

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.

Amazon Glacier Vaults

Create Vault	Delete Vault	Settings
Filter By Name: <input type="text"/>		
Name ▲	Inventory Last Updated	
roy	Jul 5, 2017 7:40:54 PM	
yonaVault	Jul 29, 2018 11:37:31 PM	

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.

BACKBOX

Region ?

Vault Name*

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

☒ **Do not enable notifications**

You can enable, set up, and change your notification settings later.

☐ **Enable notifications and create a new SNS topic**

Enable notifications and create a new Amazon SNS topic to send the notifications.

☐ **Enable notifications and use an existing SNS topic**

Enable notifications and enter an existing SNS topic to send the 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.

Add user

Delete user

Find users by username or access key

<input type="checkbox"/>	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	chanochm	admin	<div><div></div></div> 1023 days	None	699 days
<input type="checkbox"/>	ses-smtp-b...	None	<div><div></div></div> 90 days	None	None
<input type="checkbox"/>	ses-smtp-u...	None	<div><div></div></div> 90 days	None	None

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

Set user details

You can add multiple users at once with the same access type and permissions. [Learn more](#)

User name*

[+](#) Add another user

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

Select AWS access type

Select how these users will access AWS. Access keys and autogenerated passwords are provided in the last step. [Learn more](#)

- Access type* ☒ **Programmatic access**
Enables an **access key ID** and **secret access key** for the AWS API, CLI, SDK, and other development tools.
- ☒ **AWS Management Console access**
Enables a **password** that allows users to sign-in to the AWS Management Console.

Console password* ☐ Autogenerated password
☒ Custom password

☒ Show password

Require password reset ☒ User must create a new password at next sign-in

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

Cancel

Next: Permissions

© 2008 - 2018, Amazon Web Services

- 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.

Create group

Refresh

Search

Showing 2 results

Group ▾

Attached policies

☐ admin

AdministratorAccess

☐ iamGlacier

AmazonSQSFullAccess and 2 more

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

Create group

Create a group and select the policies to be attached to the group. Using groups is a best-practice way to manage users' permissions by job functions, /

Group name

BACKBOX

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.

Filter policies <input type="text" value="glacier"/>				
	Policy name	Type	Used as	Description
<input checked="" type="checkbox"/>	AmazonGlacierFullAccess	AWS managed	Permissions policy (3)	Provides full access to Amazon Glacier

- 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.

Search <input type="text"/>		Showing 3 results
Group	Attached policies	
<input checked="" type="checkbox"/> GroupGlacierBackbox	AmazonSQSFullAccess and 2 more	
<input type="checkbox"/> admin	AdministratorAccess	
<input type="checkbox"/> iamGlacier	AmazonSQSFullAccess and 2 more	
		Cancel Previous Next: Review

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

User details

User name	BackboxGlacier
AWS access type	Programmatic access and AWS Management Console access
Console password type	Custom
Require password reset	Yes
Permissions boundary	Permissions boundary is not set

Permissions summary

The user shown above will be added to the following groups.

Type	Name
Group	GroupGlacierBackbox

[Cancel](#) [Previous](#) [Create user](#)

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




User	Access key ID	Secret access key
<input checked="" type="checkbox"/> BackboxGlacier	AKIAIMHA7MAP7EVV6PNQ	qJVC4ORhlwTU0OrpqxVkpA8THISISNOTAREALKEY Hide

- 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.

▼ Permissions policies (3 policies applied)

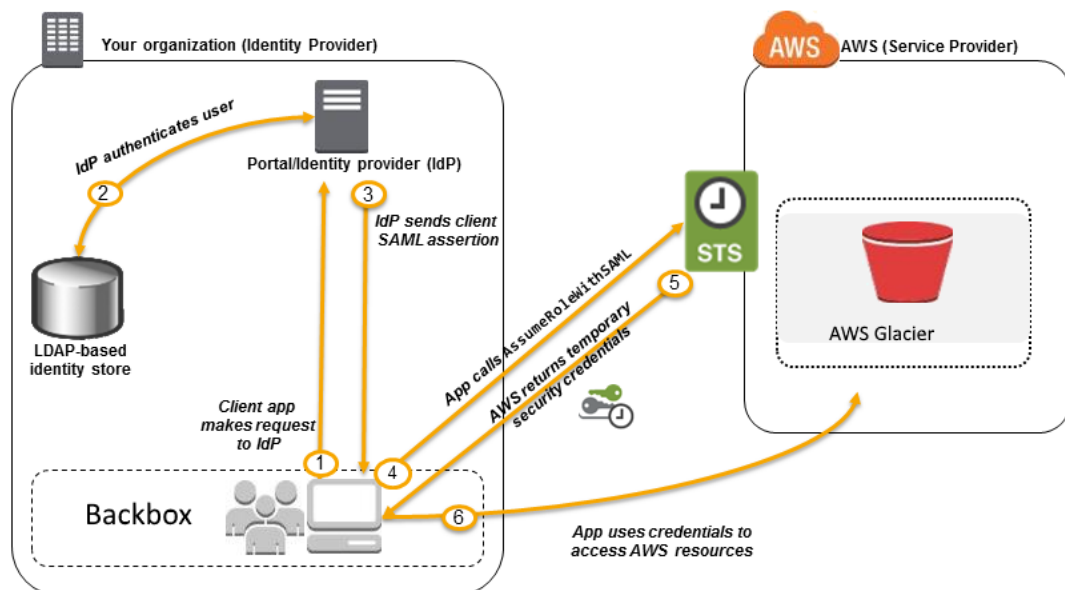
Add permissions

+ Add inline policy

Policy name ▼	Policy type ▼	
Attached from group		
▶  AmazonSQSFullAccess	AWS managed policy from group iamGlacier	✕
▶  AmazonGlacierFullAccess	AWS managed policy from group iamGlacier	✕
▶  AmazonSNSFullAccess	AWS managed policy from group iamGlacier	✕

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).



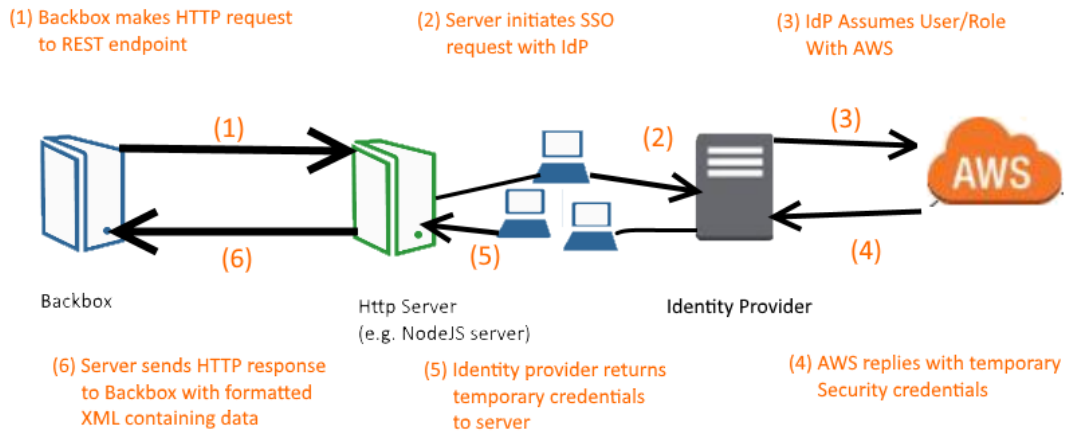
An example diagram showing the data flow for integrating Backbox with AWS Glacier Using SAML 2.0 based Federation with an LDAP server

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.

BACKBOX

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 *	Region *
.	EU (Ireland) ▼
Access Key *	Schedule ▼
.	
Secret Access Key *	Notification ▼
.	

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. The device picker will only contain devices that satisfy one of the following criteria:

- 1) The device is not assigned to any agent or agent group.
- 2) The device is assigned to an agent which has file replication enabled.

☒ Available devices
 ☐ Selected devices
 ☒ Gzip Archives
 ☒ Archive all backups

✓	Name	IP	Vendor
✓	PA253	172.31.254.253	
✓	Backbox Stressing Device	172.31.254.66	
✓	Second Checkpoint R77.30	172.31.252.78	
✓	CheckPoint R77.30 Multi-Interface	172.31.253.68	

Available Items: 4

[HELP](#)
[SAVE CONFIGURATION](#)

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.

It is also recommended that you 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.

☐ None
 ☐ SCP
 ☐ CIFS
 ☐ FTP
 ☐ NFS
 ☐ AWS
 ☒ AWS SSO

B) Configure the following fields:

Remote address *	User Role	Alias	Request Method *	Vault Name *	Region *
.	.	.	GET	.	EU (Ireland)
Access Key			Schedule		
Secret Access Key			Notification		
Retrieval speed *			Number of Backups to Archive *		
Expedited (a few minutes)			5		

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, Backbox will check each device for backups which meet the following criteria:

- 1) The backup has completed successfully
- 2) The backup does not point to a newer backup
- 3) (if assigned to an agent) The backup has been replicated to Backbox management file system.

Type	Date	Site	File Size	Status	Failure Reason	Log	Comment	ID	Remote Status	Agent...
1) Successful, Replicated, Agent			29 bytes					1584720		
2) Backup with pointer			29 bytes					1584718		
3) Backup which was not replicated			29 bytes					1584711		

Example figure: Backup 1) will be exported, because it has completed successfully and has been replicated to Backbox Management. Backup 2) will not be exported because it is a pointer to backup 1). Backup 3) will not be exported because it has not been replicated.

All backups that match the listed criteria, up to the limit set in the export configuration, will be exported to AWS.

Device Name	Export details	Local Status	AWS Status
Second Checkpoint R77.30			
CheckPoint R77.30	Exported to AWS Vault name = 'yonaVault' Region = 'eu-west-1'		
CheckPoint R77.30 Multi-Interface			

If the export was 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.

New Report Configuration

Name *

.

Description

.

Report Type *

AWS Archives

Schedule

--Select--

Notifications

--Select--

Site

Global

Available devices

Selected devices

		Name	IP	Vendor	
		Export Group			
		CheckPoint R77.30	172.31.252.123	Check Point	
		Backbox Stressing Device	172.31.254.66	Linux	

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:

aws archives report | AWS Archives

AWS Archives Report

Device ID	Device Name	Archive File Name	Archive ID	Backup History ID	Backup Date	Upload Date
205082	Backbox Monica	205082_1584492_2018-10-28 17:35:02	XHqzQ8oA84NZLsQzXVqMaPKru0M08P8FGXq2bFwweYAHfUNau7Lxwdsq0OSEJQ36sg2md9EaxS aAhJWHY3jNbwgmD5nH_Ak8Hh8yU_278Nin38V88nd8nyjyKcEUg	1584492	2018-10-28 17:34:38.0	2018-10-28 17:35:02.0
205083	AddOne	205083_1584493_2018-10-28 17:35:02	6k5l3dRmbicxiteT8vaVp7Lo3SePw-NMVoSreUGictbtgMjndDqyMx74ORQ3Iac_5XL_vB2Imzpzf54PeU5_Y4ZyvA-QEMFRAKz_W7L0BXARu3J_JX7V7bxS3VnLwP6aw	1584493	2018-10-28 17:34:38.0	2018-10-28 17:35:02.0
205084	Checkpoint R77.30 B	205084_1584487_2018-10-28 17:37:01	EU4ZqQ4Ytq7HdY4r5lVH0Llva3BNXToC43wYoaCkURJWHxplzdYw1be_x9z7B3HDJfPjv1gCiz2H7tpi 0-13XlgASKXZ2eUevG7NqFyZ04Qv4wVeS-ZY4dICGPe3i1ig-Q	1584487	2018-10-28 17:36:34.0	2018-10-28 17:37:01.0
205085	1584495	2018-10-28	aS71fNR8f8nRbaufHNSfD(GAI) aP3nmb7m1R1r4_PVnRzCTmndhAnVnSrlJ86nD7v7VufuaRHRanA8aY		2018-10-28	2018-10-28

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. Performing Retrievals

If you wish to retrieve your backups from AWS, simply select the backups you wish to retrieve and click the "Retrieve from external storage" button. Backbox will then initiate a retrieval job and request them from AWS.

Retrieve from external storage

Backup...	Device Name	Backup Date	Export Date	Export details	Local S...	AWS St...
✓	1584730	Checkpoint R77.30 B	12-10-2018 12:03 AM	12-10-2018 12:04 AM	Exported to AWS Vault name = 'yonaVault' Re...	✓
✓	1584726	Checkpoint R77.30 B	12-09-2018 12:03 AM	12-09-2018 12:04 AM	Exported to AWS Vault name = 'yonaVault' Re...	✓
✓	1584722	Checkpoint R77.30 B	12-08-2018 12:03 AM	12-08-2018 12:04 AM	Exported to AWS Vault name = 'yonaVault' Re...	✓
✓	1584720	Backbox Monica	12-07-2018 06:00 PM	12-07-2018 06:01 PM	Exported to AWS Vault name = 'yonaVault' Re...	✓
✓	1584719	AddOne	12-07-2018 05:28 PM	12-07-2018 05:29 PM	Exported to AWS Vault name = 'yonaVault' Re...	✓

Depending on the retrieval speed specified in the Remote configuration tab (standard or expedited), the retrieval may last for any time between a few minutes to several hours.

Once complete, the backup files will be downloaded to the Backbox file system, and a history record will appear in your device details screen and the backup history screen. The "Local Status" icon will change to mark that the backup exists locally.

However, there are a few cases in which Backbox will not allow the retrieval to occur and will fail the job on purpose, without downloading the files:

- 1) The device has transferred to a different agent than the one it was assigned to while running the selected backup.
- 2) The device type has changed since the backup has been executed.
- 3) The device type which was used when running the selected backup no longer exists.

In case Backbox has been shut down, it will reinitialize the retrieval jobs it has been working on before it was terminated.

Please note that the backup exports tab only keeps track of devices that currently exist in Backbox. If a device is deleted, Backbox will stop tracking its remote backups, and they will no longer be available for retrieval through the Backbox web client.

As with the backup exports, it is recommended that you select a notification in the remote configuration tab to notify yourself or other users whenever a scheduled retrieval succeeds. Backbox will notify each user assigned to the notification about the retrieval job on a per-device basis.

11. 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.