

US CONNECT 2022 IN ATLANTA



Where in the cloud is my data coming ? Presentation on how to extract cloud providers audit trails so one can maintain data custody

- Pritesh Desai

Principal Strategic Advisor at SAS HLS

May 02 2022



- Ben Bocchicchio

Sr. Manager, US Professional Services

May 02 2022



Agenda

- Introduction to Authentication and Authorization in Clinical Data Repository (CDR)
- Audit trail in CDR.
- Create a local drive mounts of CDR and Cloud for Data Exchange.
- Bring the logs in CDR.
- Confirm audit records in CDR.
- Create traceability check and visualize.

Authentication and Authorization in Clinical Data Repository

- Authentication
 - Internal
 - Authentication mechanism controlled by application
 - Active Directory
 - Authentication passed o AD
 - Single Sign-on
 - SAML

SYSTEM ACCESS

Last login: Aug 19, 2021, 9:08 AM GMT-04:00

Authentication type:

Single sign-on identifier: *

Internal

Single Sign-on

VSP AD Account

SYSTEM ACCESS

Last login: Aug 19, 2021, 9:24 AM GMT-04:00

Authentication type:

Single sign-on identifier: *

Authentication and Authorization in Clinical Data Repository

- Authorization

- Groups – Collection of principals
- Roles – Privileges controls what actions user can perform in application

- Permissions – controls what objects user can access in application

- Current
- Default

Name	Type
Admin	☐
CRO	☐
CustomerPreview	☐
Users	☐

Type	Member
☐	
☐	

Name	Privilege
Admin	☐
CustomerPreview	☐
Users	☐

Privilege	Privilege
☐	Administer Process Flows
☐	Create Process Flows
☐	Enable Versioning

Privilege	Privilege
☐	Administer Process Flows
☐	Create Process Flows
☐	Enable Versioning

Audit trail in CDR

- Audit Trail – Tracks all editable actions

Text to filter123 Items

QUERY PARAMETERS

Object:
(any object)

Name:

Location:

Action:
(any action - excluding downloaded)

Acted on by:
sajune2 (Sandeep Juneja SAML)

Mode:
(any mode)

From:
Jul 19, 2021, 12:00:00 AM

To:
Aug 19, 2021, 11:59:59 PM

FindReset

Object	Name	Location	Action	Acted On By (Display Na...	M...	Date Acted On
User	sajune2		Log on	sajune2 (Sandeep Juneja ...		Aug 19, 2021, 8:40:47 AM ...
User	sajune2		Log on	sajune2 (Sandeep Juneja ...		Aug 19, 2021, 8:40:46 AM ...
User	sajune2		Log on	sajune2 (Sandeep Juneja ...		Aug 19, 2021, 8:40:46 AM ...
User	sajune2		Timed out	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 7:07:05 PM ...
User	sajune2		Timed out	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:39:04 PM ...
File	readme.txt	/Users/sajune2	Owner changed	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:20:00 PM ...
File	readme.txt	/Users/sajune2	Permissions created	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:20:00 PM ...
File	readme.txt	/Users/sajune2	Created	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:20:00 PM ...
User Folder	sajune2	/Users	File added	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:20:00 PM ...
File	readme.txt	/Users/sajune2	Associated	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:20:00 PM ...
File	test_file.txt	/Users/sajune2	Deleted	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:08:15 PM ...
User Folder	sajune2	/Users	File removed	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:08:15 PM ...
File	test_file.txt	/Users/sajune2	Disassociated	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:08:15 PM ...
File	readme.txt	/Users/sajune2	Deleted	sajune2 (Sandeep Juneja ...		Aug 17, 2021, 6:08:15 PM ...

Attribute

File

From

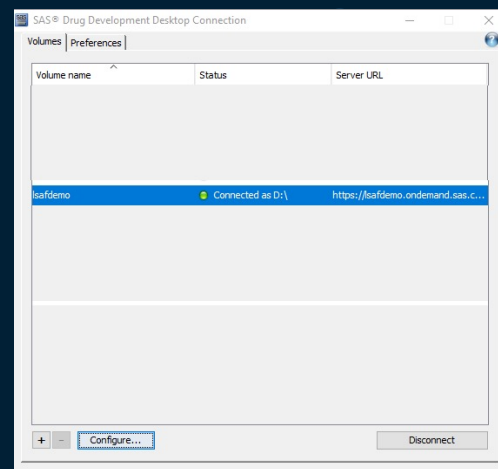
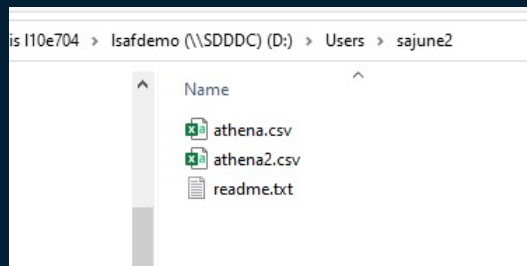
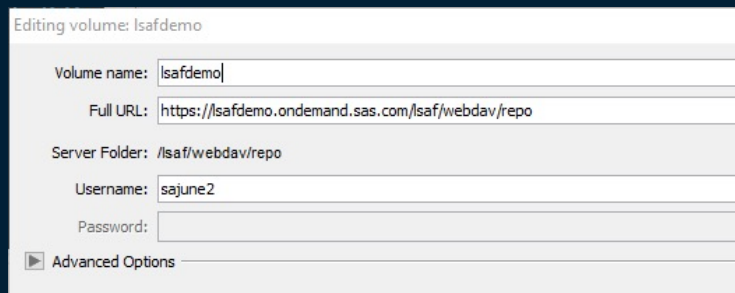
To

readme.txt

Create a local drive mounts of CDR and Cloud for Data Exchange

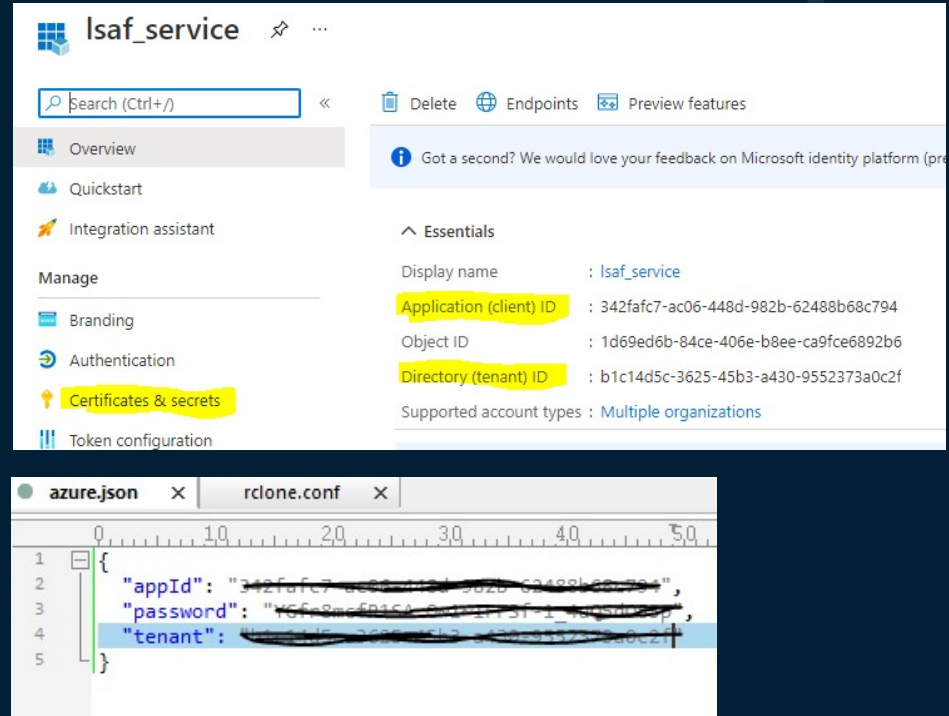
Mounting CDR as local drive

- Using SAS Drive Map tool.
- Configure URL and credentials



Azure – Mount Storage account as local drive

- An **Azure service principal** is an identity created for use with applications, hosted services, and automated tools to access Azure resources.
 - Access is restricted by the roles assigned to the service principal
 - For security reasons, it's always recommended to use service principals with automated tools rather than allowing them to log in with a user identity.



Reference: <https://docs.microsoft.com/en-us/azure/storage/blobs/authorize-data-operations-portal>

Create a local drive mounts of CDR and Cloud for Data Exchange

Azure – Mount Storage account as local drive

- Setup using RClone - command line program to manage files on cloud storage (<https://rclone.org/>)
- Follow the instructions - <https://rclone.org/azureblob/>
- Configuration file for Rclone is located - C:\Users\\AppData\Roaming\rclone

```
[azure]
type = azureblob
account = lsafadls2
service_principal_file = C:\Users\sajune\AppData\Roaming\rcclone\azure.json
y) Yes this is OK (default)
e) Edit this remote
d) Delete this remote
```

```
PS C:\Users\sajune\Downloads\rclone> .\rclone.exe ls azure:
-1 2021-08-11 09:43:29 -1 $root
-1 2021-01-22 08:15:04 -1 empty1
-1 2021-08-02 16:54:35 -1 sas-test
-1 2021-07-13 13:19:20 -1 temp-file-location
-1 2021-02-28 20:05:08 -1 test3

PS C:\Users\sajune\Downloads\rclone> .\rclone.exe mount azure: b:
The service rclone has been started.
```

[illegible]

↑ << azure (B:) > temp-file-location > ADSL_test

^	Name
	test_file.txt

Create a local drive mounts of CDR and Cloud for Data Exchange

Mount Azure storage as drive

Microsoft Azure

portal.azure.com/#@SASOffice365.onmicrosoft.com/resource/subscriptions/f330b122-1ec5-43a7-bd07-08f96c51df54/resourceGroups/LSAF_storage/providers/Microsoft.Storage/storageAccounts/Isafadls2/containersList

Microsoft Azure

Search resources, services, and docs (G+)

Home > LSAF_storage > Isafadls2

Isafadls2 | Containers

Storage account

Search (Ctrl+F)

Overview

Activity log

Tags

Diagnose and solve problems

Access Control (IAM)

Data migration

Events

Storage Explorer (preview)

Data storage

Containers

File shares

Queues

Tables

Security + networking

Networking

Access keys

Shared access signature

Encryption

Security

Data management

Geo-replication

Data protection

Windows PowerShell

PS C:\Users\sajune\Downloads\rclone-v1.56.0-windows-amd64\rclone-v1.56.0-windows-amd64> cls

Level

Lease state

Available	***
Available	***
Available	***
Available	***
Available	***
Available	***

Mount Azure Storage as drive

6:17 PM
Today
8/11/2021

sas

Create a local drive mounts of CDR and Cloud for Data Exchange

Azure Audit Trail

- Audit Records

New Query 1* x + Feedback Queries Query explorer Format query

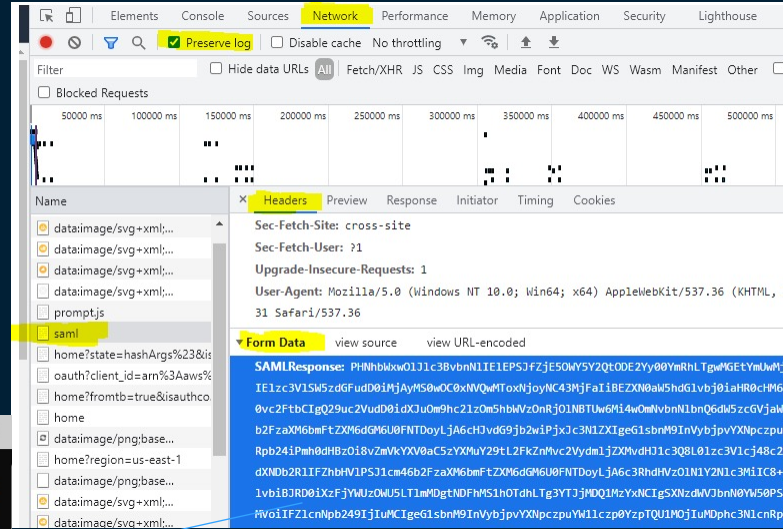
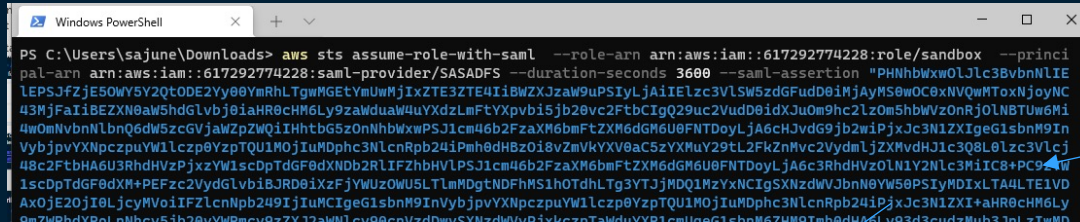
Isafadls2 Select scope Run Time range : Set in query Save Share New alert rule Export Pin to dashboard

```
1 StorageBlobLogs
2 where TimeGenerated > ago(6h)
3
```

	Uri	Uri
Completed	https://lsafadls2.blob.core.windows.net:443/temp-file-location/readme.txt	https://lsafadls2.blob.core.windows.net:443/temp-file-location/readme.txt?timeout=31536001
CallerIpAddress	149.173.8.108:18554	149.173.8.108:44567
CorrelationId	072898b3-e01e-008a-57b4-93bb4f000000	592fc727-801e-008c-0eb6-9388f0000000
SchemaVersion	1.0	1.0
OperationVersion	2020-08-04	2019-12-12
AuthenticationHash	DB27F71C18B5945C48E8BE7B1CD2CC668986E77013F47B206F349911E75F45DE	2921E5177CBC9A395EECE063879F4E892183AF0741083918ACE036C8B7917679
RequesterObjectId	7f884736-46f6-46da-b8db-c2078bd7e3b8	1854a4d8-cc19-41ec-9844-2e6f133c245c
RequesterTenantId	b1c14d5c-3625-45b3-a430-9552373a0c2f	b1c14d5c-3625-45b3-a430-9552373a0c2f
RequesterAppId	691458b9-1327-4635-9f55-ed83a7f1b41c	342fafc7-ac06-448d-982b-62488b68c794
RequesterAudience	https://storage.azure.com/	https://storage.azure.com/
RequesterTokenIssuer	https://sts.windows.net/b1c14d5c-3625-45b3-a430-9552373a0c2f/	https://sts.windows.net/b1c14d5c-3625-45b3-a430-9552373a0c2f/
RequesterUpn	Sandeep.Juneja@SAS.com	
UserAgentHeader	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like	rclone/v1.56.0
ReferrerHeader	https://portal.azure.com/	
ClientRequestId	9a06d0ab-ef90-4286-8a09-3f1a5a8110c2	

AWS – Mount S3 as local drive

- Reference you tube video – <https://www.youtube.com/watch?v=ACWRmFjG9V8>



```

"Credentials": {
  "AccessKeyId": "ASIAV7OMEHNKGDUCJPE",
  "SecretAccessKey": "XgDgEK22+AdkA14ZYqallEiZ0f76wrUiv2Cay1",
  "SessionToken": "IQ0b3p32l1uZQVjEiACxvzLWvh3QtMSJIMEYEQ1m1WBRgXb+H1os1uPGB2v125+d",
  "Expiration": "2021-08-15T02:18:00+00:00"
},
"AssumedRoleUser": {
  "AssumedRoleId": "AROAV7OMEHNKXPZDROA3:Sandeep.Juneja@SAS.com",
  "Arn": "arn:aws:sts::146969497425:assumed-role/sandbox/Sandeep.Juneja@SAS.com"
},

```

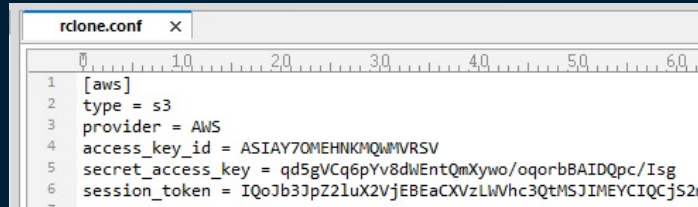
Create a local drive mounts of CDR and Cloud for Data Exchange

AWS – Mount S3 as local drive

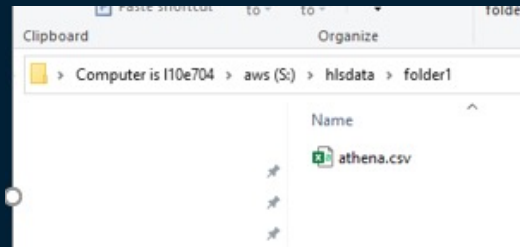
- Setup using RClone - command line program to manage files on cloud storage (<https://rclone.org/>)
- Follow the instructions - <https://rclone.org/s3/>
- Configuration file for Rclone is located - C:\Users\<userid>\AppData\Roaming\rclone

```
-----  
[aws]  
type = s3  
provider = AWS  
access_key_id = ASIAY70MEHNKMQMMVRSV  
secret_access_key = qd5gVCq6pYv8dWEntQmXywo  
session_token = IQoJb3JpZ2luX2VjEBEaCXVzLWV/  
dWByK+j8/kRBE4DIn+AXLZC20MJ8kuYCCDoAhoMnJE  
WmWQn5zd5G85LdNAiXIU40/xXpkB8xCnr9HvRwjqT+D  
KvFcVBIzznK0Kf5ZYv7Cg2ufezQDEg58jK0nQ/raLjZi  
2Eeov0Yo6aJg7dd0VsqUIdZyf/rYazsXMKT3jfnK3s3/  
WZ5ERSheaGt30SW88xrWk8Mj7ZRDkjDZz+GIBjqIAX8  
wWl+RbeEEc9zkEqQ1if3HnmsqejMLFDvEg48/mj5L5G  
+UmcBHas8BHFwhlqcg==  
-----  
y) Yes this is OK (default)  
e) Edit this remote  
d) Delete this remote  
y/e/d> |
```

```
.\rclone.exe mount aws: s:|
```

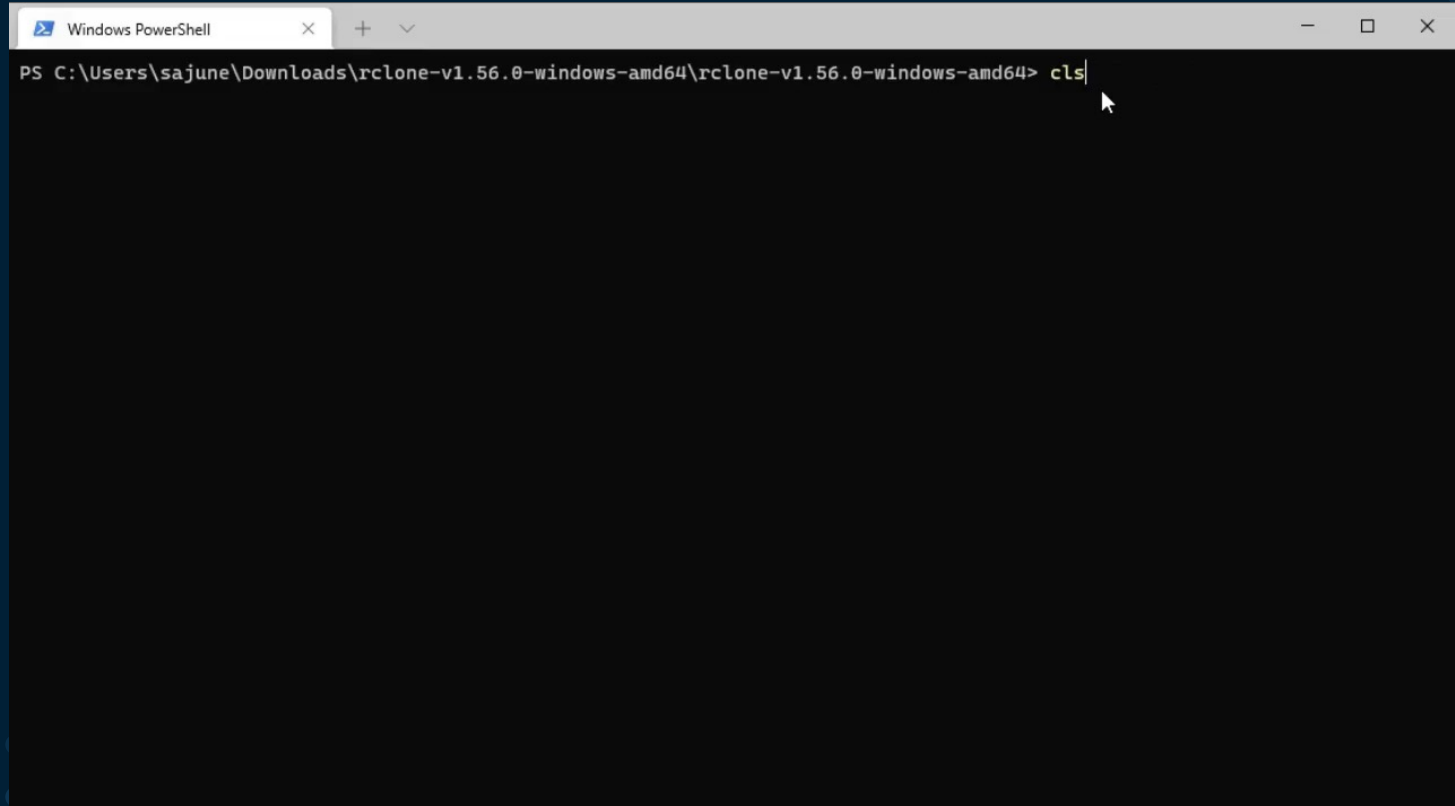


```
rclone.conf x  
1 [aws]  
2 type = s3  
3 provider = AWS  
4 access_key_id = ASIAY70MEHNKMQMMVRSV  
5 secret_access_key = qd5gVCq6pYv8dWEntQmXywo/oqorbBAIDQpc/Isq  
6 session_token = IQoJb3JpZ2luX2VjEBEaCXVzLWVhc3QtMSJIMEYCIQCjS2m
```



Create a local drive mounts of CDR and Cloud for Data Exchange

AWS – Mount S3 as local drive



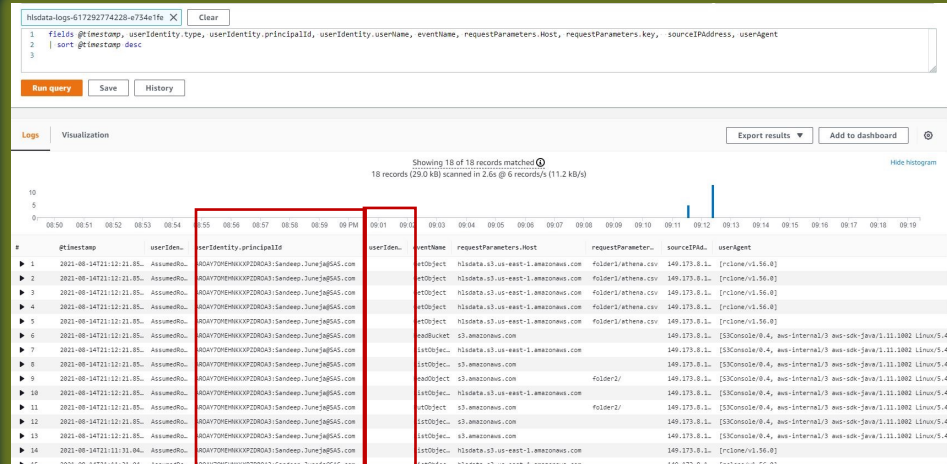
```
Windows PowerShell
PS C:\Users\sajune\Downloads\rclone-v1.56.0-windows-amd64\rclone-v1.56.0-windows-amd64> cls
```

Create a local drive mounts of CDR and Cloud for Data Exchange.

AWS Audit Trail

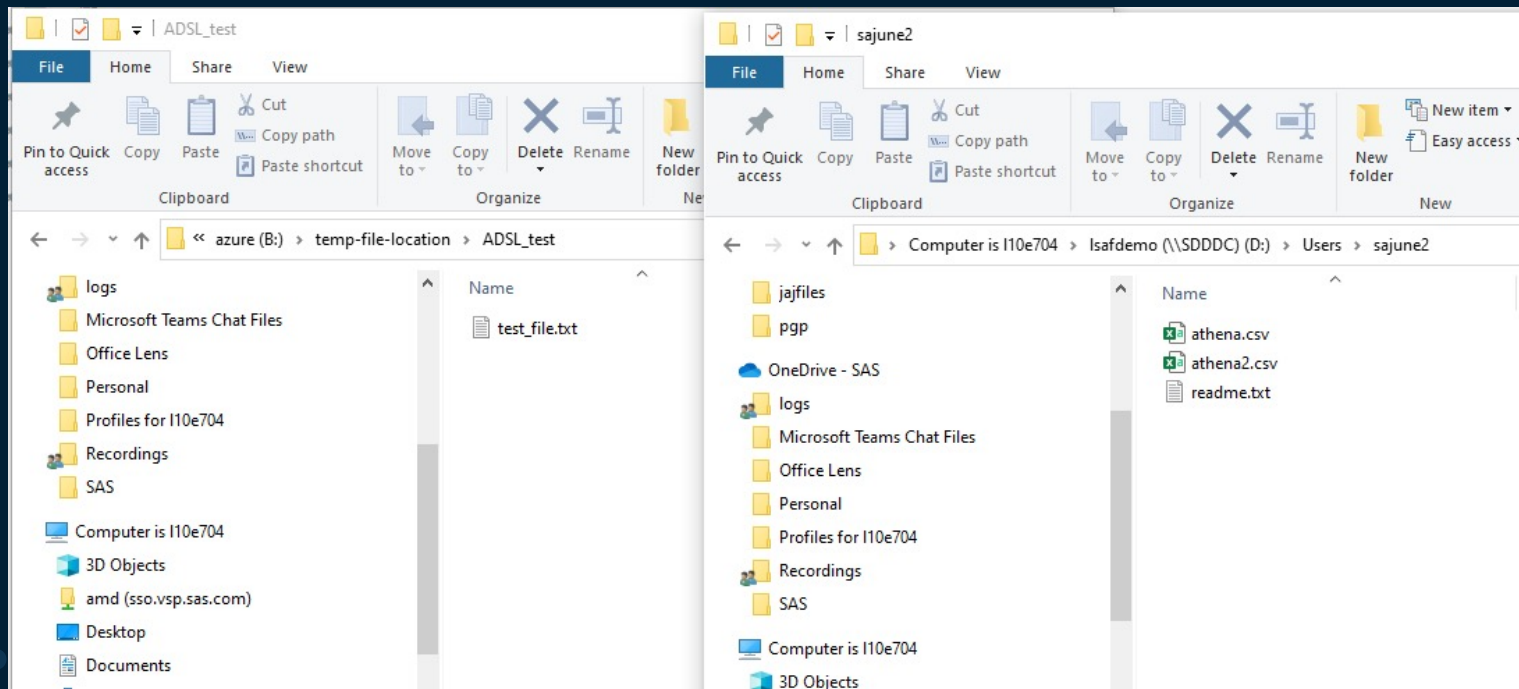
- Using IAM user to mount drive
 - Obscured Audit Trail
- Using AD User to mount drive
 - Concise Audit Trail

#	@timestamp	userIdem.	userIdentity.principalId	userIdem.	eventName	requestParameters.Host	sourceIPAd.	userAgent
▶ 35	2021-08-14T20:45:01.76.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	AUS Internal	AUS Internal
▶ 36	2021-08-14T20:22:54.73.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 37	2021-08-14T19:53:04.67.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 38	2021-08-14T19:53:04.67.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 39	2021-08-14T19:42:24.36.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 40	2021-08-14T19:36:23.03.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 41	2021-08-14T19:30:19.08.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 42	2021-08-14T19:24:39.96.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 43	2021-08-14T19:18:59.38.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 44	2021-08-14T19:13:03.31.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 45	2021-08-14T19:07:03.56.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 46	2021-08-14T19:01:53.56.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 47	2021-08-14T19:01:53.56.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 48	2021-08-14T19:01:53.56.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 49	2021-08-14T19:01:53.56.	IAFuser	AD24V70HEHKKXGQZDQW	saJume	GetObject	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 50	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 51	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 52	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 53	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 54	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 55	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 56	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 57	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 58	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 59	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 60	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]
▶ 61	2021-08-14T19:01:53.56.	AssumeRb.	AD24V70HEHKKXGQZDQW		HeadBucket	hidata.s3.us-east-1.amazonaws.com	149.173.8.1.	[rclone/v1.56.0]



Bring the logs in CDR.

Azure Storage account to CDR

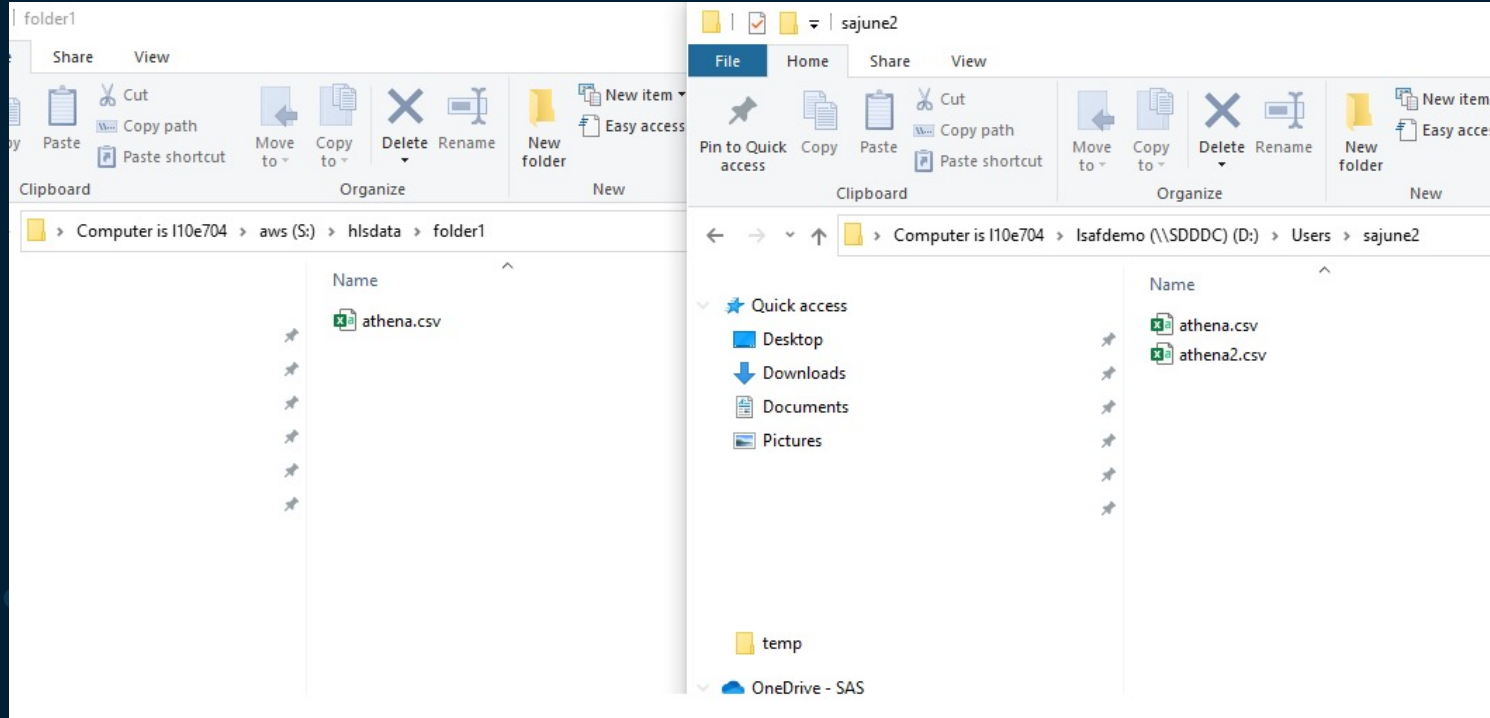


Reference:

Bring the logs in CDR

AWS S3 To CDR

- Data Exchange between cloud storages using drive mounts



- Audit Records



Create Traceability check and visualize

Data Traceability across cloud Environments

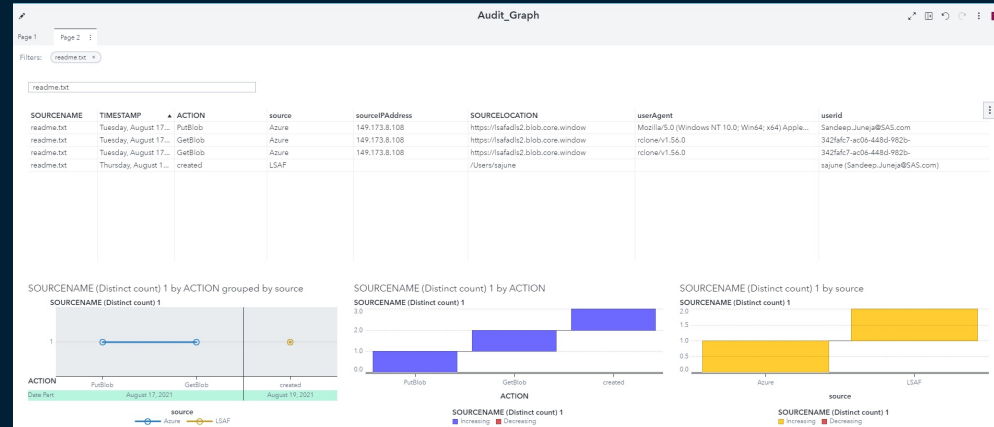
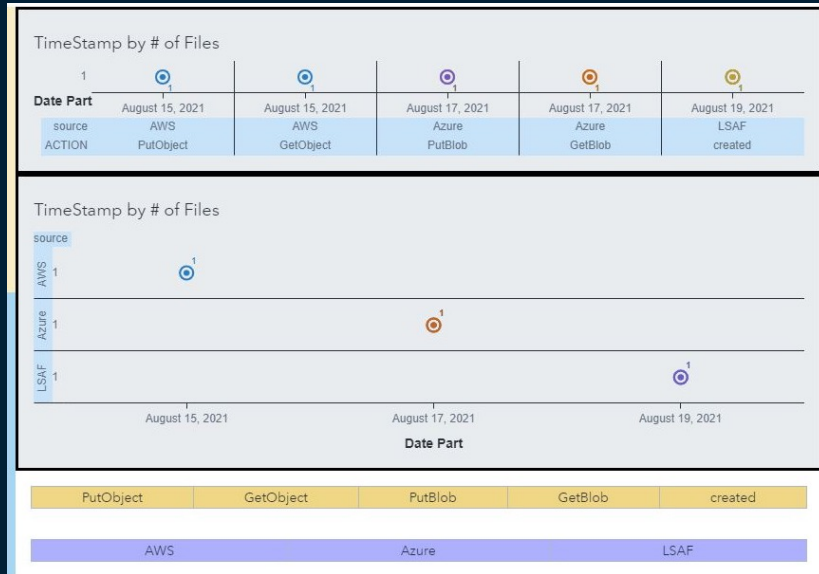
- Combining Audit Data across Cloud Environment provides data traceability

userAgent	source	action	userid	sourceLocation	sourceName
[rclone/v1.56.0]	AWS	GetObject	AROAYTOMEHNKXPZDROA3:Sandeep.Juneja@SAS.com (AssumedRole)	hlsdata.s3.us-east-1.amazonaws.com	athena2.csv
[rclone/v1.56.0]	AWS	GetObject	AROAYTOMEHNKXPZDROA3:Sandeep.Juneja@SAS.com (AssumedRole)	hlsdata.s3.us-east-1.amazonaws.com	athena2.csv
[rclone/v1.56.0]	AWS	GetObject	AROAYTOMEHNKXPZDROA3:Sandeep.Juneja@SAS.com (AssumedRole)	hlsdata.s3.us-east-1.amazonaws.com	athena2.csv
[rclone/v1.56.0]	AWS	GetObject	AROAYTOMEHNKXPZDROA3:Sandeep.Juneja@SAS.com (AssumedRole)	hlsdata.s3.us-east-1.amazonaws.com	athena2.csv
AzCopy/10.11.0 Azure-...	Azure	GetBlob	Sandeep.Juneja@SAS.com	https://lsafadls2.blob.core.window	000000.log
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	000000.log
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	000000.log
Mozilla/5.0 (Windows ...	Azure	PutBlob	Sandeep.Juneja@SAS.com	https://lsafadls2.blob.core.window	test_file.txt
Mozilla/5.0 (Windows ...	Azure	PutBlob	Sandeep.Juneja@SAS.com	https://lsafadls2.blob.core.window	readme.txt
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	readme.txt
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	readme.txt
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	readme.txt
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	readme.txt
rclone/v1.56.0	Azure	GetBlob	342fafc7-ac06-448d-982b-	https://lsafadls2.blob.core.window	readme.txt
	LSAF	created	sajune (Sandeep.Juneja@SAS.com)	/Users/sajune	athena.csv
	LSAF	created	sajune (Sandeep.Juneja@SAS.com)	/Users/sajune	athena2.csv
	LSAF	created	sajune (Sandeep.Juneja@SAS.com)	/Users/sajune	readme.txt

Create Traceability check and visualize

Data Traceability across cloud Environments

- Combining Audit Data across Cloud Environment provides data traceability



Special thanks to Sandeep Juneja for the contribution to core work!

Questions

Contact: Ben.Bocchicchio@sas.com

&

Pritesh.Desai@sas.com



sas.com

