
Important note for Scnapper 4.0.0

- Launch Scnapper from the CloudFormation template published with the AMI, not from the AMI on its own. The template creates the IAM role, the security group and the data volume the instance needs, and its outputs give you the URL, the SSH command and the setup token for the first login.

# Scnapper Getting Started Guide

# Scnapper 4.0.0

Scnapper backs up your AWS EBS volumes and EC2 instances on a schedule, keeps them under a retention policy, and starts and stops EC2 instances on a runtime schedule. Version 4.0.0 is a rebuild of the appliance on Ubuntu 24.04 LTS with MySQL 8.0, PHP 8.3 and OpenJDK 21, launched from a CloudFormation template, with every password and key generated on your own instance.

Release notes for this release are available here:

https://scnapper-getting-started.s3.amazonaws.com/ReleaseNotes-Scnapper-3.0.pdfhttps://scnapper-getting-started.s3.amazonaws.com/ReleaseNotes-Scnapper-4.0.0.pdf

The following are its features:

## Backup and Recovery

- Backup your AWS resources - EBS volumes and EC2 instances
- Schedule backups by the hour, day, week, month or year
- Keep your costs low by efficient usage of cloud resources, enabled through customizable retention policies for your backups
- Easy and rapid recovery of your backups
- Don't loose track of your backups by using our easy to use backup navigation widget
- Ensure that your backups are happening as per schedule by choosing to receive notifications by Email or SMS
- Automatically kick start the execution of other processes by chaining Scnapper's notifications.

## EC2 Scheduler

- EC2 instance costs contributes the most to your AWS bill

- Reduce your costs by more than 65% by automating the schedule of the runtime of your EC2 instances that do not have to be running 24/7
- Flexibility of scheduling the runtime of your EC2 instances each day and hour of the week
- Schedule your instances to be stopped during the weekend and non-office hours
- Ensure that your EC2 instances are started and stopped as per schedule by choosing to receive notifications by Email or SMS
- Automatically start the execution of other processes by chaining Scnapper's notifications.

## General

- Log in with a username and password you choose at first-time setup. Scnapper acts on AWS through the instance's IAM role, so no access keys are entered or stored.
- Usage based pricing model which is not based on the number of resources being backed up
- Group your EC2 instances into logical groupings and simplify your EC2 runtime workflow
- Reduce cost by managing those snapshots and AMIs created outside of Scnapper

# Prerequisites

**Scnapper 4.0.0 is launched from the CloudFormation template published with the AMI. The template creates the IAM role the instance runs with, so nothing is configured in IAM by hand.**

Upgrading from Scnapper 3.x: your groups, schedules and history move by export and import (see Upgrade). A 3.x data volume cannot be reattached to a 4.0.0 instance.

You can access the web interface of Scnapper by pointing your web browser to https://<hostname or IP address of the Scnapper instance>/tool/. The certificate is generated on the instance and self-signed, so the browser warns once. If you want a fixed address, associate an Elastic IP with the instance.https://<hostname

The stack's outputs list the URL, the SSH command and the instance ID, which is also the setup token.

The following prerequisites are required for Scnapper:

1. Scnapper should be placed in a subnet with outbound routing to the Internet so it can reach the AWS API. Give the instance a public IP if you want to reach the web interface from outside the VPC.
2. The template's security group opens port 443 (the web interface) to the Internet and port 22 to the CIDR block you give as the SSH parameter, with outbound access on port 443.

| | Direction | Ports | Source/Destination |
|---|---|---|---|
| **Inbound** | | 443 | 0.0.0.0/0 (the web interface) |
| **Inbound** | | 22 | The SSH parameter of the stack |
| **Outbound** | | 443 | 0.0.0.0/0 |

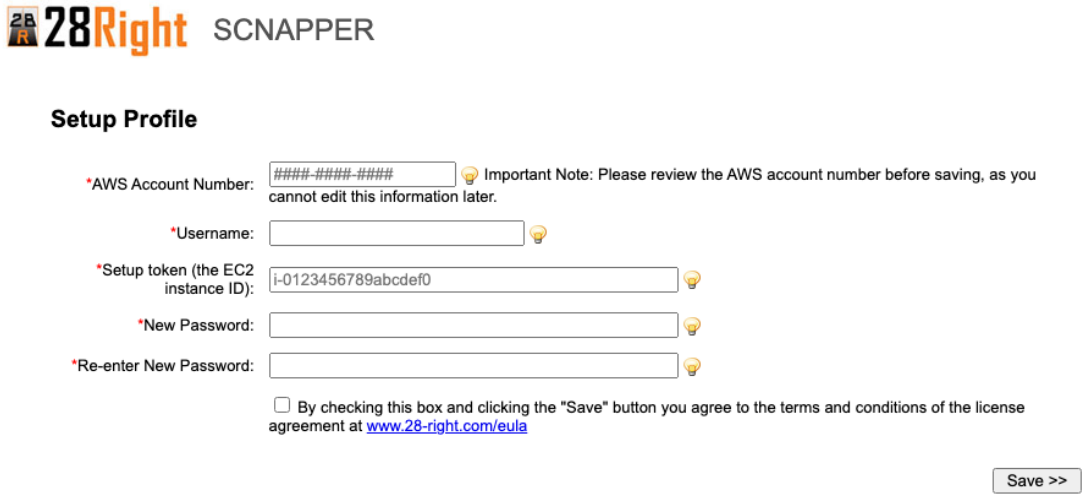
3. The instance role is created by the template. It grants only the EC2 snapshot, image, volume, instance and tag actions Scnapper uses, plus SNS publishing. Acknowledge the "CAPABILITY_IAM" prompt when you create the stack.

```
No policy to copy: the CloudFormation template creates the instance role. The full
policy is listed in the template's README.
```

# First time setup

Launch the CloudFormation stack from the listing. Choose the VPC and subnet, the CIDR block allowed to SSH in, a key pair, the instance type (t3.medium recommended) and the size of the data volume, and acknowledge the IAM capability. The stack creates the role, so there is nothing to assign at launch.

When the stack is complete, open the URL shown in its outputs (https://<public IP>/tool/) and accept the certificate warning once. You should see the following screen:https://<ipaddress




The following information must be entered:

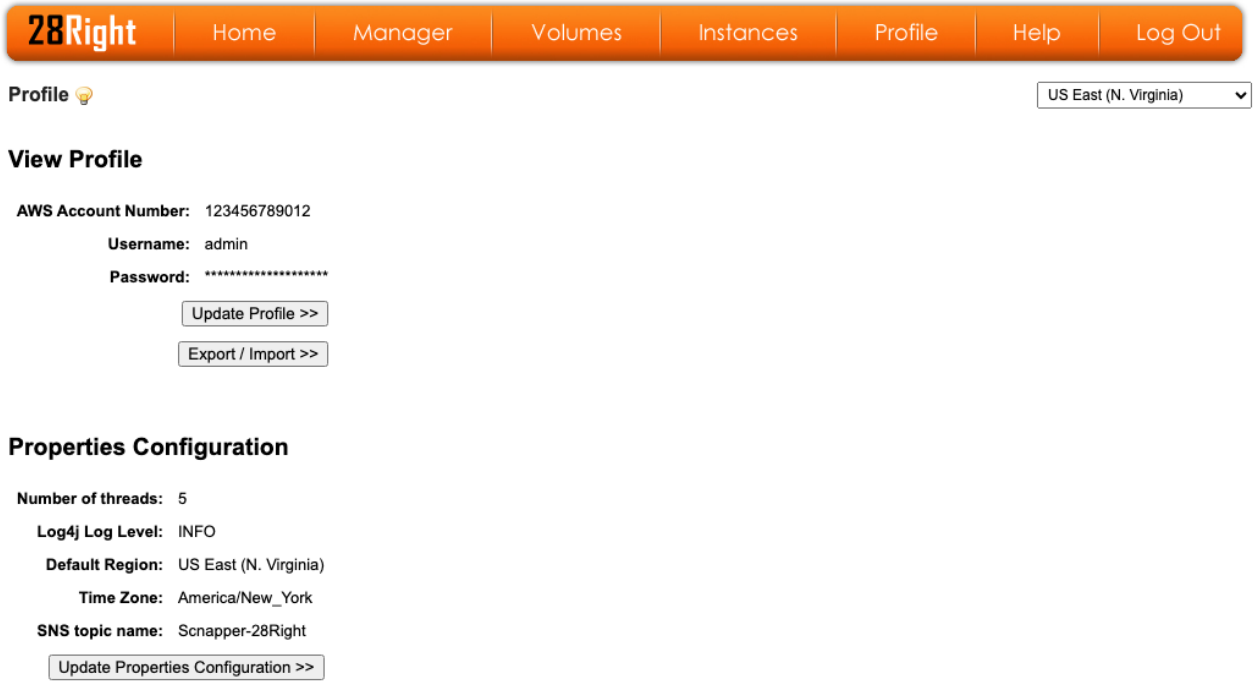
1. AWS Account Number – the 12-digit number of the AWS account the instance runs in. It identifies this Scnapper installation and cannot be changed later.
2. Username – the name you will log in with (letters, digits and . _ @ -, up to 64 characters).
3. Setup token – the EC2 instance ID of the Scnapper instance (the InstanceId output of the stack, also shown in the EC2 console). Scnapper reads its own instance ID and accepts the setup only when the two match.

4. New Password – at least 8 characters, and not the instance ID.
5. Re-enter New Password – the same password again. Tick the licence agreement box and click Save; you are taken to the login page.

# Profile

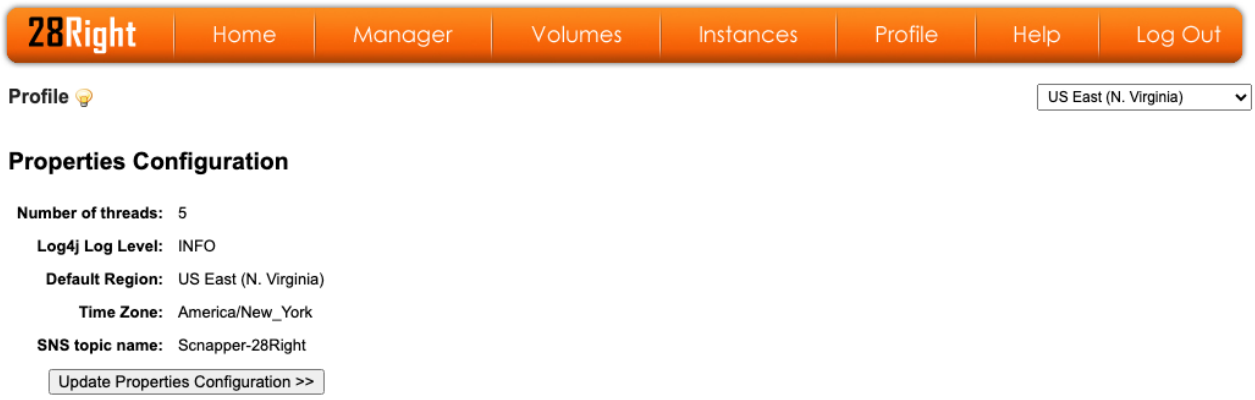
The Profile page shows the AWS account number and the username. From it you reach:

1. Edit Profile – the username and the customer name
2. Change Password – the old password, the new one and its confirmation; and Export / Import, used when migrating from Scnapper 3.x




The following parameters are set in the "Properties Configuration" page:

1. Number of threads, log level, default region and time zone (schedules are entered and shown in this time zone)
2. SNS topic name – the topic Scnapper publishes notifications to; the default is Scnapper-28Right

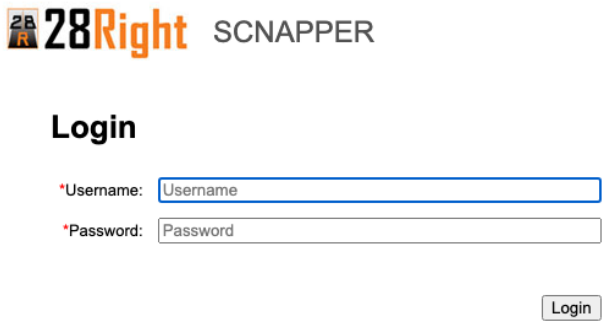



*Note: AWS Account number once set cannot be changed, if you would like to manage a different AWS account, then a new installation of Scnapper is required.*

# Login

You can login to Scnapper by following the steps below:

1. Log in with the Username and Password you chose at first-time setup, as shown below.




*Note: Only the username and password chosen at first-time setup can log in. Scnapper 4.0.0 does not use AWS access keys.*

# User guide

Scnapper's user guide is found on Help tab after you login.

# Upgrade

Upgrades are delivered as new AMIs with a new CloudFormation template. From 4.0.0 onwards the data volume carries everything, so an upgrade reattaches it to a new instance and your users, groups and schedules are kept:

1. Take a snapshot of the data volume (the DataVolumeNote output of the stack names it). This is the rollback point.
2. Note the volume's Availability Zone, then delete the old stack. The data volume is kept: it is not deleted on termination.
3. Confirm in the EC2 console that the volume shows as available.

4. Create a new stack from the new version's template with ExistingDataVolumeId set to that volume, and a Subnet in the same Availability Zone.
5. First boot applies any pending database changes and comes up with your existing users, groups and schedules. There is no export or import.
6. If an Elastic IP was associated with the previous instance, associate it with the new one.
7. Upgrading from Scnapper 3.x: install the export patch on the 3.x instance, export, launch 4.0.0 with a new data volume, complete first-time setup, then import the file on the Profile page under Export / Import. The full procedure and the patch download are in the listing's upgrade notes.
8. Downgrades are not supported. To roll back, launch the previous version's template against a volume restored from the snapshot taken in the first step.

# Upgrading from Scnapper 3.x

The steps are the same as in the user guide, in short: snapshot the 3.x data volume; install the export patch on the 3.x instance (SSH in as snapusr, download and checksum below, then tar xzf, cd into the unpacked folder and sudo sh install.sh; the installer copies the files into the webroot /opt/bitnami/apache2/htdocs/tool itself, so do not cd there or change its permissions) and export from https://<3.x address>/tool/maint/export in the browser; launch 4.0.0 from the Marketplace listing with a NEW data volume and complete the first-time setup; on the Profile page set the Properties Configuration, then Export / Import the file; verify your groups and schedules, and only then retire the 3.x instance.

Export patch: https://scnapper-getting-started.s3.amazonaws.com/scnapper-export-patch-1.1.tar.gz

SHA-256: e3ad48e50e3ab7996c84b106ecde89951e5092178b4ffd2d56cd6ef46617db01

A 3.x data volume cannot be attached to a 4.0.0 instance (MySQL 8 cannot open the 3.x database); if one is attached anyway nothing is destroyed and a banner asks you to import. Your AWS credentials do not migrate: 4.0.0 acts through the instance role.