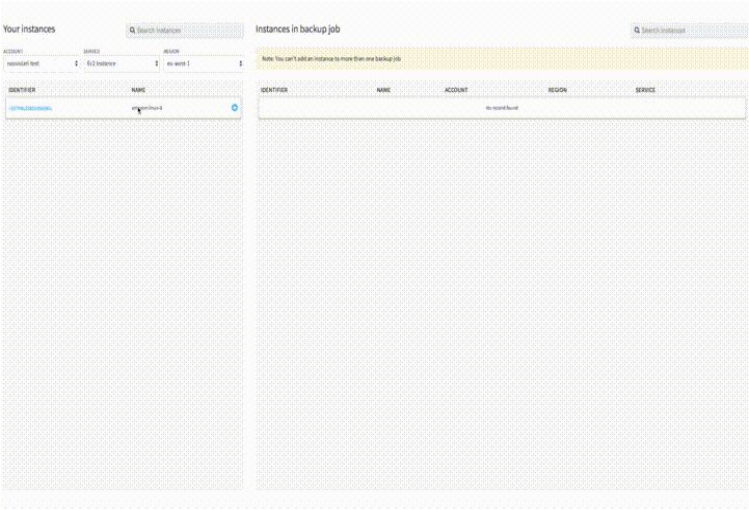
If you need to register your account manually using IAM, click on “switch to manual mode” and select “policy IAM”. First login to your AWS console and then follow the step-by-step guide on Noovolari registration page.

Register a new backup job

In this page

Create your first backup job

You can create a new backup job by clicking on “+” button on “backup job page”. After that, you will be able to associate instances to it (drag and drop). You can associate one or more virtual machine to the same backup job by dragging and dropping them to the backup job section.



Consistency

Backup jobs on running instances can be either agentfull (by installing our agent on your virtual machines, your instances will be freezed to a coherent state before snapshots are triggered) or agentless. You can choose backup typology by selecting “yes” or “no” in “consistency” section.

Infrastructure Consistency

Both associating all the instances of infrastructure to the same backup job and installing our agent on each of them ensure also a coherent recovery point of the whole infrastructure.

Activation

Select “yes” if you need to start up your backup job immediately after the creation of the new backup job. By selecting “no” you will be able to start it later.

Retention rules

You can add retention rules (max 5) to backup jobs by choosing the frequency of backups and the number of backups you need to retain.

Note: each instance associated to the backup job you are creating will follow the rules you are setting up.

If you need to change/add retention rules, you can select a backup job from the backup jobs list and, by selecting “resources” tab, you can edit retention rules associated by clicking on “edit resources” button.

Cross-region replica

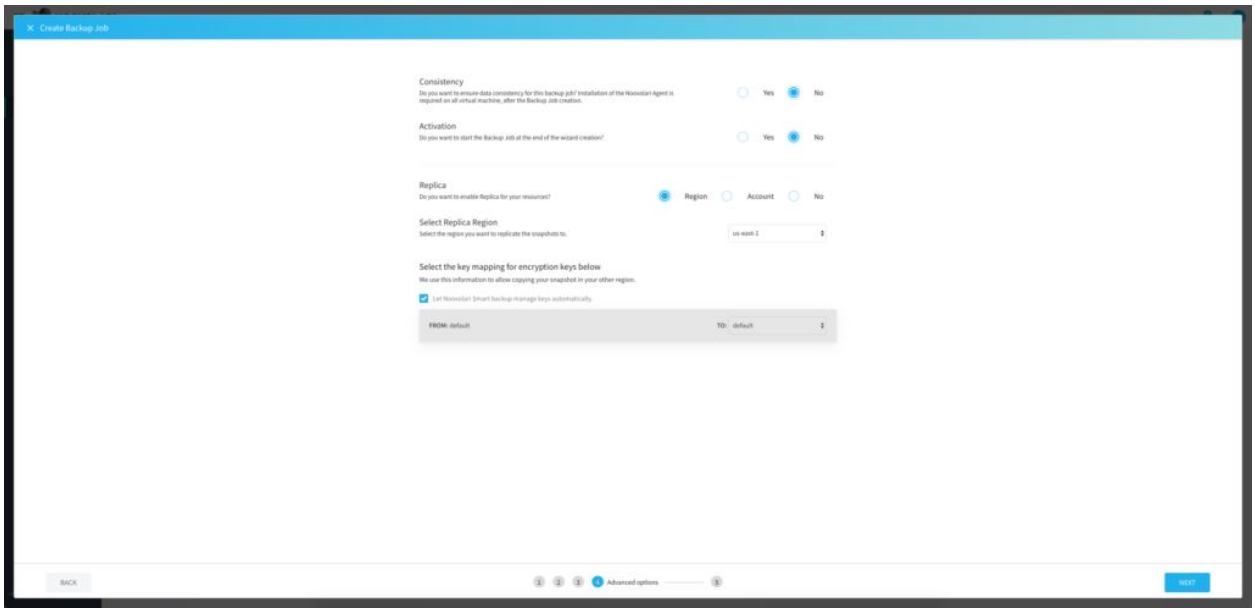
In this page

What is cross-region replica

With the Cross-region replica feature, you can replicate a recovery point of a whole infrastructure across multiple AWS Regions. The challenge is being able to move snapshots from one region to another in a safe, smart, secure, timely, automated way.

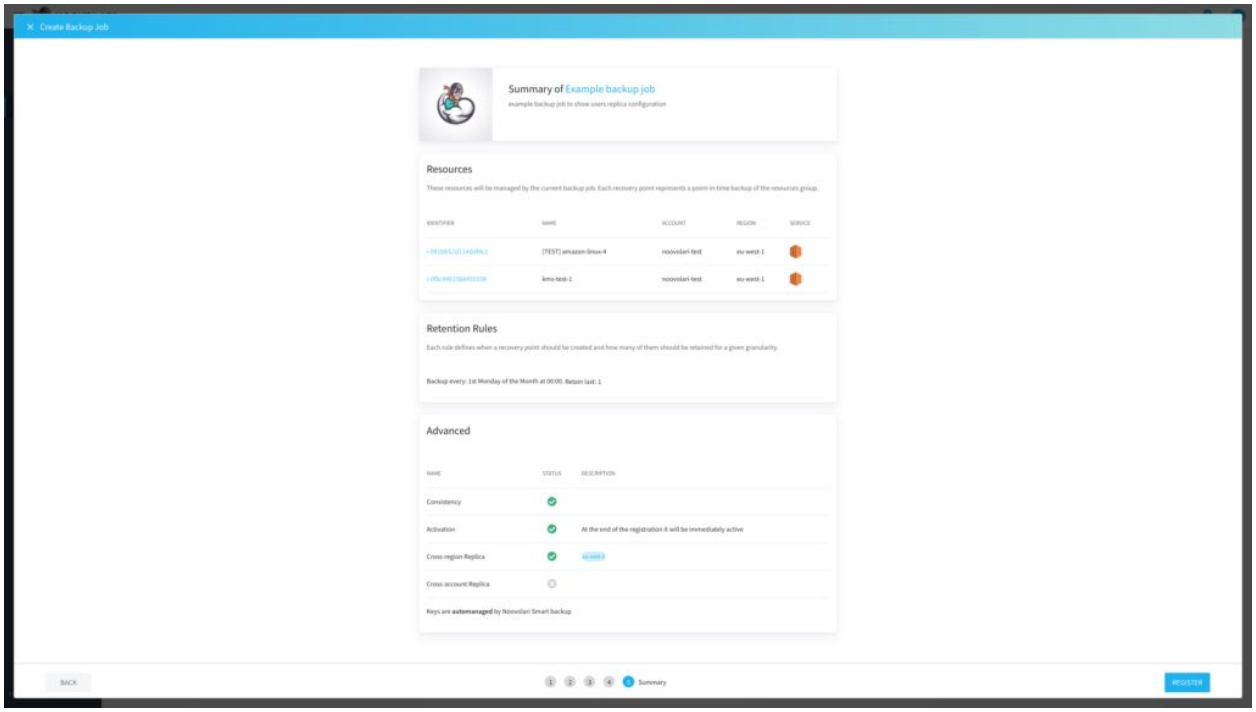
Enabling cross-region replica in a backup job

When creating a new backup job, choose first which instances your backup job will manage and then select “Region” to activate replica for every recovery point in the backup job:



By choosing region replica, Noovolari will search for you for encrypted volumes in any of the resources of the backup job, and then it will guide you in choosing the key-mapping to use to encrypt volumes in the new replica region. Noovolari is also able to manage encryption for you, if needed.

As shown above, at the end of the backup job creation process, you’ll get a summary with the region replica checked.



Cross-account replica

In this page

What is cross-account replica

Noovolari Smart backup can now create a replica in an additional AWS account. This feature ensures protection for the recovery points by replicating them in a separate AWS account, even if the main account is corrupted.

Enabling cross-account replica in a backup job

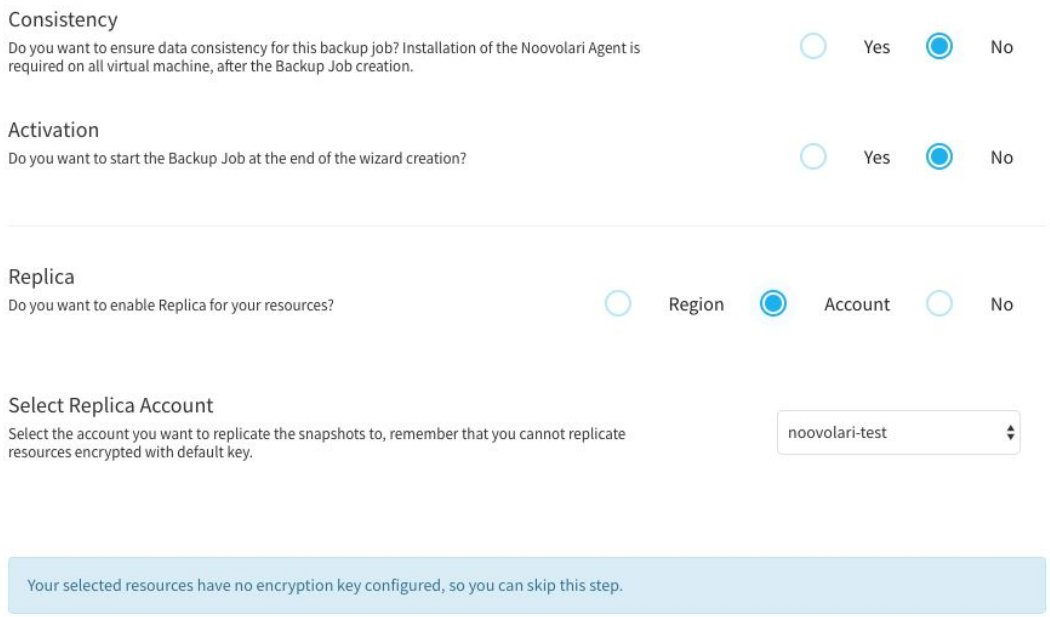
At the fourth step of the backup job creation, you can choose to replicate each recovery point in another AWS account managed by Noovolari Smart backup.

Furthermore, you can also choose to replicate each recovery point in another AWS account managed by Noovolari Smart backup.

Noovolari will identify for you encrypted volumes and it will guide you in choosing a key mapping for new snapshots in the replica AWS account.

Please note that if one of the volumes is encrypted with the default region key of KMS, you won't be able to use cross-account replication.

After the backup job creation, a snapshot replica will be created for each recovery point created based on the backup job retention rules.



Installing Noovolari agent

In this page

What is Noovolari agent

Noovolari Smart backup let you backup multiple Cloud instances together and get a single snapshot of your whole cloud infrastructure in a consistent state. That means all your instances (Ec2) will do a backup at the same moment to avoid data loss.

If you want that kind of consistency you have to install an agent on every Ec2 Instance you wants to include in your infrastructure.

Linux agent installation

Firstly you have to go to the resources view and click on the Actions tab in the row of the specified resource, and click on “Agent link”. Then:

- log on your instance
- Copy/paste the script
- Follow instructions

It’s smart to install agent in a Linux distros (Ubuntu, Amazon Linux, Centos, Debian, Red Hat, Suse), you just have to access to the instance and then copy the script in the terminal and follow the instructions.

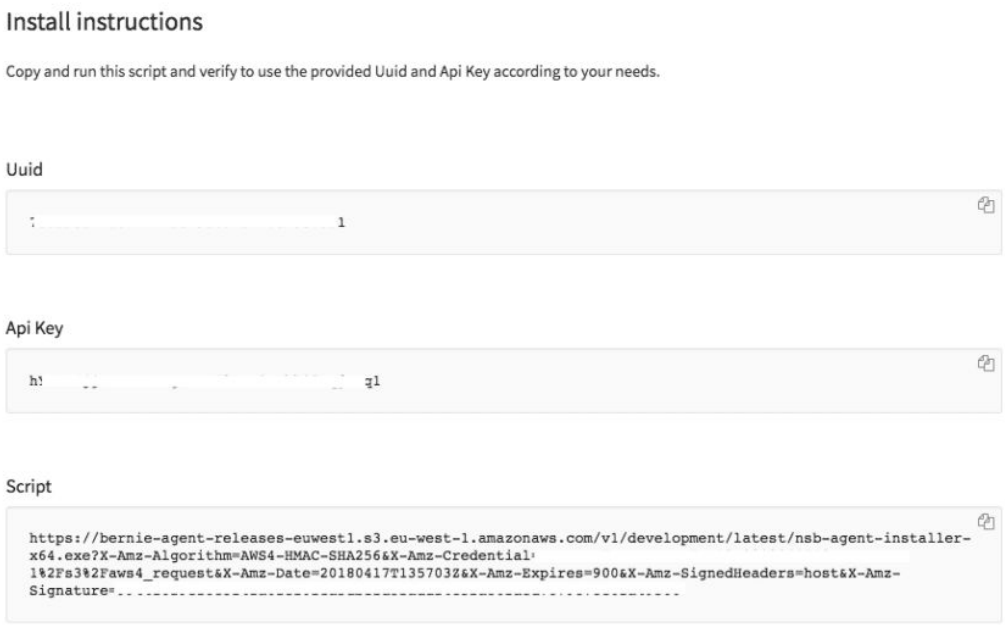
In the installation the agent will ask you if you want the MySQL consistency (username and password needs to be provided). The agent will ask you consistency on every DBs on your server.

If MySQL server in consistent every time Noovolari Smart backup do a snapshot of the infrastructure the sever will be freeze for the duration of the snapshot.

At the end remember to paste the provided UUID and Api Key that you have received in the portal.

Windows agent installation

For a Windows instance, Noovolari will provide you a custom link.



After accessing to your Windows instance, paste the given link in the browser, it will download an .exe installer.

Known issue: on older windows server versions, there’s a known bug that will make the downloaded file lose extension .exe . Just rename and add the extension to the file.

Double click on the .exe file and the installer will start. During installation you will be prompted for UUID and Api Key, you can find them in the Agent Link action.

Recovery

In this page

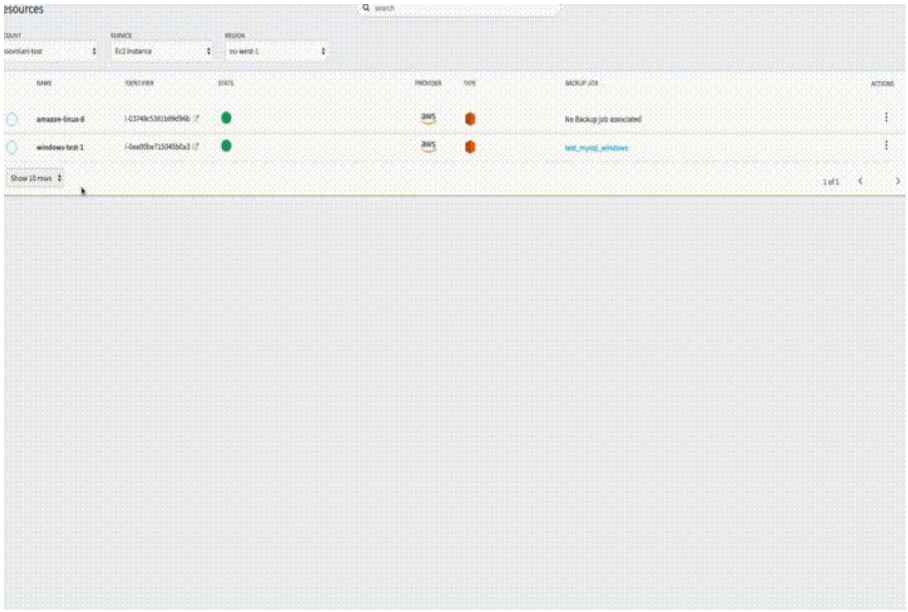
What is recovery

Recovery feature allows you to bring back your instance to a healthy, working state corresponding to a specific point-in-time.

How to restore a specific resource

Through the “recovery” function you can browse between backups made for a specific instance – created by manual backup or backup jobs – and, by restoring one of them, you can backing up to a previous state of your instances.

You can restore a backup from “backups” tab in “Resources” section.



File Level Recovery

In this page

What is File Level recovery

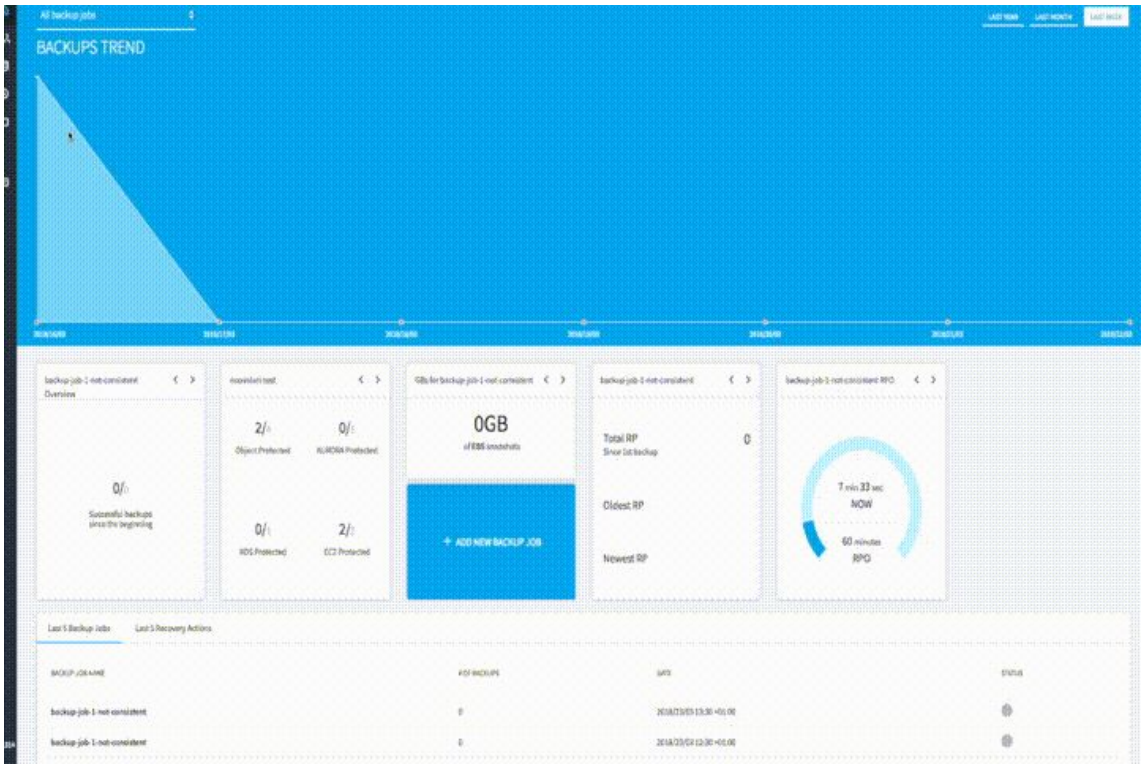
FLR allows you to browse between files included in a backup in order to pick up a specific one.

Using FLR feature

You can do so by selecting “File Level Recovery” from the menu placed on the left and by choosing a specific backup of an instance.

Once you retrieved the file needed, close the Recovery Session by clicking “close session” button placed on the top right of the window.

When you start the Recovery Session you have 60 minutes to find the file you are looking for and to download it, anyway after 60 minutes you can start a new Recovery Session.



How to backup an EC2 instance with Noovolari Smart Backup

With Noovolari Smart Backup is extremely easy to backup an EC2 instance and ensure that your data and your application are protected from accidental failures and data loss of any kind.

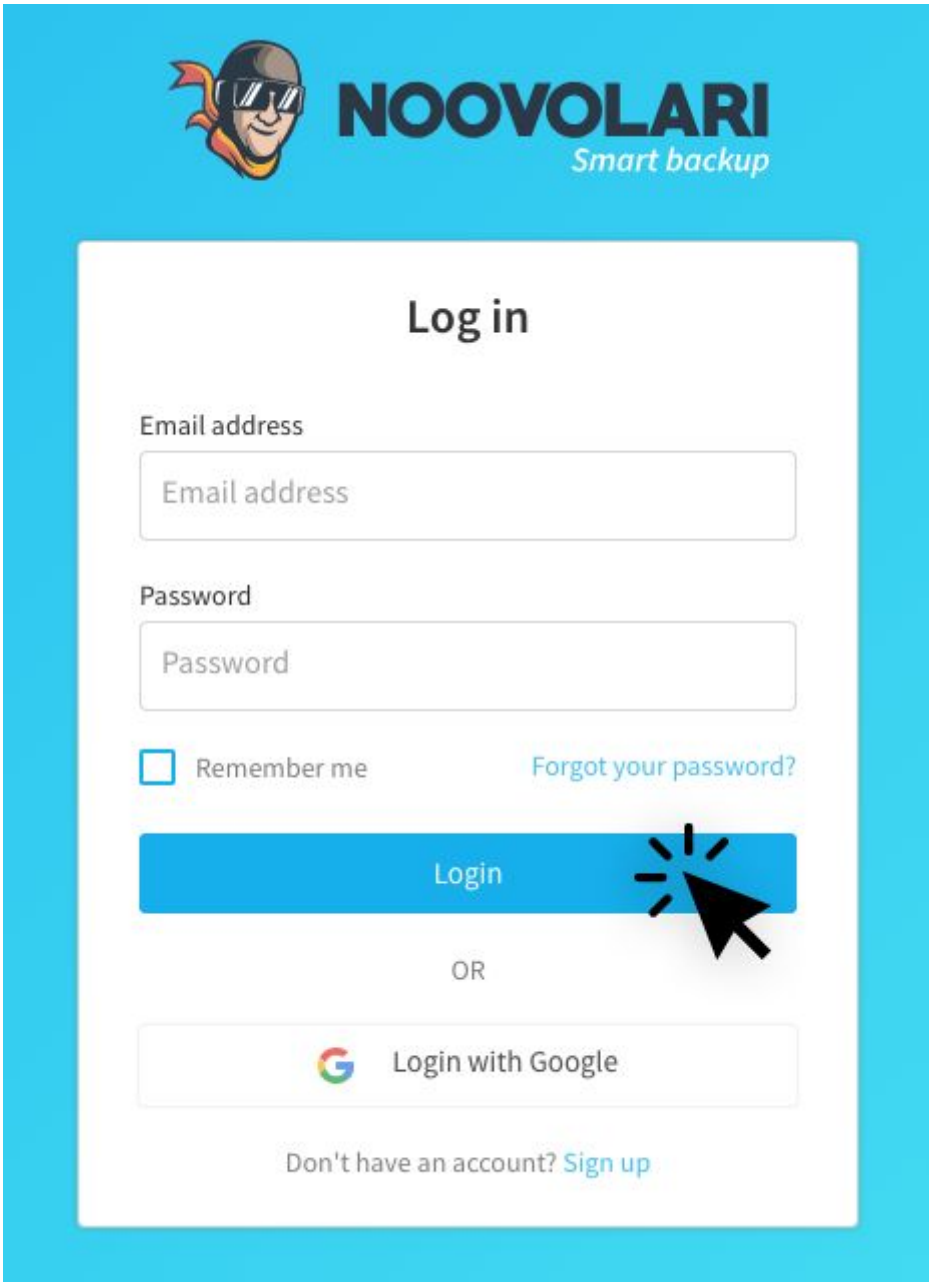
By doing a backup of your instance you can than recover it with the exact same data and resource configuration that you had when you did a snapshot of that particular cloud resource.

You can make a backup of the instance by doing these small 3 steps:

1. Login to your Noovolari Smart Backup account
2. Select an EC2 instance from the Resource View
3. Click on “Manual backup”

Login to your Noovolari Smart Backup account

(not a user, yet?Sign up now for free!);

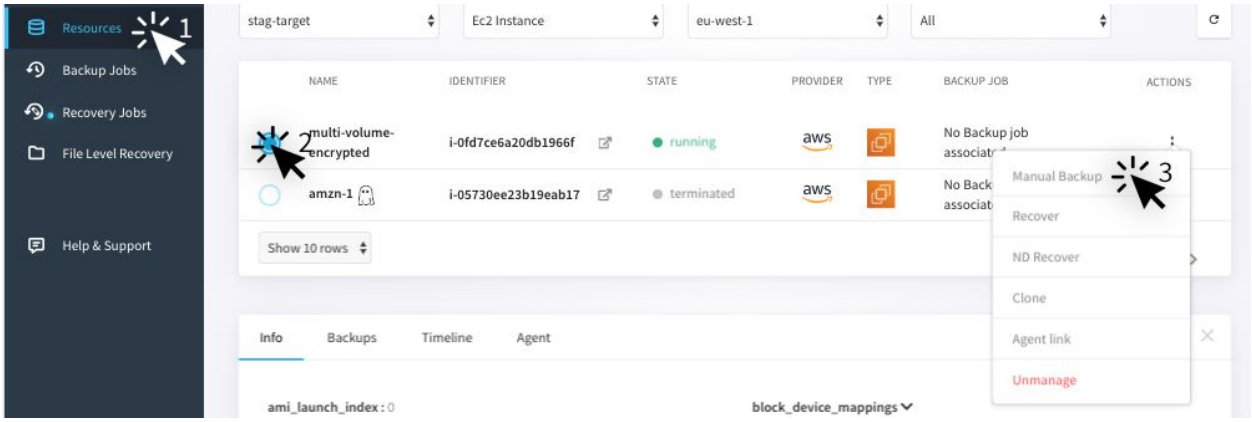


Select an EC2 instance from the Resource View

(HINT: be sure first that the EC2 instance you need to backup is not in “terminated” status. You can check your EC2 instance status from the resource table).

Click on “Manual backup”

By choosing it from the menu placed on the right.



How to backup an RDS instance with Noovolari Smart Backup

With Noovolari Smart Backup it is possible to make a point-in-time snapshot of your RDS instance, ensuring that your data is protected from errors, accidental loss or unwanted modification.

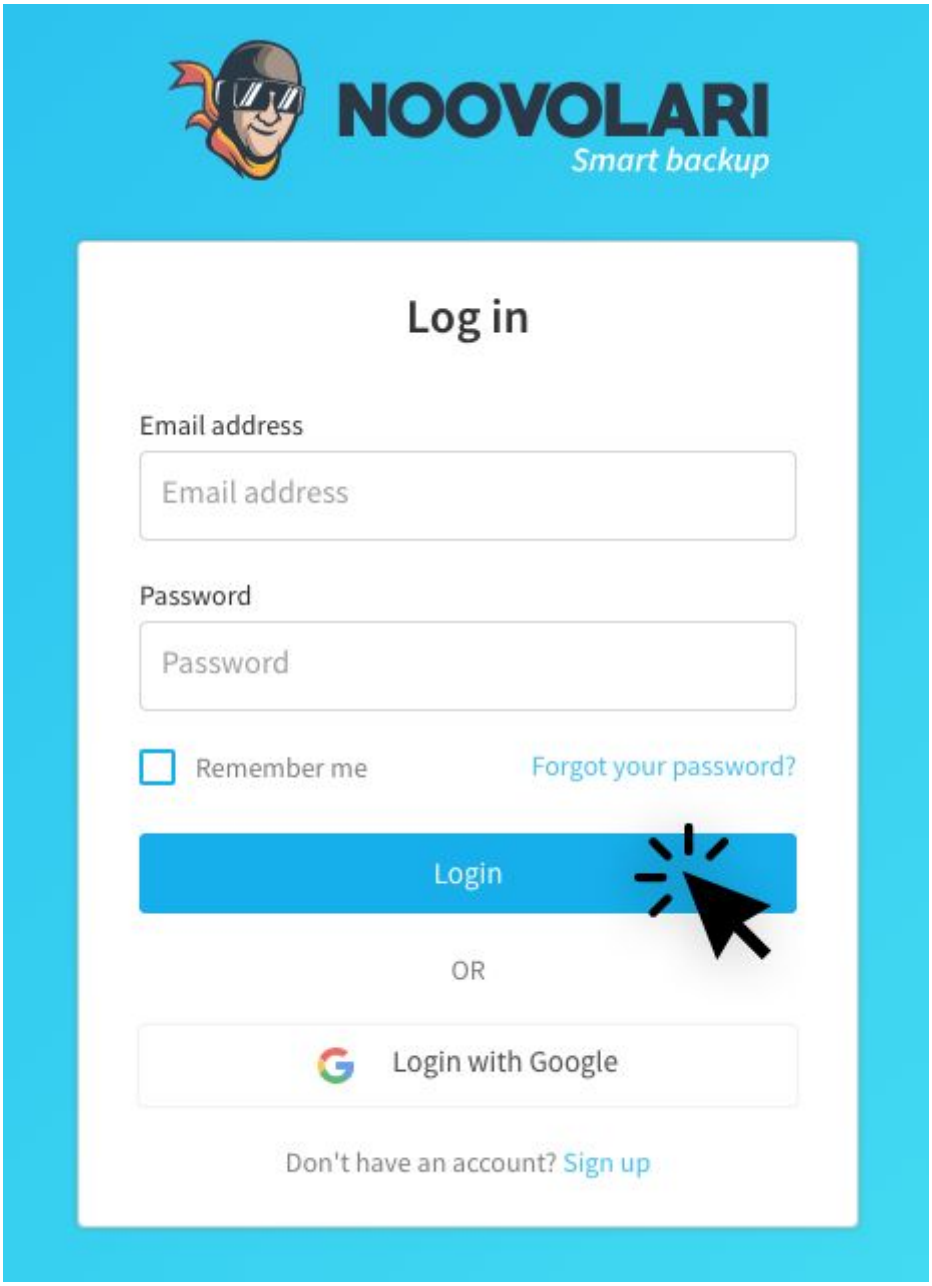
The snapshot will be visibile and fully manageable from both Noovolari Interface and AWS Console.

To make a RDS backup follow these simple steps:

1. Login to your Noovolari Smart Backup account
2. Select the RDS instance
3. Click on “manual backup”

Login to your Noovolari Smart Backup account

(not a user, yet?Sign up now for free!);

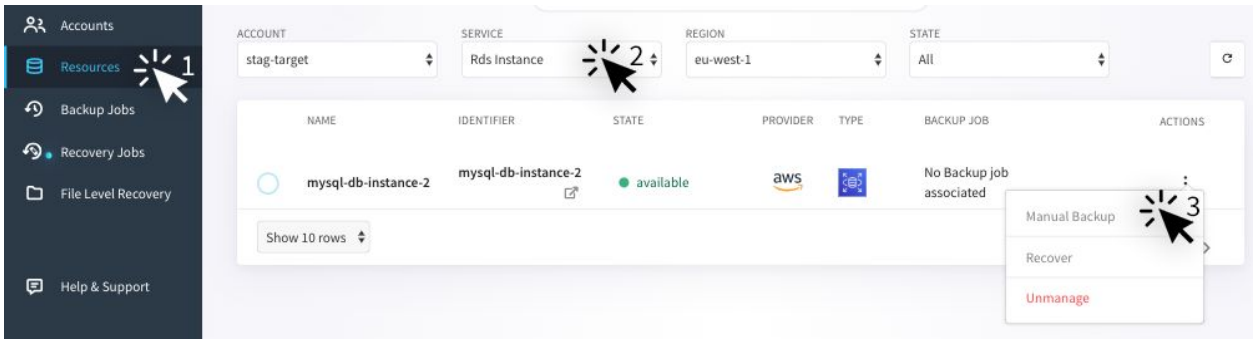


Select the RDS instance

Select the RDS instance from the Resource View by selecting “RDS Instance” from the service dropdown; this operation will filter the selected resources showing you only RDS instances.

Click on “manual backup”

Click on “Manual Backup” choosing it from the menu placed on the right.



How to backup an RDS Aurora cluster with Noovolari Smart Backup

With Noovolari Smart Backup it is possible to make a point-in-time snapshot of your RDS Aurora cluster, ensuring that your data is protected from errors, accidental loss or unwanted modification.

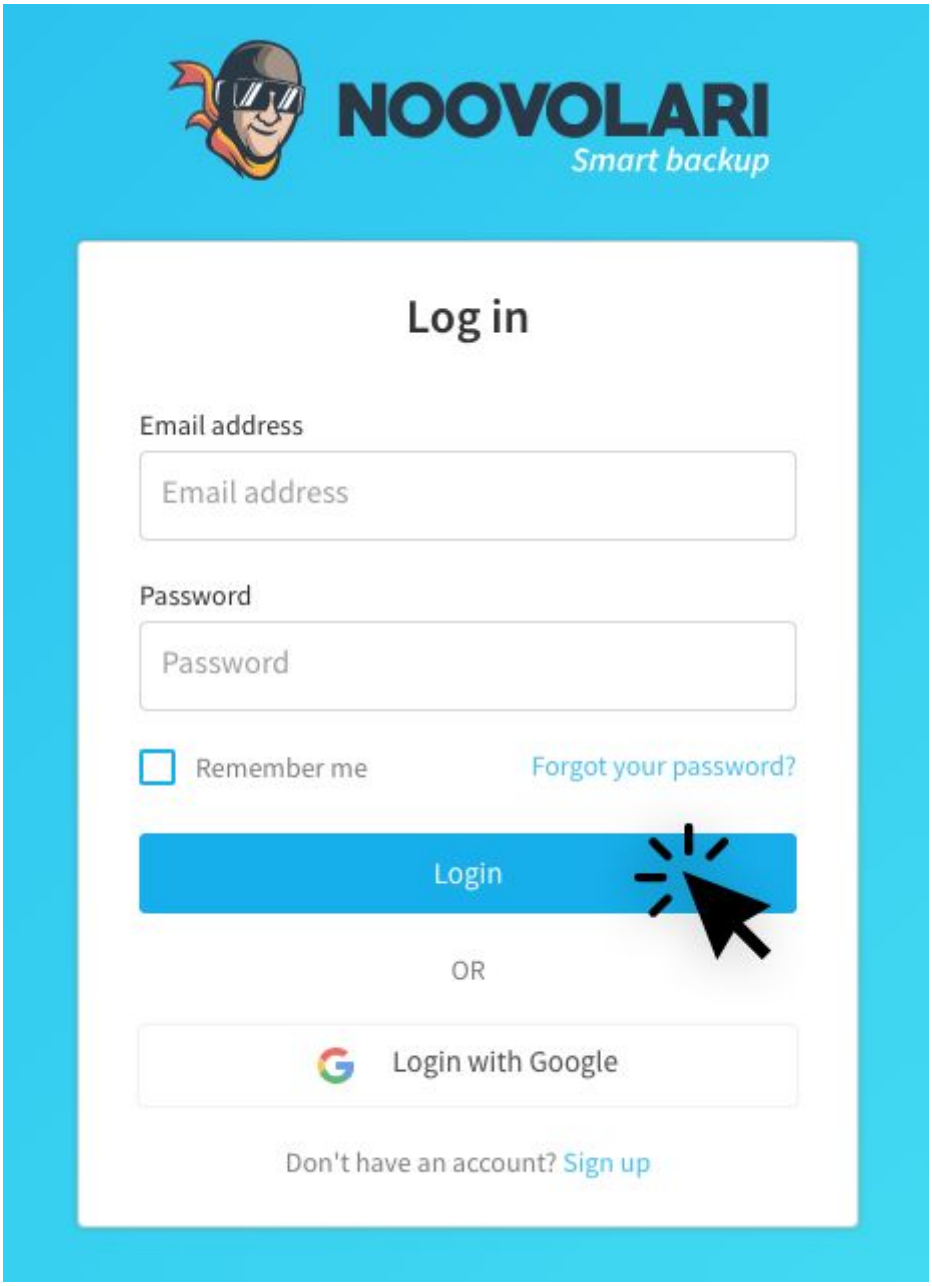
The snapshot will be visibile and fully manageable from both Noovolari Interface and AWS Console.

To make a RDS Aurora cluster backup follow these simple steps:

1. Login to your Noovolari Smart Backup account
2. Select the RDS Aurora Cluster
3. Click on “Manual backup”

Login to your Noovolari Smart Backup account

(not a user, yet?Sign up now for free!);



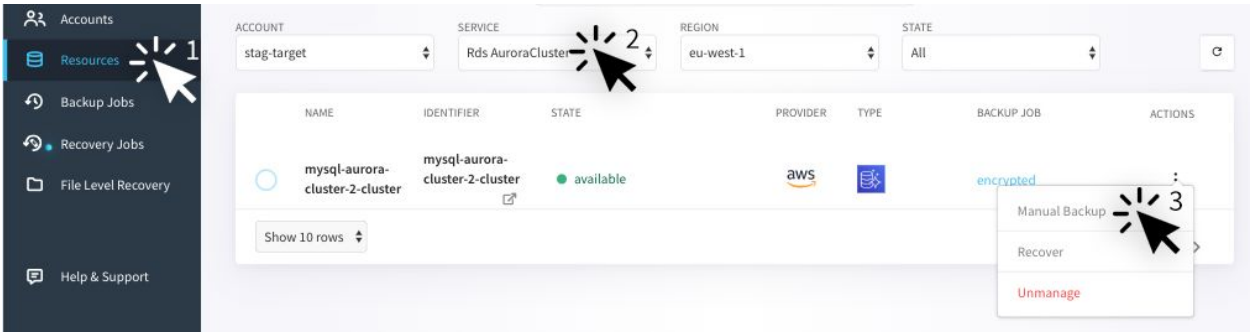
Select the RDS Aurora Cluster

Select an RDS AuroraCluster from the Resource View by selecting “RDS AuroraCluster” from the service dropdown.

This operation will filter your resources showing you only RDS Aurora clusters.

Click on “Manual backup”

Click on “Manual Backup” choosing it from the menu placed on the right.



How to backup an Dynamo DB table with Noovolari Smart Backup

With Noovolari Smart Backup it is possible to make a backup of your DynamoDB table, ensuring that your data is protected from errors, accidental loss or unwanted modification.

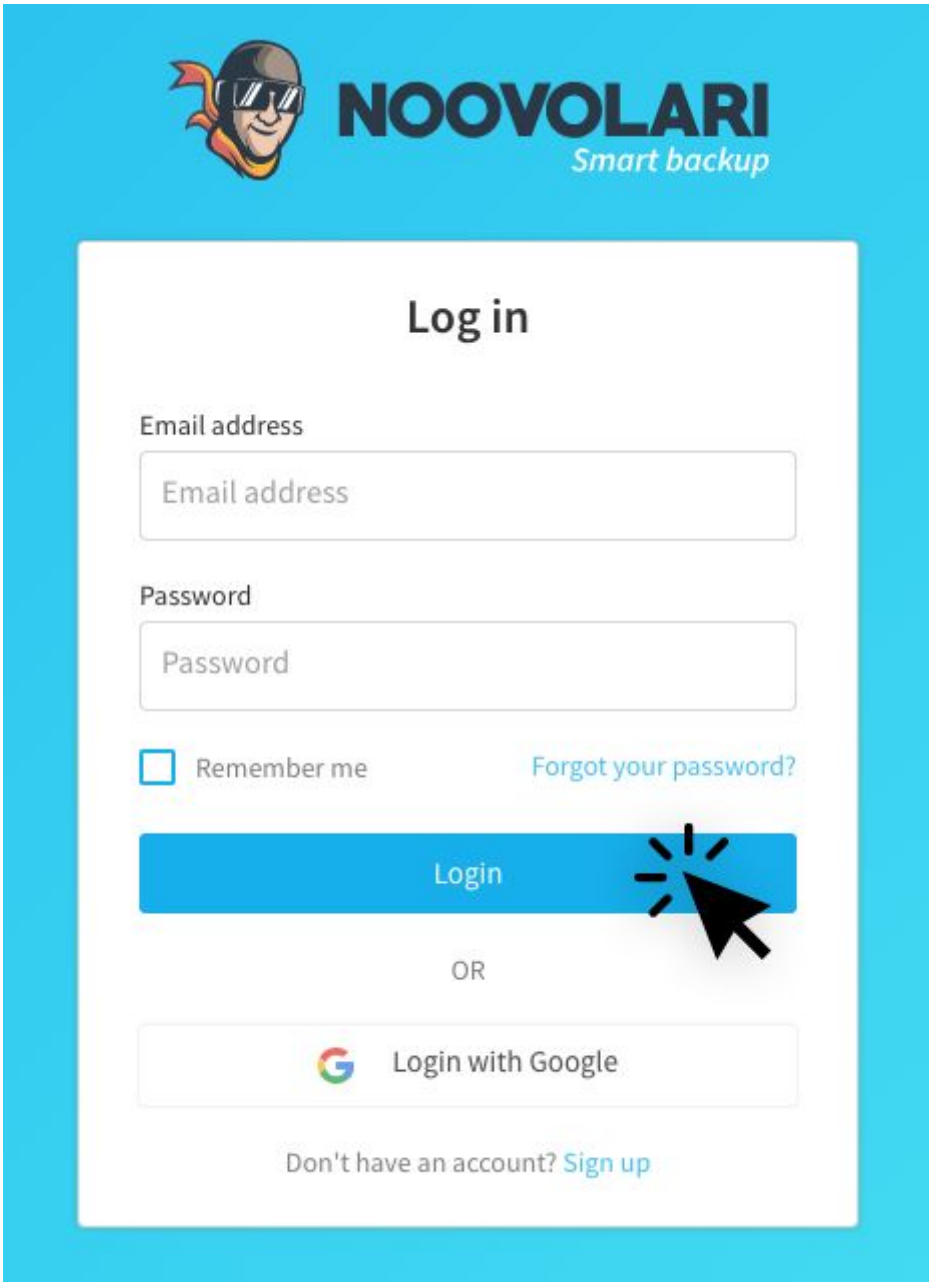
The backup will be visibile and fully manageable from both Noovolari Interface and AWS Console.

To make a DynamoDB table backup follow these simple steps:

1. Login to your Noovolari Smart Backup account
2. Select the DynamoDB table
3. Click on “Manual backup”

Login to your Noovolari Smart Backup account

(not a user, yet?Sign up now for free!);

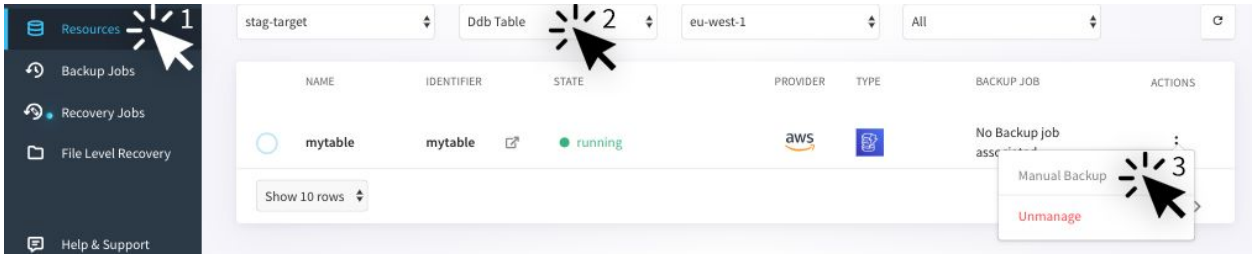


Select the DynamoDB table

Select a DynamoDB table from the Resource View by selecting “Ddb table” from the service dropdown; this operation will filter your resources showing you only DynamoDB tables.

Click on “Manual backup”

Click on “Manual Backup” choosing it from the menu placed on the right.



How to backup an Redshift cluster with Noovolari Smart Backup

With Noovolari Smart Backup it is possible to make a point-in-time snapshot of Redshift Cluster, ensuring that your data is protected from errors, accidental loss or unwanted modification.

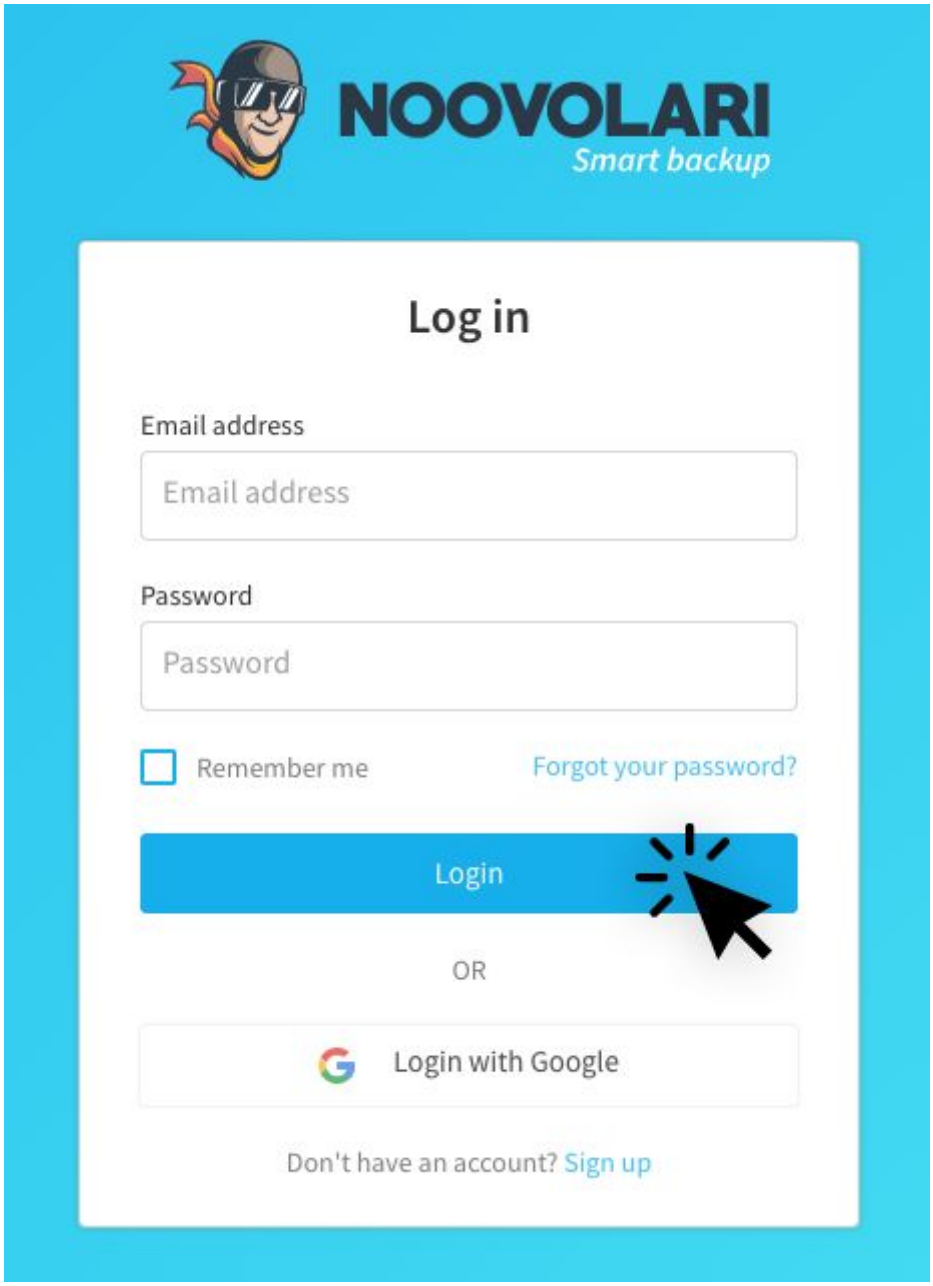
The snapshot will be visibile and fully manageable from both Noovolari Interface and AWS Console.

To make a Redshift Cluster backup follow these simple steps:

1. Login to your Noovolari Smart Backup account
2. Select the Redshift Cluster
3. Click on “Manual backup”

Login to your Noovolari Smart Backup account

(not a user, yet?Sign up now for free!);



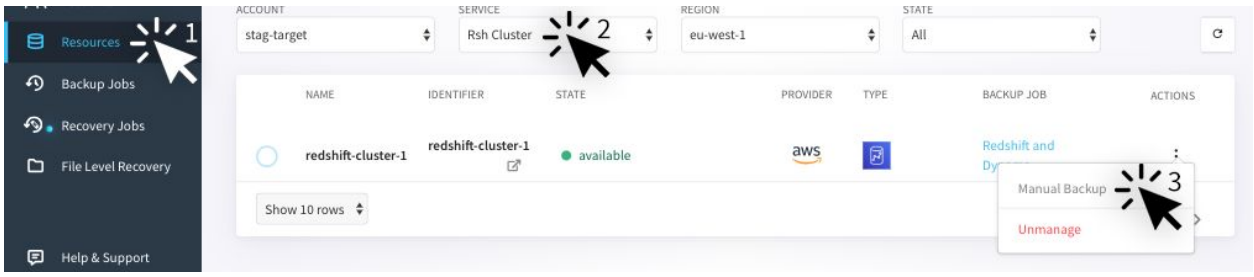
Select the Redshift Cluster

Select a Redshift Cluster resource from the Resource View by selecting “Rsh Cluster” from the service dropdown.

This operation will filter your resources showing you only Redshift Clusters.

Click on “Manual backup”

Click on “Manual Backup” choosing it from the menu placed on the right.



How to backup your MySQL server on an EC2 instance

With Noovolari Smart Backup it is possible to make a point-in-time snapshot of your MySQL server installed on your EC2 instance, ensuring that your data is protected from errors, accidental loss or unwanted modification.

Moreover, by installing NSB agent you can grant application-level consistency.

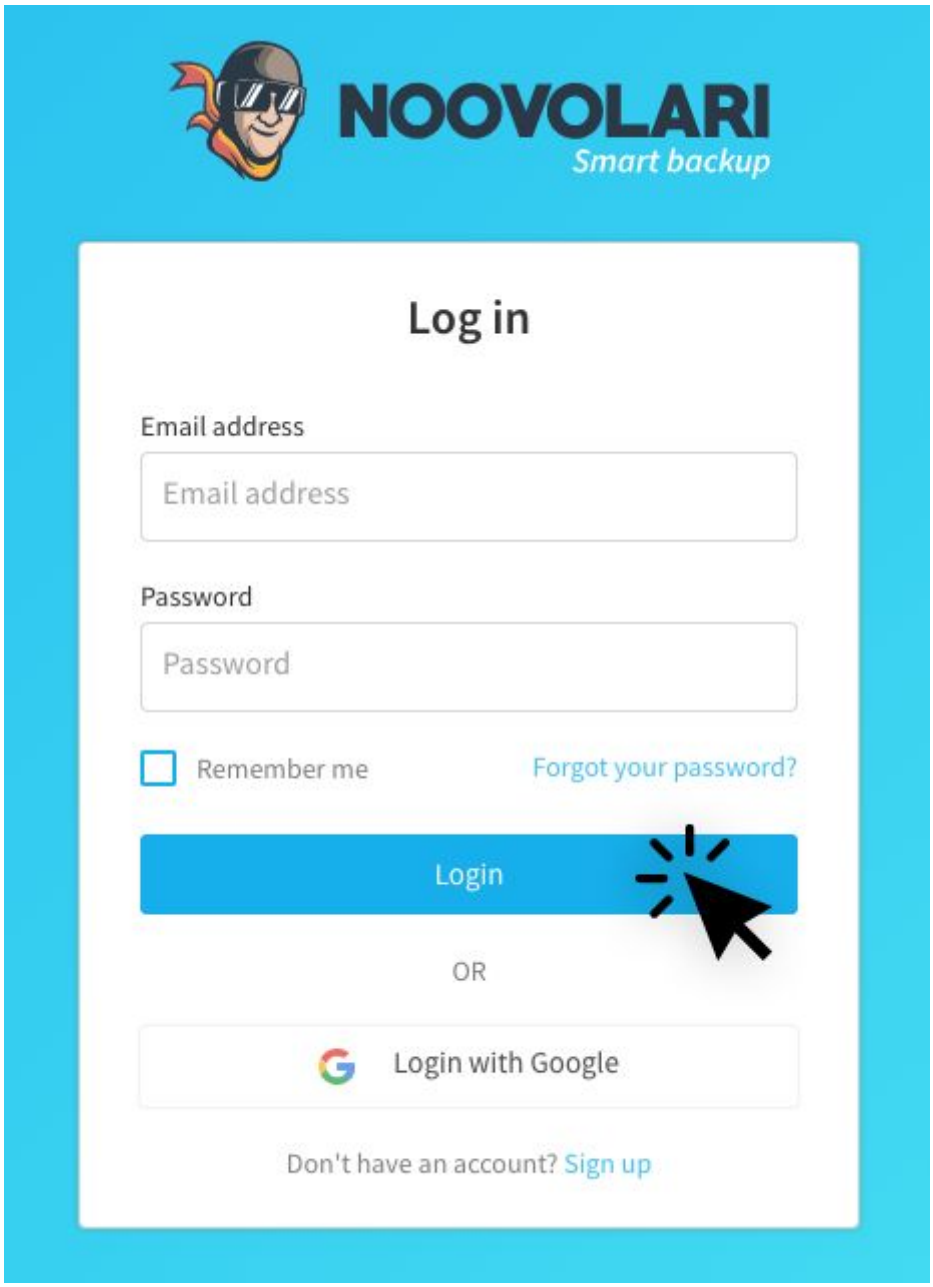
The EC2 snapshot will be visible and fully manageable both from Noovolari Interface and from AWS Console.

To make a consistent backup of your EC2 instance containing a MySQL server follow these simple steps:

1. Login to your Smart Backup account
2. Select the EC2 Instance
3. Click on “Agent link”
4. Follow the modal’s instructions
5. Access via ssh in the EC2 instance
6. Provide MySQL information to the agent
7. Return to Noovolari Smart Backup

Login to your Smart Backup account

(not a user, yet?Sign up now for free!);



Select the EC2 Instance

Select an EC2 instance from the Resource View by selecting “EC2 Instance” from the service dropdown.

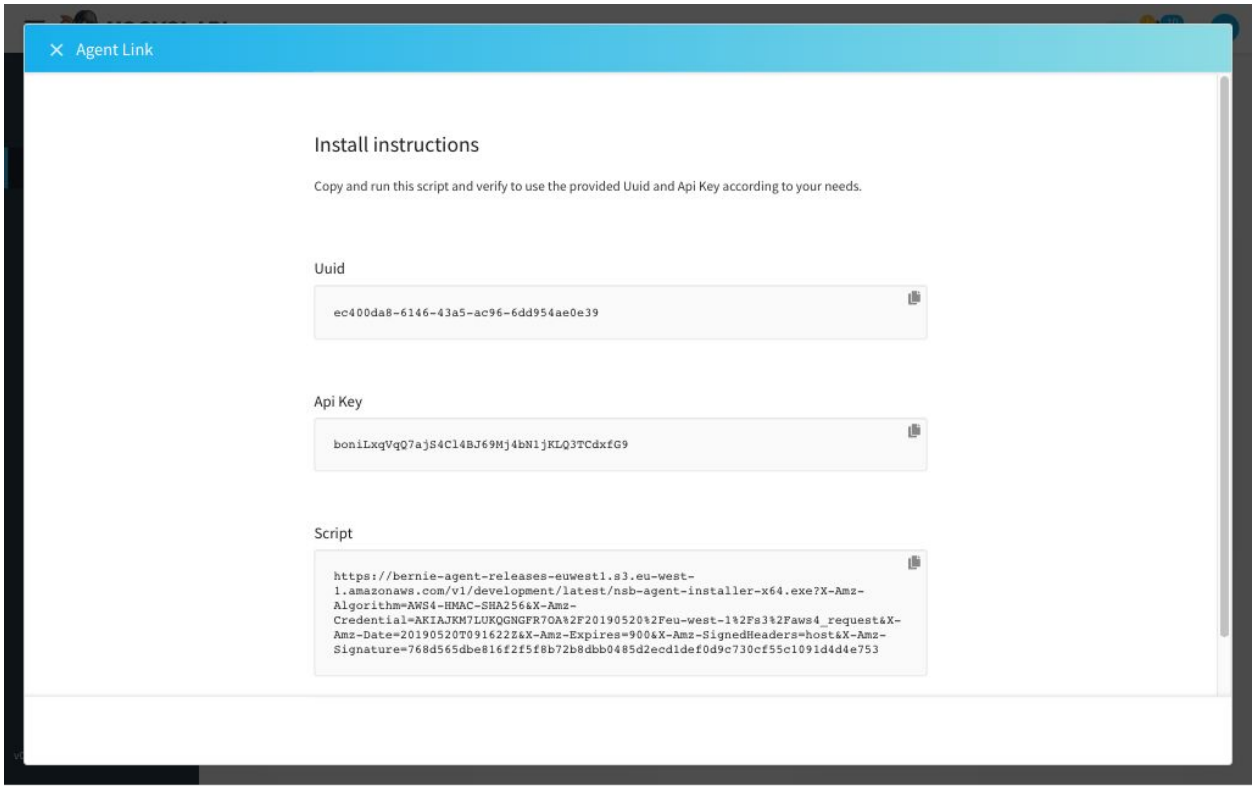
This operation will filter your resources showing you only the EC2 instances.

Click on “Agent link”

Click on “Agent Link” choosing it from the menu placed on the right or from the “Agent Tab” located in the detail section of the resource.

Follow the modal’s instructions

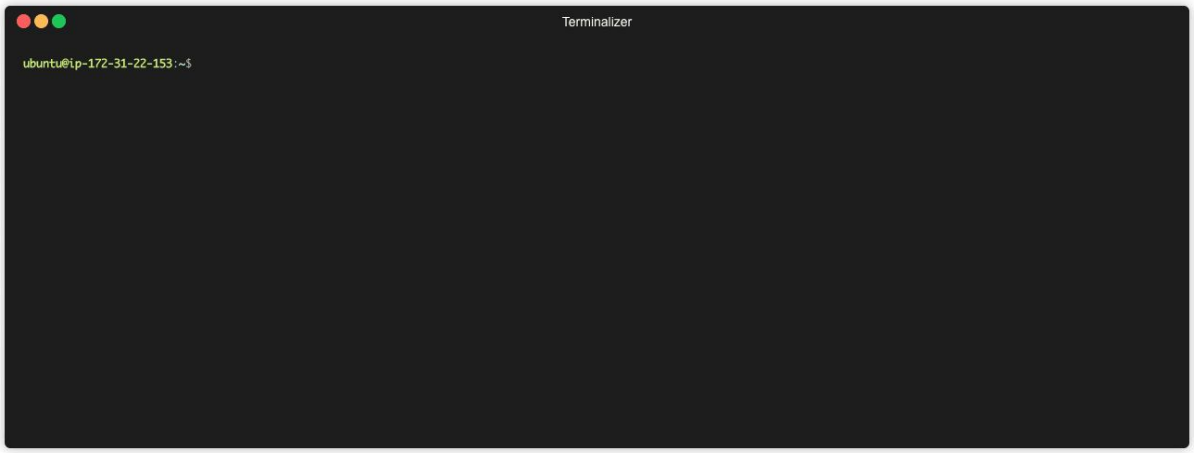
A modal will open; follow the instructions for installing Noovolari Smart Backup agent on the Ec2 instance.



Access via ssh in the EC2 instance

Access with SSH in the EC2 instance you want to install the agent on and paste the install command in the “Script” card.

If asked, insert the “Uuid” code and the “Api Key“.



Provide MySQL information to the agent

Provide the requested information (username, password) and decide if you want to provide consistency for all database in your My Sql server

```
found systemd
Do you want to configure MySQL consistency? [Yes|No] Yes
MySQL Configuration
Provide your username, password and database information
| => Insert your MySQL Username: test
| => Insert your MySQL Password: | Do you want to provide consistency for all MySQL DBs? [Yes|No]
```

How to backup your MongoDB replica set running on EC2 instances

With Noovolari Smart Backup it is possible to make a point-in-time snapshot of your MongoDB server installed on your EC2 instance, ensuring that your data is protected from errors, accidental loss or unwanted modification.

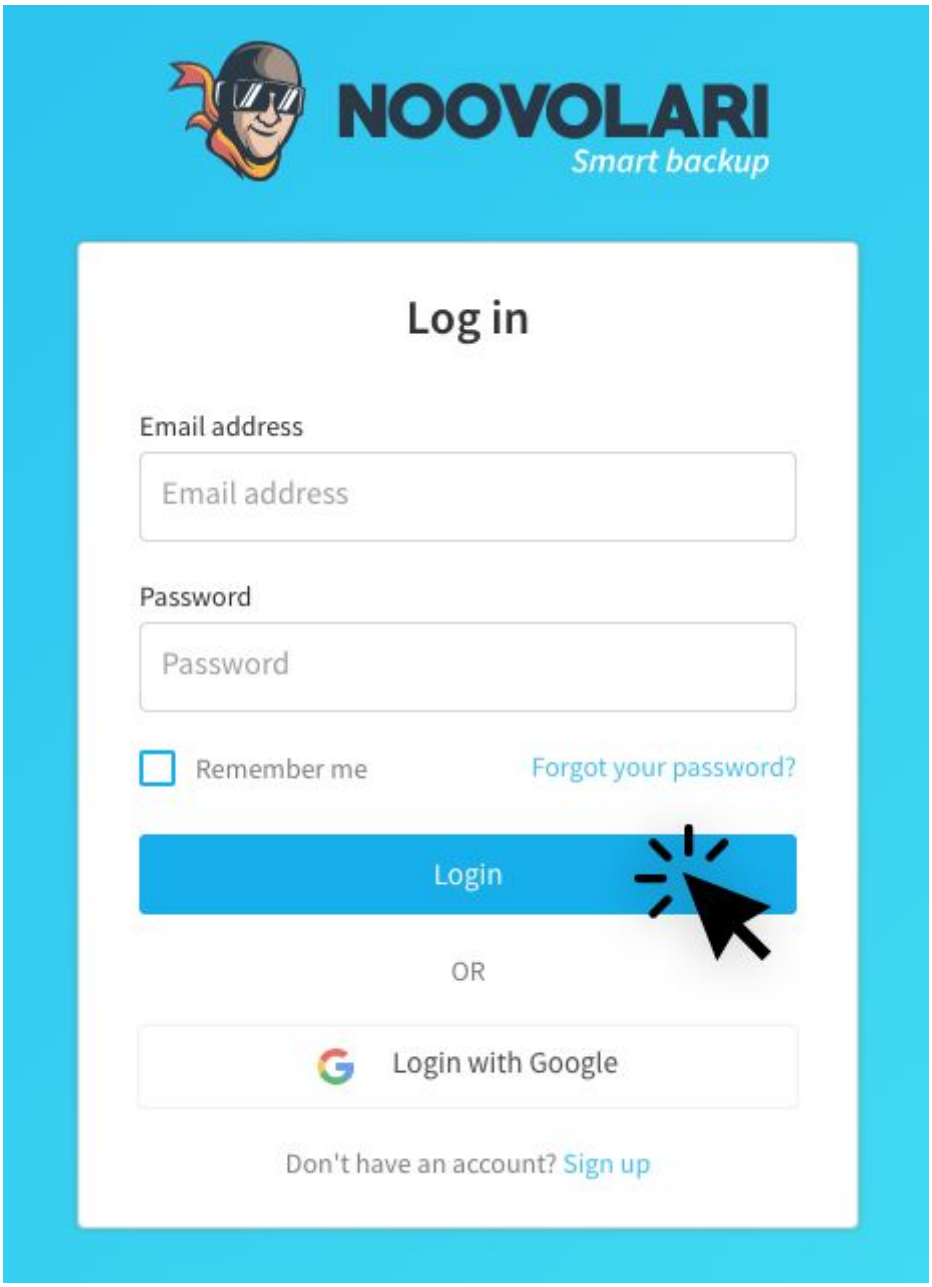
The EC2 snapshot will be visible and fully manageable both from Noovolari Interface and AWS Console.

To make a consistent backup of your EC2 instance containing a MongoDB server follow these simple steps:

1. Login to your Noovolari Smart Backup account
2. Select the EC2 Instance
3. Click on “Agent link”
4. Follow modal’s instructions
5. Access via SSH to the EC2 instance
6. Provide MongoDB authentication to the agent
7. Repeat the cycle for the Replica
8. Return to Noovolari Smart Backup

Login to your Noovolari Smart Backup account

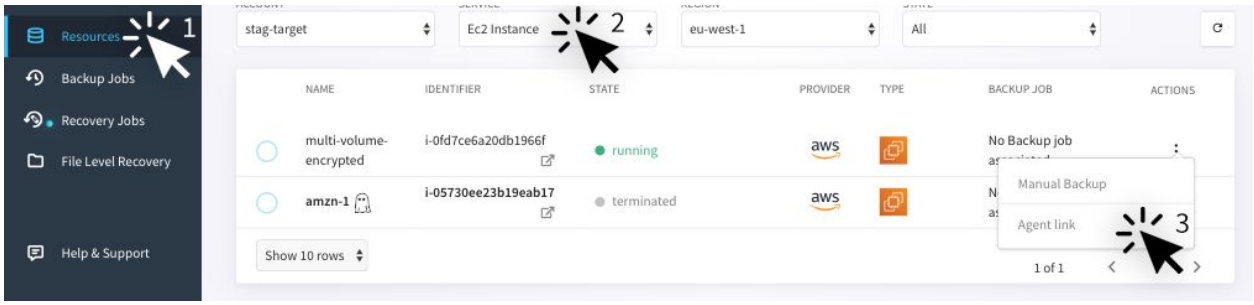
(not a user, yet?Sign up now for free!);



Select the EC2 Instance

Select the EC2 instance that contains a node of the MongoDB replica set from the Resource View by selecting “EC2 Instance” from the service dropdown.

This operation will filter your resources showing you only the EC2 instances.

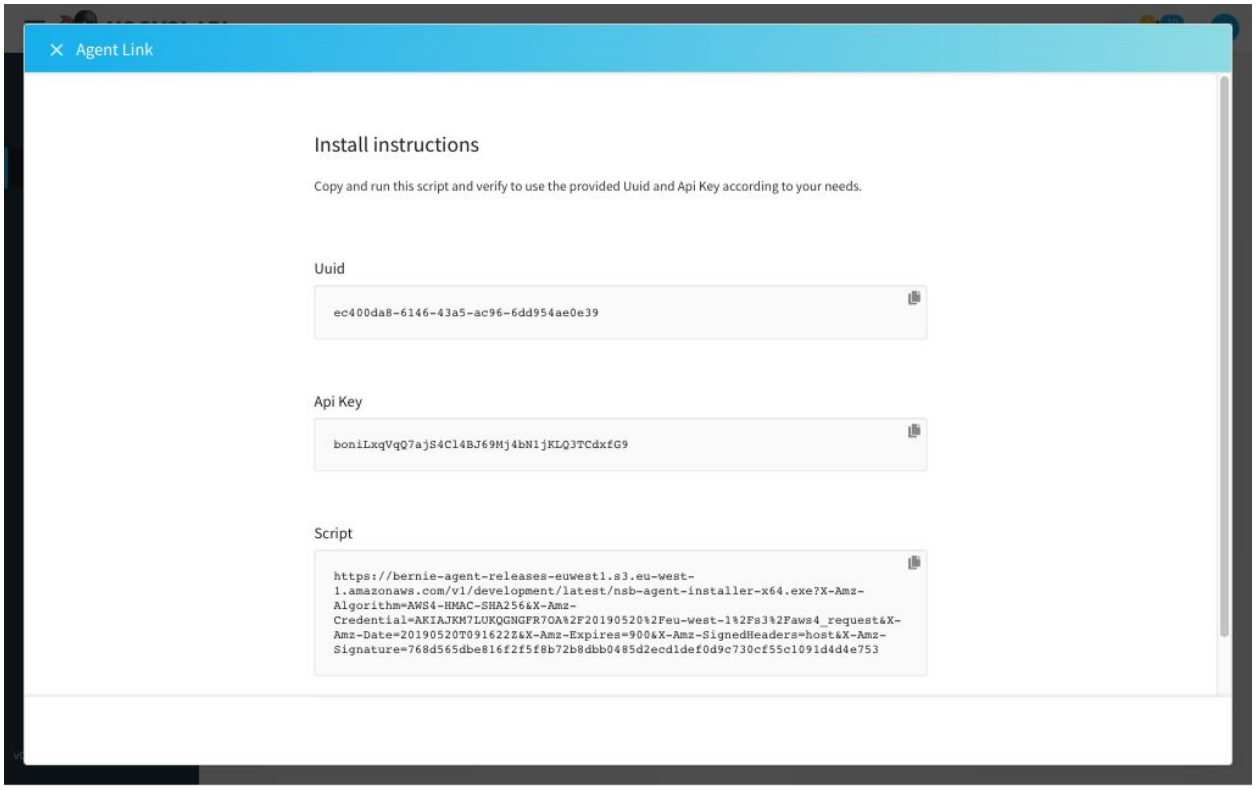


Click on “Agent link”

Click on “Agent Link” choosing it from the menu placed on the right or from the “Agent Tab” located in the detail section of the resource

Follow modal’s instructions

A modal showing the instructions for installing Noovolari Smart Backup agent on the Ec2 instance will open.



Access via SSH to the EC2 instance

Access with SSH the EC2 instance you want to install the agent on and paste the install command in the “Script” card. If asked, insert the “Uuid” code and the “Api Key“.

Provide MongoDB authentication to the agent

After that, the agent installer will ask for MongoDB authentication. Answer yes or no depending on your configuration. If the answer is yes you'll be asked to provide username, password and authentication DB name

Installing Agent with MongoDB

```
z-Credential=DEMO_CREDENTIALS%2F20190524%2Feu-west-1%2Fs3%2Faws4_request&X-Amz-Date=20190524T092916Z&X-Amz-Expires=900&X-Amz-SignedHeaders=host&X-Amz-Signature=75b36348
ddd8843a5352Zf4ca9bc64e96a9eec4dbea3565048f7860cd2144782
Resolving bernie-agent-releases-euwest1.s3.eu-west-1.amazonaws.com (bernie-agent-releases-euwest1.s3.eu-west-1.amazonaws.com)... 52.218.97.203
Connecting to bernie-agent-releases-euwest1.s3.eu-west-1.amazonaws.com (bernie-agent-releases-euwest1.s3.eu-west-1.amazonaws.com)|52.218.97.203|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 7414 (7.2K) [text/x-sh]
Saving to: 'NoovolariInstaller.sh'

NoovolariInstaller.sh                    100%[===========================================================================================>]   7.24K  --.-KB/s    in 0s

2019-05-24 09:30:10 (356 MB/s) - 'NoovolariInstaller.sh' saved [7414/7414]

/sbin/init: unrecognized option '--version'
found systemd
UUID: 2eee882d-30fa-4ada-832f-6669ec711795
API-KEY: ahqPYMpIWF1TdZoXSHMyn7FpOMFSO3w4bNUdETy1
/sbin/init: unrecognized option '--version'
found systemd
Do you want to configure MySQL consistency? [Yes|No] No
Do you want to configure mongoDB consistency? [Yes|No] Yes
mongoDB Configuration
Provide your admin username, password and database information
| Does mongoDB have authentication? [Yes|No]Yes
| => Insert your mongoDB Username: test
| => Insert your mongoDB Password:
| => Insert your mongoDB Authentication Database: admin


        +---------------------------------------+
        | Noovolari Smart Backup Agent Installed |
        +---------------------------------------+

Starting Noovolari Smart Backup Agent
```

Repeat the cycle for the Replica

Repeat all the steps shown above to backup all the EC2 instances in the replica set.

Documentation

Cloud account

In this page

Overview

Cloud Accounts in Noovolari Smart Backup are a set of data and permissions that enable the Noovolari account (on which all Noovolari Smart Backup logic resides) to manage your resources.

IAM Role

To make actions on your behalf we need to establish a trust relationship between your AWS account and Noovolari Smart Backup account, this comes in form of the creation of an IAM role inside our customer's AWS account.

This role comes with a policy with all the actions that you are authorizing to execute and a trust relationship which authorize Noovolari to execute those actions. To further ensure security all trust relationships are generated with an external id, which gives only Noovolari the permission to assume that role.

Permissions

Noovolari Smart Backup runs on the principle of least privilege. We guarantee to have only the privileges which are essential to perform our intended function.

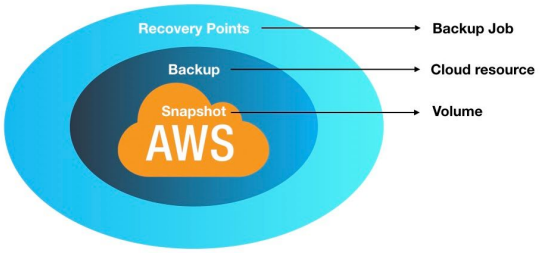
The only delete actions we need are on Snapshots (for all services) to perform the automatic rotation of backups. Other actions include create, describes and list of resource, to present all information inside Noovolari Smart Backup.

Backup concept

In this page

Overview

There are three different levels of backup managed by Noovolari Smart backup.



Snapshot

A snapshot is a physical backup of a volume, managed by AWS.

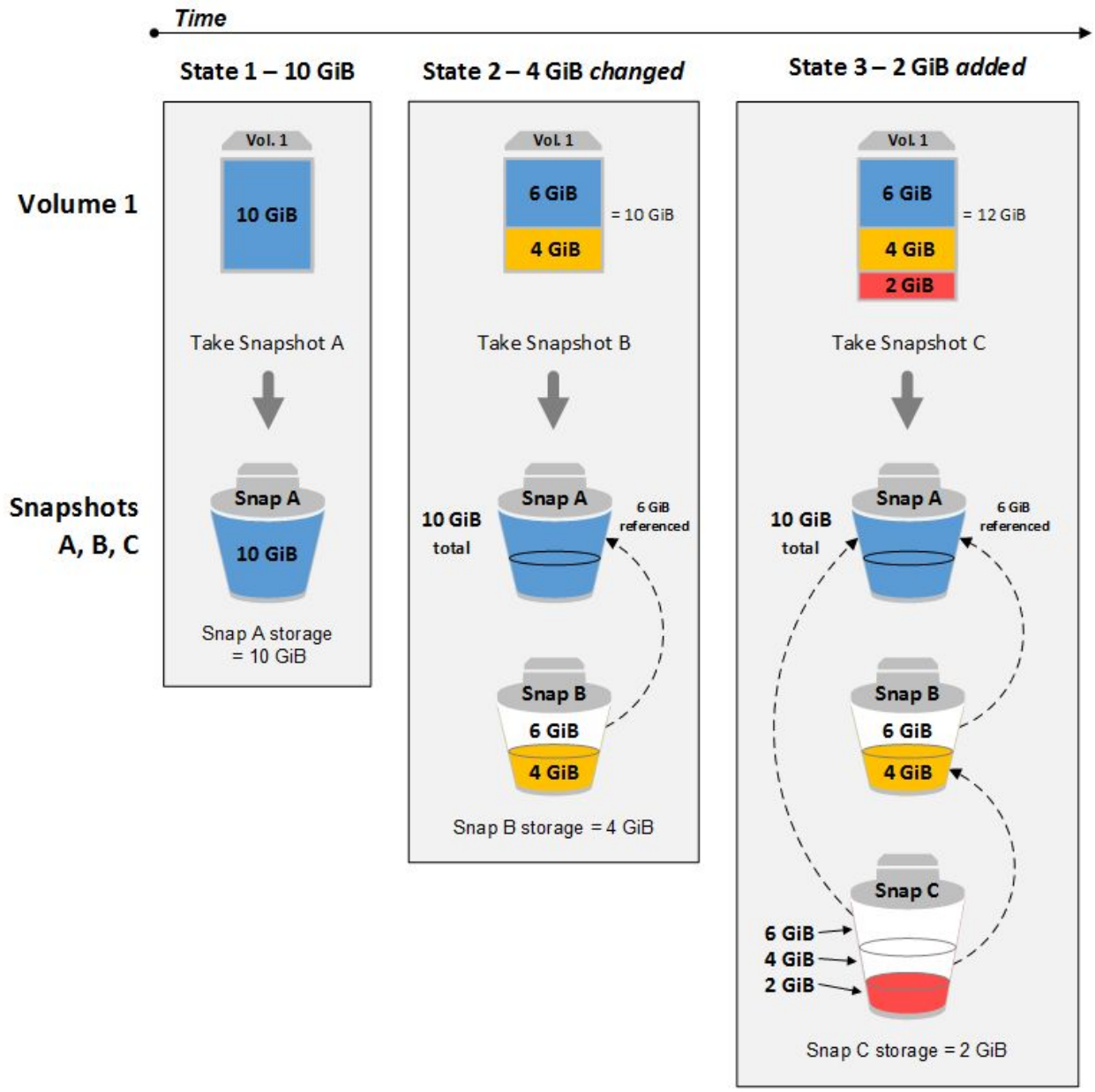
A volume is a physical block level storage which contains data in a resource (e.g. Amazon Elastic Block Store (Amazon EBS) provides block level storage volumes for use with EC2 instances).

One or more volumes can be associated with a single resource.

“Snapshots are incremental backups, which means that only the blocks on the device that have changed after your most recent snapshot are saved.

This minimizes the time required to create the snapshot and saves on storage costs by not duplicating data.

When you delete a snapshot, only the data unique to that snapshot is removed. Each snapshot contains all of the information needed to restore your data (from the moment when the snapshot was taken) to a new volume."(See Aws documentation).



A volume can be encrypted; Snapshots of encrypted volumes are consequently encrypted, too.

While AWS takes care of data, Noovolari masters how snapshots are taken and managed, for example, it manages the time in which snapshots should be created and/or deleted.

Snapshots, when created, are associated with a specific region by AWS default. Noovolari allows you to replicate a snapshot across different regions or even across different AWS accounts, even if the snapshot is encrypted.

As already described, as part of Cloud resources, volumes (one or more) can be associated with resources. Each resource is correlated to backups.

Backup

A Backup in Noovolari Smart Backup is the minimal recoverable entity of our service. When a Backup is done, not only the data are saved but the whole configuration of the Resource is taken alongside. We do this because our focus is to make Backups recoverable with predictable and known result, thus treating resources as a whole. So, inside a backup of an EC2 instance is common to find more than one snapshot, because a snapshot is taken for each volume, and when a Recovery is done all volumes are restored to the condition as they were before.

A backup is a set of snapshots. While AWS only allows you to manage single snapshots (therefore single volumes, when an instance can be made up of multiple volumes), with Noovolari you are able to manage snapshots as a block. Blocks are called backups.

Actions you can do on backups with Noovolari are “clone” and “Recovery”(destructive and Non-destructive)

Clone

When you clone a resource, a copy of a selected backup is created in the same region of the resource cloned, in a single click.

Recovery

There are two different kinds of recovery: destructive and non-destructive recovery.

By recovering a resource in a destructive way, the recovered resource will be terminated after the recovery process is finished. The new resource, created from a Noovolari backup, also inherits the same configuration, network and device mapping from the recovered one.

Non-destructive recovery, instead, saves a copy of the recovered resource after the recovery process is completed.

One or more Cloud resources are managed by Backup Jobs.

Backup jobs are a set of configurations such as how many backups in a given period of time and how many of them need to be retained. To do this, a backup job must be composed by a set of retention rules (the maximum number of retention rules you can define is 5 for each backup job).

Backup jobs create a set of backups.

Recovery points

The set of backups just mentioned above is called Recovery Point.

A recovery point is a collection of Backups taken at the same time. This ensures application level consistency not only for a single Backup but, if correctly configured, for the whole application stack.

Backup jobs manage replicas of regions or accounts; that is to say, each recovery point is duplicated in a different region or account.

By duplicating a recovery point, Noovolari Smart backup creates a copy of each backup and, consequently, of each snapshot in it.

Resources

In this page

Overview

Resources in Noovolari Smart Backup are all the concrete elements you can backup.

By default, all the resources are non-managed resources. In other words: non-managed resources are all the resources for which no backup in Noovolari Smart Backup has been created, yet.

Every resource can have one or more backups associated and it can be recovered by disaster-recovery actions in Noovolari Smart Backup.

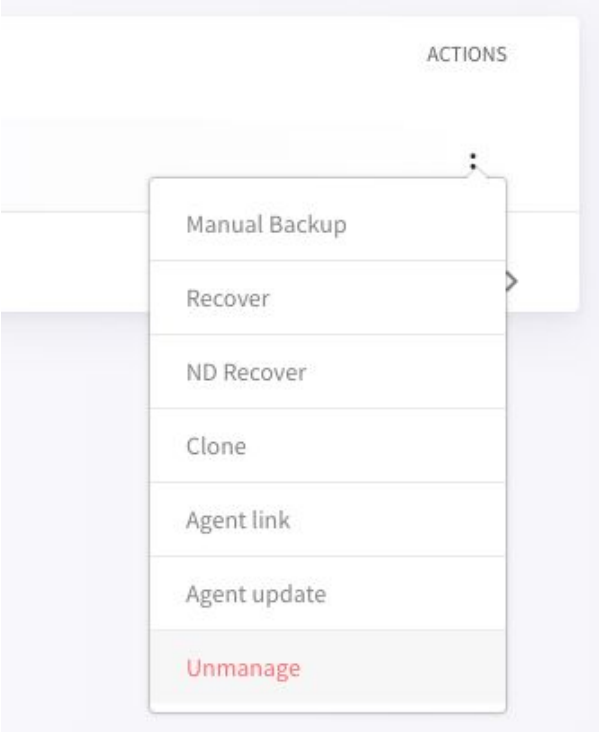
When a resource is given as managed?

A managed resource in Noovolari Smart Backup is each and every recoverable element of our supported services.

A resource becomes automatically “managed” after any operation involving the specific resource take place, such as creating a backup-job (learn more here), creating a manual backup, or going through the installation of the Noovolari Smart Backup agent (learn more here). At this point, the resource is ready to be managed and monitored by Noovolari.

Please, note that once the resource becomes managed, it is included within the Noovolari pricing plan.

While the change from “non-managed”to “managed” status comes automatically after one or more of the operation we mentioned above take place, if you need to rollback to a “non-managed” status, you have to change it manually from the “actions” menu of the specific resource.



When changing the status to “non-managed”, you can decide to keep all the backups done for the specific resource or to delete them. In case you decide to keep them, they are saved to the user’s account.

Note that once a resource is unmanaged, you won’t be able to do any recovery actions on the previous backups anymore, even if you decide to re-manage it.

What are the supported AWS services?

Noovolari smart backup support:

- EC2 instances
- RDS instances
- RDS Aurora Cluster

NSB Agent

In this page

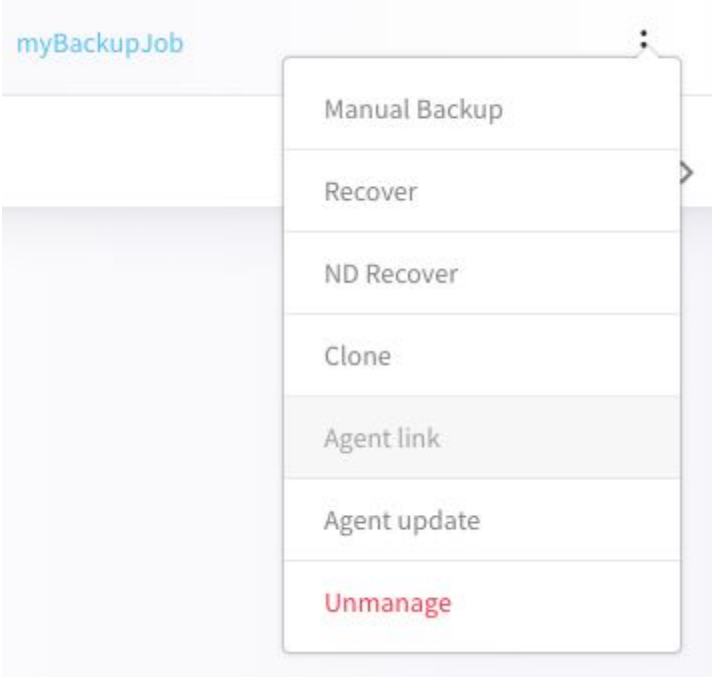
Agent

When Point in Time consistency is not enough to meet your backup policy needs, you can install and configure the Noovolari Smart Backup Agent to ensure Transaction consistency for file-system and databases. Once you install the Agent, file-system consistency is enabled by default.

You need to configure the Agent only to connect to the database and issue commands that ensure Transaction consistency on the snapshot.

Installing

To install the Agent on an instance, you have to click on the Agent Link action in the Resources section. Once done a page will appear and let you copy a script that will automatically download executable and configure the communication with Noovolari Smart Backup application.



Follow this guide if you need a help in installing Noovolari Smart Backup agent.

MySQL

The Agent enables consistency on MySQL databases by flushing all writes and placing a read lock on all tables. This puts the database in a read-only state where any INSERT/UPDATE/DELETE/REPLACE/ALTER statements will not run until the lock is released.

When Noovolari Smart Backup notifies that the snapshot started, the Agent removes the read lock and the database can resume its normal operations.

MongoDB

The Agent enables consistency on MongoDB databases without the risk of compromising data present in the DB. It supports consistent backups of entire Replica Sets with the exclusion of consistent backups of sharded MongoDB databases.

Single Instance

For a single instance, the Agent forces all pending writes, stops new writes while READ operations can proceed as normal. However, because of the MongoDB locking model, writing to the database while performing a read lock hangs even reads. Most of the time this doesn't pose a problem because the freezing time of the MongoDB database is usually less than any client timeout. With a huge amount of data, however, this isn't guaranteed and eventual exceptions/retries should be handled by clients.

Replica Set – single node

The Agent is installed on one secondary node of the Replica Set. This configuration guarantees the consistency of the backup without the drawbacks of a temporary lock of the database operations as the primary node continue its normal operations. Once the backup is done the node is updated with the data from the primary node.

This ensures the total availability of the database even during backups but comes at the price that the Replica Set can't be automatically recovered with a Point in Time recovery. It must be recovered as in the MongoDB documentation using the data from the secondary node. Another problem can arise if following the failure of the primary node, the secondary node is elected as the primary node. In this case, backups operations will block momentarily all writes on the Replica Set.

Replica Set – all nodes

The Agent is installed on all nodes of the MongoDB Replica Set. This configuration enables the simplest recovery solution by recovering all nodes to the desired Point in Time. However in this configuration, all write operations on the Replica Set are stopped for the time necessary to start the snapshots of all instances, causing the database to be unreachable for some time, from few seconds to one minute.

Linux

The Agent enables consistency on Linux by stopping all the writes on the file system. When Noovolari Smart Backup notifies that the snapshot has started, the Agent restores the normal operation of the file system.

The Agent has a default timeout of 30 seconds, after which it automatically restores functionality in case of communication problems.

Windows

The Agent enables consistency on Windows by leveraging the Volume Shadow Copy (VSS).

When notified, the Agent starts a shadow copy and ensures that the snapshot is taken only when consistency is achieved.

By default, the Noovolari Agent subscribes all VSS Writers when starting the Shadow Copy. Therefore all VSS compliant applications are Transaction consistent without any further configuration.

Uninstall

To uninstall the Agent from an instance, you have to connect to the instance and remove it with the correct procedure. The Uninstall button in the Agent tab only flag the instance as Agentless.

It does not automatically remove the program from your instance.

Windows
You can remove the Agent by using the default uninstall procedure in Programs and Features.

Linux
All Agents are shipped with a script that determines the default Linux system manager (systemd, SystemV or initctl) and automatically installs the program as a service. You can use the helper in scripts/init_service_case.sh in the Agent directory to let it determine your system manager and issue the correct procedure.

You can run this command for uninstalling the agent:

```
/usr/local/noovolari/smartbackup/scripts/init_service_case.sh uninstall
```

Troubleshoot

Where can I find the Agent?

Linux: /usr/local/noovolari/smartbackup

Windows: C:\Program Files\Noovolari\SmartBackup

Where can I find the Agent logs?

You can find the logs inside the installation directory.

They named info.log and errors.log .

Consistency

In this page

Consistency

Consistency involves the integrity of the data and should be considered within individual programs, databases, and application systems.

This concept is strongly tied with data usability to enable correct recovery of potential failures.

In this documentation, we will refer to three levels of consistency:

- Crash-consistency
- Transaction-consistency
- Application-consistency

Crash-consistency

This kind of consistency ensures that system elements data are all related to a specific moment. Certainly, without this, there would be no guarantee that all information could be restored. It results in that all of the interrelated data components are preserved as they were at any single instant in the past.

Contemporary file-systems implements this behavior with techniques like file-system checker or journaling. By default, a snapshot is crash-consistent because it relies on techniques implemented by the file-system.

For example, consider the failure of a single logical volume containing data from one or several applications. If the only option is to restore that volume from a crash consistent backup, the data contained in the restored volume could not be consistent with the other volumes, and additional recovery steps must be undertaken.

Transaction-consistency

A transaction is a logical unit of work that may include any number of file or database updates.

Transaction consistency occurs only before any transaction starts, following the completion of a successful transaction, before the next transaction begins, and when the persistence layer is closed or stopped. After a failure, the data will not be transaction consistent if transactions were in-flight.

The techniques used to implement transaction consistency generally flush all I/O operations from memory to the persistence layer and stops any subsequent I/O operation, until the snapshot starts.

The same logic can be applied to any file-system or application that works with persisted data. It’s important to note that only the primitives on which these techniques are not built on are generally available. The actual implementation of the technique must be done and maintained.

Application-consistency

Similar to transaction consistency but on a bigger scale. Instead of data integrity within the scope of a single system element or transaction, data must be consistent within the boundaries of many different components of one or more applications.

Application consistency is the state in which all related data are in sync and represents the reliable status of the application.

Retention Rules

In this page

What is a Retention Rule?

When registering a new Backup Job you can specify retention rules that are applied to all recovery points (learn morehere) related to it.

Each Retention Rule takes into account two different concepts: schedule and retention.

Schedule refers to a plan that specifies the instants in which a specific Backup Job should be triggered.

Retention refers to the operation of filtering out, from a list of recovery points, only recovery points contained in a specific time window.

Each retention rule applies to a specific time granularity. Supported time granularities are “hours”, “days”, “weeks” and “months”.

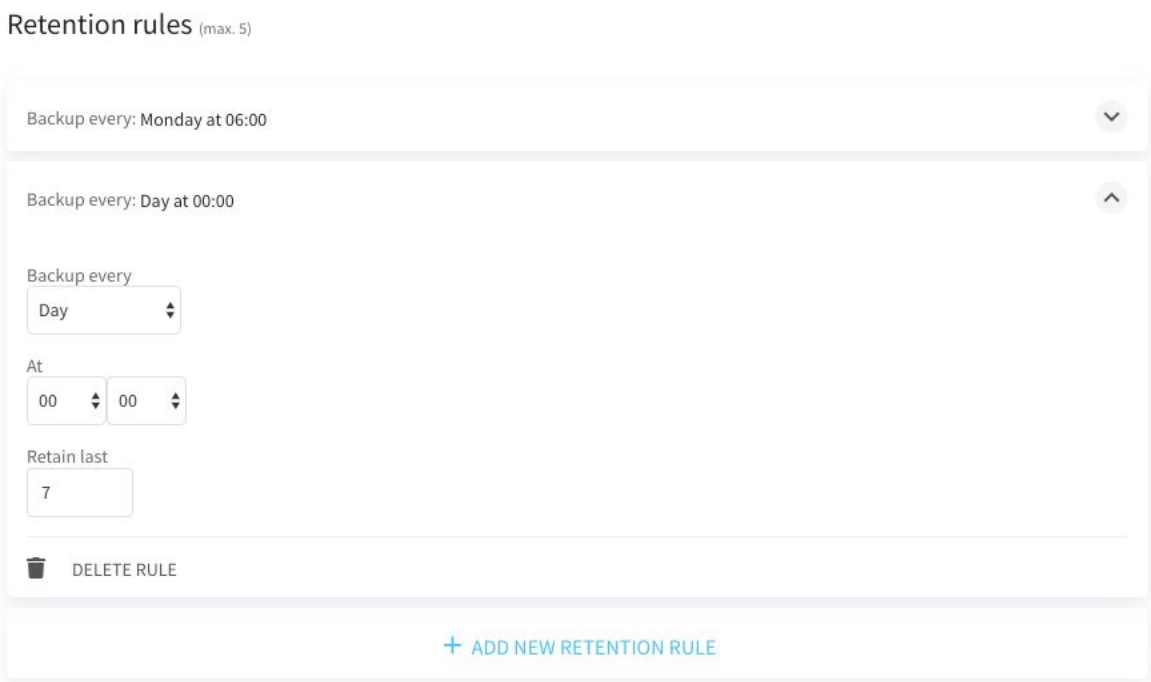
Retention Rules can be created both during Backup Job registration and update.

The maximum number of Retention Rules admitted for each Backup Job is 5.

Use Case

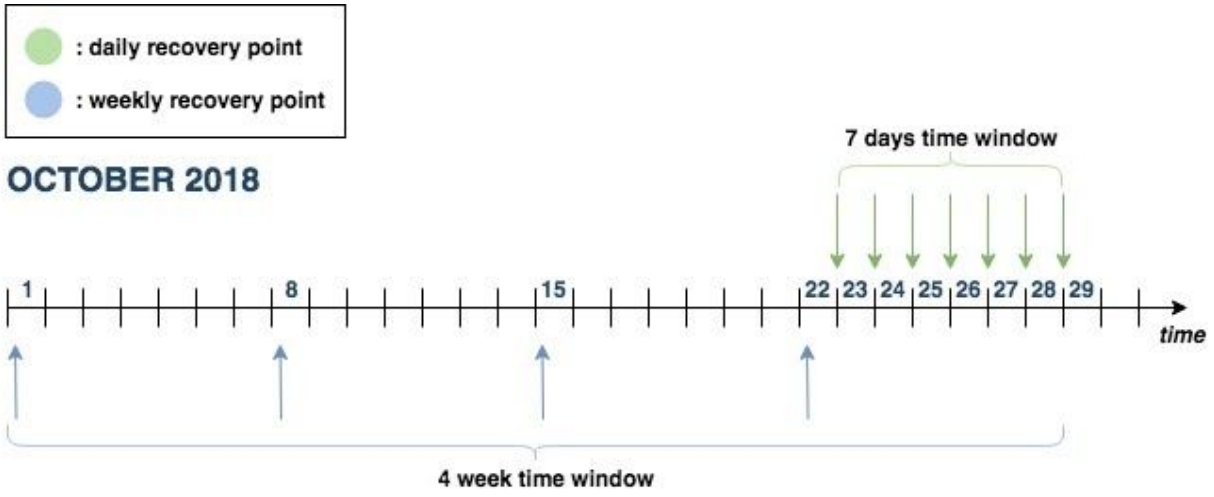
Suppose you want to create a Backup Job with the following rules:

- Every day at 00:00, keep 7 recovery points
- Every Monday at 06:00, keep 4 recovery points



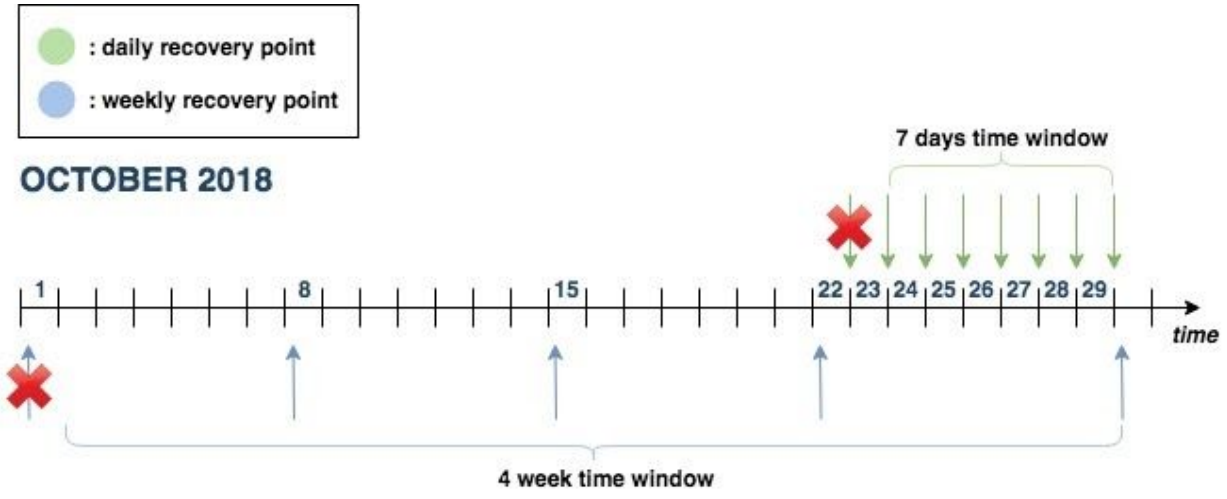
The granularity of the first rule is a day. Keeping 7 recovery points means filtering out from a time window of 7 days the recovery points created with the first rule. The same applies to the second rule.

Suppose on October 1st, 2018, you've activated the Backup Job with the just defined Retention Rules; on October 29th, at 00:00 am, Noovolari Smart Backup would be managing the following recovery points.



Next recovery points will be taken on October 29th, at 06:00 am, for the Weekly Retention Rule and on October 30th, at 00:00 am, for the Daily Retention Rule.

Thus, on October 30th, at 00:00 am, after the daily recovery point was taken, the scenario would change as described below.



As you can see, as time windows shift, recovery points that are no more included in them will be deleted.

What is File level Recovery

In this page

Introducing File-Level Recovery

Being a small or a big company, sooner or later you'll face the need for a disaster recovery solution.

Even if AWS or Cloud Computing solutions in general, can well fulfill this kind of needs, many adjustments have to be applied; some particular tasks are still difficult, especially for non-IT users.

As Noovolari Smart Backup solution is based on snapshots, our backups are incremental backups, as previously explained. But snapshots still have some shortcomings, regarding picking up single files from a specific EBS snapshot.

A skilled user can even pick files from a previous backup by recovering a resource from older snapshots. Anyway, doing this on our own an be a long hard slog. Rolling back an entire instance could be really time-consuming and more expensive then exploring a snapshot with File-level recovery.

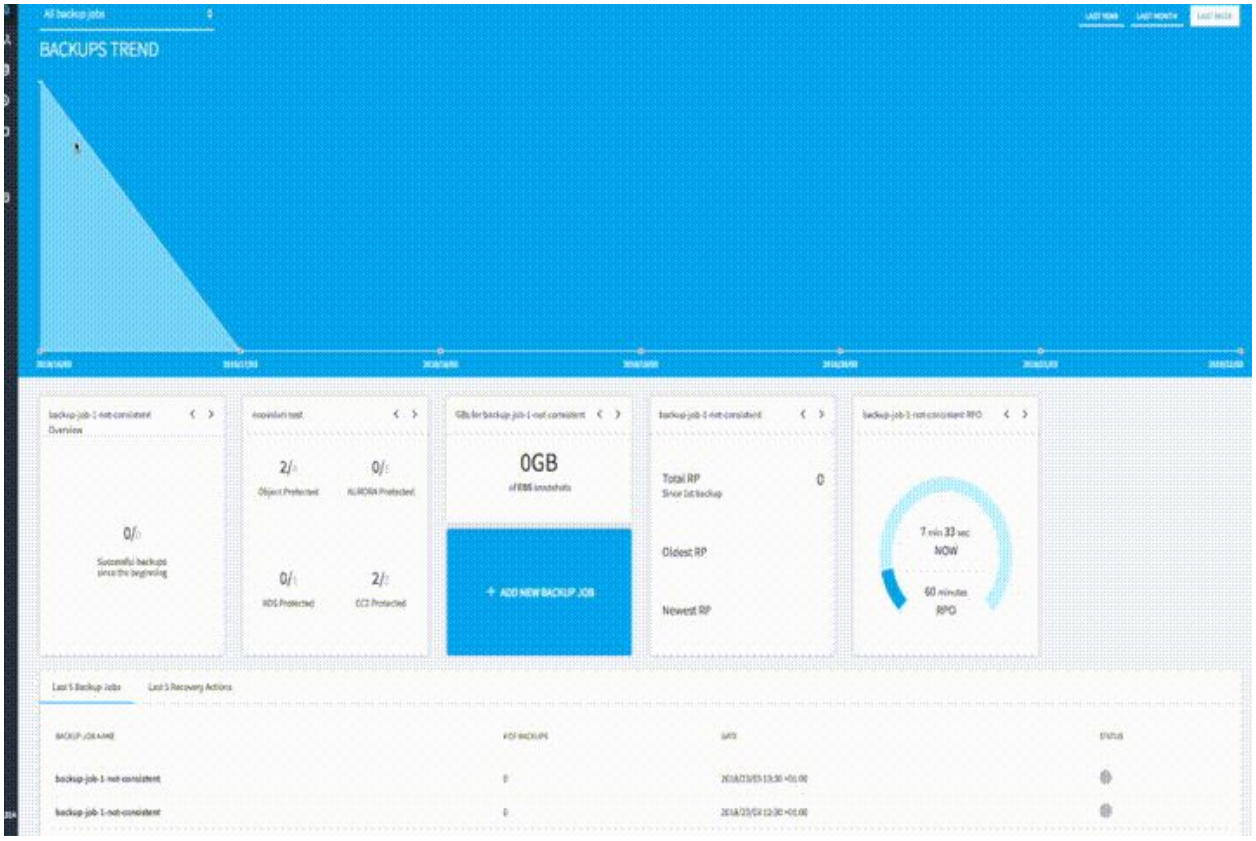
If you want to know how to use it, check our getting started article.

When FLR runs to your rescue

It is quite common to need to recover a file backed up in the past containing critical business data.

Moreover, it happens to face the need to check snapshots' content in order to verify in advance if a specific file exists in specific point-in-time referred to the snapshot.

By choosing a backup from the list of backups managed by Noovolari, you can quickly browse files contained in your backed up volumes through our File manager application. Our user-friendly file explorer allows users to navigate through volumes, to pick up a single file (or more than one file), and to finally download it (or them) in an extremely easy way.



Please note that File-Level Recovery is only available for EC2 EBS-backed backups of a given resource and exclusively in case all the volumes are not encrypted.

When backing up a multi-EBS volumes EC2 instance, the resulting backup will contain a snapshot for each volume. So, when FLR is done for that particular backup, the user will be able to explore each volume mounted on the resource at the time the backup was made, with the same block-device mapping as the starting resource.

Available regions

FLR is available in the following regions:

- eu-west-1 EU West (Ireland)
- eu-central-1 EU Central (Frankfurt)
- sa-east-1 South America (Sao Paulo)
- us-east-1 US East (Virginia)
- ap-southeast-1 Asia Pacific (Singapore)
- other regions coming soon…

If the region you need to use is not the list yet, press the exclamation point on the top-right of the card to contact us. Our team will be happy to get back to you!

What is a session?

Noovolari Smart Backup allows you to navigate through a backup's snapshots with the user-friendly File Explorer.

To do this, the user has 60 minutes of active Session to browse inside backup volumes

After 60 minutes the session is automatically closed and the user has to create a new one to navigate through a snapshot.

Notifications

In this page

Overview

Notifications are a primary concern for Noovolari Smart Backup as they allow the User to check Cloud resources and the related backups status.

Noovolari's notification system is roughly divided into 3 main area of interest: in-app alerts, email notifications, in-app notifications.

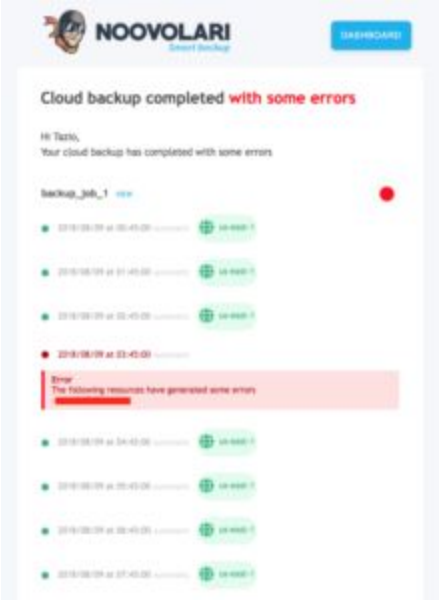
In-app alerts

The in-app notifications are useful to show the user if he/she is doing right in operating on Noovolari Smart Backup; they are presented as simple color-coded alerts to make easier for the user to understand what is going on. As per every software, they are triggered when something ends in a successful/unsuccessful way.

Email notifications

Noovolari always keeps the user up-to-date with accounts and resources status.

The user will receive emails on a regular basis containing daily recaps.



The email contains a detailed recap of each backup job and replica associated (if available) and potential errors (if existing).

This report also shows if a specific backup job has failed, for what reason, and what resources are implied.

These allow the users, for example, to be notified on their smartphone and thus being updated on their cloud backup status anytime, anywhere.

The email receiving address can be changed from Noovolari profile view so that you can be notified even if you are not the owner of the registered account.

In-app notifications

In-app notifications alert the user about failed tasks or errors affecting backups. They also provide the user with a detailed description of the reason why the error occurred.

Moreover, in-app notifications notify you with the final status (succeeded or not) of an ongoing task such as Recovery operations or FLR.

Faq

Backup questions

In this page

Is there a maximum number of snapshots you can create with Noovolari Smart Backup?

Noovolari Smart Backup allows you to create from your AWS resources many backups as you want.

Each Noovolari plan offers you a given number of managed resources. For each of them, it is possible to create an infinite number of backups, based on your needs. Each backup creates one or more snapshots on AWS.

AWS accounts can manage a limited number of snapshots. Each limit changes depending on the service you are using:

- EC2 instances support a maximum number of 10000 EBS backed snapshots (it is possible to increase the number of snapshots following this steps).
- RDS instances support a maximum number of 100 manual snapshots per account (click here for more infos)

My RDS instance backup failed, what can be a possible reason?

If an RDS instance is not checked as “available”, AWS fails in doing backups.

Anyway, it takes a few minutes for the instance to change its status to “available”, and you cannot access the instance, as explained in the following AWS FAQ

File Level Recovery questions

In this page

“No FLR instances available in region REGION NAME”: what does it mean?

If you fall into this problem, FLR feature is not available in the chosen region, yet.

You can check available regions in our documentation.

If you need the FLR to be available in your region, feel free to contact us; just complete the form in the bottom card of the File Level Recovery page.

We will be glad to accomplish your request as soon as possible to make File Level Recovery available in the specific region.