Backbox AWS and SSO Integration

1. Introduction

Backbox, as a tool for performing configuration backups on network devices, allows for exporting the configurations it retains to remote destinations which are independent of Backbox.

One of the possible destinations for exporting the backup configurations is to long-term storage in AWS Glacier. In addition to supporting exporting backups to Glacier and supporting the ability to retrieve them later, Backbox also supports performing these actions using Single-Sign-on credentials.

For the purpose of this guide, it is assumed you have at least a basic acquaintance with Amazon Glacier, and some understanding of the terms and concepts required for working with Amazon Glacier. If this is not the case, please visit https://docs.aws.amazon.com/amazonglacier/latest/dev/amazon-glacier-getting-started.html before reading this guide.

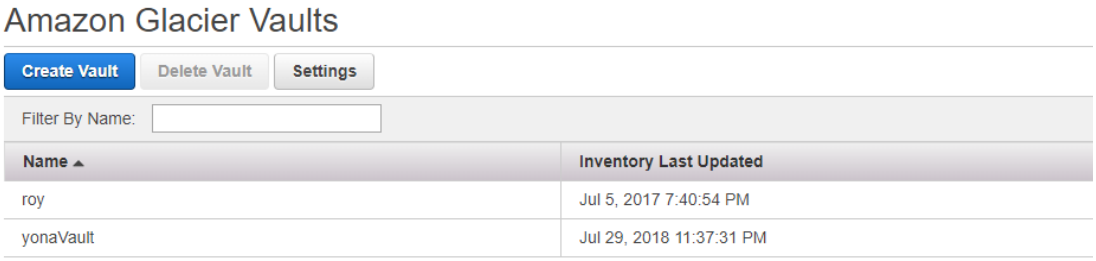
2. Prerequisites

- A fully working and licensed Backbox installation – At least version 6.10.00.
- An AWS account – Free tier is sufficient, but Expedited retrievals incur additional charges.

3. Configuring your AWS account

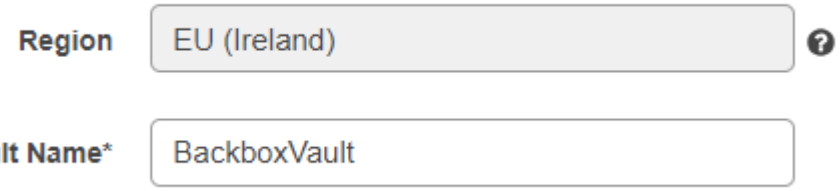
Log in to your AWS account and select your desired availability zone. For this guide, we have chosen the Ireland (eu-west-1) availability zone.

Once selected, go to your Amazon Glacier console using the following link: https://eu-west-1.console.aws.amazon.com/glacier/home and click the "Create vault" button.

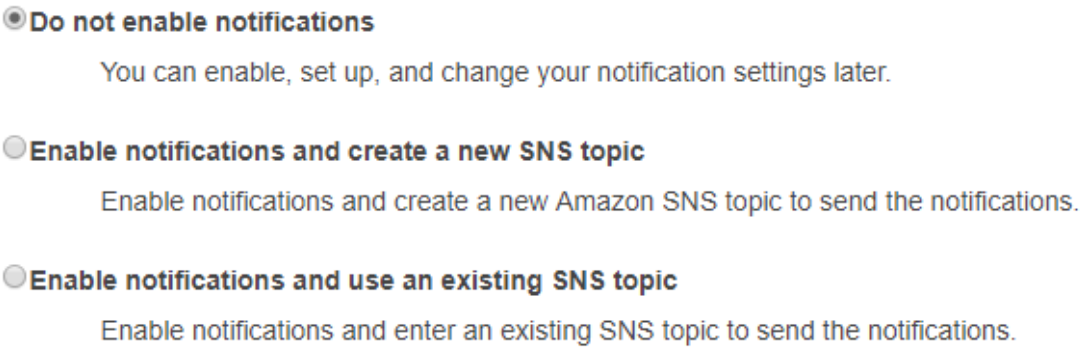


Follow these steps to create a vault for storing your Backup configurations:

A) Enter a vault name for later reference. We chose "BackboxVault" for this guide, but you may choose any name.



B) Keep the event notifications for the vault on "Do not enable notifications"



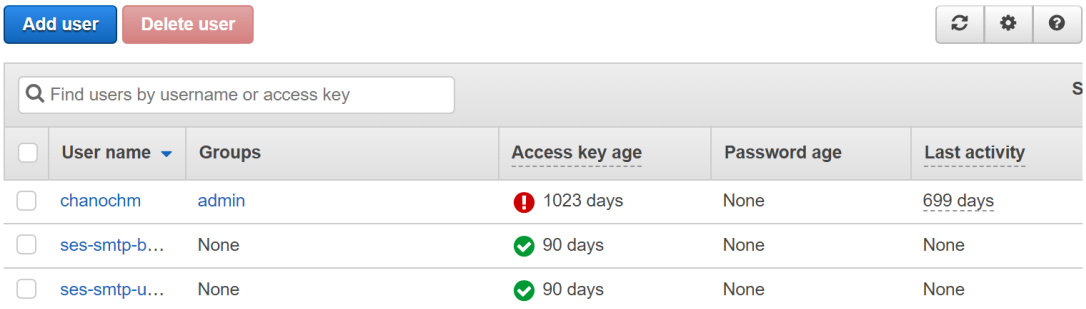
C) Review your vault details and click the blue "Submit" button to create your vault.

4. Create IAM user with IAM role and alias

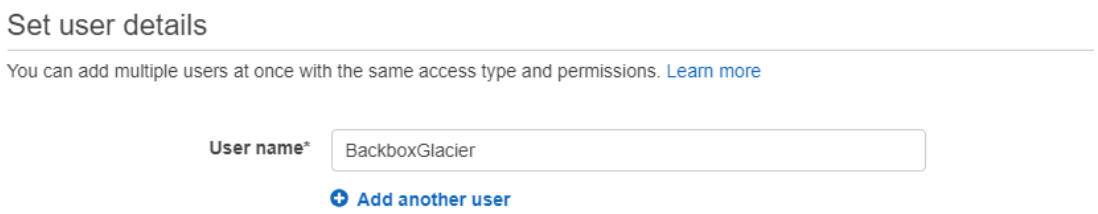
While you may provide the details of your root AWS user, it is highly recommended to create an IAM user. With a dedicated IAM user, you can grant Backbox the exact permissions required for exporting and retrieving backups without compromising the security of your root user and your other AWS services.

Login to your AWS account, and go to your IAM management console using the following link: https://console.aws.amazon.com/iam/home. Navigate to the "Users" tab and follow the next steps to create an IAM user for Backbox:

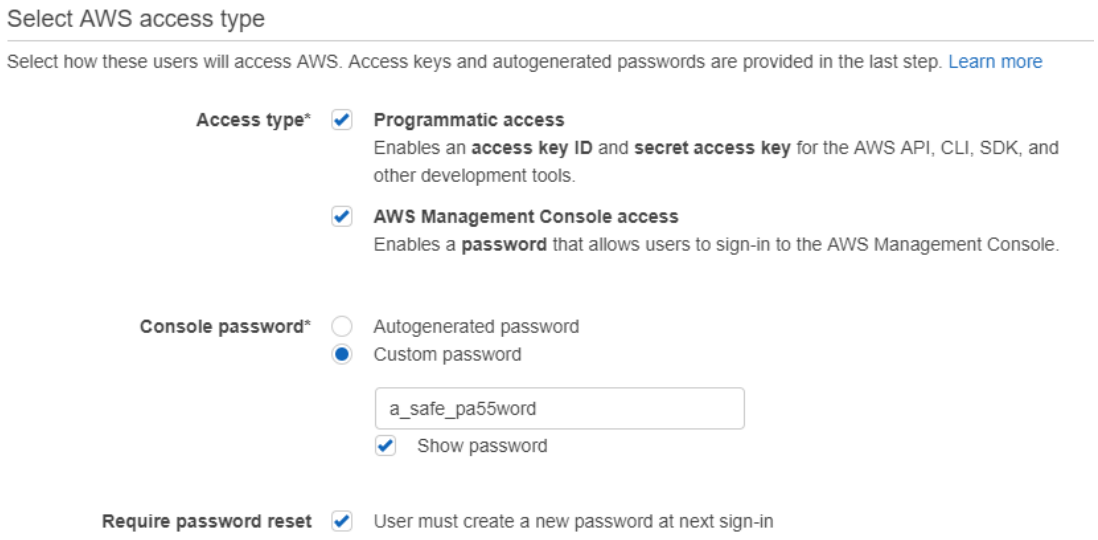
A) Click the "Add user button for create a new IAM user.



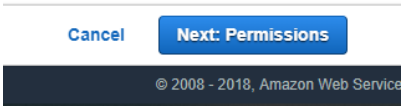
B) Choose a user name for our new user. We chose "BackboxGlacier" for this guide, but you may choose any name.



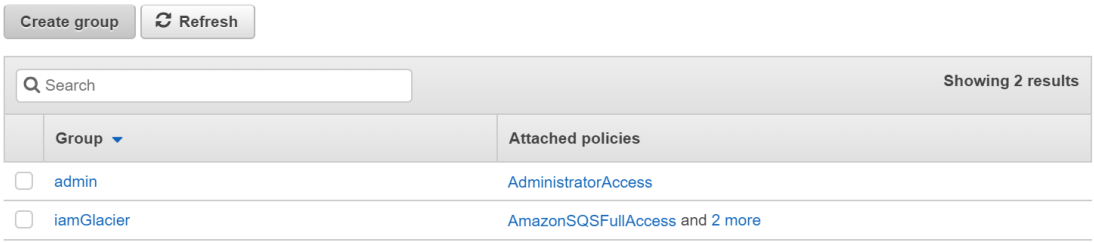
Tick both "Access type" checkboxes and enter a password for the web console in the "Console password" field.



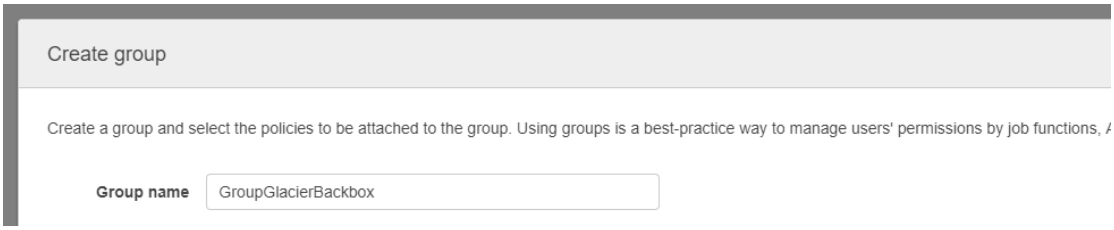
Once finished, click on the "Next: Permissions" button to the bottom right of the screen.



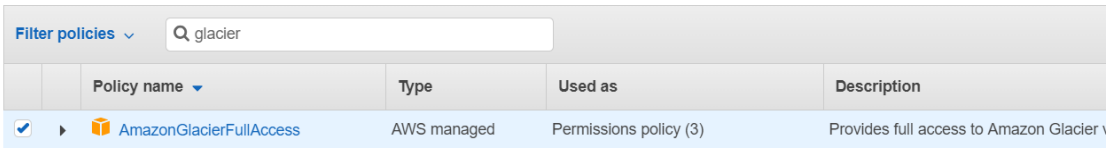
C) We will need to define the proper security policies for our new user. In order to do so, click the "Create group" button to create an IAM group with the needed policies.



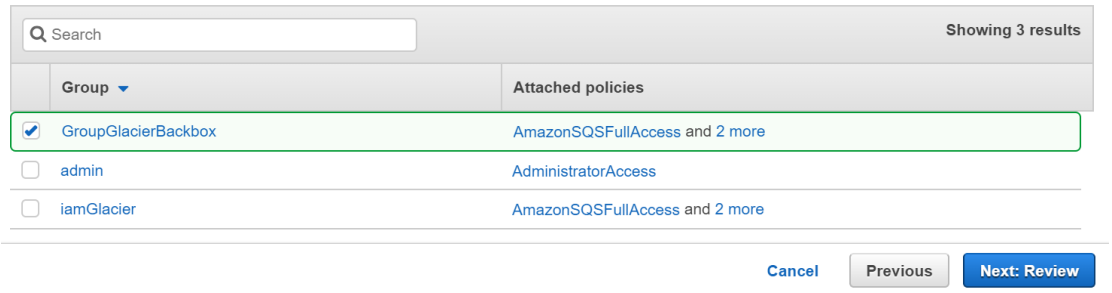
D) Choose a user name for our new user. We chose "GroupGlacierBackbox" for this guide, but again - you may choose any name you want.



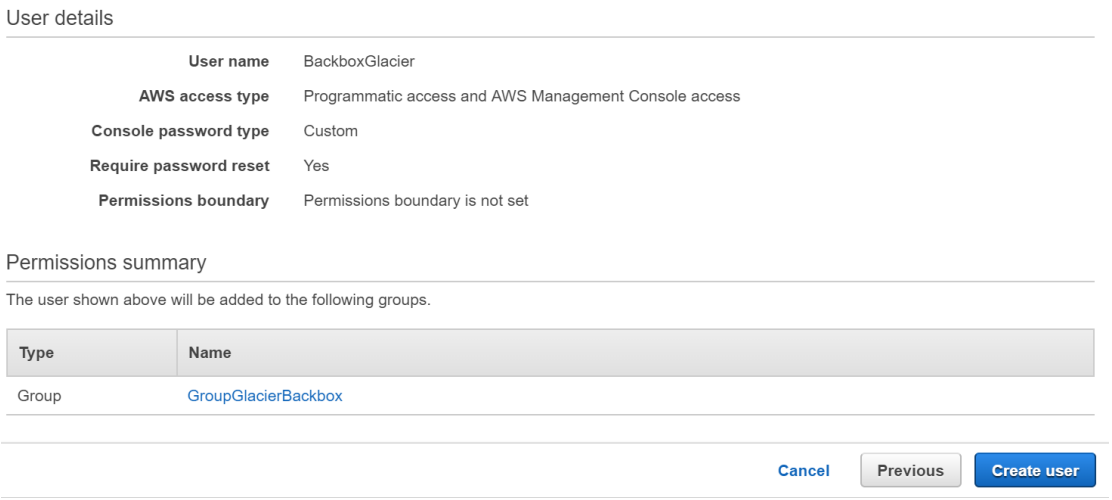
Our new group requires three policies to properly perform exports and retrievals from our vault: AmazonGlacierFullAccess, AmazonSNSFullAccess and AmazonSQSFullAccess. Make sure you tick each policy before clicking the blue "Create group" button to the bottom right of the screen.



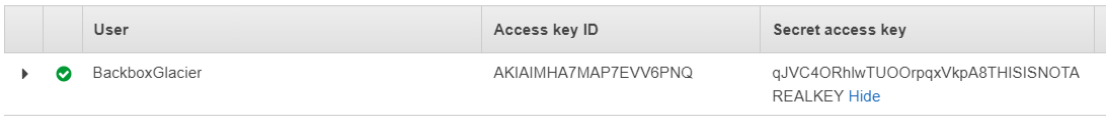
E) Once the new group had been created, make sure the group is checked and click the "Next: Review" button to the bottom right of the screen.



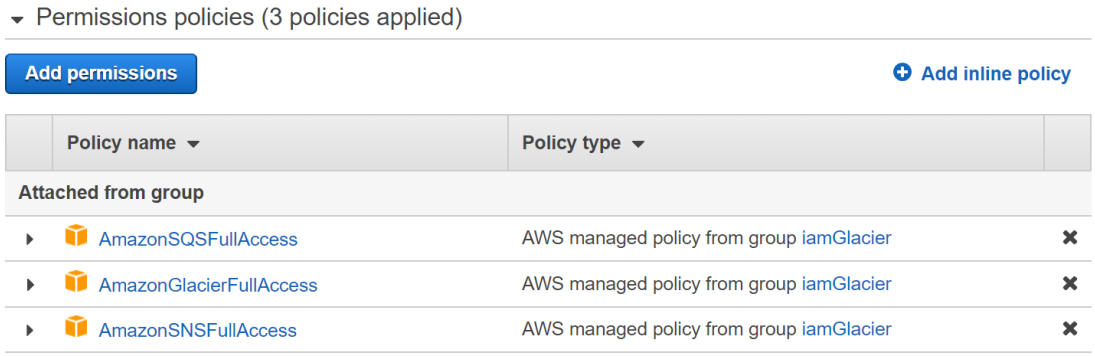
F) Review that all details are correct and click the "Create user" button to the bottom right of the screen.



G) Copy your Access key ID and Secret access key for and keep them in a safe place until integrating them with Backbox.

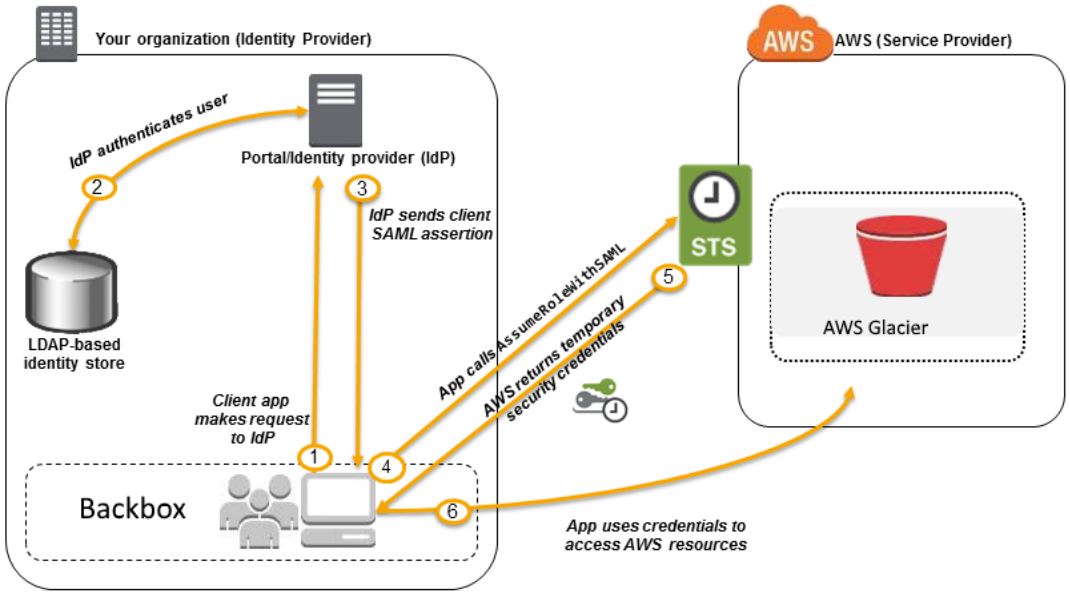


H) Back in the Users tab, click on our new user, and make sure it has all required permissions. Otherwise, Backbox may not be able to properly export or retrieve backups from your Glacier vault.



5. Connect your Identity provider with Backbox and AWS

Backbox supports performing backup exports and retrievals using Single Sign on credentials. AWS supports several different ways to integrate an organization's Identity provider servers with AWS, but the two most common ways are using SAML 2.0 Federation (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_roles_providers_saml.html) and assuming IAM roles with temporary credentials (https://docs.aws.amazon.com/IAM/latest/UserGuide/id_credentials_temp.html).

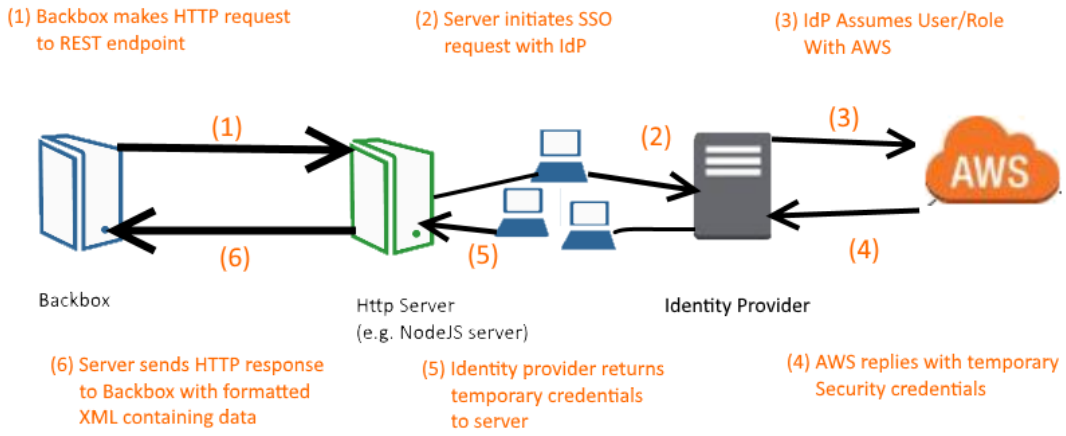


An example diagram showing the data flow for integrating Backbox with AWS Glacier
Using SAML 2.0 based Federation with an LDAP server

The one thing in common for all methods is the way they work: Regardless of the exact specifications of integration (which, as we said, vary between each solution) your Identity provider must assume an IAM user or an IAM role, and receive temporary credentials to access the IAM user or the IAM role.

Should you wish your Backbox installation to perform Single Sign on requests when exporting to your Glacier vault or retrieving from it, you will need to provide an HTTP endpoint for Backbox to query.

It is up to you to return an HTTP response for requests made to the endpoint you provide, with the temporary credentials required for the Single Sign on request.



The response must be a UTF-8 encoded XML formatted like the following example:

```
<?xml version="1.0" encoding="UTF-8"?>
<StsCredentials>
      <accessKeyId>{{AWS Access Key ID}}</accessKeyId>
      <secretAccessKey>{{AWS Secret Access Key}}</secretAccessKey>
      <sessionToken>{{Session Token}}</sessionToken>
      <sessionExpiredDate>Tue Feb 13 13:02:39 EST 2018</sessionExpiredDate>
      <credsLifeInSec>3600</credsLifeInSec>
</StsCredentials>
```

Backbox will query your Http server whenever needed, in order to obtain single sign on credentials for your backup exports and retrievals.

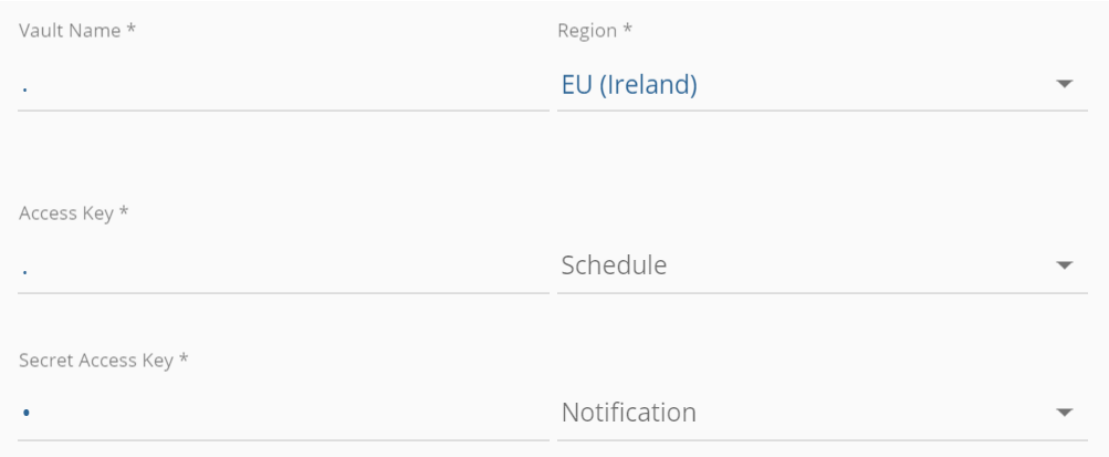
6. Integrate with Backbox

In order to integrate with Backbox, we shall now teach Backbox how to interface with our AWS account so Backbox can send it our backup configurations.

From your Backbox web console, navigate to Backups => Exports => Remote Configuration. We will first configure an AWS export configuration:

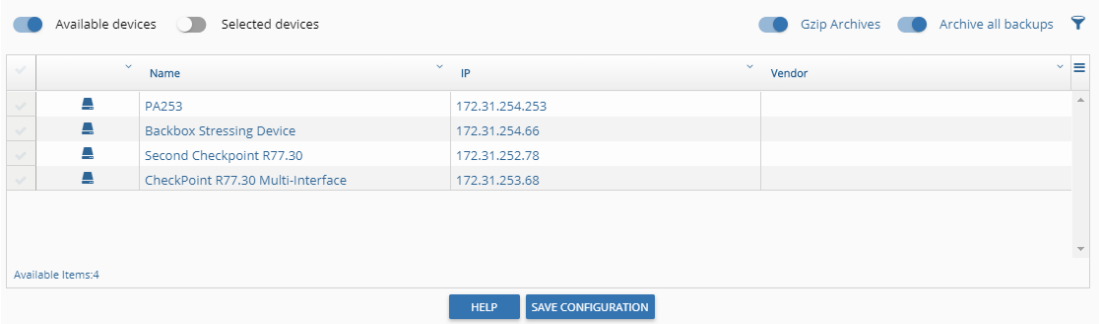
A) Select the "AWS" radio button from the top of the screen.

B) Configure the following fields:



Vault name: Enter the name of the Glacier vault you have created.
Region: Enter the availability region in which you created your vault.
Access key: Enter the access key of the root user / your IAM user.
Secret access key: Enter the secret key of the root user / your IAM user.

Once you have provided all required fields, select which devices you wish to back up remotely.



C) Select a schedule from your created schedule list, to specify at which interval Backbox will upload your backups as archives to your Glacier vault.

You may also (optionally) select a notification to notify yourself or other users whenever a scheduled export succeeds.

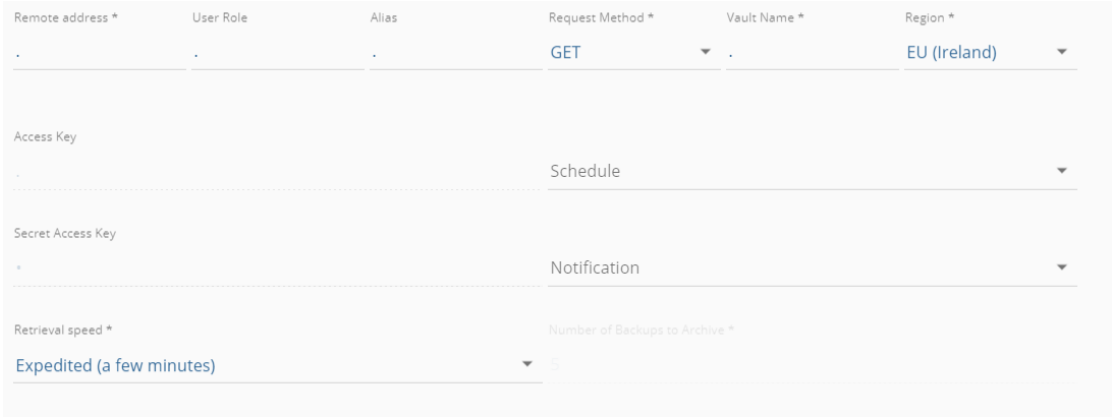
Save your configuration, and we are good to go.

7. Backbox SSO configuration

If you have connected an Identity provider for single sign on requests in step 5, you will need to make a few additional configurations in order to finalize the configuration:

A) Select the "AWS SSO" radio button from the top of the screen.

B) Configure the following fields:

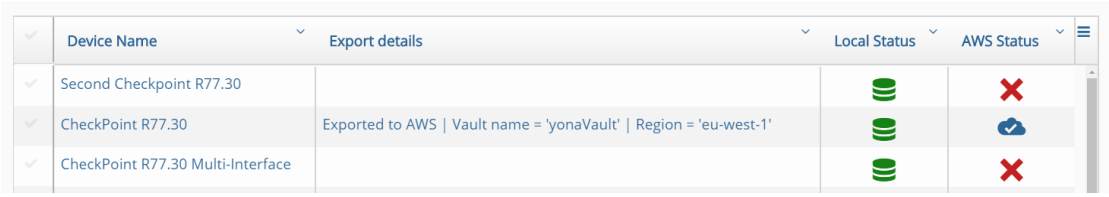


Remote address: Enter the REST endpoint (URL) from which to request temporary SSO credentials.
User role: (Optional) Allows to specify which IAM user or role to assume.
Alias: (Optional) The alias of the account belonging to the IAM user being assumed.
Request Method: Whether the HTTP request should be a GET or a POST request.

C) Click the "Save" button in order for the changes to take place.

8. Run backups and await upload

Run your selected devices manually, or by assigning them to a backup job and executing it. When your schedule reaches its next interval, it will check each device to see which one has performed successful backups and upload them to AWS.



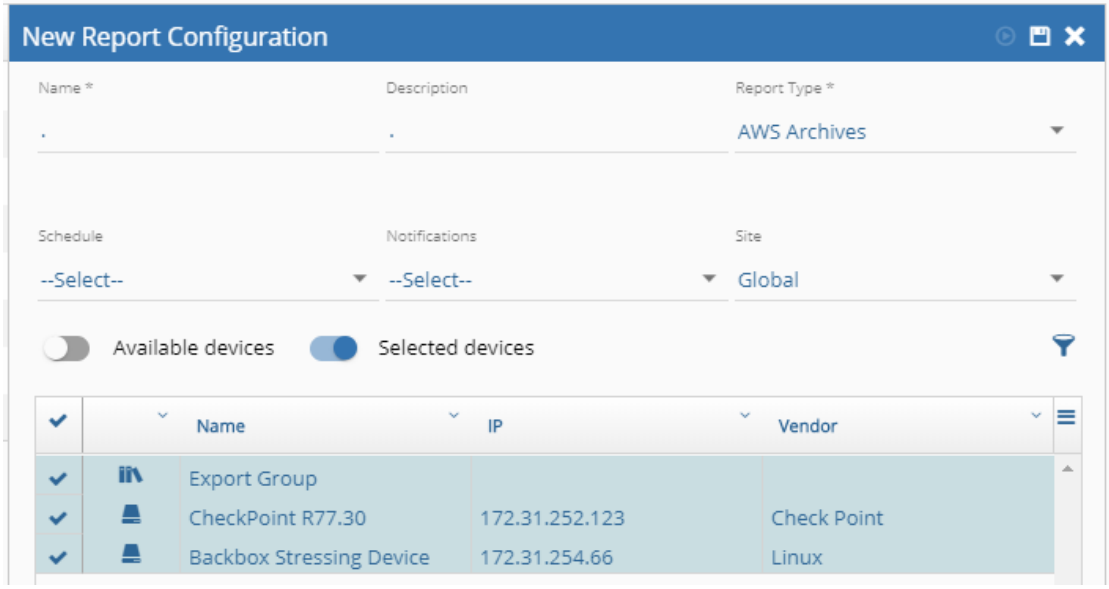
If successful, your backup will have it's AWS status marked with a cloud icon confirming it has been exported, along with an Export details column specifying the exact details of the export job.

In case you have selected a notification, Backbox will notify each user assigned to the notification about the export job on a per-device basis. That is – which devices have succeeded, and (in case of failures) which devices have failed to export.

9. Create an AWS report

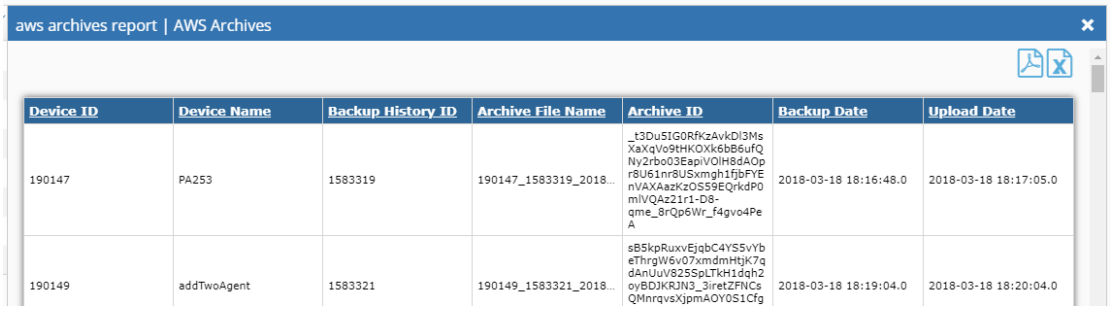
If you wish to receive a more detailed report regarding your Backup configurations that have been stored in AWS, you can create an AWS archive report to provide you with the full details of each backup exported to AWS.

Navigate to Dashboard => Reports and click the "Add" button to create a new report.



Give your report a name, and an optional description, and select "AWS Archives" as the report type. You can then choose which devices you wish to include in the report from the device picker to the bottom of the configuration sheet.

Save your report and click the "Run" button to the top right corner of the side sheet. Backbox will summarize the data collected about your AWS exports in the following window:



The report is available, as with all Backbox reports, for download as a pdf document or an Excel sheet.

Optionally, you may also assign a schedule and a notification to your new report, to receive the updated report periodically according to the details specified by the notification you chose.

10. Troubleshooting and errors

Backbox is dedicated to providing cutting-edge and reliable solutions for backup configuration and restoring. However, due to the complex nature of the feature being discussed, some errors may still occur during backup export or retrieval.

Should Backbox fail to export or retrieve a backup configuration, it will output an error message to the general log located in /backbox/backbox-3.0/app-server/apache-tomcat-7.0.37/logs/general.log

If you have a notification configured, Backbox will alert you on any such failure and instruct you to access your general log if you wish to further understand the nature of the failure.

This is a brief list of the most common errors that may be encountered:

Error: `com.amazonaws.SdkClientException: Unable to execute HTTP request: sns.eu-west-1.amazonaws.com`

Cause: Backbox does not recognize any DNS servers, and cannot resolve any URLS.

Solution: Navigate to Settings => DNS and configure a primary and secondary DNS server. After Backbox restarts, the error should not persist.

Error: `com.amazonaws.services.sns.model.AmazonSNSException: The security token included in the request is invalid`

Cause: The Access key, Secret key or Temporary credentials you provided are incorrect.

Solution: Double-check with your AWS account or IAM role that the credentials you provided Backbox are correct.

Error: `com.amazonaws.services.glacier.model.ResourceNotFoundException: Vault not found for ARN: arn:aws:glacier:eu-west-1:1234567890123:vaults/anyRandomVault`

Cause: The Vault name you have provided does not exist. Or alternately, exists but not in the same region you have specified.

Solution: Double-check with your Glacier console that you are uploading to an existing vault in the correct region.

Error: `com.amazonaws.services.glacier.model.InsufficientCapacityException: There is insufficient capacity to process this Expedited request.`

Cause: The Remote configuration attempted a retrieval using expedited capacity, which exceeds the expedited capacity currently available for your account.

Solution: If you did not purchase any expedited capacity from AWS, this is the time to do so. Alternately, if you perform large amounts of retrievals simultaneously, this is the time to purchase some more.