The background features a blurred server room with rows of server racks. A hand with pink floral nail polish is holding a smartphone in the lower-left corner. The page is overlaid with large, abstract geometric shapes in blue and black.

GTB DLP Suite

GTB Amazon S3 Discovery

Reference, Version 15.18.3

GTB Technologies, Inc
December 2023

Intellectual property rights This document is the property of GTB Technologies, Inc. No part of this document shall be reproduced, stored in a retrieval system, translated, transcribed, or transmitted by any means without permission from GTB Technologies. Information contained within this document is confidential and proprietary to GTB Technologies and should not be disclosed to anyone other than the recipients and reviewers of this document. However, in the event of award to GTB Technologies, this information may be disclosed to and will be used on behalf of and according to the interests of the client to whom it is addressed.

Confidentiality Statement The descriptive materials and related information in this document contain information that is confidential and proprietary to GTB Technologies. This information is submitted with the express understanding that it will be held in strict confidence and will not be disclosed, duplicated, or used, in whole or in part, for any purpose other than evaluation of this document.

Patents Statement GTB Technologies has pending patent applications for this product.

Copyright statement Copyright © GTB Technologies, Inc 2005-2024 www.gttb.com

Contacts
GTB Technologies, Inc.
2054 Vista Parkway, Suite 400
West Palm Beach, FL 33411

Phone: 1 (800) 626-0557
Email: support@gttb.com

Confidential

Contents

1	Introduction	3
1.1	Definitions	3
1.2	Requirements	3
2	Add OneDrive Service Account	4
3	Install Discovery Server	2
4	Start the Discovery scan	3
5	Check scan result	6

1 Introduction

This document explains the necessary steps for running the GTB Amazon S3 Discovery.

1.1 Definitions

Scanning server – The Windows Server machine which performs the Discovery scan.

1.2 Requirements

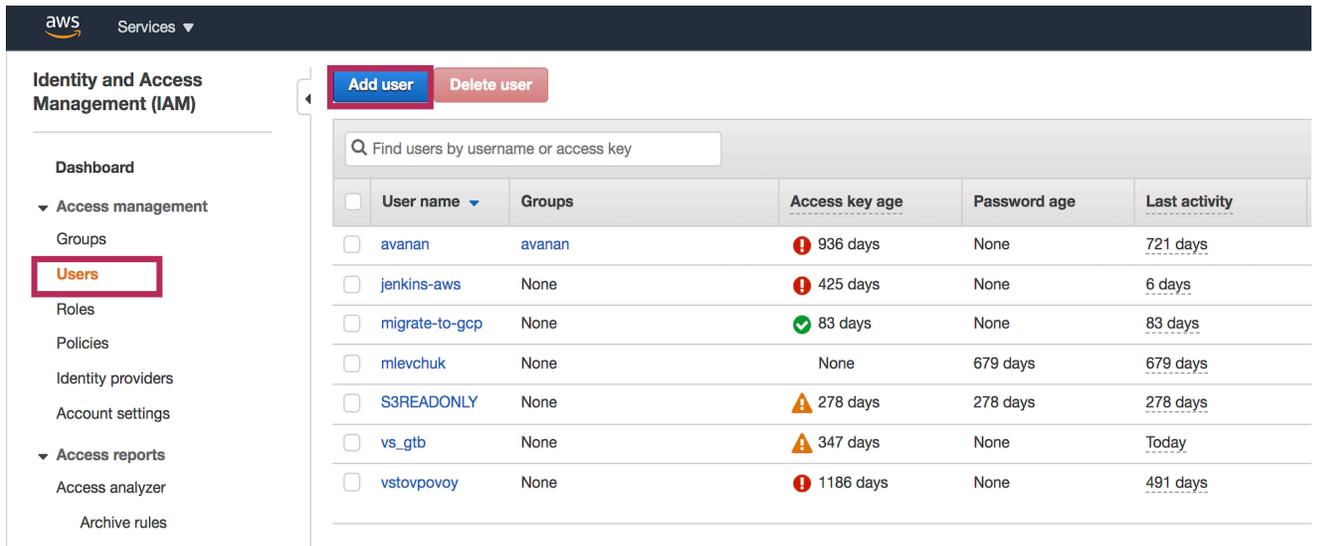
- ❖ **Scanning Server** – The GTB Discovery Server installed on any Windows Server. Provide at least 2 CPU cores and 2GB RAM for each.

The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster is scanning speed.

- ❖ **Amazon S3 account** - Service Account, which has access to the Amazon S3.

2 Create Secret Access key and ID

1. Open [AWS Console page](#) and go to the **IAM** page. Click on the **Users** tab.
2. Click the **Add** user button, as shown in the Figure below.



The screenshot shows the AWS IAM console interface. On the left, the 'Users' tab is highlighted in red. In the main content area, the 'Add user' button is also highlighted in red. Below the button is a search bar and a table of existing users.

	User name	Groups	Access key age	Password age	Last activity
<input type="checkbox"/>	avanan	avanan	936 days	None	721 days
<input type="checkbox"/>	jenkins-aws	None	425 days	None	6 days
<input type="checkbox"/>	migrate-to-gcp	None	83 days	None	83 days
<input type="checkbox"/>	mlevchuk	None	None	679 days	679 days
<input type="checkbox"/>	S3READONLY	None	278 days	278 days	278 days
<input type="checkbox"/>	vs_gtb	None	347 days	None	Today
<input type="checkbox"/>	vstovpovoy	None	1186 days	None	491 days

3. Type **User name**, select **Programmatic access**, and click the **Next** button.

Add user



Set user details

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

User name*

[+ Add another user](#)

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.

- Select *Attach existing policies directly*. Search by 'S3' in Filter policies. Select AmazonS3FullAccess policy. Press the **Next** button.

Add user 1 2 3 4 5

▼ Set permissions

Add user to group

Copy permissions from existing user

Attach existing policies directly

Create policy ↻

Filter policies Showing 9 results

	Policy name	Type	Used as
<input type="checkbox"/>	▶ AmazonDMSRedshiftS3Role	AWS managed	None
<input checked="" type="checkbox"/>	▶ AmazonS3FullAccess	AWS managed	Permissions policy (5)
<input type="checkbox"/>	▶ AmazonS3OutpostsFullAccess	AWS managed	None
<input type="checkbox"/>	▶ AmazonS3OutpostsReadOnlyAccess	AWS managed	None
<input type="checkbox"/>	▶ AmazonS3ReadOnlyAccess	AWS managed	Permissions policy (1)
<input type="checkbox"/>	▶ QuickSightAccessForS3StorageManagementAnalyticsReadOnly	AWS managed	None
<input type="checkbox"/>	▶ s3crr_for_gtb-download-us-east_to_gtb-download-us-west	Customer managed	Permissions policy (1)
<input type="checkbox"/>	▶ s3crr_for_gttbdownloads.com_to_gttbdownloads.nodrdamerica.com	Customer managed	Permissions policy (1)

▶ Set permissions boundary

Cancel
Previous
Next: Tags

- Add tags (optional). Press **Next**.

Add user 1 2 3 4 5

Add tags (optional)

IAM tags are key-value pairs you can add to your user. Tags can include user information, such as an email address, or can be descriptive, such as a job title. You can use the tags to organize, track, or control access for this user. [Learn more](#)

Key	Value (optional)	Remove
<input type="text" value="Name"/>	<input type="text" value="GTB-S3-Scan"/>	✕
<input type="text" value="Add new key"/>	<input type="text"/>	

You can add 49 more tags.

6. Press **Create user**.

Add user

- 1
- 2
- 3
- 4
- 5

Review

Review your choices. After you create the user, you can view and download the autogenerated password and access key.

User details

User name	S3Scan
AWS access type	Programmatic access - with an access key
Permissions boundary	Permissions boundary is not set

Permissions summary

The following policies will be attached to the user shown above.

Type	Name
Managed policy	AmazonS3FullAccess

Tags

The new user will receive the following tag

Key	Value
Name	GTB-S3-Scan

Cancel
Previous
Create user

7. Copy or download **Access key ID** and **Secret access key**. Press **Close**.

Add user

- 1
- 2
- 3
- 4
- 5

✔ Success
 You successfully created the users shown below. You can view and download user security credentials. You can also email users instructions for signing in to the AWS Management Console. This is the last time these credentials will be available to download. However, you can create new credentials at any time.

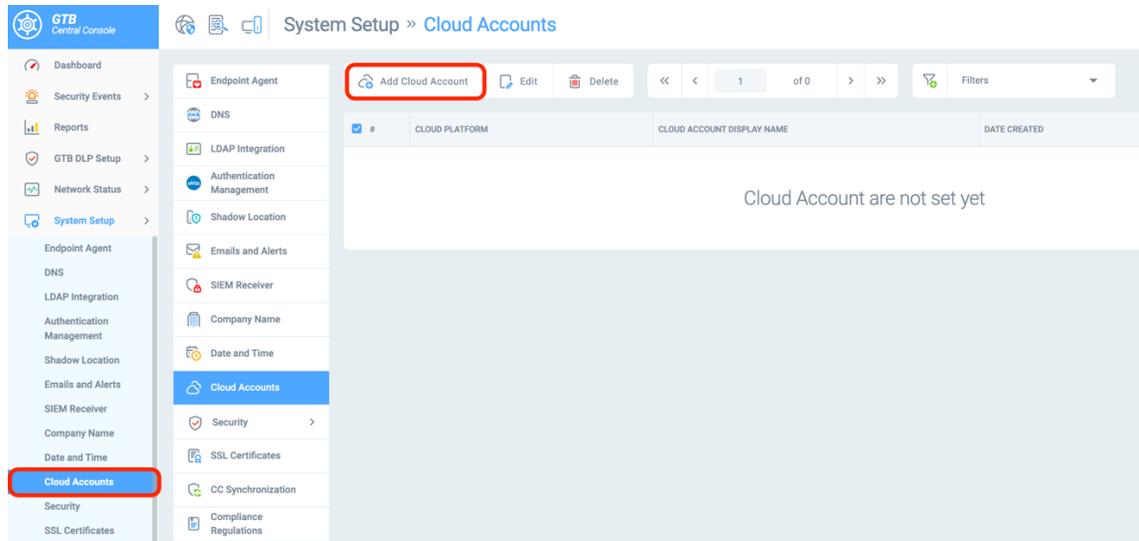
Users with AWS Management Console access can sign-in at: <https://354506356745.signin.aws.amazon.com/console>

Download .csv

	User	Access key ID	Secret access key
▶	✔ S3Scan	AKIAVFCRZXAEXUG6CD63	***** Show

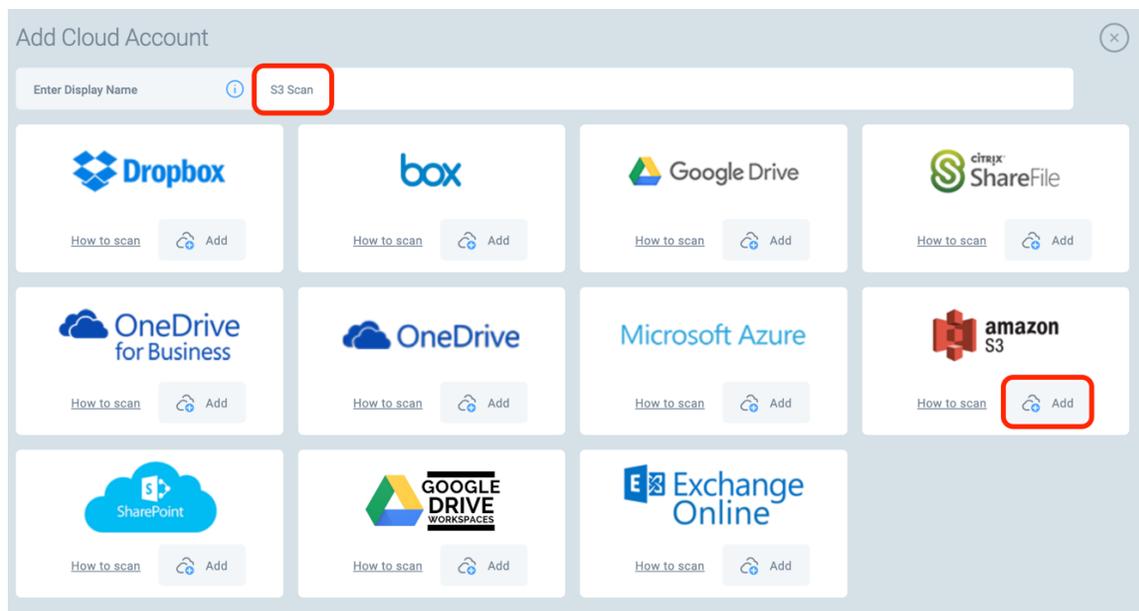
3 Add Amazon S3 Cloud Account Credential

1. Sign in to the Central Console.
2. Go to **System > Cloud Accounts** and press the **Add Cloud Account** button.

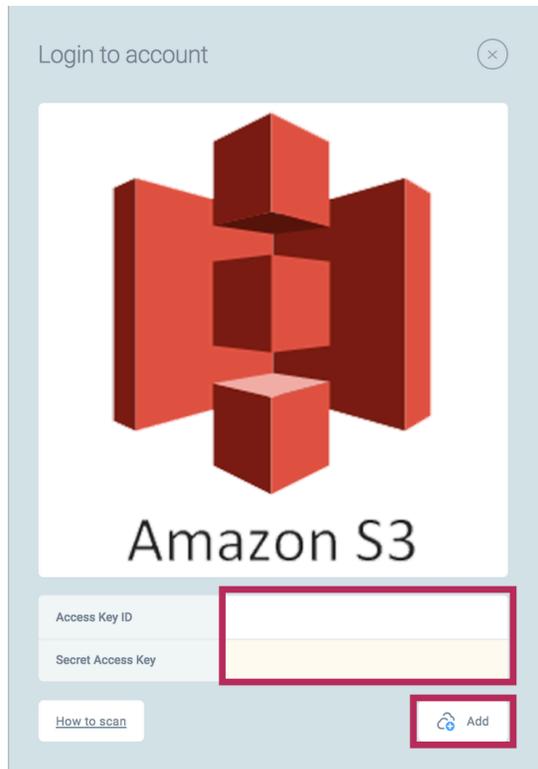


3. Type the **Name**, and select the **Amazon S3** card. Press the **Add** button.

The page should be redirected to the Cloud sign-in page.



4. Enter the **Access key ID** and **Secret Access key**, which you got before. Press **Add**.

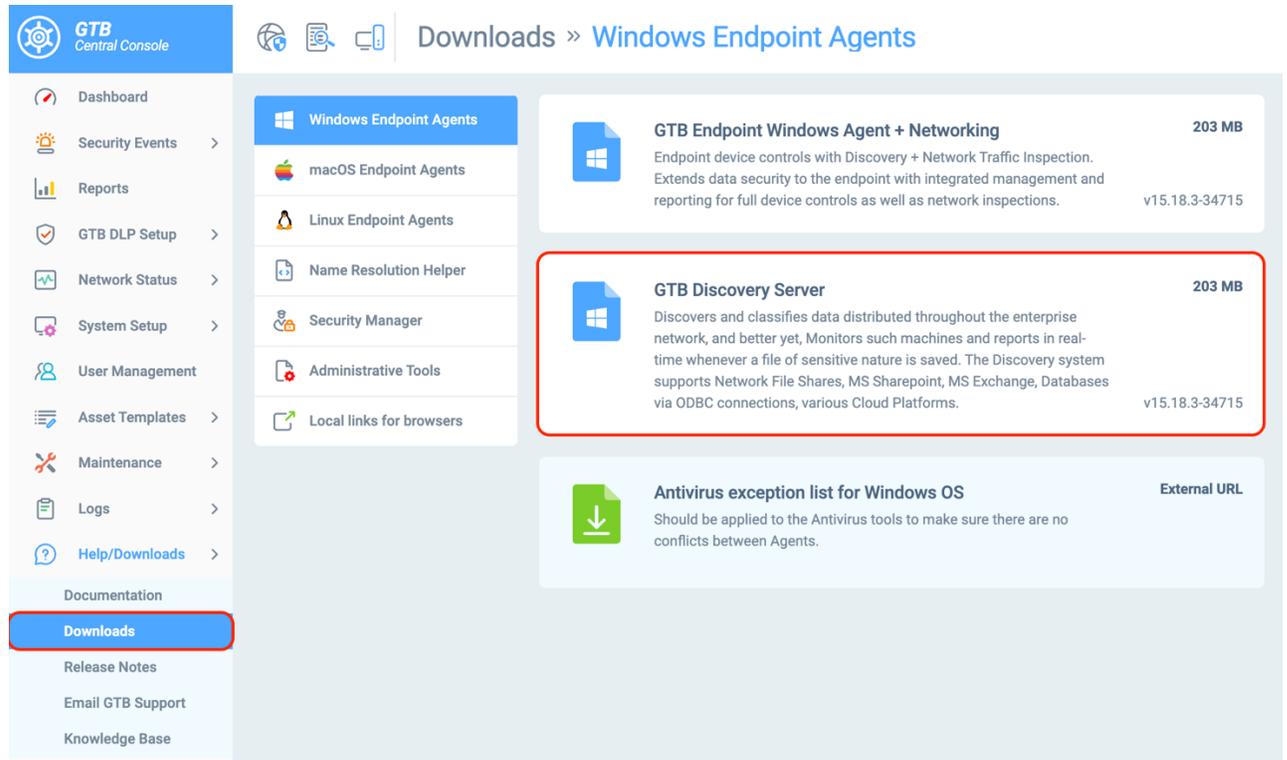


The screenshot shows a 'Login to account' dialog box with the Amazon S3 logo and the text 'Amazon S3'. Below the logo are two input fields: 'Access Key ID' and 'Secret Access Key'. A red box highlights both input fields. At the bottom right, there is an 'Add' button with a plus icon, also highlighted with a red box. A 'How to scan' link is visible at the bottom left.

5. The Central Console uses Amazon S3 API to store the authentication token and use it by Discovery Server.

4 Install Discovery Server

1. Sign in to the **Central Console** using an account with Administrator privileges.
2. Go to the **Help > Download** tab of the GTB Central Console and download the GTB Discovery Server MSI package.



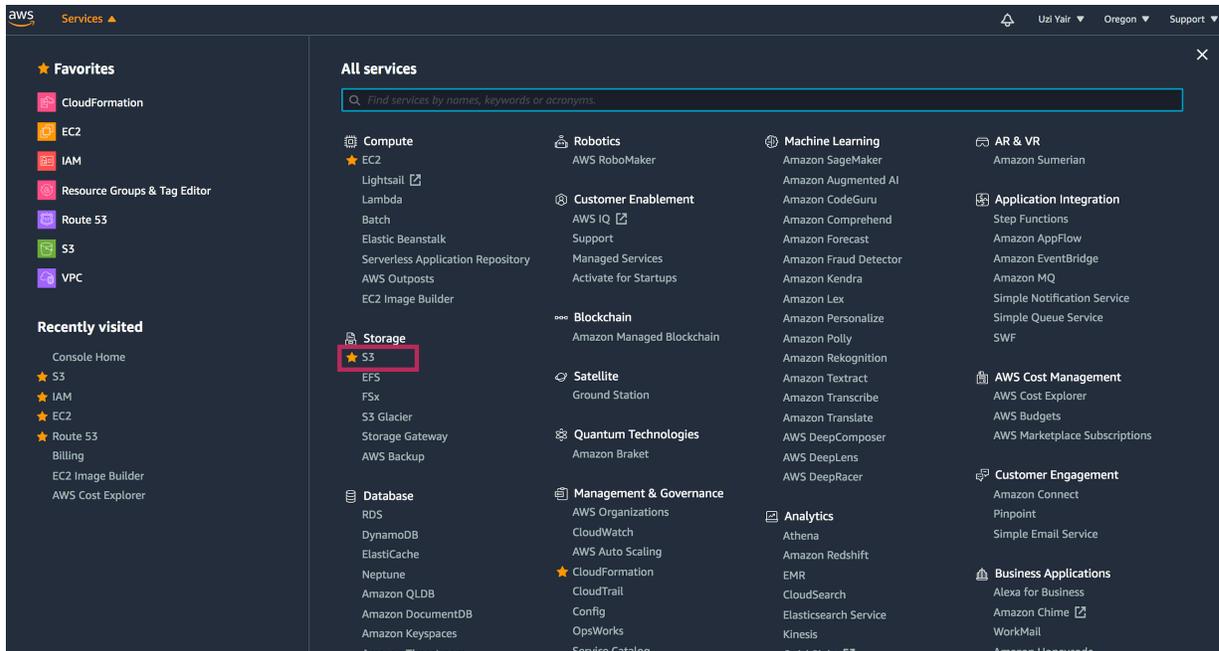
The screenshot shows the GTB Central Console interface. The left sidebar contains a navigation menu with the following items: Dashboard, Security Events, Reports, GTB DLP Setup, Network Status, System Setup, User Management, Asset Templates, Maintenance, Logs, Help/Downloads, Documentation, Downloads (highlighted with a red box), Release Notes, Email GTB Support, and Knowledge Base. The main content area is titled 'Downloads >> Windows Endpoint Agents'. It features a list of download options on the left and three detailed cards on the right. The 'GTB Discovery Server' card is highlighted with a red border. The cards are:

- Windows Endpoint Agents** (selected in the left list)
- macOS Endpoint Agents**
- Linux Endpoint Agents**
- Name Resolution Helper**
- Security Manager**
- Administrative Tools**
- Local links for browsers**
- GTB Endpoint Windows Agent + Networking** (203 MB, v15.18.3-34715)
- GTB Discovery Server** (203 MB, v15.18.3-34715) - highlighted with a red border
- Antivirus exception list for Windows OS** (External URL)

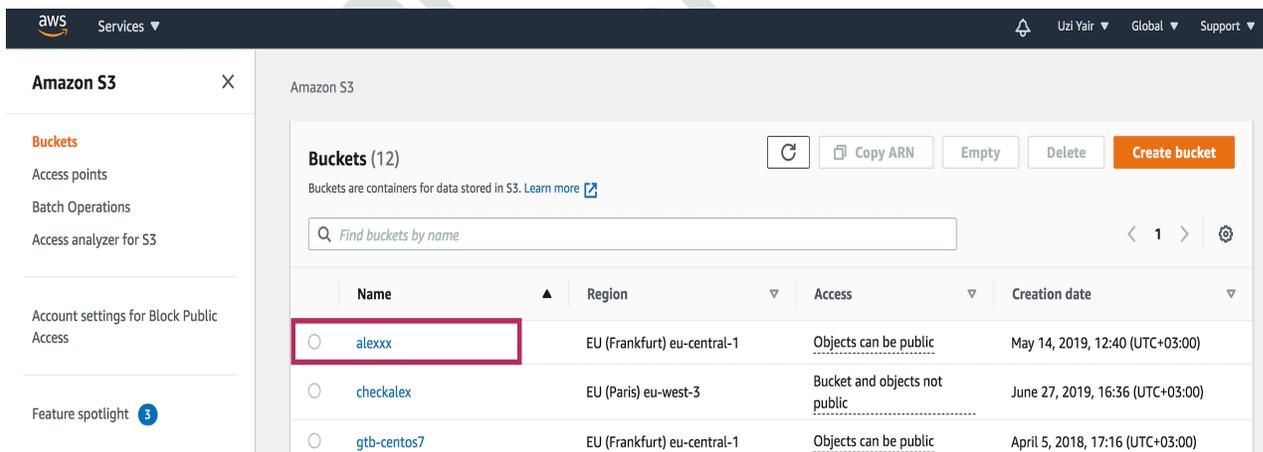
3. Install the **GTB Discovery Server** on any Windows PC where you want to scan from.
4. The Discovery Server scans 1 file per CPU core at a time. The more cores provided, the faster is scanning speed.

5 Start the Discovery scan

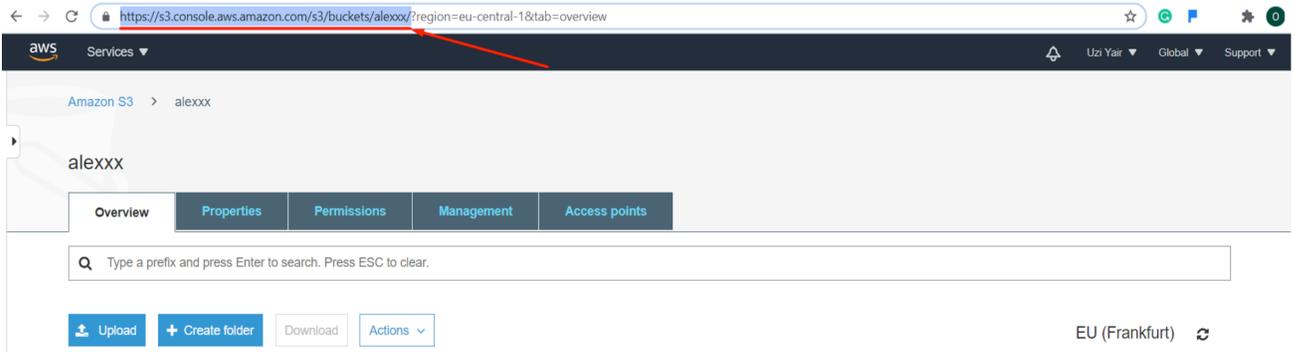
1. Go back to the Amazon page. In **Services** press on **S3**.



2. Choose the required **Bucket** that you want to scan and press on it.

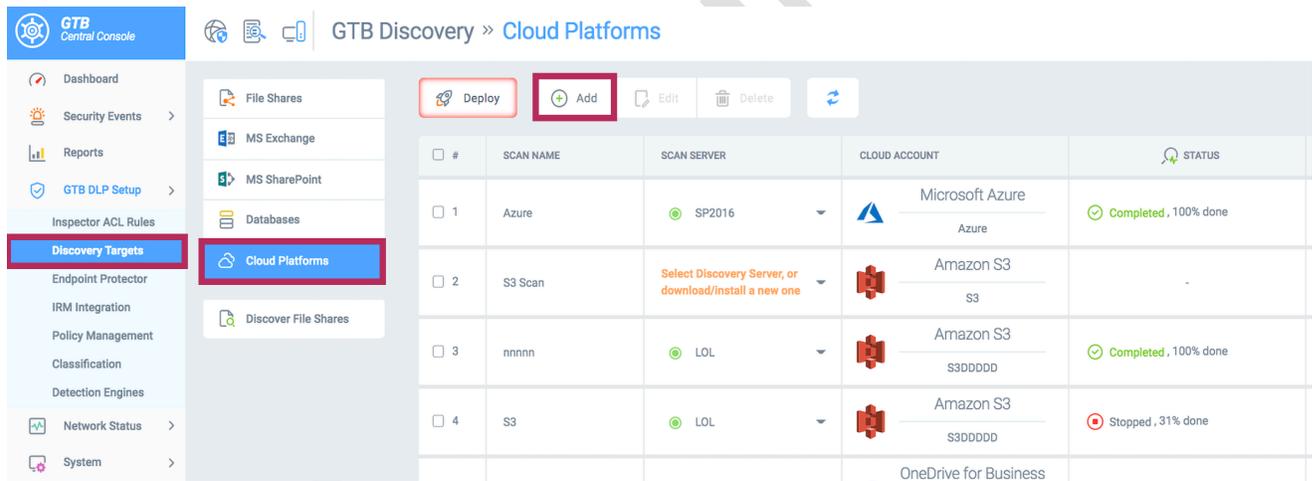


3. Copy The **URL** till ? symbol as shown in the pictures below.



4. On the Central Console go to **GTB DLP Setup > Discovery Targets > Cloud Platforms** page.

Press the **Add** button.



5. Enter the **Scan Name**, select **Scan Server**, select **Cloud Account**, and insert **URL** of scanned **Amazon S3**. Press the **Save** button.

Enter Scan Name

S3 Scan

Cloud Platforms Scan | Scan For / Filters / Remedial Actions | Schedule | Report | Advanced

Designated Scan Server: MAXVM2

Target Cloud Platforms

Cloud Account: Amazon S3 - S3

URL: https://s3.console.aws.amazon.com/s3/buckets/alex

Incremental Scan:

Scan Images: GTB OCR | External OCR Server URL

Save | Cancel

6. Start the scan by pressing the **Start** icon.

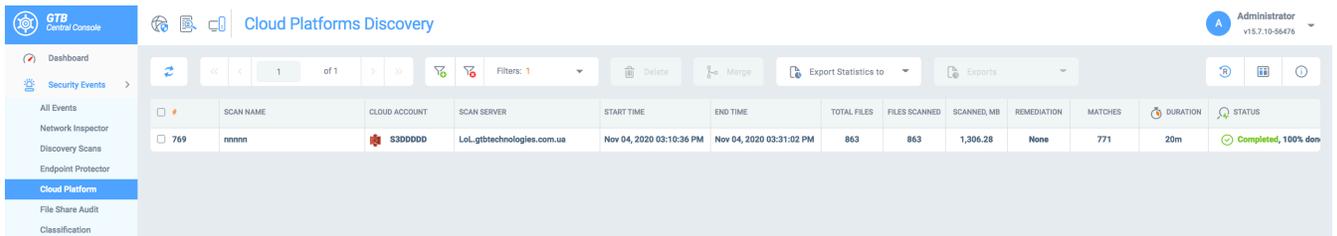
GTB Central Console | GTB Discovery » Cloud Platforms | Administrator v15.7.10-56476

Deploy | Add | Edit | Delete | Refresh

#	SCAN NAME	SCAN SERVER	CLOUD ACCOUNT	STATUS	DURATION	TOTAL FILES	SCANNED FILES	REMEDATIONS	MATCHES
1	S3 Scan	MAXVM2	Amazon S3 S3						

6 Check scan result

1. Sign in to the Central Console.
2. Go to the **Security Events > Cloud Platform** page and check the scan results.



The screenshot shows the GTB Central Console interface. The main content area displays a table of scan results under the 'Cloud Platform' section. The table has the following columns: SCAN NAME, CLOUD ACCOUNT, SCAN SERVER, START TIME, END TIME, TOTAL FILES, FILES SCANNED, SCANNED MB, REMEDIATION, MATCHES, DURATION, and STATUS. A single scan is listed with ID 769, name 'nmmn', cloud account 'S300000', scan server 'LoL.gtbertechnologies.com.ua', start time 'Nov 04, 2020 03:10:36 PM', end time 'Nov 04, 2020 03:31:02 PM', 863 total files, 863 files scanned, 1,306.28 MB scanned, no remediation, 771 matches, a duration of 20m, and a status of 'Completed, 100% done'.

SCAN NAME	CLOUD ACCOUNT	SCAN SERVER	START TIME	END TIME	TOTAL FILES	FILES SCANNED	SCANNED MB	REMIEDIATION	MATCHES	DURATION	STATUS	
769	nmmn	S300000	LoL.gtbertechnologies.com.ua	Nov 04, 2020 03:10:36 PM	Nov 04, 2020 03:31:02 PM	863	863	1,306.28	None	771	20m	Completed, 100% done

3. Each line represents a separate Discovery scan. Double click to see the details.

If you have any questions, please, email support@gttb.com and any of our engineers would be happy to help you.