

Configuration Manual

MSc Research Project MSc in CyberSecurity

Mahesh Gavhane Student ID: 23111984

School of Computing National College of Ireland

Supervisor: Prof. Khadija Hafiz

National College of Ireland Project Submission Sheet School of Computing



Student Name:	Mahesh Gavhane	
Student ID:	23111984	
Programme:	MSc in CyberSecurity	
Year:	2024-2025	
Module:	MSc Research Project	
Supervisor:	Prof. Khadija Hafiz	
Submission Due Date:	12/12/2024	
Project Title:	Configuration Manual	
Word Count:	XXX	
Page Count:	24	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.

<u>ALL</u> internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature:	Mahesh Gavhane
Date:	27th January 2025

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST:

Attach a completed copy of this sheet to each project (including multiple copies).Attach a Moodle submission receipt of the online project submission, to
each project (including multiple copies).You must ensure that you retain a HARD COPY of the project, both for

your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.

Assignments that are submitted to the Programme Coordinator office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Mahesh Gavhane 23111984

1 Introduction

The purpose of this document is to provide the basic information regarding the Logic App cloud setup which had been taken place, required systems specification for this project and the tools like Wireshark for testing purpose, PROM and Jupyter Notebook for visualization. With an aim to increase security and execution of Secure File Transfer in multi cloud (Azure to AWS) and within cloud (Azure to Azure) with log analysis and process mining. This configuration manual is created for the one who wants to replicate the same project as it contains all the steps for setting up the Cloud environment to implementation steps along with all the snapshots which will assist the user. This manual has all the information such as from where all the tools downloaded with software versions, and the URLs are added for reference.

2 System Specification

Tool Version	Version	
Visual Studio	Visual Studio 2022 (64-bit) - Version 17.11.5	
Postman	Version - 11.21.0	
PROM Tool	PROM 6.14 with 64 bit JRE8	
Jupyter Notebook	v7.2.3 version	
Wireshark	Version 4.4.2	
WINSCP	Version 6.3.5	

This Project uses a combination of tools, all are mentioned below:

Figure 1: List of tools used

3 Environment Setups and Installation Steps Along with Scenario-based results

To execute the proposed solution, commence with Azure Environment Setup, AWS cloud setup, and install the tool required for executing the process, testing, and visualization.

• Step 1: Create an Azure Resource Group with details like subscriptions name and the name of the Resource Group with Azure Region, for this project, North Europe has been selected as Azure Region.

Microsoft Azure			
Home > Resource groups >			
Create a resource	group		
Basics Tags Review + cre			
resources for the solution, or only	y those resources that you want to m	re solution. The resource group can include all the anage as a group. You decide how you want to sense for your organization. Learn more 더	
resources for the solution, or onl allocate resources to resource gr	y those resources that you want to m	anage as a group. You decide how you want to	
resources for the solution, or only allocate resources to resource gr Project details	y those resources that you want to m oups based on what makes the most	anage as a group. You decide how you want to	
resources for the solution, or only allocate resources to resource gr Project details Subscription * ①	y those resources that you want to m oups based on what makes the most	anage as a group. You decide how you want to	

• Step 2: After Resource Group, create an Integration Account with the details like Subscription and select the resource group that is already created in Step 1. Give the name of the Integration Account select the pricing tier and Azure Region and enable the Log Analytics Workspace for further analysis.

≡ Microsoft Azure		
Home > Integration accounts >		
Create an integration a	ccount	
Build enterprise integration and B2B/EDI s	olutions with logic apps. Learn more 급	
Project details		
Select the subscription to manage deployed manage all your resources.	ed resources and costs. Use resource groups like folders	to organize and
Subscription *	Azure for Students	~
Resource group *	rg_x23111984	
	Create Dew	
Instance details		
Integration account name *	Enter name	
Pricing Tier *		
-		
Region *	North Europe	~
Associate with integration service environment $\hfill \odot$		
Integration service environment		~
Enable log analytics ①		
Review + create < Previous : E	Basics Next : Tags > Download a templ	ate for automation ①

• Step 3: Create a Storage Account for hosting SFTP and setting up a Container for storing files, set up a Storage Account with a Subscription and existing Resource Group and give the proper Storage Account name.

 \equiv Microsoft Azure

Home > Storage accounts >

Create a storage account

Azure Storage is a Microsoft-managed service providing cloud storage that is highly available, secure, durable, scalable, and redundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure Tables. The cost of your storage account depends on the usage and the options you choose below. Learn more about Azure storage accounts c³

Project details

Select the subscription in which to create the new storage account. Choose a new or existing resource group to organize and manage your storage account together with other resources.

Azure for Students \checkmark
DefaultResourceGroup-NEU ~
Create new
(Europe) North Europe
Deploy to an Azure Extended Zone
Select a primary service \checkmark
Standard: Recommended for most scenarios (general-purpose v2 account)
O Premium: Recommended for scenarios that require low latency.

• Step 4: Set up SFTP server in Storage Account, Add 2 "Local User" and their "Authentication Method" and "Home Landing Directory". One is for the source directory and the second is for the destination Directory.

		,P Search resources, services, and docs (G+/)	🚱 Cop	oilot 🗵 🗘 🌾	이 저 x23111984@student.r NATIONAL COLLEGE OF IRELA	псі анр
Home > Storage accounts > x231119	4					
Storage accounts	« x23111984 SFTP storage account	* * …				×
+ Create 🏷 Restore …	Search Oragnose and some problems		iocal users 🕐 Refresh			
Filter for any field	Access Control (IAM)	 Local users and/or SFTP is disabled for this account. 	To connect to storage account via SFTP endpoint, e	nable Local users and SFTP.		
Name 🛧	Pata migration	Create or edit local users below in order to utilize SS	H File Transfer Protocol (SFTP). Learn more			
gx2311198483e5	••• 🗲 Events	Filter local users by prefix (case-sensitive)				
gx231119849dcc	*** 🛅 Storage browser					
x 23111984	*** 📑 Partner solutions	Connection string	Authentication method	Permissions	Home (landing) directory	
	✓ Favorites	x23111984.maheshserrver2@x23111984.b	SSH Password (Regenerate)	Set	x23111984container/outgoing	Û
	SFTP	x23111984.maheshserver1@x23111984.bl	SSH Password (Regenerate)	Set	x23111984container/incoming	Û
	Containers Data storage		-			

• Step 5: Setup Azure Container using a storage account for storing and processing purposes. After creating the container, create different directories for dropping and uploading the file in the source and destination directories. For this project, 3 directories have been created Incoming, Outgoing, and Logs for dropping, uploading and storing the generated logs.

\equiv Microsoft Azure			rices, and docs (G+/)		🥠 Copi
Home >					
x23111984container					
	↑ Upload + Add Directory ひ Refresh	🖓 Rename 🔟 Delete	\rightleftharpoons Change tier $ \mathscr{S} $	Acquire lease 🖉 Breal	k lease 🔗 Give feedback
Overview	Authentication method: Access key (Switch to Mi	crosoft Entra user account)			
Diagnose and solve problems	Location: x23111984container				
Access Control (IAM)	Search blobs by prefix (case-sensitive)				
✓ Settings					
Shared access tokens	Name		Modified	Access tier	Archive status
A Manage ACL	incoming		10/15/2024, 1:27:32 P	М	
Access policy	🗌 📜 logs		11/8/2024, 7:49:39 PN	1	
• • •	🗌 ៉ outgoing		10/15/2024, 1:34:06 P	м	
Properties					
 Metadata 					

• Step 6: Install WinSCP to login to SFTP local user created in step 4 using credential and check if credentials are working properly and are able to login to WinSCP.¹





• Step 7: Create Azure Log Analytics Workspace and check Enable Log Analytics checkbox is ticked while creating the integration account. Give your workspace a proper name and select the same Resource Group, which is used while creating the Storage Account and Integration Account.

¹https://winscp.net/eng/download.php

Microsoft Azure		$ \mathcal{P} $ Search resources, services, and c
Home > Log Analytics workspaces >		
Create Log Analytics	workspace	
Basics Tags Review + Create		
	asic management unit of Azure Monitor Logs. There are specific ew Log Analytics workspace. <u>Learn more</u>	c considerations \times
	y store, retain, and query data collected from your monitor sights. A Log Analytics workspace is the logical storage uni	
Project details Select the subscription to manage dep manage all your resources.	loyed resources and costs. Use resource groups like folders	to organize and
Subscription * ①	Azure for Students	\sim
Resource group * ①	Create new	~
Instance details Name * ①		
Region * 🕕	North Europe	~
Review + Create « Previou	s Next : Tags >	

• Step 8: Search for Logic App in the Azure portal, and click on the Add option to create the New Logic App. While creating the LA, select a Hosting Option – Consumption. Use Subscription, Resource Group and give proper name to Logic App.

\equiv Microsoft Azure		
Home > Logic apps > Create Logic App	o >	
Create Logic App (Mult	ti-tenant)	
Basics Tags Review + create		
	vorkflows as a logical unit for easier management, deplo · business-critical apps and services with Azure Logic Ap code.	
Project Details		
Select a subscription to manage deployed all your resources.	resources and costs. Use resource groups like folders to	organize and manage
Subscription * ①	Azure for Students	\checkmark
Resource Group * 🕕	(New) Resource group	\sim
	Create new	
Instance Details		
Logic App name *	Logic App name	
Region *	North Central US	\checkmark
Enable log analytics *	🔿 Yes 💿 No	
() Looking for the classic consumption c	reate experience? <u>Click here</u>	
Review + create < Previous	Next : Tags >	

- Step 9: For this project two Logic Apps is created one is "x23111984_sftp" for Secure File Process within the cloud (AWS) and multi cloud (AWS). And another one is "x23111984_logcapture" for capturing the logs.
 - A. Logic App "x23111984_sftp" is created by using designer and codeview. In the designer view click on add action to add action as shown below. For this project, the below flow has been created, if want to replicate the flow the same workflow. Designer View



Code View



- B. Logic App: "x23111984_logcapture" is created by using designer and codeview. Click on Logic App Designer and select an action to create a flow as shown below. For this project, the below flow has been created, if want to replicate the flow of the same workflow. This flow helps in capturing all logs and saving the generated logs in JSON and CSV format and uses the director created in the storage account to the logs in the "Logs Folder".

Logic App Designer View

Microsoft Azure	,2 Search resources, services, and docs (G+/)	② & x23111984@student.nci NATIONAL COLLEGE OF IRELAND
e > Logic apps > x23111984_logcapture		
x23111984_logcapture Logic ap	p designer 🔹 🐃	:
	X Discard [@] Parameters {} Code view ⊗ Errors ① Info 🖞 File a bug	
👗 Overview	8 Recurrence Trigger in	
Activity log	every 2 Min	
Ba Access control (IAM)	\oplus	
🗳 Tags	Get Logs From Log	
Diagnose and solve problems	Analytics Workspace	
✓ Development Tools		
🖧 Logic app designer	Ť.	
Logic app code view	O Parse JSON Using Specific Schema	
③ Run history		
Versions	(+)	
API connections	(0) Convert the JSON in	
📣 Quick start guides	csv	
✓ Settings	\oplus	
Workflow settings		
Authorization +	\oplus \oplus	
Access keys	😥 Create CSV file	
1 Identity		
Properties	$(\overline{})$	
🔒 Locks 👻 👘		

Logic App CodeView



• Step 10: Search for Function App in Azure Portal, create Function App, give proper function name, select Runtime Stack, and make sure was to select the same resource group that created while setting up the Integration Account. Upload the created function in Azure Function App under the name of the created function.



Add Function App Action in Azure Logic App, select the created Function App, add the request body to execute, and call the function from the logic app only.



Setup AWS environment for storing processed file, create AWS S3 bucket with proper S3 bucket name. In this project, AWS S3 bucket is created to store the transmitted file which shows Azure to AWS workflow.

Amazon S3 > Buckets > my-fil	iletransfer-bucke	t									(i)	•
Amazon S3 <	my-file	transfer-buc	ket Info									
General purpose buckets Directory buckets	Objects	Properties	Permissio	ons Metrics	Management Acces	ss Points						
able buckets New												
ccess Grants												
ccess Points	Object	(4) Info										
		_					ions 🔻 🔪 🤇		· · · ·	-		
oject Lambda Access Points	(C) (I	🗖 Copy S3 URI	🛛 🗖 Copy UR	tL) (<u>↓</u> Downloa	d)(Open 🖪)(Dele	te (Act	ions 🔹) (Create	folder)	→ Upload		
·	Objects a	re the fundamental e	ntities stored ir	n Amazon S3. You can	d Open 🔄 Dele use Amazon S3 inventory 🖸 to						bjects, you'l	ı
ulti-Region Access Points	Objects a		ntities stored ir	n Amazon S3. You can							bjects, you'l	I
ulti-Region Access Points atch Operations	Objects a need to e	re the fundamental e	ntities stored ir	n Amazon S3. You can						s to access your o	objects, you'l	e B
bject Lambda Access Points ulti-Region Access Points atch Operations M Access Analyzer for S3	Objects a need to e	re the fundamental e xplicitly grant them p	ntities stored in ermissions. <u>Lea</u>	n Amazon S3. You can						s to access your o		
, dit-Region Access Points tch Operations M Access Analyzer for S3 	Objects a need to e	re the fundamental e xplicitly grant them p d objects by prefix	ntities stored ir ermissions. Lez	n Amazon S3. You can arn more 2	use Amazon 53 inventory [2] to	o get a list of a	ll objects in yo		et. For other	s to access your o		\$
vit-Region Access Points tch Operations M Access Analyzer for S3 ock Public Access settings for is account	Objects a need to e	re the fundamental e xplicitly grant them p d objects by prefix Name Azure-To-AWS-file	ntities stored ir rermissions. <u>Lea</u>	n Amazon S3. You can arn more 2	v Last modified December 3, 2024, (UT€4000) December 4, 2024,	▼ 12:25:14	ll objects in yo		et. For other	s to access your o Storage class		\$
ulti-Region Access Points atch Operations	Objects a need to e	re the fundamental e xplicitly grant them p d objects by prefix Name Azure-To-AWS-file uploaded-test.txt	ntities stored ir rermissions. <u>Lea</u>	n Amazon S3. You can arn more 2	Last modified Lest modified December 3, 2024, (UTC+00:00) December 4, 2024, (UTC+00:00)	▼ 12:25:14 00:46:04	ll objects in yo		et. For other ▼ 102.0 B	s to access your o Storage class Standard		\$
tit-Region Access Points tch Operations M Access Analyzer for S3 ack Public Access settings for is account orage Lens	Objects a need to e	re the fundamental e xplicitly grant them p d objects by prefix Name Azure-To-AWS-file uploaded-test.txt	ntities stored ir rermissions. <u>Lea</u>	n Amazon S3. You can arn more 2	v Last modified December 3, 2024, (UT€4000) December 4, 2024,	▼ 12:25:14 00:46:04	ll objects in yo		et. For other ▼ 102.0 B	s to access your o Storage class Standard		\$

- Step 11: Using Logic App "x23111984logcapture", generate the logs and once created, download them from Storage Account for further analysis. Below is the CSV structure generated by Logic App. To capture the logs from Log Analytics Workspace and to convert the required JSON format into CVS format KQL query, Schema, and JavaScript code have been used as shown below.
 - Use Action called "Log Analytics Workspace" with their URI and KQL query to capture the log from the workspace.

-	» 🔮 Get Logs From Log Analytic	cs Workspace	:
Ø Recurrence Trigger in every 2 Min	Parameters Settings Code view	v Testing About	
Get Logs From Log Analytics Workspace	https://api.loganalytics.io/v1/work: 8eda9569bfdc/query Method *	spaces/0212621c-bef4-41f6-8846-	
÷	POST Headers		~
Parse JSON UsingSpecific Schema	Content-Type	application/json	÷
(+)	Queries Enter key	Enter value	÷
() Convert the JSON in CSV	resource_actionName_s order by }	ect TimeGenerated, resource_runId_s, status_s, TimeGenerated asc"	, ,
÷	Cookie Enter HTTP cookie		

 Use the action "Parse JSON" with the given schema to convert the JSON into format JSON format.



- For converting JSON to CSV format, use the "JavaScript" action with the code shown below.



 After converting JSON to CSV, Logic App stores both 'logs.json' and 'logs.csv' in the storage account as shown below.

Result: Logic App generates Logs.csv

Microsoft Azure	,P Search resources, services, and docs (G+/)	🧔 Copilot	D Q	© 0) <u>R</u>	x23111984@student.nci NATIONAL COLLEGE OF IRELANI
me > x23111984_logcapture >						
puts						
ate_CSV_file_						
method": "post".						
"queries": {						
"folderPath": "/logs/", "name": "log-2024-11-14-15-50-33.csv",						
"queryParametersSingleEncoded": "True"						
Ъ						
"headers": { "ReadFileMetadataFromServer": "True"						
},						
<pre>"path": "/datasets/default/files", "host": {</pre>						
"connection": {						
"name": "/subscriptions/6aee45a5-419e	-4727-b279-861d9d3f8269/resourceGroups/rg_x23111984/providers/Microsoft.Web	/connections/sftpwithssh-1"				
)						
"body": "TimeGenerated, resource_runId_s, statu	s_s,resource_actionName_s\n\"2024-10-25T00:30:48.7130657Z\",\"0858471790636	7962677905454645CU14\",\"Running\"	,\"\"\n\"20	4-10-25T00	:30:48.	7184385Z\",
	\",\"\"\n\"2024-10-25T00:30:48.7276286Z\",\"08584717906367962677905454645CU					
	<pre>,\"List_files_in_folder\"\n\"2024-10-25T00:30:48.9728565Z\",\"0858471790636 \"Running\",\"For each\"\n\"2024-10-25T00:30:49.0536601Z\",\"08584717906367</pre>					
	\"AzureToAWSFileTransfer-UploadToS3\"\n\"2024-10-25T00:30:49.16156222\",\"				-10-251	00:30:45.00142222(,
	25T00:30:49.1755433Z\",\"08584717906367962677905454645CU14\",\"Failed\",\"\				0100407	1564CH25\" \"Puppipg\"

Result: Logic App generates Logs.json

	Microsoft Azure	Search resources, services, and docs (G+/)	🧔 Copilot		0	x23111984@student.nci x23111984@student.nci
Hom	e > x23111984_logcapture >					
	JSON_file					×
	<pre>"method": "post", "method": "post", "foidePeth": "/logy/", "mame": "log-2044.11-41-5-60-33.json", "gueryParametrisSingleIncoded": "True") "hoodfildeEadataFrowServer": "True") path": "/datasets/default/files", "hoot": { "commetion": { "commetion: { "commetion": { "commetion: { "commetion: {</pre>	39/resourceGroups/rg x23111984/providers/Microsoft.Web/connections/sf				
		syn eson cen oppyn Excertised provider synter oson cines connections si				
	"body": { "tables": [
	<pre>{ "name": "Primary@esult", "colums": [{</pre>					

• Step 12: Install PROM tool (version 6.14) for process mining, from the official website. PROM lite 1.4 also works for executing the workflows.²



²https://promtools.org/

 a) Installing PROM tool, Open the Process Minig PROM tool package manager to import packages like CSV import and required packages based on Process Mining methods.

😸 ProM UlTopia Packa	ge Manager	- • ×
ProM	3	
	arte 🔳 📖	
Up to date	Vest tar	AbstractEventsSupervised
\checkmark	Addine Addre (to literat Ween 63.7	Version 6.9.10 License: L-GPL
Out of date	ActionUnitestedProcessMining Operan Test Versun 5 % 5	Description: Abstract Events Supervised
X Not installed	Activity Filtering Itel Tag It	(Install
	Administrim A form wears 6.9.8	Rt Show parents
Selection	AdvancedEvent.ogFiltering Dard: bio granet Utestvg Versent 11,20	RI Show children
100	AlphaPrecision Sadori Learann nd Aan Ruite Verent 1.3.1	
	AlphaRevisitExperiments Associations Vesson 5:10	
	AntiAlignments 87 van Stopun Verwent St.4	
23.5	BPUNMiner Ratael Cotent Veenn C3.30	
	BPANNonaliter A Industrian Version 5.347	
Manage memory se	tog	Manage Plugin Cache
	▶ 100 MB ▶ 2 GB ▶ 3 GB ▶ 4 GB ¥ GB	Clear

b) By using generated logs.CSV from log capture Logic App, import that CSV file in the PROM tool and create Labelled Event Logs by using the action – "Infer Case ID", select the attribute and click on continue. The structure of Labeled Event Logs are shown below.



 c)Export log to workspace with name starts "XESLog" and using that created Event Log in input, apply the method which can create a graph for analyzing the workflow. For this project, we use the "Petri Net Flow method" and "Direct Follow method" as shown below.

ProM UlTopia		- o x
ss Prom Unopia		
ProM		owigned by Fluxicon
Actions		Activity O
	Actions	
Input	🕈 🕑 🐨 🖬 🔍 peti	Output
XES log - log-2024-11-14-15-35-35.csv	Convert to Replay Results RMW. Verbeek (Junux verbeek glucus)	Click to add output object
Click to add input object	Create Matrix RMAW. Verbeek ((truc.w.verbeek ((truc.nt)	
	DISCover Petri net (process tree) RLM.W. Verbeek (punw.verbeek (punw.verbeek (punw.	
	DISCover Petri net (User selects noise) KLAW. Verliesek (Juan. werbesk (Juan. 2)	
	DISCover Petri net (user) KLAVE. Verbeek (gluum verbeek (gluum)	
	Discover using Decomposition U.M.W. Verbeek (Junuwsetbeek (Junus)	
	Discover using Decomposition RMAW. Verbeek (Unixw.verbeek (Unixw.v	
	Enrich Petri Net with performance data (default mapping) A. Rogge-Sold (unit-texa rogge-solid)(tipLark potestam.de)	
	Eilter events based on transition manning	
	K Reet Start	

Direct Follow Graph :



Petri Net Flow Graph:



 $\bullet\,$ Step 13: For visualization, install Jupyter Notebook from the official website, and use Python libraries for visualizing the graphs. 3



a) Import Python libraries like "Pandas" and "Numpy" as shown below.
 ³https://jupyter.org/

.0]:	import pandas as pd							-+:	Ð	\uparrow	\downarrow	÷	Ŧ
	import numpy as np												
	from sklearn.preprocessing impor	rt LabelEncoder											
	<pre>import matplotlib.pyplot as plt</pre>												ſ
]:	<pre>data = pd.read_csv("C:\\Users\\I</pre>	<pre>Lenovo\\Desktop\\Thesis Part 2\\impl</pre>	ementation\	\log-2024	-11-14-15-	35-35.csv")							
]:	<pre>print(data.head())</pre>												
	TimeGenerated	resource_runId_s	status_s	X									
	0 2024-10-25T00:30:48.7130657Z	08584717906367962677905454645CU14	Running										
	1 2024-10-25T00:30:48.7184385Z												
	2 2024-10-25T00:30:48.7276286Z												
	3 2024-10-25T00:30:48.7776523Z		Running										
	4 2024-10-25T00:30:48.9728565Z	08584717906367962677905454645CU14	Succeeded										
	resource_actionName_s												
	Ø NaN												
	1 NaN												
	2 NaN												
	3 List_files_in_folder												
	4 List_files_in_folder												

 b) After installing the jupyter and importing libraries, generate various graph which helps in analyzing the overall workflow and any irregularities and deviation in the graphs. For this project, various graphs has been generated as shown below.





Action frequency distribution
data['resource_actionName_s'].value_counts().plot(kind='bar', title='Action Frequency')
plt.show()

```
# Extract hour and day from the `TimeGenerated` column
data['hour'] = data['TimeGenerated'].dt.hour
data['day'] = data['TimeGenerated'].dt.date
# Group by hour to detect hourLy patterns
hourly_activity = data.groupby('hour').size()
# Plot hourly patterns
import matplotlib.pyplot as plt
hourly_activity.plot(kind='bar', title='Hourly Log Activity')
plt.xlabel('Hour of Day')
plt.ylabel('Number of Logs')
plt.show()
# Group by day to detect daily activity patterns
daily_activity = data.groupby('day').size()
# Plot daily patterns
daily_activity.plot(title='Daily Log Activity')
plt.xlabel('Date')
plt.ylabel('Number of Logs')
plt.show()
```



import plotly.graph_objects as go

```
# Prepare data for Sankey diagram
sankey_data = data.groupby(['resource_actionName_s', 'status_s']).size().reset_index(name='count')
# Create mappings for source and target nodes
all_nodes = list(set(sankey_data['resource_actionName_s']).union(set(sankey_data['status_s'])))
node_map = {node: i for i, node in enumerate(all_nodes)} # Map node names to indices
# Map source and target columns to their indices
sankey_data['source'] = sankey_data['resource_actionName_s'].map(node_map)
sankey_data['target'] = sankey_data['status_s'].map(node_map)
# Build the Sankey diagram
fig = go.Figure(go.Sankey(
    node=dict(
       pad=15,
        thickness=20,
        line=dict(color="black", width=0.5),
        label=all_nodes # Use all unique nodes as labels
   ),
    link=dict(
        source=sankey_data['source'], # Map sources
        target=sankey_data['target'], # Map targets
value=sankey_data['count'] # Use count as the weight
    )
))
# Set title and display the figure
fig.update_layout(title_text="Sankey Diagram: Actions to Statuses", font_size=10)
fig.show()
```

Sankey Diagram: Actions to Statuses

Initiat-files-in_folder Initiats-antable Get-file-content_using_path Get-file-content_using_path_1 Decreate_file_1 Parses_ISON	
HTTP	Succeeded
Create_file	
For_each	Running
For_each_1	
Execute_JavaScript_Code	• Skipped
Condition	Failed 💳
AzureToAWSFileTransfer-UploadToS3 AzureToAWSFileTransfer-UploadToS3_1	
Send_an_email_(V2)	
Ocnd_dn_c(vz)	

```
import plotly.graph_objects as go
# Step 1: Prepare Nodes and Edges
unique_nodes = list(set(data['resource_actionName_s']).union(set(data['status_s'])))
node_indices = {node: i for i, node in enumerate(unique_nodes)}
edge_x = []
edge_y = []
for action, status in edges:
    edge_x.append(node_indices[action])
    edge_y.append(node_indices[status])
# Step 2: Create Network Graph
fig = go.Figure()
# Add edges
for action, status in edges:
    fig.add_trace(go.Scatter(
        x=[node_indices[action], node_indices[status]],
        y=[0, 1],
        mode='lines',
        line=dict(width=0.5, color='gray'),
        hoverinfo='none'
```



• Step 14: Install Wireshark, after installing, start the WireShark application and start capturing the packet and simultaneously start file transmission from WinSCP to hosted Azure to an azure hosted SFTP and by using tcp.port==22 filter in Wireshark to capture the SFTP's traffic only. This step verify that the packet during the transmission is encrypted.

p.port == 22				
			Protocol Lene	
6574 1762.143830	10.13.87.152	20,60,145,164	SSHv2	230 Client: Encrypted packet (len=176)
6575 1762.147524	20.60.145.164	10.13.87.152	SSHv2	102 Server: Encrypted packet (len-48)
5576 1762,186185	10.13.87.152	20.60.145.164	SSHv2	118 Client: Encrypted packet (len-64)
577 1762.189671	20,60,145,164	10.13.87.152	SSHv2	118 Server: Encrypted packet (len=64)
5578 1762.190063	10.13.87.152	20.60.145.164	SSHv2	134 Client: Encrypted packet (len=80)
5579 1762.192876	20.60.145.164	10.13.87.152	SSHv2	150 Server: Encrypted packet (len=96)
5580 1762.193973	10.13.87.152	20.60.145.164	SSHv2	134 Client: Encrypted packet (len=80)
5581 1762.200228	20.60.145.164	10.13.87.152	SSHv2	150 Server: Encrypted packet (len=96)
5582 1762.253574	10.13.87.152	20.60.145.164	TCP	54 62275 → 22 [ACK] Seq=2655 Ack=1697 Win=4194048 Len=0
5583 1762.253894	10.13.87.152	20.60.145.164	SSHv2	134 Client: Encrypted packet (len=80)
584 1762.261430	20.60.145.164	10.13.87.152	SSHv2	166 Server: Encrypted packet (len=112)
585 1762.261731		20.60.145.164	SSHv2	166 Client: Encrypted packet (len=112)
586 1762.269614		10.13.87.152	SSHv2	262 Server: Encrypted packet (len=208)
587 1762.270400	10.13.87.152	20,60,145,164	SSHv2	
				166 Client: Encrypted packet (len=112)
588 1762.273212	20.60.145.164	10.13.87.152	SSHv2	134 Server: Encrypted packet (len=80)
588 1762.273212 589 1762.316450	20.60.145.164 10.13.87.152	10.13.87.152 20.60.145.164	SSHv2 TCP	134 Server: Encrypted packet (len=80) 54 62275 → 22 [ACK] Seq=2959 Ack=2097.Win=4193536 Len=0
588 1762.273212 589 1762.316450 594 1763.312869	20.60.145.164 10.13.87.152 10.13.87.152	10.13.87.152 20.60.145.164 20.60.145.164	SSHv2 TCP SSHv2	134 Server: Encrypted packet (le=59) 54.6225 + 22.1672 (seq=255 + Ack=3067, Vin=4193536 Len=0 136 Client: Encrypted packet (len=112)
588 1762.273212 589 1762.316450 594 1763.312869 595 1763.317286	20.60.145.164 10.13.87.152	10.13.87.152 20.60.145.164	SSHv2 TCP	134 Server: Encrypted packet (len=80) 54 62275 → 22 [ACK] Seq=2959 Ack=2097.Win=4193536 Len=0
588 1762.273212 589 1762.316450 594 1763.312869 595 1763.317286 596 1763.358295	20.60.145.164 10.13.87.152 10.13.87.152 20.60.145.164 10.13.87.152	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encrypted packet (lens0) 54 (237 - 2) (ACL) Gen2026 Analad27, Wind19536 Lenv0 166 (lient: Encrypted packet (lens12) 134 Server: Incrypted packet (lens10)
588 1762.273212 589 1762.316459 594 1763.312869 595 1763.317286 596 1763.358295 [Next Sequence 1	20.60.145.164 10.13.87.152 10.13.87.152 20.60.145.164 10.13.87.152 Number: 3071 (re	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryfeld packet (lens80) 54 (2017 - 2) (Act) Seq 2026 Act=2027 Win=419536 Len=0 136 (Client: Encryfeld packet (lens80) 54 62275 + 22 (Act) Seq=3071 Act=2177 Win=4195336 Len=0
588 1762.273212 589 1762.316450 594 1763.312869 595 1763.317286 596 1763.358295 [Next Sequence Acknowledgment	20.60.145.164 10.13.87.152 10.13.87.152 20.60.145.164 10.13.87.152 Number: 3071 (re	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence number lative ack number)	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryfeid packet (lens80) 54 (235 - 4) [Ckc] 5eq385 - 4k-3927 Min4193536 Len+0 156 (216mt: Encryfeid packet (lens81) 54 62275 - 42 (Ack] 5eq3971 Ack=2177 Min4193536 Len+0 54 62275 - 42 (Ack] 5eq3971 Ack=2177 Min4193536 Len+0 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 75 98 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 88 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 55 88 15 k - regi N - 6 (010) 69 69 72 63 40 60 80 00 60 80 65 88 15 k - regi N - 6 (010) 60 60 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi N - 6 (010) 60 68 75 68 75 68 15 k - regi - reg N - 6 (010) 60 68 75 68 75 68 15 k - regi - reg N - 6 (010) 60 68 75 68 75 68 15 k - regi - reg N - 6 (010) 60 68 75 68 75 68 15 k - reg - reg N - 6 (010) 75 68 75 75 75 75 75 75 75 75 75 75 75 75 75
588 1762.273212 589 1763.312869 594 1763.312869 595 1763.312869 595 1763.317286 596 1763.358295 [Next Sequence Acknowledgment Acknowledgment	20.60.145.164 10.13.87.152 10.13.87.152 20.00.145.164 10.13.87.152 Number: 3071 (re Number: 2097 (re	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryfeld picket (lene30) 54 (2027 - 2) (Act) 5eg:280 Acta020, Winn4195356 Lene0 166 (lient: Encryfeld picket (lene312) 54 62275 + 22 (Act) Seg:3071 Act=2177 Winn4195356 Lene0 *
588 1762.273212 589 1763.316450 594 1763.312869 595 1763.317286 596 1763.358295 [Next Sequence Acknowledgment Acknowledgment Acknowledgment Acknowledgment Acknowledgment Acknowledgment	20.60.145.164 10.13.87.152 20.60.145.164 10.13.87.152 20.60.145.164 10.13.87.152 Number: 3071 (re Number: 2097 (re number (raw): 29001 der Length: 20 byte	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryfeid packet (lens80) 54 (237 - 4) Excl 5eq:264 Actio221 Win4195356 Lens0 166 (216mt Encryfeid packet (lens80) 54 62275 + 22 (ACK) Seq:3871 Actic2177 Win4195356 Lens0 6 000 6 dd 75 06 8 40 65 06 00 6 00 6 00 6 00 6 00 0 6 0 0 5 0 1 3 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
588 1762.273212 589 1763.312659 594 1763.312869 595 1763.312869 596 1763.358295 [Next Sequence I Acknowledgment I Acknowledgment I 0101 = Hoas Flags: 0x018 (P: Window: 32762	20.60.145.164 10.13.07.152 10.13.07.152 20.00.155.164 10.13.07.152 Wumber: 3071 (re Wumber: 2097 (re wumber (rew): 29001 der Length: 20 byte SH, ACK)	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encrypted packet (LensB0) 146 S2T# -2 [CK-] 562 S64 LensB0 146 S2T# -2 [CK-] 562 S64 LensB0 146 S2T# -2 [CK-] 562 S65 LensB0 54 62275 + 22 [CK-] 566 S65 LensB0 54 62275 + 22 [CK-] 566 S65 LensB0 66 87 59 86 86 66 d8 67 c a 8e bc 30 08 00 45 00 h.h.******0.**E 010 06 98 72 63 40 08 00 66 00 00 ba d5 79 88 13 c
588 1762.273212 589 1763.312669 594 1763.312869 595 1763.312869 595 1763.317280 596 1763.358295 [Next Sequence Acknowledgment 0101 = Hear Flags: 0x018 (P; Window: 32762 [Calculated win.	20.60.145.164 10.13.07.152 10.13.07.152 20.00.145.164 10.13.07.152 Number: 3071 (re Number: 3077 (re number (rsw): 25001 dor Length: 20 byte SH, ACK) dow size: 4193536]	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lem50) 54 62275 + 22 (AcK) 5eq:250 Acke327 Win4195356 Lem0 54 62275 + 22 (AcK) 5eq:3071 Acke327 Win4195356 Lem0 6 0000 68 d7 9a 68 ea 60 d8 f2 ca 8e bc 30 08 00 45 00 h h.h.*
588 1762,273212 580 1762,312869 594 1763,312869 595 1763,317286 596 1763,317286 [Next Sequence Acknowledgment Acknowledgment Acknowledgment 81081 = Hea Flags: 0x018 (P Window: 32762 [Calculated win Window :ze sc:	20.60.145.164 10.13.27.152 10.13.87.152 20.007.157.164 10.13.87.152 Wumber: 2097 (re wumber: 2097 (re unaber (raw): 20901 let length: 20 byte 5H, ACK) dow size: 4193536] aling factor: 128]	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lens0) 54 (235 - 4) [CK] 5eg 265 (Lens0) 54 (235 - 4) [CK] 5eg 265 (Lens0) 54 (235 - 4) [CK] 5eg 265 (Lens0) 54 (225 - 4) [CK] 5eg 265 (Lens0) 56 (Lens0) [CK] 5eg 265 (Lens0) 56 (Lens0) [CK] 5eg 265 (Lens0) 56 (Lens0) [CK] 5eg 265 (Lens0) [CK] 5
588 1762.273212 599 1763.312869 596 1763.312869 595 1763.317280 596 1763.358295 [Next Sequence I Acknowledgment I Acknowledgment I 0101 = Hean Flags: 0x018 (P; Window: 32762 [Calculated winn [Window size sc. (becksum: 0x081	20.60.145.164 10.13.07.152 10.13.87.152 20.00.145.164 10.13.87.152 10.13.87.152 10.13.87.152 10.13.87.152 10.142.162 10.1	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lem50) 54 62275 + 22 [ACK] 5eq:230 Acke327 Winn:195356 Lem0 54 62275 + 22 [ACK] 5eq:3071 Acke327 Winn:195356 Lem0 54 62275 + 22 [ACK] 5eq:3071 Acke3277 Winn:195356 Lem0 6 0000 68 df 7 9a 68 aa 60 df 7 c a 6e bc 30 68 00 45 00 h h h.*. · · · · 0 · E 0 000 68 df 7 9a 68 aa 60 df 7 c a 6e bc 30 68 00 45 00 h h h.*. · · · · 0 · E 0 000 68 df 7 9a 68 aa 60 df 7 c a 6e bc 30 68 00 45 00 h h h.*. · · · · 0 · E 0 000 68 df 7 9a 68 aa 60 df 7 c a 6e bc 30 68 00 45 00 h h h.*. · · · · 0 · E 0 000 7 f f 68 10 00 07 77 s 65 10 bs 30 63 17 6 c - · · · 0 · C 0 000 6 df 7 a 43 10 00 10 df 31 00 56 af 3 c 78 bd 64 f 7 c - · · · 0 · C 0 000 6 df 7 a 78 10 10 10 00 56 af 2 c 2 a 60 68 00 c - · · · · 0 · C 0 000 6 df 7 a 68 10 00 07 77 s 0 c - · · · 0 · 0 · · · · · · · · · · · · ·
588 1762.273212 559 1763.312869 599 1763.312869 599 1763.312869 599 1763.312809 599 1763.315209 590 1763.3152095 [Next Sequence 1 Acknowledgment Acknowledgment Acknowledgment Acknowledgment Flags: 0x018 (P Window: 32762 (Calculated wim [Window size sc Checksum: 0x081 (Checksum: Statu	20.60.145.164 10.13.27.152 10.13.87.152 20.007135.164 10.13.87.152 Number: 2097 (re Number: 2097 (re Number: 2097 (re SH, ACK) dow izze: 4193536] aling factor: 128] 8 [unverified]	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encrypted packet [lens80] 146 Silenti Encrypted packet [lens30] 146 Silenti Encrypted packet [lens132] 146 Silenti Encrypted packet [lens132] 147 Silenti Encrypted packet [lens132] 148 Sil
588 1762.773212 594 1763.312869 595 1763.312669 595 1763.31266 595 1763.31266 596 1763.358295 [Next Sequence Acknowledgment Acknowledgment Acknowledgment Acknowledgment States Clacksus Statu (Checksum Statu Urgent Pointer:	20.60.145.164 10.13.27.152 10.13.87.152 20.007135.164 10.13.87.152 Number: 2097 (re Number: 2097 (re Number: 2097 (re SH, ACK) dow izze: 4193536] aling factor: 128] 8 [unverified]	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lense) 54 (237 + 2) (Acl 5 eq:36 Acl 302) Winn 199356 Lense 166 (218mt Encryted packet (lense) 54 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 6 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 100 00 00 00 72 63 40 00 00 00 00 00 00 00 00 00 00 00 00
588 1762, 273212 591 1763, 312460 592 1763, 312460 595 1763, 35295 [Next Sequence Acknowledgment 6101 = Haa Flags: Bv018 (P Window: 32762 [Calculated winw: 32762 [Calculated winw: 32762 [Calculated winw: 32762 [Calculated winw: 32762 [Checksum: 0488]]	20.60.145.164 10.13.07.152 10.13.87.152 20.00.135.164 10.13.87.152 10.15.152 10.1	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lense) 54 (237 + 2) (Acl 5 eq:36 Acl 302) Winn 199356 Lense 166 (218mt Encryted packet (lense) 54 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 6 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 100 00 00 00 72 63 40 00 00 00 00 00 00 00 00 00 00 00 00
588 1762.773212 501 7763.312869 502 1763.312669 502 1763.312669 505 1763.358295 506 1763.358295 506 1763.358295 6103 = h03 Flags: 0x018 (M Kindow: 32762 [Calculated wim (Kindow: 32762 [Calculated wim (Checksum: 0x081] [Checksum Statu Urgent Pointer: [Timestamp5] [Stp(AKK analys)	20:60:145:164 10:13:87:152 10:13:87:152 20:00125:108 10:13:87:152 Number: 3071 (re Number: 3071 (re Number: 3097 (re Number: 2097 (re 2097 (re 2007 (re) 2097 (re) 2090 Jack (re) 2090	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lense) 54 (237 + 2) (Acl 5 eq:36 Acl 302) Winn 199356 Lense 166 (218mt Encryted packet (lense) 54 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 6 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 100 00 00 00 72 63 40 00 00 00 00 00 00 00 00 00 00 00 00
588 1762.273212 501 1763 116460. 501 1763 116460. 501 1763 116460. 505 1763 135225 [Next Sequence Acknowledgment Acknowledgment 6101 = Hea Flags: Bv018 (P Window: 32762 [Calculated win Window: 32762 [Calculated win [Uindows statu Urgent Pointer: [Timestangs] [StQ/ACK analys]	20:60:145:164 10:13:87:152 10:13:87:152 20:00125:108 10:13:87:152 Number: 3071 (re Number: 3071 (re Number: 3097 (re Number: 2097 (re 2097 (re 2007 (re) 2097 (re) 2090 Jack (re) 2090	10.13.87.152 20.60.145.164 20.60.145.164 10.13.87.152 20.60.145.164 lative sequence numbe lative ack number) 79710	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encryted packet (lense) 54 (237 + 2) (Acl 5 eq:36 Acl 302) Winn 199356 Lense 166 (218mt Encryted packet (lense) 54 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 6 (227 + 2) (Acl 5 eq:3071 Acl 2177 Winn 199356 Lense 100 00 00 00 72 63 40 00 00 00 00 00 00 00 00 00 00 00 00
558 1762.773212 550 1763.17460 550 1763.17460 550 1763.17460 550 1763.158295 [Next Sequence Acknowledgment 6181	20.60.145.164 10.13.67.152 10.13.87.152 10.13.87.152 10.13.87.152 10.13.87.152 10.13.87.152 Number: 2097 (re number (rem): 20901 drw size: 4193536] [umverifiel] 0 0 10] 2 bytes)	10.13.07.152 20.60.145.164 20.60.145.164 10.135.154 10.135.154 20.60.145.164 1ative sequence number 1ative sequence number) 79710 (5)	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encrypted packet (Lems0) 146 (2014 - 2) (Acc) 529 (2014 (Lems0) 146 (2014 - 1) (Acc) 247 (Marc 1915356 Lem-0 146 (2014 - 1) (Acc) 247 (Marc 1915356 Lem-0 146 (2014 - 1) (Marc 1914 (Marc 1915 - 1) (Marc 1914 (Marc 191
5568 1762, 275212 5504 1763, 312600 5504 1763, 312600 5506 1763, 3156205 []Next Sequence & Acknowledgment t Acknowledgment t Acknowledgment t Acknowledgment t Acknowledgment t Charles 10018 (]Clarles 10018 (]Clarles 10018 (]Clarles 10018 (]Checksum: 0x081 []SteQ/ACK analys []SteQ/ACK analys []]SteQ/ACK analys []]	20.60.145.164 10.13.67.152 10.13.67.152 20.00.165.164 20.00.165.164 10.13.07.152 Number: 2071 (re number (cms): 5001 st, 40, 12.0001 st, 40, 12.0001 st, 40, 12.0001 b) (unverified) b) (b) (unverified) b) (unveri	10.13.47.152 20.40.45.164 20.40.145.164 20.40.145.164 20.40.145.164 20.40.455.164 20.40.455.164 20.40.455.164 20.455.16420.455.164 20.455.164 20.455.16420.455.164 20.455.164 20.455.16420.455.164 20.455.164	SSHv2 TCP SSHv2 SSHv2 TCP	134 Server: Encrypted packet (Lems0) 146 (2014 - 2) (Acc) 529 (2014 (Lems0) 146 (2014 - 1) (Acc) 247 (Marc 1915356 Lem-0 146 (2014 - 1) (Acc) 247 (Marc 1915356 Lem-0 146 (2014 - 1) (Marc 1914 (Marc 1915 - 1) (Marc 1914 (Marc 191
558 1762, 273212 554 1763, 31280 556 1763, 352825 [Next Sequence b 163, 352825 [Next Sequence b 1010] = Noa Flags: 0x108 (M Nindow: 32762 [Calculated wim Mindow: 32762 [Calculated wim [Jimstans: 32762 [Calculated wim [Jimstans: 32762 [Stef/Act analys TCP payload (11 Protocol SSH Version 2 () Packet Length	20.60.145.164 20.60.145.752 10.13.87.152 20.01.87.152 20.00.153.87.152 20.00.153.87.152 20.00.153.87.152 20.00.157.157.152 20.00.157.157.152 20.00.157.157.152 20.00.157.157.157.157.157.157.157.157.157.157	10.13.47.152 20.40.45.164 20.40.135.164 20.43.154 20.40.145.164 20.43.164 20.445.164 20.445.164 20.445.164 20.445.164 20.445.164 20.445.164 20.457 20	SSHv2 TCP SSHv2 SSHv2 TCP m)]	134 Server: Encrypted packet (Lenso) 146 (216 + 1 / 164 (5 + 20 / 26 / 164 /
5568 1762, 37242 5504 1762, 312600 5504 1763, 312600 5506 1763, 3156205 []Next Sequence & Acknoxledgment t Acknoxledgment t Acknoxledgment t Acknoxledgment t Acknoxledgment t Acknoxledgment t Clobel	20.60.145.164 10.13.67.152 10.13.67.152 10.13.67.152 10.13.67.152 10.13.67.152 Number: 2071 (re Number: 2071 (re Number: 2077 (re number (rem): 25001 dws/siz: 4139536) aling factor: 1283 0 (unverified) 0 (s) 10 (unverified) 0 (s) 10 (unverified) 0 (unverif	10.13.47.152 20.40.45.164 20.40.135.164 20.43.154 20.40.145.164 20.43.164 20.445.164 20.445.164 20.445.164 20.445.164 20.445.164 20.445.164 20.457 20	SSHv2 TCP SSHv2 TCP TCP rr)]	134 Server: Excrypted picket (lems8) 145 Server: Excrypted picket (lems8) 145 Server: Excrypted picket (lems8) 154 Server: Excrypted picket (lems8) 155 Server: Excrypted picket (le

4 Senario Based Results

4.1 Senario I

–Within Azure: From the SFTP server to designated storage folders.

$\mathbf{RunId} \ \textbf{-} \ \textbf{08584688499449355123761745814CU47}$

File Name - testfile drops in maheshserver1 (Home Directory x23111984container/incoming)

x23111984.maheshserver	1@x231119	34.blob.core.windows.n	et 🗙 💻 x23111984.mahes	shserrver2@x23111984.blob.core.windows.net 🗙 🍯	New Tab 🔹						
📲 My documents 🔹 🍯	- 🝸 - 🔤	🗕 • 🔶 • 📴 🔯 1	<u>ង</u> ធ 🐁		🛅 in 🛛 🕤 • 🟹 • 🔶 • 🔶 •	🗈 🕅	। 🏫 😋 🚊 Find Files 📍	-			
🛃 Upload 👻 📝 Edit 👻	× 🎿 🕞	Properties 👻 🞽 Nev	- 🛨 📰 🔽		🛃 Download 👻 📓 Edit 🔹 🗙 🚅 関	Properties	- 🎽 New - 📑 📰 💟	1			
C:\Users\Lenovo\Downloads\	Documents	Downloads\			/incoming/						
Name	Size		Changed		Name	Size	Changed	Rights	Owner		
<u>a</u>			11/14/2024 3:55:14 PM		testfile						
CA1_NSPT Report.pdf Final_CA1_NSPT Repor		Adobe Acrobat Do			testille	I KB	11/20/2024 7:01:53 PM				
testfile	1 KB		11/20/2024 7:01:53 PM								
0 B of 20.1 MB in 0 of 3					0 B of 102 B in 0 of 1						
										SFTP-3	0:00:28

-Logic App successfully triggered and after processing the file content is encoded during transit. Initially, the file Content of test file shown below:



Encoded Content:

"\$content": "dGVzdGluZyAtIHNlbmRpbmcgZmlsZSBmcm9tIG1haGVzaHNlcnZlcj EgdG8gbWFoZXNoc2VydmVyMiBhbmQgc2ltdWx0YW5lb3VzbHkgaW4gQVdTIF MzIGJ1Y2tldCBzZXJ2ZXIu"

Decode Content:

Testing - Sending file from maheshserver1 to maheshserver2 and simultaneously in AWS S3 bucket server.



-After processing, the file is in the destination (Outgoing) folder.

Microsoft Azure	∠ Search	resources, services, and docs (G+/)	0	Copilot 돈		x23111984@student.n NATIONAL COLLEGE OF IRELA	
Home > x23111984 Containers >							
x23111984container							×
₽ Search × «	↑ Upload + Add Directory 🖒 Refr	esh │ < <p>C Rename</p>	외 Acquire lease 🔗 Break l	lease 🕺 Give feedb	ack		
Overview	Authentication method: Access key (Switch	to Microsoft Entra user account)					
Diagnose and solve problems	Location: x23111984container / outgoing						
Access Control (IAM)	Search blobs by prefix (case-sensitive)				Show deleted ob	ojects	
✓ Settings							
Shared access tokens	Name	Modified Access tier	Archive status	Blob type	Size	Lease state	
R Manage ACL							
Access policy	🔄 📄 testfile	11/28/2024, 1:22:22 Hot (Inferred		Block blob	102 B	Available	
Properties							

4.2 Senario II

Across Clouds: From Azure to AWS S3 using Azure Functions and the AWS S3 client.

-Same test file has been dropped in an incoming folder.

				shserrver2@x23111984.blob.core.windows.net 🗙 🍯	New Tab 🔹						
📑 My documents 🛛 🝷 🖆	- 🗹 -	🔶 e 🔶 e 📩	n 🕄 🐁		<u>□in</u> • 📁 • 🝸 • 🔶 • → •	🔁 🔽	🏫 😋 🚊 Find Files 📍	-			
🛃 Upload 👻 📝 Edit 👻	🗙 🎿 🕞	Properties 👻 📑 Ner	N 🕶 📑 📰 🔽		📲 Download 👻 📓 Edit 🕶 🗙 🛃 📵		- 🎽 New - 📑 📰 🔽	1			
C:\Users\Lenovo\Downloads	\Documents	\Downloads\			/incoming/						
Name	Size	Туре	Changed		Name		Changed	Rights	Owner		
<u>a</u>			11/14/2024 3:55:14 PM		1						
CA1_NSPT Report.pdf		Adobe Acrobat Do			testfile	1 KB	11/20/2024 7:01:53 PM				
Final_CA1_NSPT Repor testfile	10,323 KB 1 KB		4/8/2024 1:46:32 AM 11/20/2024 7:01:53 PM								
testille	I KD	rile	11/20/2024 7.01:55 PM								
0 B of 20.1 MB in 0 of 3					0 B of 102 B in 0 of 1						
										SFTP-3	0:00:28

-Azure Logic App, Action - Azure Function App is triggered and invoked function – UploadToS3 as shown below.

=	Microsoft Azure		𝒫 Search reso	urces, services, and docs (G+/)	📀 Copilot	Σ	Ω	۲	?	R	x23111984@student.nci NATIONAL COLLEGE OF IRELAND
Home	> Function App > AzureToAWSFileTransf	er > UploadToS3									
Upl	oadToS3 Invocations										×
AzureTo	AWSFileTransfer										
Code	Code + Test Integration Function Keys Invocations Logs Metrics										
😰 Open in Application Insights 🕐 Refersth 🔗 Send us your feedback											
Query	20 of the most recent function invocation trac	ar. For more advanced	analyzic run the quer	via Apolication Invictor							
00102	o or the most recent function involution data	es. For more advanced	analysis, full the quer	ni Appicatori insigno.							
	ess count Error count										
⊘2	2 SO days Last 30 days										
LdSU	Last 50 days										
ء م	Search										
Date	Status	Result Code	Duration (ms)	Operation ID							
11/2	8/2024, 1:22:23 AM Success	200	1518	6dfad49d32e830bd25f80d6dffda47c8							

–After successfully processing the logic app, testfile uploaded to AWS S3 Bucket and Logic App sent confirmation email as shown below.

aws	Q Search	[Alt+S]	E L	🕽 🕜 😂 Stockholm 🔻	Mahesh Gavhane 🔻				
Ama	azon S3 > Buckets > my-fil	etransfer-bucket			() ₽ ©				
Amazo	on S3 <	my-filetransfer-bucket Info							
Buckets Access Gi Access Po		Objects Properties Permissions Metrics	Management Access Points						
Multi-Reg Batch Op	ambda Access Points gion Access Points perations sss Analyzer for S3	Objects (1) Info Copy S3 URI Copy S3 URI Solution Objects are the fundamental entities stored in Amazon S3. You can to explicitly orant them permissions. Learn more [2]		te folder Typload	cts, you'll need				
Block Pul this accor Storage Dashboar	Lens	C Find objects by prefix Name MarmeTorAWS-file txt	♥ Last modified ♥ Size November 28, 2024, 01:22:25 JUTC-00:00,	 ✓ Storage class 102.0 B Standard 	1 > ⊛ ⊽				
AWS Org	Lens groups panizations settings spotlight 8								
CloudSh	ell Feedback		© 2024, Amazon Web Services,	inc. or its affiliates. Privacy Term	s Cookie preferences				
	CONFIRMATIO	N!!! FILE SUCCESSFULLY UPLOADED TO	D YOUR AWS S3 BUCKET > Index ×	0	8 C				
	outlook_78AE45A299 to x23111984@student.ncirl	554011@outlook.com 624374mahesh@gmail.com <u>via</u> outlook.com ie, me ▼	n 12	2:15 PM (6 hours ago) 🔥 🕻	9 ← :				
	Hi Mahesh (X23111984) ,								
	We are pleased to inform you that your encrypted file - "Azure-To-AWS-file-uploaded-test.txt" with Id - "L2luY29taW5nL3Rlc3RmaWxlLmRlcg==" has been successfully uploaded to your AWS S3 bucket.								
	Thanks Azure Logic App								

-If Logic App terminates, send alert mail with subject line "Alert File Not Found".

ALERT !!! FILE NOT FOUND > Inbox ×				₽	ß
outlook_78AE45A299654011@outlook.com 624374mahesh@gmail.com <u>via</u> outlook.com to me ▼	12:22 PM (4 hours ago)	☆	٢	¢	:
Hi Mahesh,					
Mert!!! There is no file present in sftp server (maheshserver1) that contains "testfile".					
Thanks					
Logic App					

After processing the file successfully and capturing the log, generate the graphs for Visualization using PROM Tool and Jupyter Notebook as mentioned in Step 3.