

Region: N. Virginia

Select Create Bucket

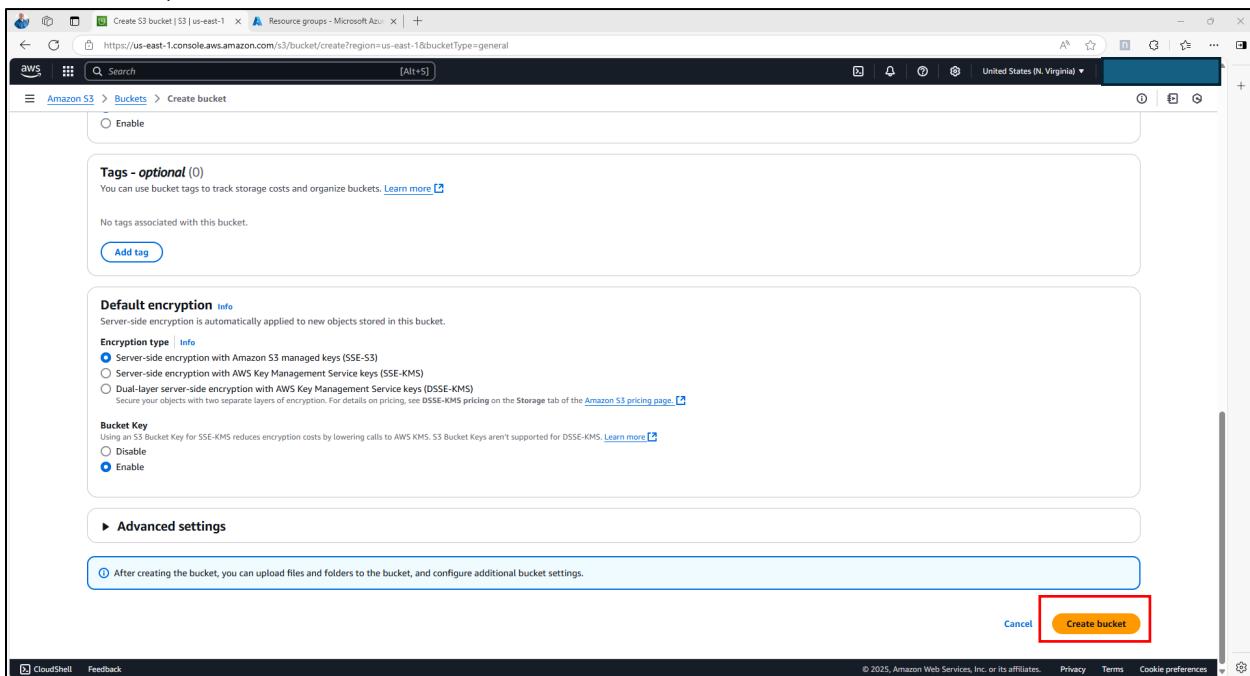
The screenshot shows the 'Amazon S3' landing page. At the top right, the region 'United States (N. Virginia)' is selected. On the right side, there's a 'Create a bucket' button. Below it, sections for 'Pricing' and 'Resources' are visible. In the center, there's a video player titled 'Introduction to Amazon S3' with the URL 'aws.amazon.com/S3'. To the left, a 'How it works' section is shown.

Bucket Type: General Purpose

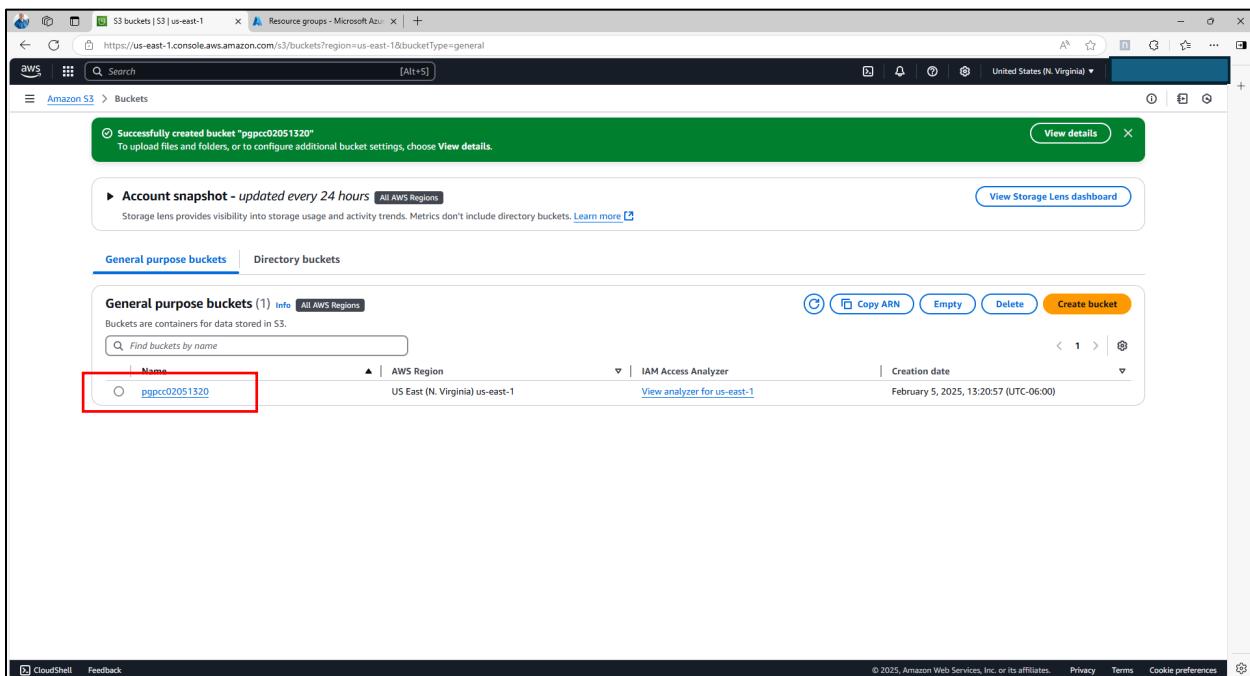
Bucket Name: pgpcc02051320

The screenshot shows the 'Create bucket' configuration page. The 'General configuration' section is highlighted with a red box. It includes fields for 'Bucket type' (set to 'General purpose'), 'Bucket name' (set to 'pgpcc02051320'), and 'Copy settings from existing bucket - optional'. The 'Object Ownership' and 'Block Public Access settings for this bucket' sections are also partially visible at the bottom.

Scroll down, select Create Bucket



Bucket created



IAM Dashboard, select Policies

The screenshot shows the AWS IAM Dashboard. On the left sidebar, under 'Access management', the 'Policies' option is selected and highlighted with a red box. The main content area displays various sections: 'Security recommendations', 'IAM resources' (with counts for User groups, Users, Roles, Policies, and Identity providers), 'What's new' (listing recent changes like RCPs and AWS IAM supports Privatelink), and 'AWS Account' and 'Quick Links' sections. The bottom right corner includes links for 'Security best practices in IAM', 'IAM documentation', and 'Videos, blog posts, and additional resources'.

Select Create Policy

The screenshot shows the 'Policies' page in the AWS IAM console. The 'Policies' section title is at the top, followed by a description: 'A policy is an object in AWS that defines permissions.' Below this is a search bar and a 'Filter by Type' dropdown set to 'All types'. A table lists 1324 policies, each with a checkbox, a preview icon, a name, a type (e.g., AWS managed, Permissions policy), and a 'Used as' field. The first few entries include 'AccessAnalyzerServiceRolePolicy', 'AdministratorAccess', and 'AdministratorAccess-Amplify'. At the top right of the table, there are 'Actions' and 'Delete' buttons, and a prominent orange 'Create policy' button is highlighted with a red box. The bottom right corner includes links for 'Security best practices in IAM', 'IAM documentation', and 'Videos, blog posts, and additional resources'.

Policy Editor: Visual

Select a service: S3

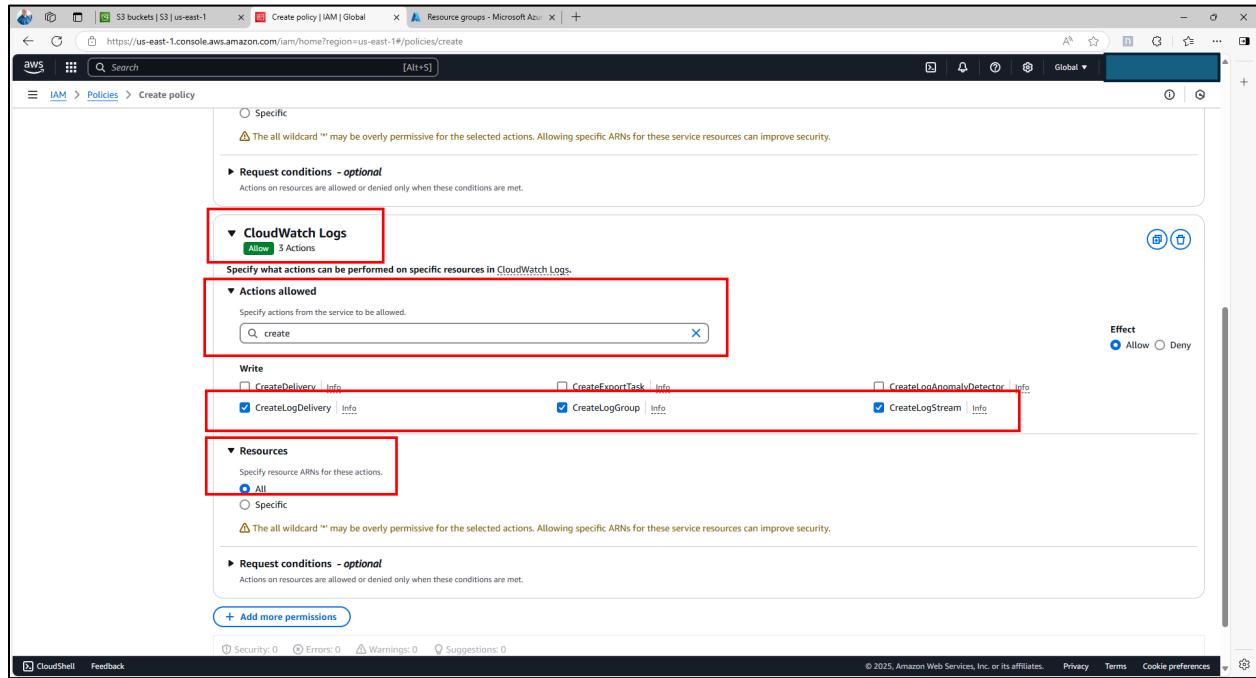
Actions Allowed: **GetObject**, select **Read** checkbox next to **GetObject**

Resources: All

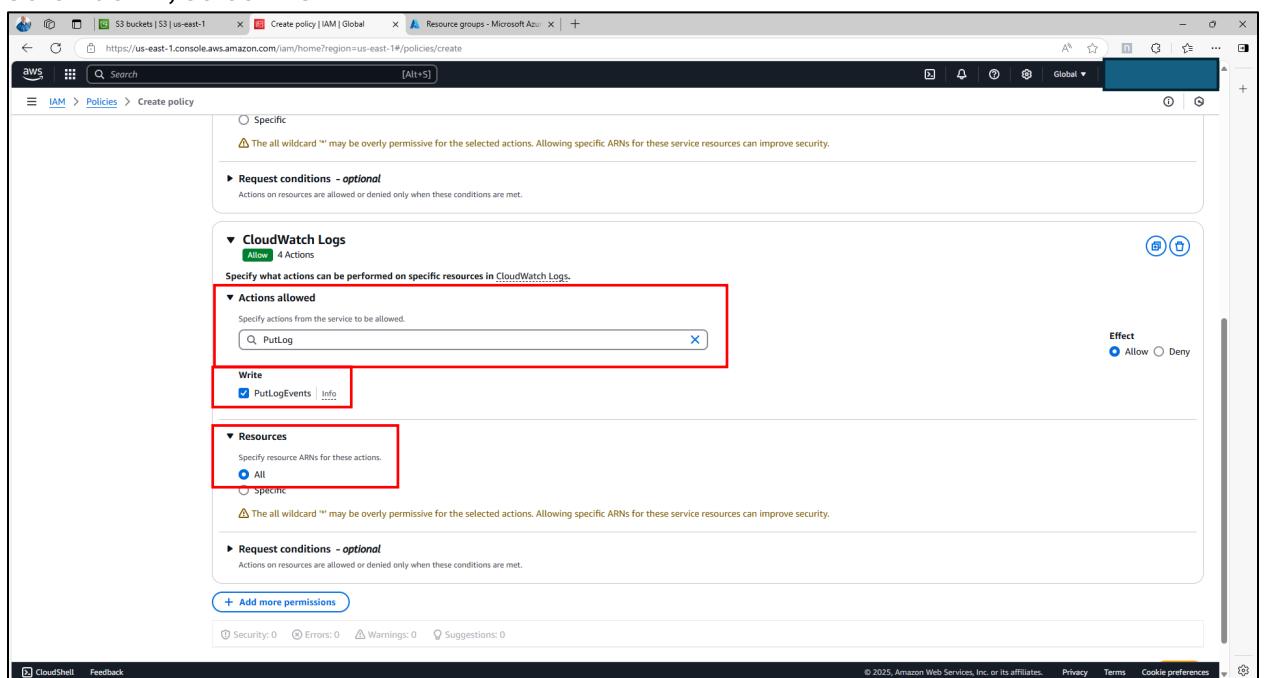
Scroll down, select +Add more permissions

The screenshot shows the AWS IAM 'Create policy' interface. The 'Visual' tab is highlighted with a red box. The 'S3' service is selected, and the 'GetObject' action is chosen under the 'Read' section. The 'Effect' dropdown shows 'Allow'. The 'Resources' section is set to 'All'. The bottom right corner of the interface shows the copyright notice: '© 2025, Amazon Web Services, Inc. or its affiliates.'

- Select a service, **CloudWatch Logs**
- Actions allowed, enter **Create and select CreateLogDelivery, CreateLogGroup, CreateLogStream**
- Resources: **All**



- Clear Actions Allowed, enter **PutLog**
- Select checkbox next to **PutLogEvents**
- Resources, Select **All**
- Scroll down, select **Next**



Policy Details, enter Policy name **MultiCloudPolicyAWSandAzure** Select Create Policy

Policy details

Policy name
Enter a meaningful name to identify this policy.
 Maximum 128 characters. Use alphanumeric and '-' characters.

Description - optional
Add a short explanation for this policy.

Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it.

Service	Access level	Resource	Request condition
CloudWatch Logs	Limited: Write	All resources	None
S3	Limited: Read	All resources	None

Add tags - optional Info

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

[Add new tag](#)

You can add up to 50 more tags.

[Cancel](#) [Previous](#) **Create policy** [Next](#) [Finish](#)

Select Roles

Policies (1325) Info

A policy is an object in AWS that defines permissions.

Filter by Type

Policy name	Type	Used as	Description
AccessAnalyzerServiceRolePolicy	AWS managed	None	Allow Access Analyzer to analyze resou...
AdministratorAccess	AWS managed - job function	Permissions policy (2)	Provides full access to AWS services an...
AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permis...
AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permiss...
AIOpsAssistantPolicy	AWS managed	None	Provides ReadOnly permissions requir...
AIOpsConsoleAdminPolicy	AWS managed	None	Grants full access to Amazon AI Opera...
AIOpsOperatorAccess	AWS managed	None	Grants access to the Amazon AI Opera...
AIOpsReadOnlyAccess	AWS managed	None	Grants ReadOnly permissions to the A...
AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaFo...
AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness ...
AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to A...
AlexaForBusinessLifesizeDelegatedAccessPolicy	AWS managed	None	Provide access to Lifesize AVS devices
AlexaForBusinessNetworkProfileServicePolicy	AWS managed	None	This policy enables Alexa for Business ...
AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForB...

[View policy](#) [Actions](#) [Delete](#) **Create policy**

Select Create role

The screenshot shows the AWS IAM Roles page. On the left, there's a sidebar with 'Identity and Access Management (IAM)' selected. The main area displays a table of existing roles, each with a 'Delete' button and an orange 'Create role' button at the top right. The table includes columns for Role name, Trusted entities, and Last activity.

- Under Trusted entity type, select **AWS Service**
- Use Case, Service or Use Case, enter **Lambda**
- Select **Next**

The screenshot shows the 'Select trusted entity' step of the IAM role creation wizard. It has three tabs: Step 1 (selected), Step 2, and Step 3. The 'Trusted entity type' section contains four options: 'AWS service' (selected and highlighted with a red box), 'AWS account', 'Web identity', and 'SAML 2.0 federation'. Below this is the 'Use case' section, which contains a dropdown menu set to 'Lambda' (also highlighted with a red box). At the bottom right are 'Cancel' and 'Next' buttons, with 'Next' also highlighted with a red box.

- Permissions policies, enter policy name created earlier, **MultiCloudPolicyAWSandAzure**
- Select checkbox next to **MultiCloudPolicyAWSandAzure**
- Select **Next**

The screenshot shows the 'Add permissions' step of creating a new IAM role. The search bar at the top has 'Multi' typed into it. A list of policies is shown, with one policy, 'MultiCloudPolicyAWSandAzure', highlighted with a blue border and checked. At the bottom right of the screen, there is a red box around the 'Next' button.

Role name, enter **MultiCloudAWSandAzure**

The screenshot shows the 'Name, review, and create' step of creating a new IAM role. The 'Role name' input field contains 'MultiCloudAWSandAzure' and is highlighted with a red box. Below the input field is a 'Description' section with a short explanatory text. At the bottom right of the screen, there is a red box around the 'Edit' button.

- Scroll down, ensure Policy name is **MultiCloudPolicyAWSandAzure** is under **Permissions policy summary**
- Select **Create role**

The screenshot shows the AWS IAM 'Create role' wizard. Step 2: Add permissions. In the 'Permissions policy summary' section, the 'Policy name' dropdown is set to 'MultiCloudPolicyAWSandAzure'. The 'Create role' button at the bottom right is highlighted with a red box.

From Microsoft Azure portal, select **+Create** to create a Resource Group

The screenshot shows the Microsoft Azure portal 'Resource groups' page. The '+ Create' button is highlighted with a red box. The page displays a list of existing resource groups, each with a checkbox, a blue square icon, and a name like 'redacted'. The 'Subscription' and 'Location' columns are also visible.

Choose Subscription

Enter Resource group name, **AWSandAzureMultiCloud**

Select **Review + Create**

Screenshot of the Microsoft Azure 'Create a resource group' Basics step. The 'Resource group name' field contains 'AWSandAzureMultiCloud'. The 'Region' dropdown is set to '(US) East US'. The 'Review + create' button at the bottom is highlighted with a red box.

Select Create

Screenshot of the Microsoft Azure 'Create a resource group' Review + Create step. The 'Resource group name' field shows 'AWSandAzureMultiCloud' and the 'Region' field shows 'East US'. The 'Create' button at the bottom is highlighted with a red box.

Select **AWSandAzureMultiCloud** Resource Group

Resource groups

Name	Subscription	Location
AWSandAzureMultiCloud	East US	East US
[Redacted]	East US	East US
[Redacted]	East US	East US

< Previous Page 1 of 1 Next >

Select +Create

The screenshot shows the Microsoft Azure portal interface. The top navigation bar includes links for S3 buckets, Roles, IAM, AWSAndAzureMultiCloud, and Copilot. The main title is 'AWSAndAzureMultiCloud - Microsoft Azure'. The left sidebar shows 'Resource groups' with a list of existing groups and a '+ Create' button. The main content area is titled 'AWSAndAzureMultiCloud' and shows the 'Essentials' tab selected. It displays information like Subscription (move), Subscription ID, Tags, Deployments (No deployments), and Location (East US). Below this is the 'Resources' section, which is currently empty as indicated by the message 'No resources match your filters'. There are filter options for Name, Type, and Location, along with buttons for 'Create resources' and 'Clear filters'. The bottom of the screen shows a page navigation bar with 'Page 1 of 1'.

Enter Storage Account, select Create under Storage Account

New! Get AI-generated suggestions for your search.
Ask AI to suggest products, articles, and solutions for what you need.

storage account

Pricing : All × Operating System : All × Publisher Type : All × Product Type : All × Publisher name : All ×

Showing 1 to 20 of 221 results for 'storage account'. Clear search

Preview	Name	Provider	Description	Price	Create
	Storage Account Using ARM	DIGISTORM LTD.	Azure Application storage account arm	Price varies	Create
	Storage account	Microsoft	Azure Service Use Blob, Tables, Queues, Files, and Data Lake Gen 2 for reliable, economical cloud storage.	Price varies	Create
	Storage Account Using ARM Template	VIRTUCLLOUD LTD.	Azure Application storage account arm template	Price varies	Create
	Storage Account Using ARM Template	CloudGate LLC	Azure Application storage account arm template	Price varies	Create
	Storage task - Azure Storage Actions	Microsoft	Azure Service Perform common operations on millions of objects based on logical conditions using object properties for Blob and Data Lake Storage Gen2.	Price varies	Create
	Azure Storage Mover	Microsoft	Azure Storage solution for Sentinel	Price varies	Create
	Blob Storage Digests Backed by Confidential Ledger	Azure Confidential Ledger	Spin Systems Inc	Price varies	Create
	RamSoft Image Storage	RamSoft Inc.	Flexify Inc.	Price varies	Create
	S3 API for Azure Blob Storage (Flexify.IO)	Flexify Inc.		Price varies	Create

Select Create

Storage account

Microsoft

Storage account Add to Favorites

Microsoft | Azure Service

★ 4.3 (1883 ratings)

Plan

Storage account **Create**

Overview Plans Usage Information + Support Ratings + Reviews

Microsoft Azure provides scalable, durable cloud storage, backup, and recovery solutions for any data, big or small. It works with the infrastructure you already have to cost-effectively enhance your existing applications and business continuity strategy, and provide the storage required by your cloud applications, including unstructured text or binary data such as video, audio, and images.

More products from Microsoft [See All](#)

Active Directory Health Check Microsoft Azure Service Assess the risk and health of Active Directory environments.	AD Replication Status Microsoft Azure Service Identify Active Directory replication issues in your environment.	Device Update for IoT Hub Microsoft Azure Service Securely and Reliably update your devices with Device Update for IoT Hub.	Front Door and CDN profiles Microsoft Azure Service Azure Front Door and CDN profiles is a security-led, modern cloud CDN that provides static and dynamic content acceleration, global load balancing and enhanced security for your apps.

- Ensure Subscription and ResourceGroup is selected
- Storage Account Name, enter **awsandazuremulticloud**
- Performance, select **Standard**
- Redundancy, select **Locally-redundant storage (LRS)**
- Select **Review + Create**

Create a storage account

Basics **Advanced** **Networking** **Data protection** **Encryption** **Tags** **Review + create**

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](#)

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.

Subscription * (selected)

Resource group * AWSAndAzureMultiCloud [Create new](#)

Instance details

Storage account name * awsandazuremulticloud

Region * (US) East US [Deploy to an Azure Extended Zone](#)

Primary service Select a primary service

Performance * Standard: Recommended for most scenarios (general-purpose v2 account) Premium: Recommended for scenarios that require low latency.

Redundancy * Locally-redundant storage (LRS)

[Previous](#) [Next](#) **Review + create** [Give feedback](#)

Select Create

Create a storage account

Basics **Advanced** **Networking** **Data protection** **Encryption** **Tags** **Review + create**

[View automation template](#)

Basics

Subscription	<input type="text"/>
Resource group	AWSAndAzureMultiCloud
Location	East US
Storage account name	awsandazuremulticloud
Primary service	Standard
Performance	Locally-redundant storage (LRS)

Advanced

Enable hierarchical namespace	Disabled
Enable SFTP	Disabled
Enable network file system v3	Disabled
Allow cross-tenant replication	Disabled
Access tier	Hot
Enable large file shares	Enabled

Security

Secure transfer	Enabled
Blob anonymous access	Disabled
Allow storage account key access	Enabled

[Previous](#) [Next](#) **Create** [Give feedback](#)

Select Go to resource

The screenshot shows the Microsoft Azure Deployment Overview page for a deployment named "awsandazuremulticloud_1738785866015". The status is "Your deployment is complete". A "Deployment details" section shows the deployment name, subscription, and resource group. Below it, under "Next steps", there is a "Go to resource" button, which is highlighted with a red box. To the right of the main content area, there are several promotional cards: "Cost Management", "Microsoft Defender for Cloud", "Free Microsoft tutorials", and "Work with an expert".

Expand Data Storage Select Containers

The screenshot shows the Microsoft Azure Storage account overview page for "awsandazuremulticloud". The left sidebar has a "Data storage" section with a "Containers" item, which is highlighted with a red box. The main content area displays the storage account's configuration, including sections for "Essentials", "Properties", "Blob service", "File service", and "Networking".

Essentials	
Resource group (move)	: AWSandAzureMultiCloud
Location	: eastus
Subscription (move)	: [REDACTED]
Subscription ID	: [REDACTED]
Disk state	: Available
Tags (edit)	: Add tags

Properties	
Performance	: Standard
Replication	: Locally-redundant storage (LRS)
Account kind	: StorageV2 (general purpose v2)
Provisioning state	: Succeeded
Created	: 2/5/2025, 2:05:47 PM

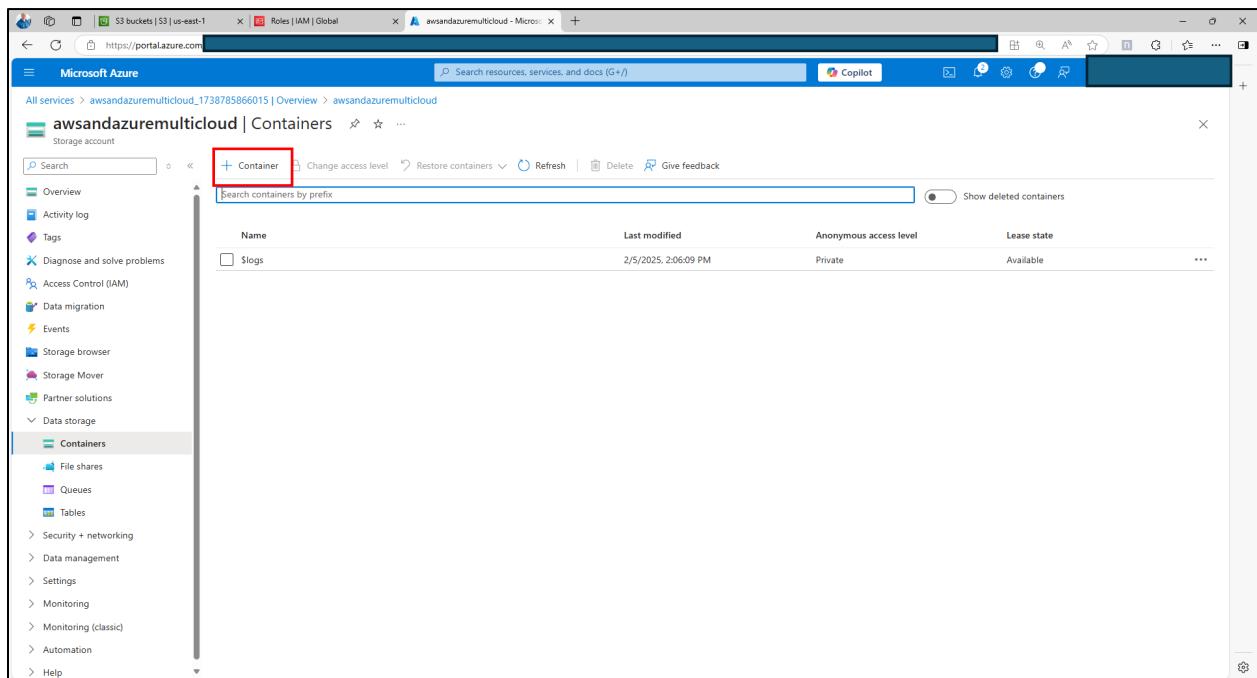
Blob service	
Hierarchical namespace	: Disabled
Default access tier	: Hot
Blob anonymous access	: Disabled
Blob soft delete	: Enabled (7 days)
Container soft delete	: Enabled (7 days)
Versioning	: Disabled
Change feed	: Disabled
NFS v3	: Disabled
Allow cross-tenant replication	: Disabled
Storage tasks assignments	: None

File service	
Large file share	: Enabled
Identity-based access	: Not configured

Security	
Require secure transfer for REST API operations	: Enabled
Storage account key access	: Enabled
Minimum TLS version	: Version 1.2
Infrastructure encryption	: Disabled

Networking	
Allow access from	: All networks
Private endpoint connections	: 0
Network routing	: Microsoft network routing
Access for trusted Microsoft services	: Yes
Endpoint type	: Standard

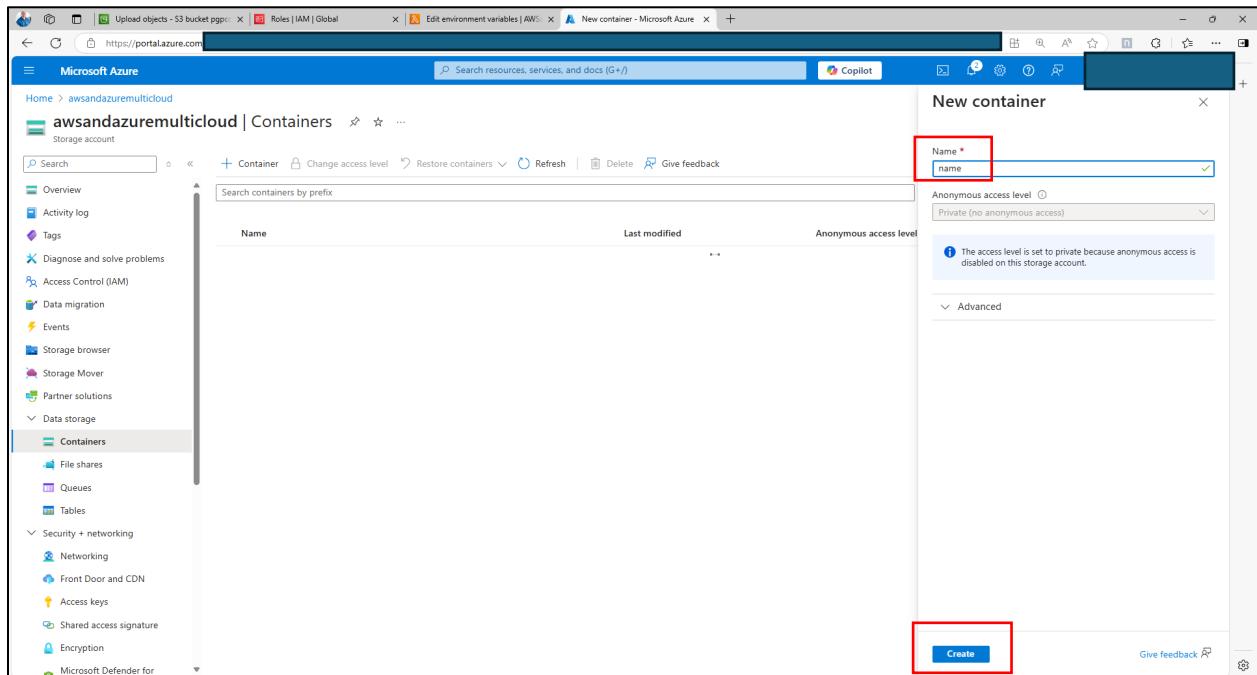
Select +Container



The screenshot shows the Microsoft Azure Storage account interface. On the left, there's a sidebar with various storage-related options like Overview, Activity log, Tags, Diagnose and solve problems, Access Control (IAM), Data migration, Events, Storage browser, Storage Mover, Partner solutions, and Data storage. Under Data storage, 'Containers' is selected. In the main pane, there's a table showing one container named 'Logs'. At the top of the main area, there's a search bar and a '+ Container' button, which is highlighted with a red box. Other buttons include 'Change access level', 'Restore containers', 'Refresh', 'Delete', and 'Give feedback'.

Name, enter name

Select Create



This screenshot shows the 'New container' dialog box overlaid on the Azure Storage account interface. The dialog has fields for 'Name' (with 'name' typed in) and 'Anonymous access level' (set to 'Private (no anonymous access)'). There's also an 'Advanced' section with a note about anonymous access being disabled. At the bottom right of the dialog, there's a large blue 'Create' button, which is highlighted with a red box. The background shows the same storage account interface as the previous screenshot.

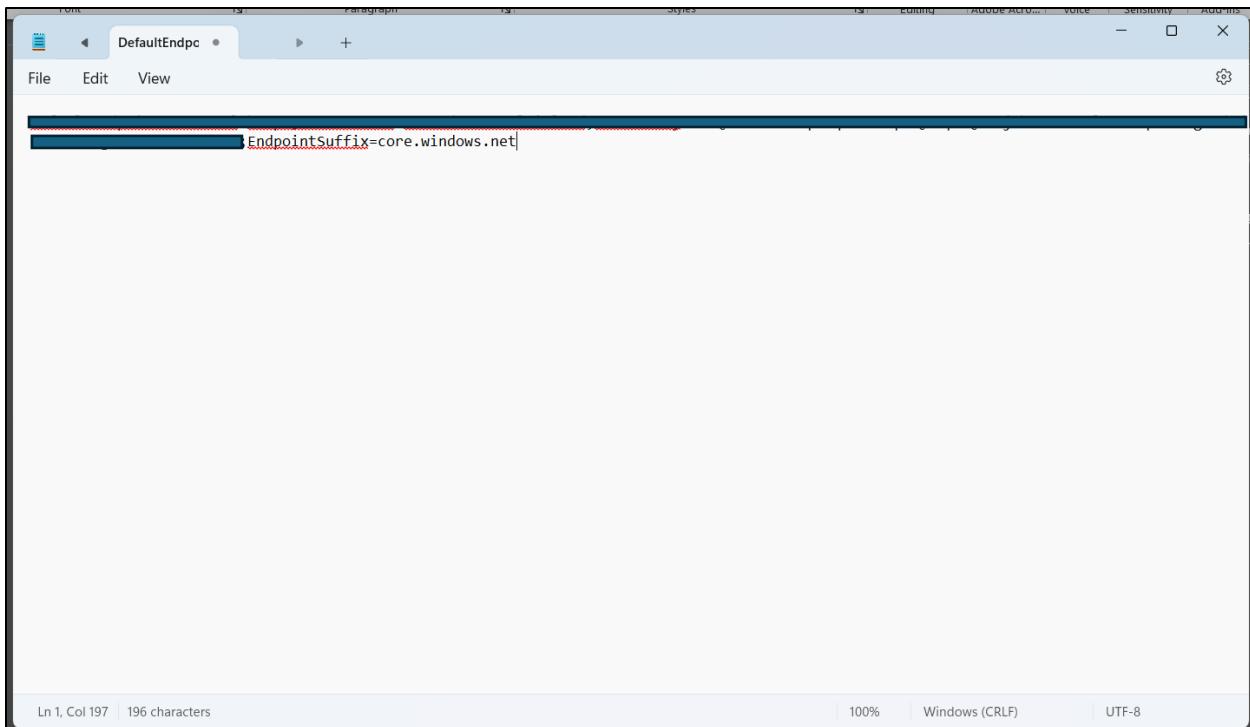
After **name** is created, expand **Security + networking**

Select **Access keys**

The screenshot shows the Microsoft Azure portal interface. The left sidebar navigation includes 'Overview', 'Activity log', 'Tags', 'Diagnose and solve problems', 'Access Control (IAM)', 'Data migration', 'Events', 'Storage browser', 'Storage Mover', 'Partner solutions', 'Data storage' (with 'Containers' selected), 'File shares', 'Queues', 'Tables', 'Security + networking' (with 'Access keys' highlighted by a red box), 'Networking', 'Front Door and CDN', 'Shared access signature', 'Encryption', and 'Microsoft Defender for Cloud'. The main content area displays a table of containers with columns for Name, Last modified, Anonymous access level, and Lease state. Two containers are listed: 'Logs' and 'name'. Both are private and available.

Under key1, **Connection string**, select **Show** and copy the Connection string in a Notepad

The screenshot shows the Microsoft Azure portal interface under the 'Access keys' section of a storage account. It displays two sets of access keys: 'key1' and 'key2'. For 'key1', the 'Connection string' field is highlighted with a red box. The 'Show' button next to it is also highlighted. The 'key2' section is partially visible below it. The left sidebar is identical to the previous screenshot, showing the 'Access keys' option selected.



Open Lambda console, expand left panel and select **Layers** under **Additional Resources**
Ensure **N. Virginia** is selected for Region

A screenshot of the AWS Lambda console in a web browser. The left sidebar shows "Lambda" with sections for "Dashboard", "Applications", "Functions", "Additional resources" (with "Layers" highlighted by a red box), "Event source mappings", and "Related AWS resources". The main content area displays the "Compute" section for AWS Lambda, featuring the heading "lets you run code without thinking about servers." and a "Get started" button. A red box highlights the "United States (N. Virginia)" dropdown menu in the top right corner. The bottom of the page includes standard AWS footer links like CloudShell, Feedback, Privacy, Terms, and Cookie preferences.

Select Create layer

The screenshot shows the AWS Lambda Layers page. A green success message at the top states: "The version 1 of your Lambda layer 'AWSandAzureMultiCloud' was successfully deleted." Below this, there is a table header for "Layers (0)" with columns: Name, Version, Description, Compatible runtimes, Compatible architectures, and Created. A note below the table says "There is no data to display." On the right side of the table, there is a yellow "Create layer" button. The left sidebar includes sections for Lambda Dashboard, Applications, Functions, Additional resources (Code signing configurations, Event source mappings, Layers, Replicas), and Related AWS resources (Step Functions state machines). The bottom of the page includes CloudShell, Feedback, and standard footer links.

- Enter name as **AWSAzureMultiCloud**
- Select **Choose File**
- Upload **S3azurelayer.zip** (provided by exercise)
- Compatible architectures, select **x86_64**
- Compatible runtimes, select **Python 3.9**
- Select **Create**

The screenshot shows the "Create layer" wizard. The first step, "Successfully created layer AWSAzureMultiCloud version 1.", is completed. The configuration fields are as follows:

- Name:** AWSAzureMultiCloud (highlighted with a red box)
- Description - optional:** (empty field)
- Upload a zip file:** (radio button selected) (highlighted with a red box)
 - Choose file: (button) (highlighted with a red box)
 - s3azurerulelayer.zip (7.31 MB) (highlighted with a red box)
 - For files larger than 10 MB, consider uploading using Amazon S3.
- Compatible architectures - optional:** (info) (highlighted with a red box)
 - x86_64 (highlighted with a red box)
- Compatible runtimes - optional:** (info) (highlighted with a red box)
 - Python 3.9 (highlighted with a red box)
- License - optional:** (info) (highlighted with a red box)

Under Lambda, select Functions

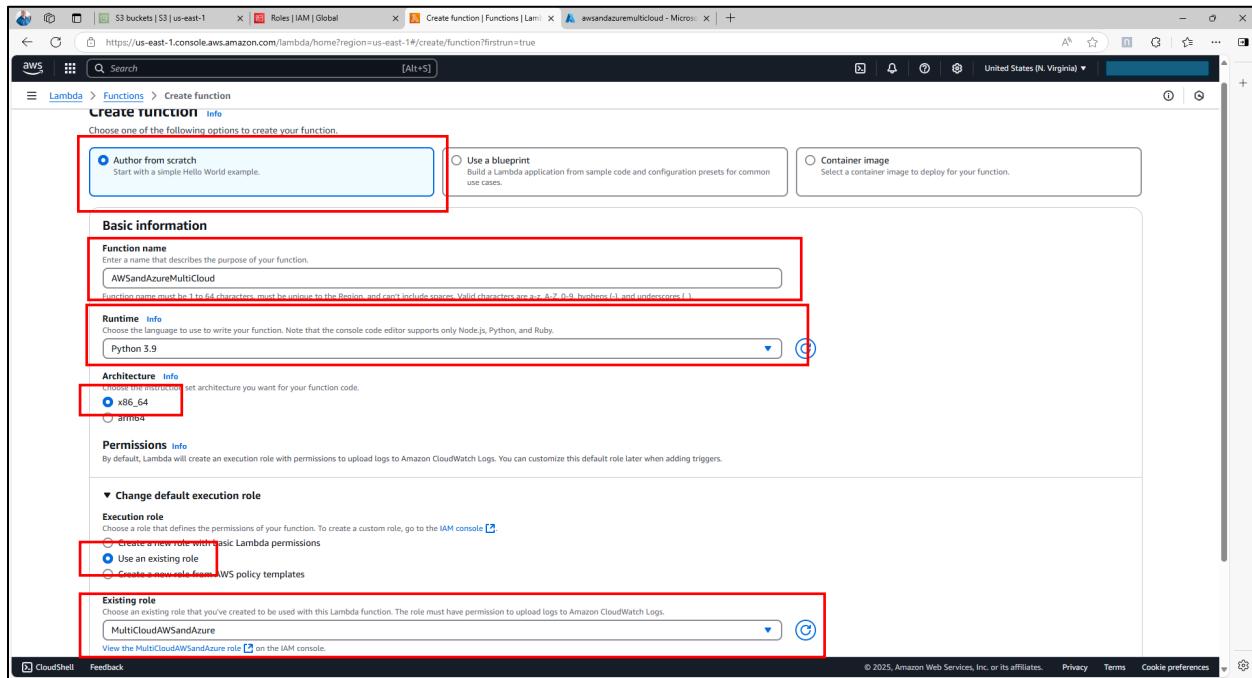
The screenshot shows the AWS Lambda Layers page. On the left, there's a navigation sidebar with 'Lambda' selected under 'Functions'. The main area displays a table titled 'Layers (1)'. The table has columns for Name, Version, Description, Compatible runtimes, Compatible architectures, and Created. One row is visible: 'AWSAzureMultiCloud' (Version 2), compatible with 'python3.9', 'x86_64', and was created '48 seconds ago'. A red box highlights the 'Functions' link in the sidebar.

Select Create function

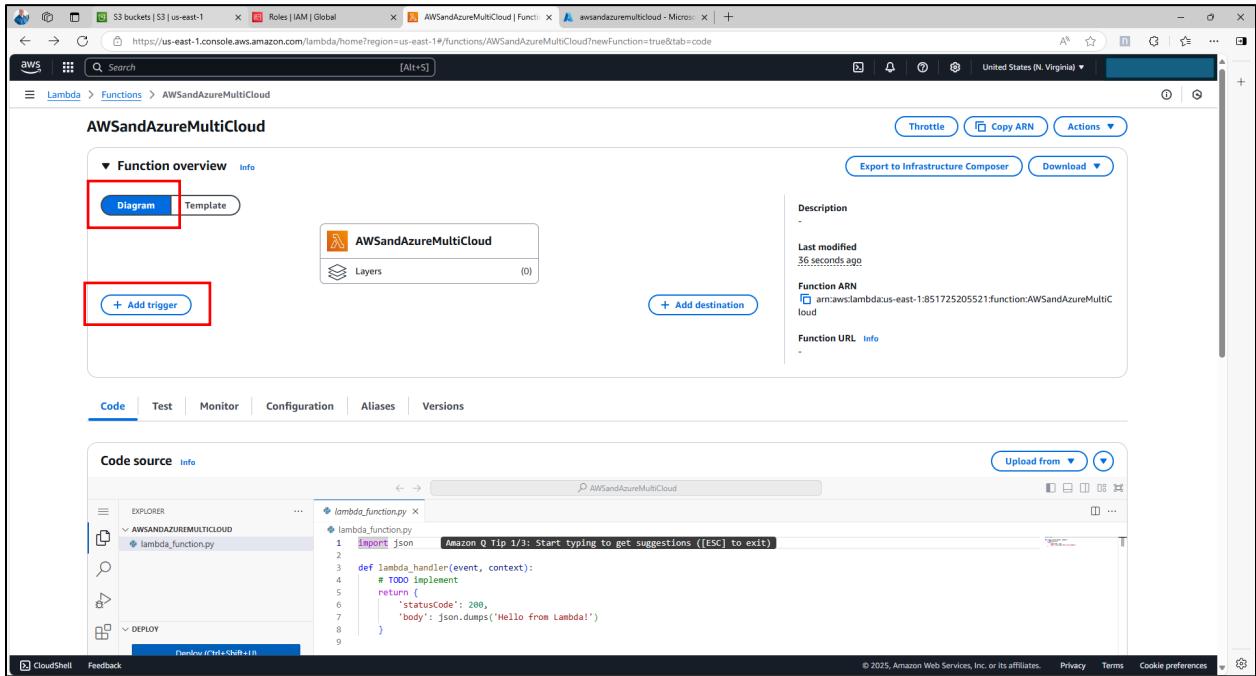
The screenshot shows the AWS Lambda landing page. It features a dark header with the AWS logo and a 'Compute' dropdown. Below the header, there's a large 'AWS Lambda' heading with the tagline 'lets you run code without thinking about servers.' A 'Get started' callout box contains the text 'Author a Lambda function from scratch, or choose from one of many preconfigured examples.' A red box highlights the 'Create a function' button. At the bottom, there's a 'How it works' section with tabs for '.NET', 'Java', 'Node.js' (selected), 'Python', 'Ruby', and 'Custom runtime'. A code snippet for Node.js is shown:

```
1* exports.handler = async (event) => {
2  console.log(event);
3  return 'Hello from Lambda!';
4};
```

- Select **Author from scratch**
- Enter Function name **AWSandAzureMultiCloud**
- Runtime: **Python 3.9**
- Architecture: **x86_64**
- Execution role, select dropdown and select existing role created earlier: **MultiCloudAWSandAzure**
- Scroll down and select **Create Function**

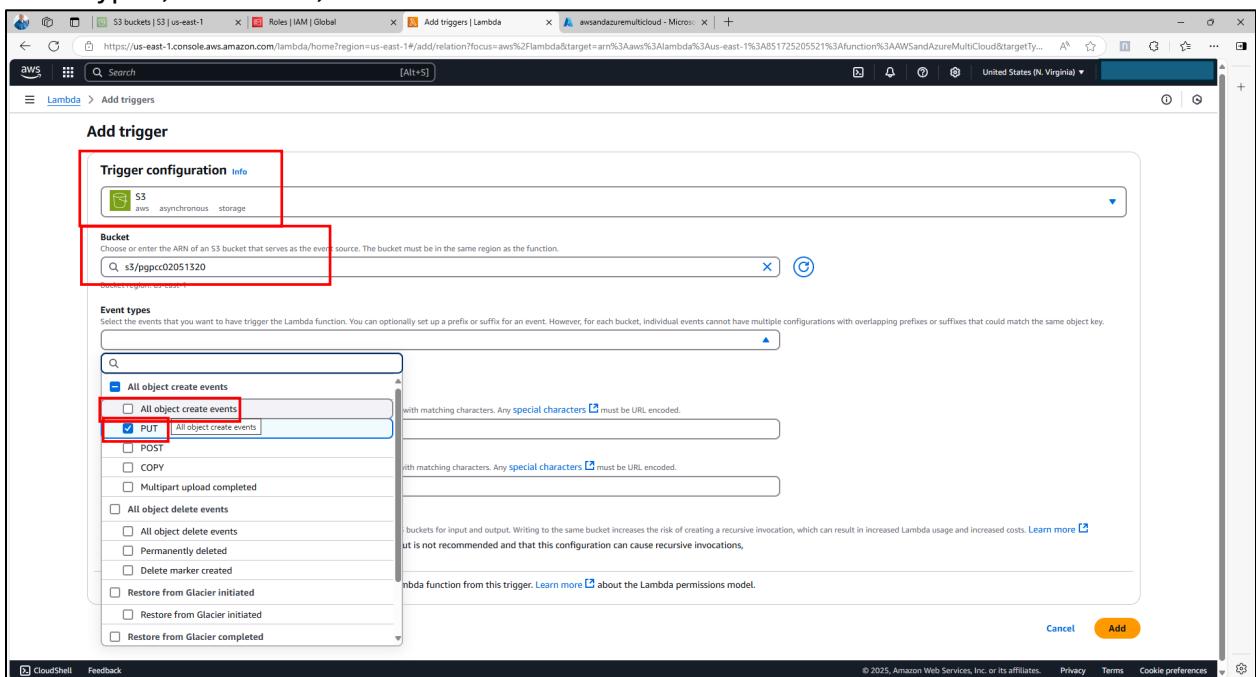


Ensure **Diagram** is selected
Select + Add trigger



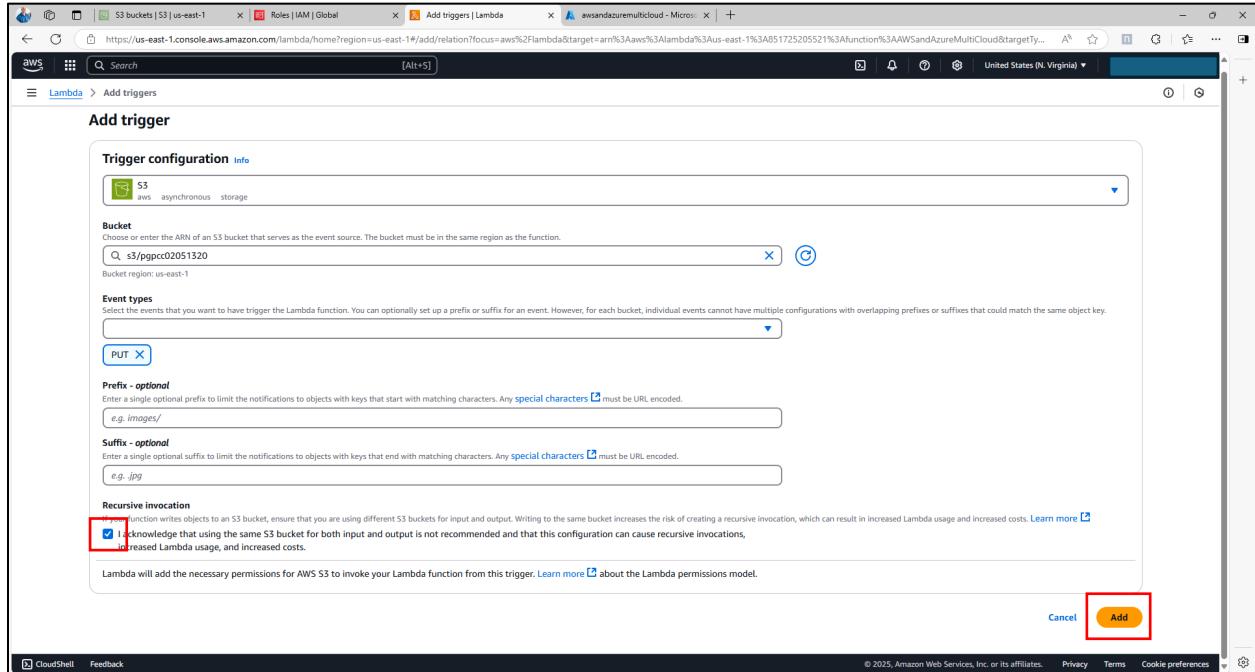
The screenshot shows the AWS Lambda Functions interface. In the top navigation bar, the path is 'Lambda > Functions > AWSandAzureMultiCloud'. The main area displays the 'Function overview' section. A red box highlights the 'Diagram' tab under 'Function overview' and another red box highlights the '+ Add trigger' button below it. To the right, there's a description panel with fields like 'Last modified 36 seconds ago', 'Function ARN', and 'Function URL'. Below the overview, tabs for 'Code', 'Test', 'Monitor', 'Configuration', 'Aliases', and 'Versions' are visible.

Trigger configuration, select S3
Bucket, select bucket created earlier titled **pgpcc02051320**
Event types, select **Put**, deselect **All**

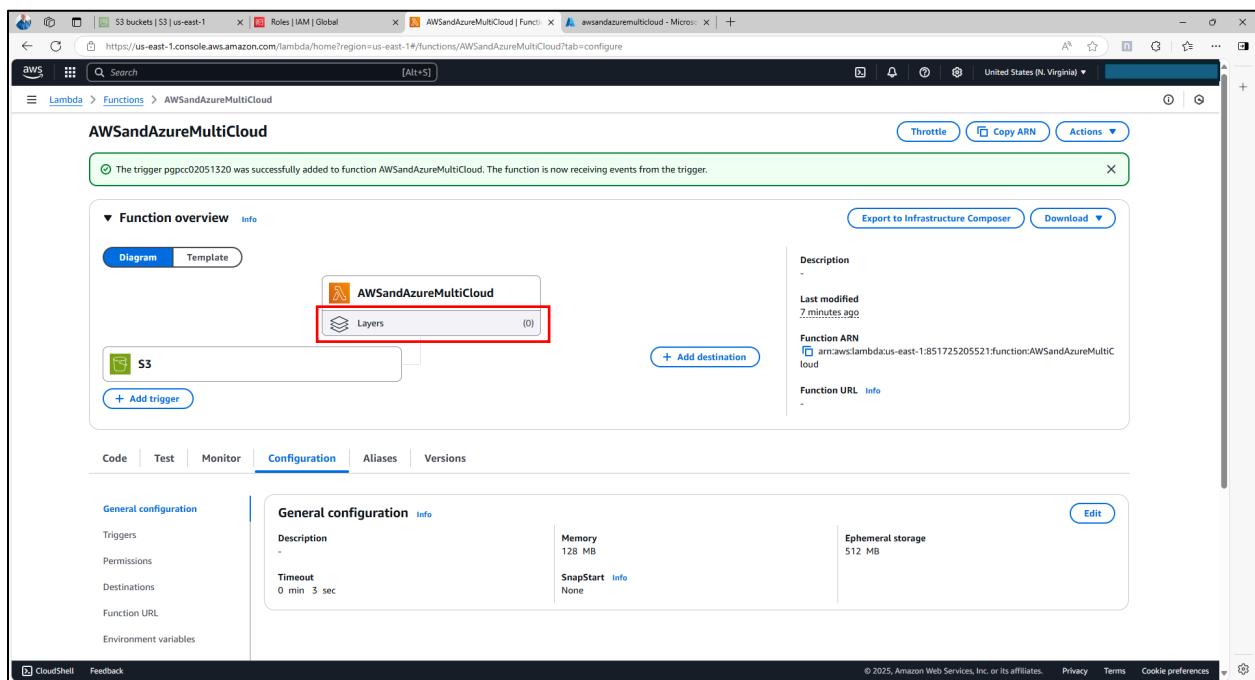


The screenshot shows the 'Add trigger' dialog box. Under 'Trigger configuration', 'S3' is selected. In the 'Bucket' field, 's3/pgpcc02051320' is entered. The 'Event types' section lists various events. 'All object create events' is expanded, showing 'PUT' selected (with a red box) and 'All object create events' deselected (with a red box). Other event types listed include POST, COPY, Multipart upload completed, All object delete events, All object delete events, Permanently deleted, Delete marker created, Restore from Glacier initiated, Restore from Glacier initiated, and Restore from Glacier completed.

- Select checkbox next to **I acknowledge that using the same S3 bucket for both input and output is not recommended and that this configuration can cause recursive invocations, increased Lambda usage, and increased costs.**
- Select **Add**



Select Layers under Function name **AWSandAzureMultiCloud**



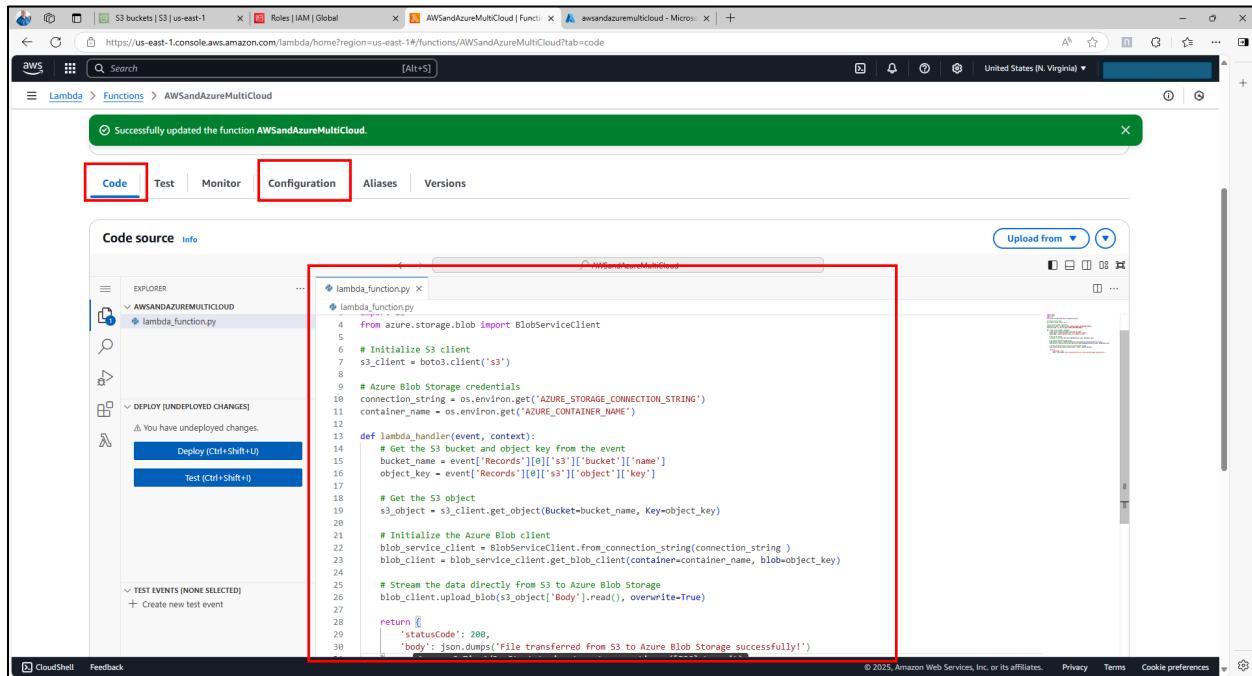
Scroll down and select **Add a layer** under **Layers** section

The screenshot shows the AWS Lambda function configuration page for 'AWSandAzureMultiCloud'. In the 'Layers' section, the 'Add a layer' button is highlighted with a red box.

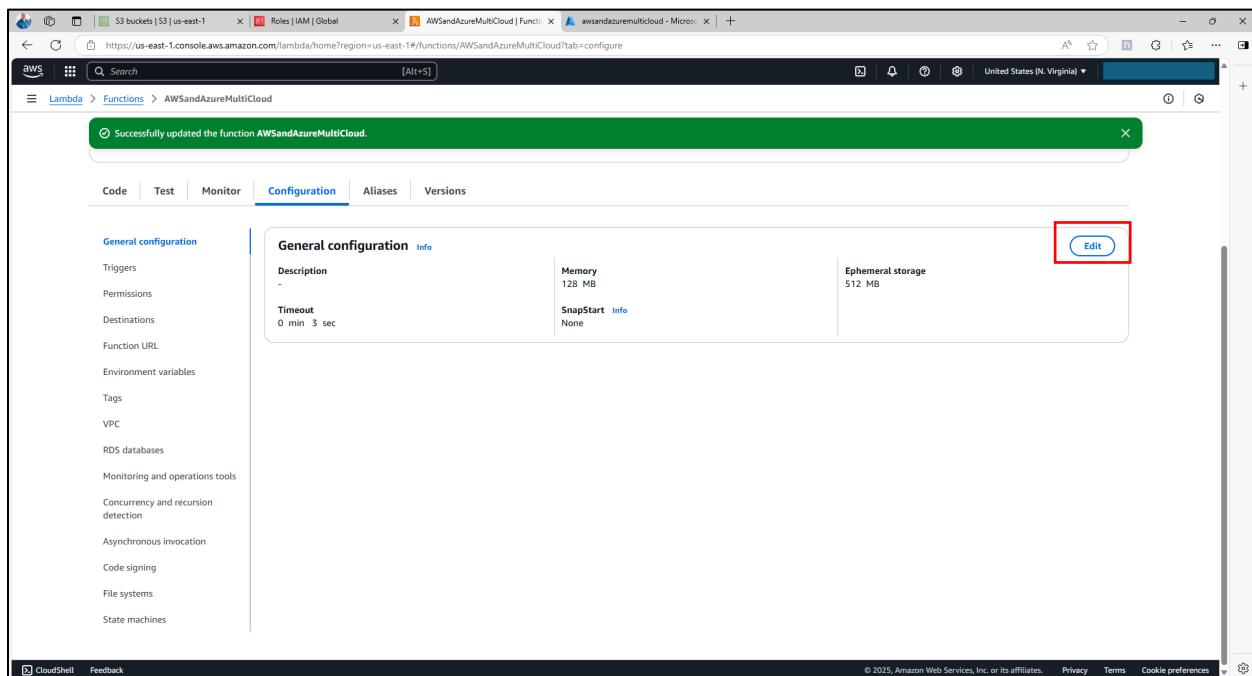
- Choose a layer, select **Custom Layers**
- Custom Layers, select **AWSandAzureMultiCloud**
- Version, select **2** (latest version)
- Select **Add**

The screenshot shows the 'Add layer' dialog box. The 'Custom layers' section is highlighted with a red box, and the 'Add' button is also highlighted with a red box.

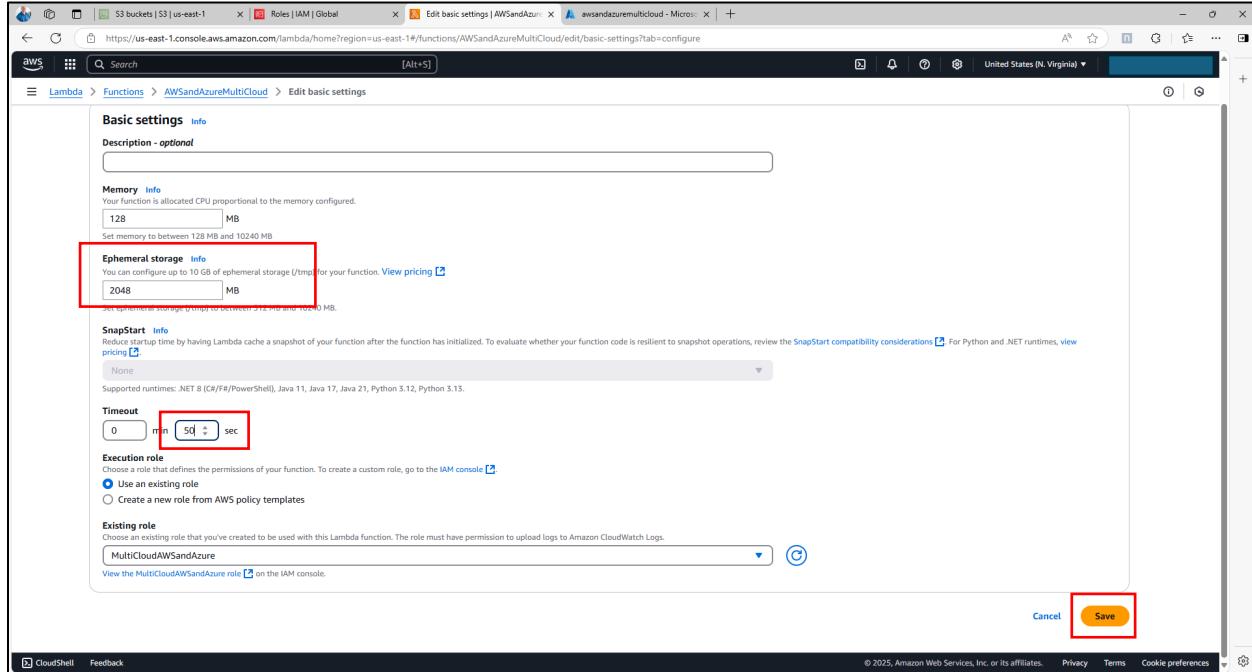
- Under **Code source**, **Code** tab, delete code in the editor
- Paste the **lambda_function.py** file code (provided from exercise)
- Select **Configuration** tab



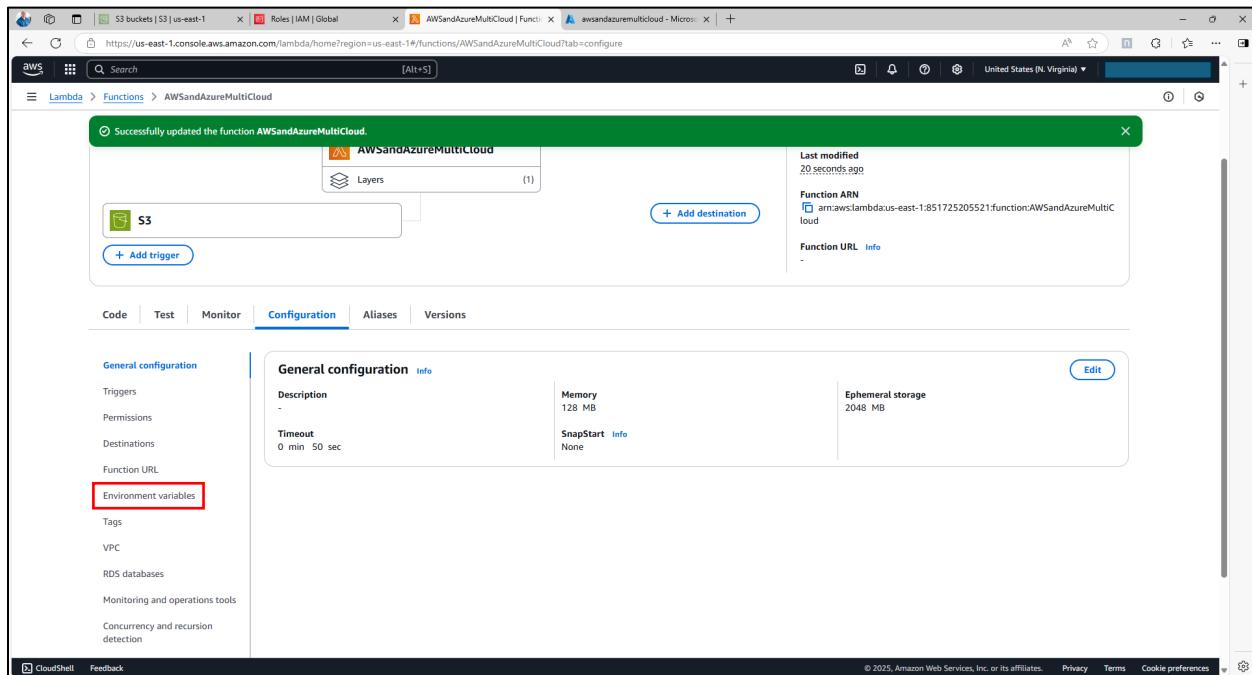
Select Edit



- Ephemeral storage, change from **512** to **2048 MB**
- Timeout, change from **3** to **50** seconds
- Select **Save**



Select Environment variables



Select Edit

Successfully updated the function AWSandAzureMultiCloud.

Last modified 50 seconds ago

Function ARN arn:aws:lambda:us-east-1:851725205521:function:AWSandAzureMultiCloud

Function URL Info

Code Test Monitor Configuration Aliases Versions

General configuration

Triggers

Permissions

Destinations

Function URL

Environment variables (0) Edit

No environment variables

Key Value

Find environment variables

Tags

VPC

RDS databases

Monitoring and operations tools

Concurrency and recursion detection

CloudShell Feedback

Select Add environment variable

Edit environment variables

Environment variables

You can define environment variables as key-value pairs that are accessible from your function code. These are useful to store configuration settings without the need to change function code. [Learn more](#)

There are no environment variables on this function.

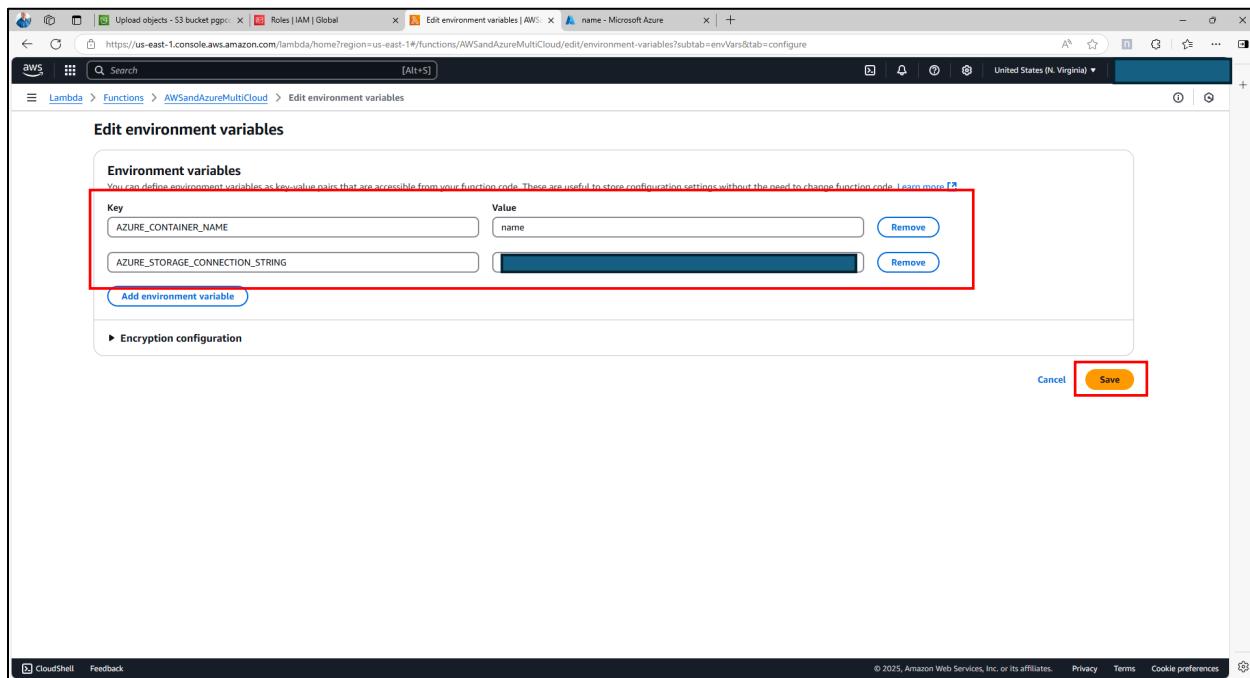
Add environment variable

Encryption configuration

Cancel Save

CloudShell Feedback

- Select **Add environment variable**, for Key name, enter **AZURE_CONTAINER_NAME**. Value, enter Azure container name created earlier, **name**
- Select **Add environment variable**, for Key name, enter **AZURE_STORAGE_CONNECTION_STRING**. Value, enter Azure Connection String copied and pasted earlier from **awsandazurecontainer**
- Select **Save**



Select **Code** tab

Select **Deploy**

The screenshot shows the AWS Lambda console interface. At the top, there are tabs for S3, Roles, IAM, Global, AWSandAzureMultiCloud Function, and awsandazuremulticloud - Microsoft Edge. The URL is https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/AWSandAzureMultiCloud?subtab=envVars&tab=code. The page title is "AWSandAzureMultiCloud - Microsoft Edge". The location bar shows "United States (N. Virginia)". The main area has a green success message: "Successfully updated the function AWSandAzureMultiCloud." Below it is a "S3" section with "Add destination" and "Add trigger" buttons. The navigation bar at the bottom includes Code, Test, Monitor, Configuration, Aliases, and Versions, with "Code" being the active tab. A red box highlights the "Code" tab. In the center, there's a "Code source" section with "Info" and "Upload from" buttons. On the left, there's an "EXPLORER" sidebar showing "AWSANDAZUREMULTICLOUD" with "lambda_function.py" selected. The code editor shows "lambda_function.py" with the following content:

```
lambda_function.py
1 #!/usr/bin/env python3
2
3 from azure.storage.blob import BlobServiceClient
4
5 # Initialize S3 client
6 s3_client = boto3.client('s3')
7
8 # Azure Blob Storage credentials
9 connection_string = os.environ.get('AZURE_STORAGE_CONNECTION_STRING')
10 container_name = os.environ.get('AZURE_CONTAINER_NAME')
11
12 def lambda_handler(event, context):
13     # Get the S3 bucket and object key from the event
14     bucket_name = event['Records'][0]['s3']['bucket']['name']
15     object_key = event['Records'][0]['s3']['object']['key']
16
17     # Get the S3 object
18     s3_object = s3_client.get_object(Bucket=bucket_name, Key=object_key)
19
20     # Initialize the Azure Blob client
21     blob_service_client = BlobServiceClient.from_connection_string(connection_string)
22     blob_client = blob_service_client.get_blob_client(container_name, blob=object_key)
23
24     # Stream the data directly from S3 to Azure Blob Storage
25     blob_client.upload_blob(s3_object['Body'])
```

A red box highlights the "Deploy (Ctrl+Shift+U)" button in the "DEPLOY (UNDEPLOYED CHANGES)" section. Other options shown are "Test (Ctrl+Shift+I)" and "Deploy (Ctrl+Shift+U)". The status bar at the bottom shows the URL https://us-east-1.console.aws.amazon.com/lambda/home?region=us-east-1#/functions/AWSandAzureMultiCloud?tab=code.

Navigate back to Amazon S3

Select pgpcc02051320 bucket

The screenshot shows the Amazon S3 console interface. At the top, there are tabs for S3 buckets, S3 us-east-1, Roles, IAM, Global, AWSandAzureMultiCloud Function, and awsandazuremulticloud - Microsoft Edge. The URL is https://us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general. The page title is "AWSandAzureMultiCloud - Microsoft Edge". The location bar shows "United States (N. Virginia)". The main area has a "Account snapshot - updated every 24 hours" section with "All AWS Regions" and a "View Storage Lens dashboard" button. Below it is a "General purpose buckets" section with a "Find buckets by name" search bar. A red box highlights the "pgpcc02051320" bucket entry in the list. The table columns are Name, AWS Region, IAM Access Analyzer, and Creation date. The "pgpcc02051320" row shows "Name" as "pgpcc02051320", "AWS Region" as "US East (N. Virginia) us-east-1", "IAM Access Analyzer" as "View analyzer for us-east-1", and "Creation date" as "February 5, 2025, 13:20:57 (UTC-06:00)". The left sidebar includes sections for General purpose buckets, Directory buckets, Storage Lens, and AWS Marketplace for S3. The status bar at the bottom shows the URL https://us-east-1.console.aws.amazon.com/s3/buckets?region=us-east-1&bucketType=general.

Select Upload

The screenshot shows the AWS S3 console interface. On the left, there's a sidebar with various options like 'General purpose buckets', 'Storage Lens', and 'Feature spotlight'. The main area is titled 'pgpcc02051320 Info' and has a tab bar with 'Objects' selected. Below this, there's a table header for 'Objects (0)' with columns for Name, Type, Last modified, Size, and Storage class. A message says 'No objects' and 'You don't have any objects in this bucket.' At the bottom right of this section, there's a prominent blue 'Upload' button with a white arrow icon, which is highlighted with a red box.

Select Add files

This screenshot shows the 'Upload' wizard in the AWS S3 console. The first step is 'Upload info', which contains a large dashed box for dragging and dropping files and a 'Choose files' button. The second step is 'Files and folders (0)', which shows a table with columns for Name, Folder, Type, and Size. It says 'No files or folders' and 'You have not chosen any files or folders to upload.' To the right of the table are 'Remove', 'Add files' (which is highlighted with a red box), and 'Add folder' buttons. The third step is 'Destination info', showing the destination as 's3://pgpcc02051320'. Below it are sections for 'Destination details', 'Permissions', and 'Properties'. At the bottom right of the wizard, there are 'Cancel' and 'Upload' buttons, with 'Upload' being highlighted with a red box.

Upload sample .csv file from exercise, wine.csv

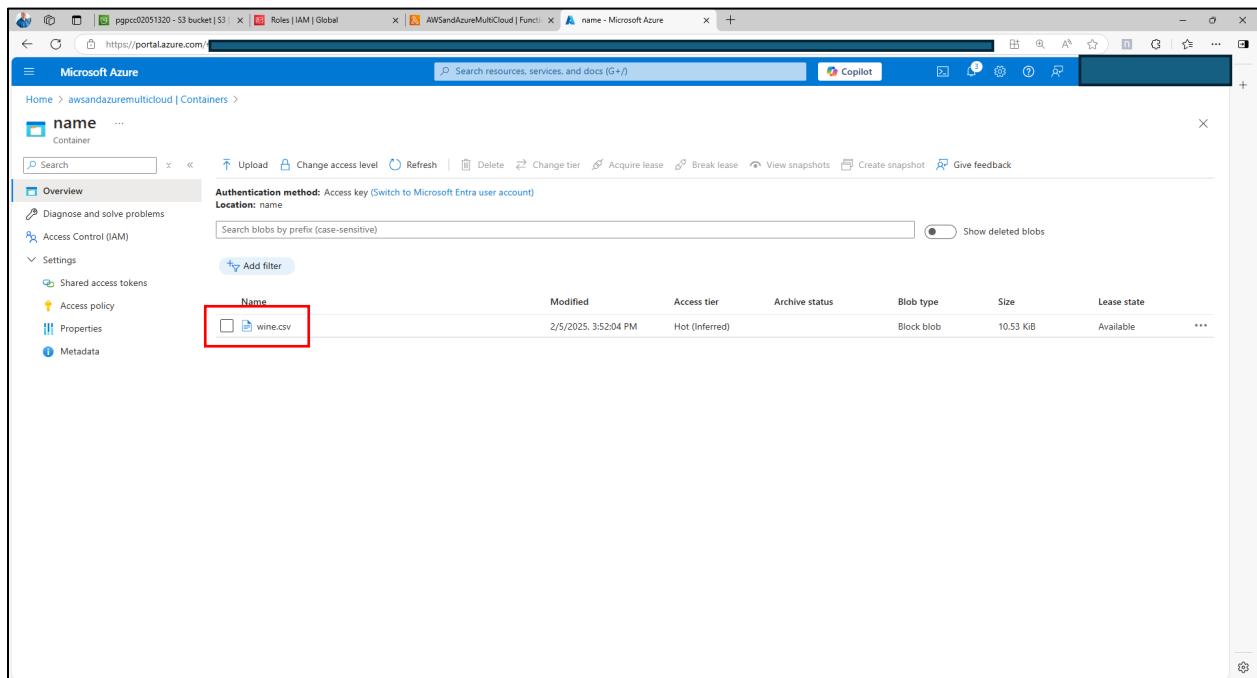
Select Upload

The screenshot shows the AWS S3 'Upload' interface. At the top, there's a navigation bar with tabs like 'Upload objects - S3 bucket pgpc...', 'Roles | IAM | Global', 'AWSandAzureMultiCloud | Function...', and 'awsandazuremulticloud - Microsoft'. Below the navigation bar, the URL is https://us-east-1.console.aws.amazon.com/s3/upload/pgpcc02051320?region=us-east-1&bucketType=general. The main area has a title 'Upload info' with a note about uploading files larger than 160GB. A large blue dashed box allows dragging and dropping files. Below it, a table lists 'Files and folders (1 total, 10.5 KB)'. The single entry is 'wine.csv', which is highlighted with a red box. To the right of the table are buttons for 'Remove', 'Add files', and 'Add folder'. Under 'Destination info', the destination is set to 's3://pgpcc02051320'. A section for 'Destination details' follows. In the bottom right corner of the main form, there are 'Cancel' and 'Upload' buttons, with the 'Upload' button highlighted by a red box.

File upload successful into AWS S3 Bucket

The screenshot shows the 'Upload: status' page after a successful upload. At the top, a green banner says 'Upload succeeded' with a link to 'See the Files and folders table'. Below it, a summary table shows 'Succeeded' (1 file, 10.5 KB (100.0%)) and 'Failed' (0 files, 0 B (0%)). The 'Files and folders' tab is selected, showing a table with one entry: 'wine.csv' (10.5 KB, Status: Succeeded). The 'wine.csv' entry is highlighted with a red box. The table has columns for Name, Folder, Type, Size, Status, and Error. The bottom of the page includes standard AWS footer links: CloudShell, Feedback, © 2025, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

wine.csv successfully uploaded into Microsoft Azure Container titled name



The screenshot shows the Microsoft Azure portal interface for managing blobs in a container named 'name'. The left sidebar includes links for 'Search', 'Upload', 'Change access level', 'Refresh', 'Delete', 'Change tier', 'Acquire lease', 'Break lease', 'View snapshots', 'Create snapshot', and 'Give feedback'. The main area displays a table of blobs with columns: Name, Modified, Access tier, Archive status, Blob type, Size, and Lease state. A single row is present, showing 'wine.csv' as the blob name, modified on 2/5/2025 at 3:52:04 PM, in the Hot (Inferred) tier, as a Block blob, with a size of 10.53 KiB and an available lease state. A red box highlights the 'wine.csv' entry in the list.

Name	Modified	Access tier	Archive status	Blob type	Size	Lease state
wine.csv	2/5/2025, 3:52:04 PM	Hot (Inferred)		Block blob	10.53 KiB	Available