### **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* 



### Contents

1	1 Introduction	
	<ul><li>1.1 Definitions</li><li>1.2 Requirements</li></ul>	
2	Add OneDrive Service Account	4
3	Install Discovery Server	2
4	Start the Discovery scan	3
5	6 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 cares 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.

aws Services ▼				
Identity and Access Management (IAM)	Add user Delete user			
Dashboard	Q Find users by username or access key			
<ul> <li>Access management</li> </ul>	User name 🗸 Groups	Access key age	Password age	Last activity
Groups	avanan avanan	<b>()</b> 936 days	None	721 days
Users	jenkins-aws None	<b>()</b> 425 days	None	6 days
Roles	migrate-to-gcp None	📀 83 days	None	83 days
Policies	mlevchuk None	None	679 days	679 days
Account settings	S3READONLY None	🛕 278 days	278 days	278 days
<ul> <li>Access reports</li> </ul>	vs_gtb None	🛕 347 days	None	Today
Access analyzer	vstovpovoy None	1186 days	None	491 days
Archive rules				

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	e same access type and permissions. Learn more
User name*	3Scan
Select AWS access type	
Select how these users will access AWS. A	ccess keys and autogenerated passwords are provided in the last step. Learn more
Access type* 🥑	<b>Programmatic access</b> Enables an <b>access key ID</b> and <b>secret access key</b> 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.



4. 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	
<ul> <li>✓ Set permissions</li> </ul>			
Add user to group	ach existing policies ectly	]	
Create policy		3	
Filter policies v Q S3		Showing 9 results	
Policy name 👻	Туре	Used as	
AmazonDMSRedshiftS3Role	AWS managed	None	_
AmazonS3FullAccess	AWS managed	Permissions policy (5)	
AmazonS3OutpostsFullAccess	AWS managed	None	-
AmazonS3OutpostsReadOnlyAccess	AWS managed	None	
AmazonS3ReadOnlyAccess	AWS managed	Permissions policy (1)	
	AWS managed	None	
s3crr_for_gtb-download-us-east_to_gtb-download-us-west	Customer managed	Permissions policy (1)	
s3crr_for_gttbdownloads.com_to_gttbdownloads.nodrdamerica.com	Customer managed	Permissions policy (1)	
<ul> <li>Set permissions boundary</li> </ul>			
	Ca	ncel Previous Next: Tags	
5. Add tags (optional). Press <b>Next</b> .			
Add user		1 2	3 4
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

Кеу	Value (optional)	Remove
Name	GTB-S3-Scan	×
Add new key		

You can add 49 more tags.



5)

#### 6. Press Create user.

Add user		1 2 3 4 5		
Review				
Review your choices. Afte	r you create th	e user, you can view and download the autogenerated password and access key.		
User details				
1	User name	S3Scan		
AWS a	ccess type	Programmatic access - with an access key		
Permissions	s boundary	Permissions boundary is not set		
Permissions summa	iry			
The following policies will	be attached to	the user shown above.		
Туре	Name			
Managed policy	AmazonS3Full	Access		
Tags				
The new user will receive the following tag				
Кеу		Value		
Name		GTB-S3-Scan		

7. Copy or down	load Access key ID and Secret	access key. Press Close.
Add user		
Success You successfully instructions for s you can create n	created the users shown below. You can view and igning in to the AWS Management Console. This is ew credentials at any time.	d download user security credentials. You can also email users s the last time these credentials will be available to download. However,

		User	Access key ID	Secret access key
►	٢	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.

Central Console	m Setup » Cloud Accounts		
Dashboard     Endpoint Agent	Add Cloud Account	< <ul> <li>of 0</li> <li>&gt;</li> <li>&gt;</li> <li>?:</li> </ul>	7 Filters
Reports	# CLOUD PLATFORM	CLOUD ACCOUNT DISPLAY NAME	DATE CREATED
GTB DLP Setup >			
Network Status >		Cloud Account are not	set yet
System Setup > 0 Shadow Location			
DNS			
LDAP Integration			
Management Shadow Location			
Emails and Alerts			
Company Name			
Date and Time			
Security Compliance			
SSL Certificates			

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.

Add Cloud Account			(
Enter Display Name (i) S3 S	ican		
How to scan	How to scan	How to scan	How to scan
How to scan	How to scan	Microsoft Azure	How to scan
SharePoint How to scan	How to scan	How to scan	



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



5. The Central Console uses Amazon S3 API to store the authentification 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.

	<b>GTB</b> Central Console		6		ids » Win	dows Endpoint Agents	
$\bigcirc$	Dashboard			lindowo Endaciat Agonto			
ë	Security Events	>		Andows Endpoint Agents		GTB Endpoint Windows Agent + Networking	203 MB
.1	Reports		📫 ma	nacOS Endpoint Agents		Extends data security to the endpoint with integrated management and reporting for full device controls as well as network inspections.	v15.18.3-34715
$\overline{\mathbf{v}}$	GTB DLP Setup	>	👌 Lir	inux Endpoint Agents			
	Network Status	>	🔂 Na	lame Resolution Helper		GTR Discovery Server	203 MB
Ģ	System Setup	>	ලී Se	ecurity Manager		Discovers and classifies data distributed throughout the enterprise network, and better yet, Monitors such machines and reports in real-	
8	User Management		🔓 Ad	dministrative Tools		time whenever a file of sensitive nature is saved. The Discovery system supports Network File Shares, MS Sharepoint, MS Exchange, Databases	
=	Asset Templates	>	C Lo	ocal links for browsers		via ODBC connections, various Cloud Platforms.	v15.18.3-34715
Х	Maintenance	>					
Ē	Logs	>			Antivirus exception list for Windows OS Should be applied to the Antivirus tools to make sure there are no	External URL	
?	Help/Downloads	>				conflicts between Agents.	
	Documentation						
	Downloads						
	Release Notes						
	Email GTB Support						
	Knowledge Base						

- 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.

aws Services 🔺				🗘 Uzi Yair 🔻 Oregon 🔻 Support 🖲						
★ Favorites	All services			×						
CloudFormation	Q Find services by names, keywords o	Q. Find services by names, keywords or acronyms.								
<u></u> EC2	🗇 Compute	ක Robotics	Machine Learning	🛱 AR & VR						
IAM	★ EC2	AWS RoboMaker	Amazon SageMaker	Amazon Sumerian						
Resource Groups & Tag Editor	Lightsail 🔀	*** • • · ·	Amazon Augmented Al							
	Lambda	B Customer Enablement	Amazon CodeGuru	By Application Integration						
Route 53	Batch	AWS IQ 2	Amazon Comprehend	Step Functions						
🛐 S3	Elastic Beanstalk	Support	Amazon Forecast	Amazon AppFlow						
	Serverless Application Repository	Managed Services	Amazon Fraud Detector	Amazon EventBridge						
	AWS Outposts	Activate for Startups	Amazon Kendra	Amazon MQ						
	EC2 Image Builder		Amazon Lex	Simple Notification Service						
Recently visited		Blockchain	Amazon Personalize	Simple Queue Service						
	🔒 Storage	Amazon Managed Blockchain	Amazon Polly	SWF						
Console Home	★ S3		Amazon Rekognition							
★ S3	EFS		Amazon Textract	AWS Cost Management						
🚖 IAM	FSx	Ground Station	Amazon Transcribe	AWS Cost Explorer						
★ EC2	S3 Glacier		Amazon Translate	AWS Budgets						
🚖 Route 53	Storage Gateway	Se Quantum Technologies	AWS DeepComposer	AWS Marketplace Subscriptions						
Billing	AWS Backup	Amazon Braket	AWS DeepLens							
EC2 Image Builder			AWS DeepRacer	୍ବଟି Customer Engagement						
AWS Cost Explorer	Database	Management & Governance		Amazon Connect						
	RDS	AWS Organizations	Analytics	Pinpoint						
	DynamoDB	CloudWatch	Athena	Simple Email Service						
	ElastiCache	AWS Auto Scaling	Amazon Redshift							
	Neptune	🔶 CloudFormation	EMR	Business Applications						
	Amazon QLDB	CloudTrail	CloudSearch	Alexa for Business						
	Amazon DocumentDB	Config	Elasticsearch Service	Amazon Chime 🖸						
	Amazon Keyspaces	OpsWorks	Kinesis	WorkMail						
	Amazon Timestream	Service Catalog	OuickSight 72	Amazon Honevcode						

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

aws Services ▼				🗘 Uzi Yair 🔻 Global 🔻 Support 🔻
Amazon S3 ×	Amazon S3			
Buckets Access points Batch Operations Access analyzer for S3	Buckets (12) Buckets are containers for data stored in St Q. Find buckets by name	5. Learn more [2]	C Copy ARN Empty	Delete Create bucket
Account settings for Block Public	Name	▲ Region ▽	Access $\triangledown$	Creation date v
Access	O alexxx	EU (Frankfurt) eu-central-1	Objects can be public	May 14, 2019, 12:40 (UTC+03:00)
Feature spotlight 3	Checkalex	EU (Paris) eu-west-3	Bucket and objects not public	June 27, 2019, 16:36 (UTC+03:00)
	O gtb-centos7	EU (Frankfurt) eu-central-1	Objects can be public	April 5, 2018, 17:16 (UTC+03:00)



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

$\leftarrow \   \rightarrow $	C https://s3	.console.aws.amazon.e	com/s3/buckets/alexxx/	?region=eu-central-1&t	ab=overview						z	7) <b>G</b>	۰.	* 0
aws	Services 🔻									¢	Uzi Yair	<b>7</b> Glo	obal 🔻	Support 🔻
	Amazon S3 >	alexxx												
5														
	alexxx													
	Overview	Properties	Permissions	Management	Access points									
	Q Type a prefit	x and press Enter to s	search. Press ESC to cl	ear.										
	🔔 Upload -	Create folder	Download Actions	~							EU (Fra	nkfurt)	2	

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

Press the												
GTB Central Console												
<ul> <li>⊘ Dashboard</li> <li>☆ Security Events &gt;</li> </ul>	File Shares	🧐 Dep	loy (+) Add	Glit 🗎 Delete								
Reports	MS Exchange	<b>#</b>	SCAN NAME	SCAN SERVER	CLOUD A	CCOUNT	📿 status					
GTB DLP Setup >	S> MS SharePoint				4	Microsoft Azure						
Inspector ACL Rules	Databases	U 1	Azure	SP2016	4	Azure	Completed , 100% done					
Discovery Targets	Cloud Platforms			Select Discovery Server, or		Amazon S3						
IRM Integration		U 2	S3 Scan	download/install a new one	ų,	S3						
Policy Management	Discover File Shares				<b>s</b> he	Amazon S3						
Classification		3	nnnn	• LOL •	ų	S3DDDDD	Completed, 100% done					
Detection Engines						Amazon S3						
Network Status >		4	S3 ( LOL -		R.	S3DDDDD	Stopped , 31% done					
Co System >						OneDrive for Business						



 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		×
C Cloud Platforms Scan	Scan For / Filters / Remedial Actions	Go Advanced	
Designated Scan Server	MAXVM2	~	
Target Cloud Platfor	rms		
Cloud Account	🏟 Amazon S3 - S3	- 6	ò
URL	i https://s3.console.aws.amazon.com/s3/buckets/alexxx	کم	5
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 D	iscovery » Cloud Platforr	ns					4	Administr v15.7.10-5	rator 56476
Dashboard     Security Events >	File Shares	😵 Deploy (+) Add (		Schedule						
Reports	■ MS Exchange	# SCAN NAME	SCAN SERVER	CLOUD ACCOUNT	💭 STATUS	TOTAL FILES	SCANNED FILES	REMEDIATIONS	MATCHES	
GTB DLP Setup >	MS SharePoint			Amazon S3						
Inspector ACL Rules	Databases	🔲 1 S3 Scan	MAXVM2 ~	<b>S3</b>						øv
Endpoint Protector	Cloud Platforms									
IRM Integration Policy Management	Discover File Shares									



### 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.

Č	GTB Central Console	r 🗟	Cloud Platforms	Discovery									(	Administrate	ər 76 —
( 1	Dashboard     Security Events >	<b>2</b> «	< 1 of 1	>	₩ Filters: 1 ▼	Delete	🏷 Merge 🕻 E	ort Statistics t	•	C Exports	v			8	•
	All Events	•	SCAN NAME	CLOUD ACCOUNT	SCAN SERVER	START TIME	END TIME	TOTAL FILES	FILES SCANNED	SCANNED, MB	REMEDIATION	MATCHES		Q STATUS	
	Discovery Scans	769	nnnn	S3DDDDD	LoL.gtbtechnologies.com.ua	Nov 04, 2020 03:10:36 PM	Nov 04, 2020 03:31:02 PM	863	863	1,306.28	None	771	20m	<ul> <li>Completed, 1</li> </ul>	00% don
	Endpoint Protector														
	Cloud Platform														
	File Share Audit														
	Classification														

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.

