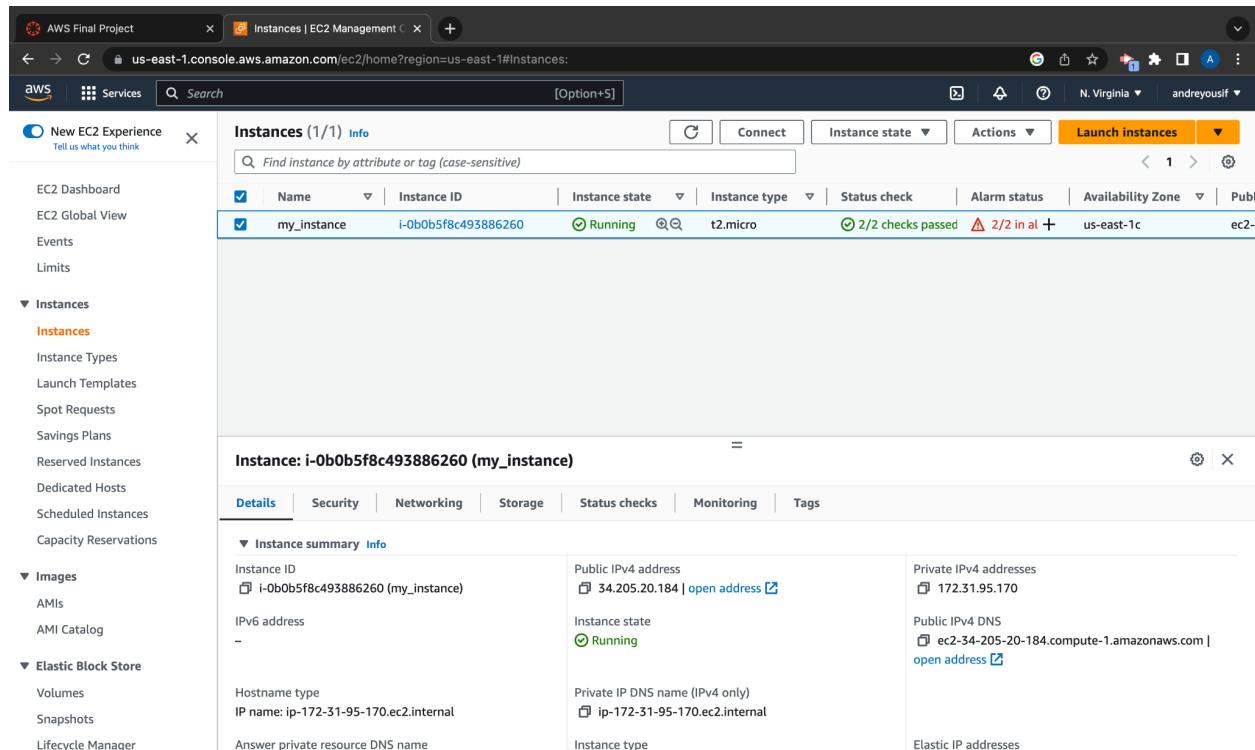
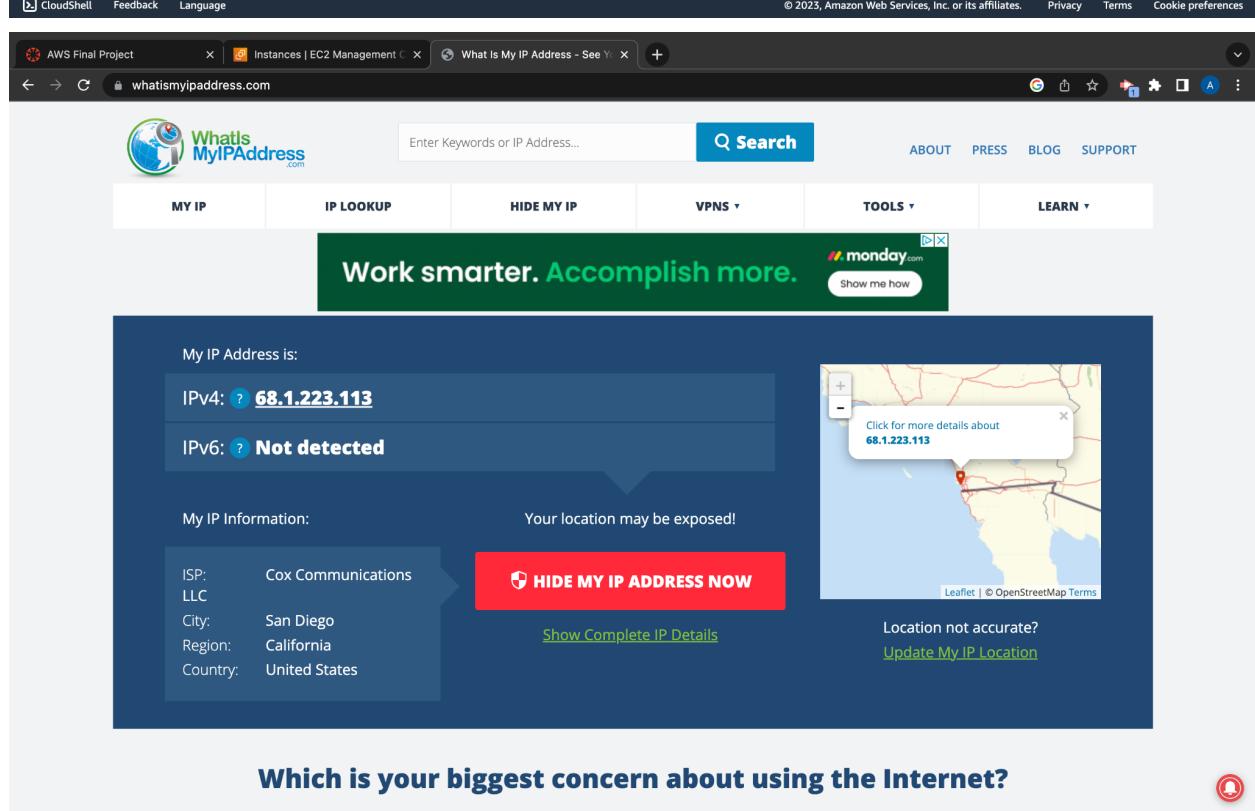


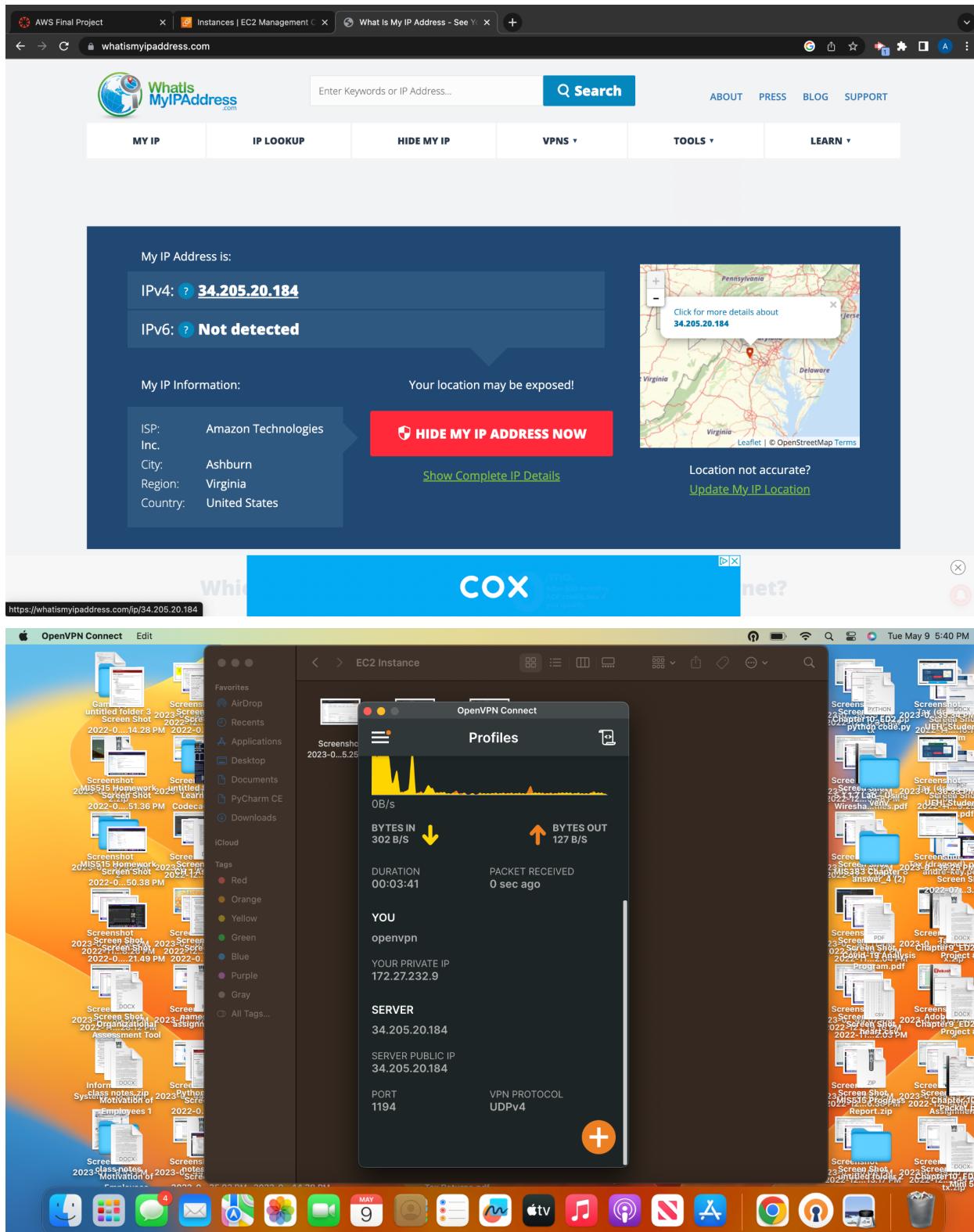
Launching an EC2 instance for OpenVPN - IP before and after connecting to VPN



The screenshot shows the AWS EC2 Management console. On the left, a sidebar lists various services like EC2 Dashboard, EC2 Global View, Events, Limits, Instances, Images, AMIs, AMI Catalog, and Elastic Block Store. The main area displays a table titled 'Instances (1/1) Info' with one entry: 'my_instance' (Instance ID: i-0b0b5f8c493886260, Instance state: Running, Instance type: t2.micro). Below this, a detailed view for 'Instance: i-0b0b5f8c493886260 (my_instance)' is shown, including sections for Details, Security, Networking, Storage, Status checks, Monitoring, and Tags. The 'Details' tab is selected, showing fields like Instance ID, Public IPv4 address (34.205.20.184), Instance state (Running), and Private IPv4 addresses (172.31.95.170).



The screenshot shows the whatismyipaddress.com website. At the top, there's a search bar with 'Enter Keywords or IP Address...' and a 'Search' button. Below the search bar, it says 'My IP Address is:' followed by 'IPv4: 68.1.223.113'. It also shows 'IPv6: Not detected'. To the right, there's a map of California with a callout bubble pointing to the location of the IP address (San Diego, California). A red button says 'HIDE MY IP ADDRESS NOW'. At the bottom, a question asks 'Which is your biggest concern about using the Internet?' with a red bell icon.



Setting up monitoring for traffic on the instance - CloudWatch Alarms and Simple Notification Service (SNS).

Screenshot of a Gmail inbox showing an alarm notification from AWS Notifications.

ALARM: "my_primary_alarm" in US East (N. Virginia)

You are receiving this email because your Amazon CloudWatch Alarm "my_primary_alarm" in the US East (N. Virginia) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [0909337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Wednesday 10 May, 2023 01:33:25 UTC".

View this alarm in the AWS Management Console: https://us-east-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-east-1#alarmsV2:alarm/my_primary_alarm

Alarm Details:

- Name: my_primary_alarm
- Description: This is my alarm to trigger an email
- State Change: INSUFFICIENT_DATA -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [0909337.0 (10/05/23 01:28:00)] was greater than or equal to the threshold (150.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Wednesday 10 May, 2023 01:33:25 UTC
- AWS Account: 844137130423
- Alarm Arn: arn:aws:cloudwatch:us-east-1:844137130423:alarm:my_primary_alarm

Threshold:

- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 150.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:

- MetricNamespace: AWS/EC2
- MetricName: NetworkOut
- Dimensions: [InstanceId = i-0b0b5f8c493886260]
- Period: 300 seconds
- Statistic: Sum
- Unit: not specified
- TreatMissingData: missing

State Change Actions:

- OK:
- ALARM: [arn:aws:sns:us-east-1:844137130423:429_sns_andre]
- INSUFFICIENT_DATA:

Screenshot of the AWS CloudWatch Metrics console showing the "my_primary_alarm" metric.

CloudWatch > Alarms > my_primary_alarm

Graph

NetworkOut

NetworkOut >= 150 for 1 datapoints within 5 minutes

Bytes

98.5M
49.3M
150M

22:30 22:45 23:00 23:15 23:30 23:45 00:00 00:30 01:00 01:15 01:30

Click timeline to see the state change at the selected time.

Legend:

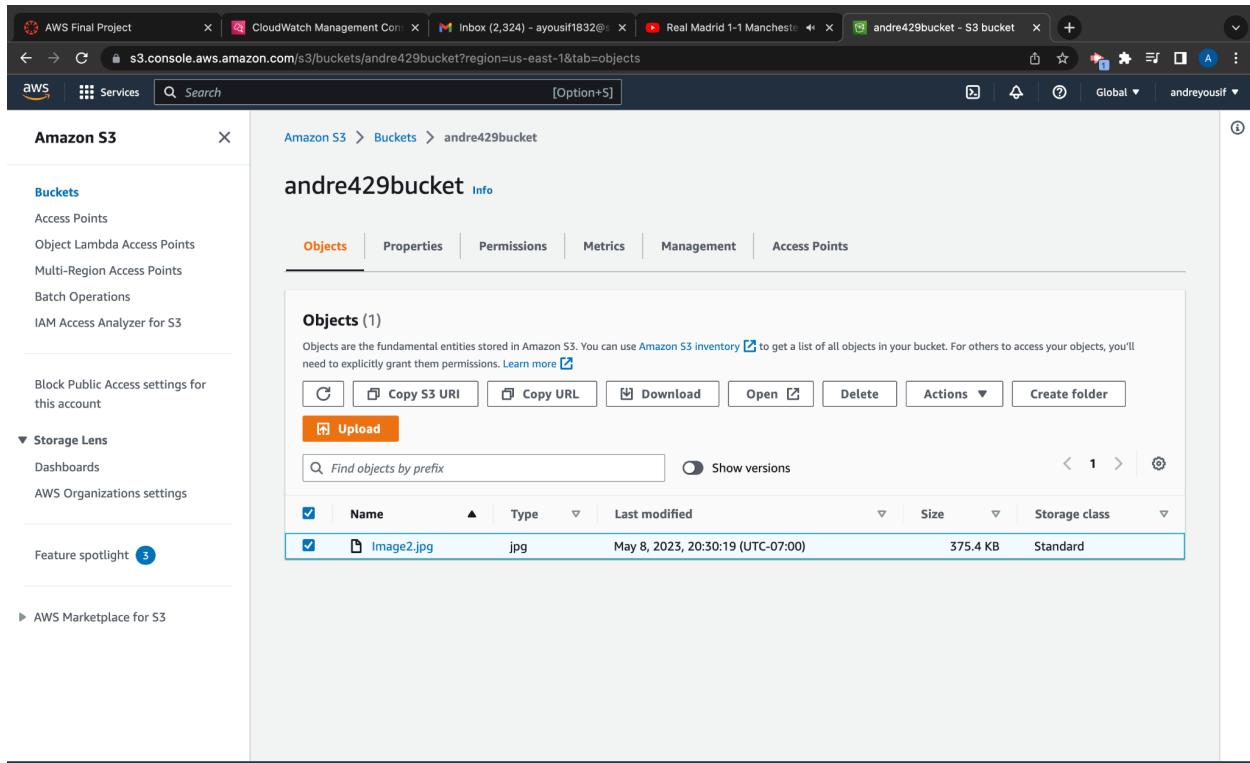
- In alarm (Red)
- OK (Green)
- Insufficient data (Grey)
- Disabled actions (Blue)

Details | Tags | Actions | History | Parent alarms

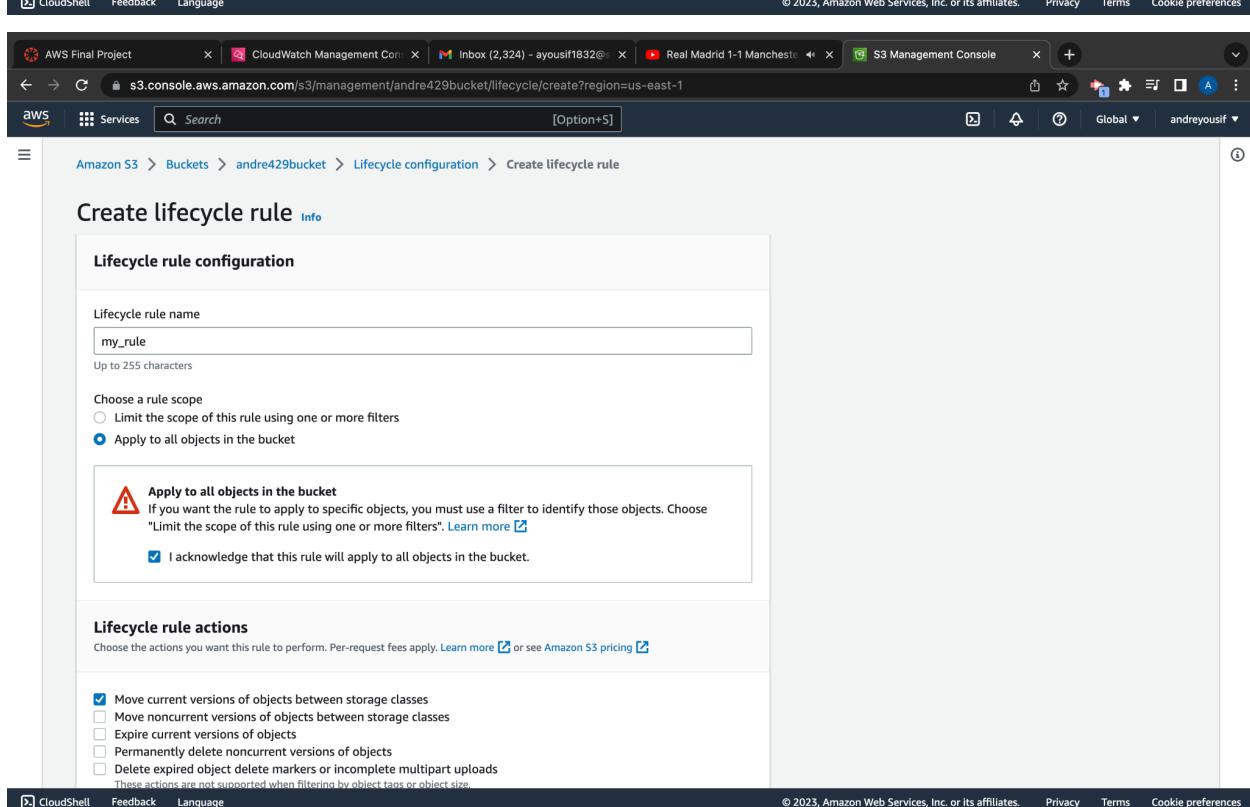
The screenshot shows the AWS CloudWatch Management Console with the URL [us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:~\(alarmStateFilter=~'ALARM'\)](https://us-east-1.console.aws.amazon.com/cloudwatch/home?region=us-east-1#alarmsV2:~(alarmStateFilter=~'ALARM')). The left sidebar is titled "CloudWatch" and includes sections for Favorites and recents, Dashboards, Alarms (with 1 In alarm), All alarms, Billing, Logs, Metrics, X-Ray traces, Events, Application monitoring, Insights, Settings, and Getting Started. The main content area is titled "CloudWatch > Alarms" and shows a table of alarms. The table has columns for Name, State, Last state update, Conditions, and Actions. There is one entry: "my_primary_alarm" (In alarm, last updated 2023-05-09 18:33:25, condition: NetworkOut >= 150 for 1 datapoints within 5 minutes, Actions enabled). The top right of the main area has buttons for Hide Auto Scaling alarms, Clear selection, Create composite alarm, Actions, and Create alarm.

Name	State	Last state update	Conditions	Actions
my_primary_alarm	In alarm	2023-05-09 18:33:25	NetworkOut >= 150 for 1 datapoints within 5 minutes	Actions enabled

Configuring S3 storage to hold backups



The screenshot shows the AWS S3 Management Console interface. On the left, a sidebar menu is open under 'Amazon S3' with options like 'Buckets', 'Access Points', 'Storage Lens', and 'Feature spotlight'. The main area displays the 'andre429bucket' page. At the top, there are tabs for 'Objects' (which is selected), 'Properties', 'Permissions', 'Metrics', 'Management', and 'Access Points'. Below the tabs, a section titled 'Objects (1)' shows a single item: 'Image2.jpg' (jpg type, last modified May 8, 2023, at 20:30:19 UTC-07:00, 375.4 KB, Standard storage class). There are buttons for 'Upload', 'Copy S3 URI', 'Copy URL', 'Download', 'Open', 'Delete', and 'Actions'. A search bar and a 'Show versions' toggle are also present.



The screenshot shows the 'Create lifecycle rule' configuration page. The title is 'Create lifecycle rule' with an 'Info' link. The first section is 'Lifecycle rule configuration' with a 'Lifecycle rule name' field containing 'my_rule' (with a note that it can be up to 255 characters) and a 'Choose a rule scope' section where 'Apply to all objects in the bucket' is selected. A warning message states: '⚠️ Apply to all objects in the bucket. If you want the rule to apply to specific objects, you must use a filter to identify those objects. Choose "Limit the scope of this rule using one or more filters". Learn more' with a checkbox below it labeled 'I acknowledge that this rule will apply to all objects in the bucket.' The second section is 'Lifecycle rule actions' with a note: 'Choose the actions you want this rule to perform. Per-request fees apply. Learn more or see Amazon S3 pricing'. Under this, several checkboxes are available: 'Move current versions of objects between storage classes' (selected), 'Move noncurrent versions of objects between storage classes', 'Expire current versions of objects', 'Permanently delete noncurrent versions of objects', and 'Delete expired object delete markers or incomplete multipart uploads' (with a note: 'These actions are not supported when filtering by object tags or object size').

Transition current versions of objects between storage classes

Choose transitions to move current versions of objects between storage classes based on your use case scenario and performance access requirements. These transitions start from when the objects are created and are consecutively applied. [Learn more](#)

Choose storage class transitions Days after object creation

Glacier Instant Retrieval ▾ 7 Remove

Add transition

Review transition and expiration actions

Current version actions	Noncurrent versions actions
Day 0 • Objects uploaded	Day 0 No actions defined.
↓	
Day 7 • Objects move to Glacier Instant Retrieval	

Create rule

The lifecycle configuration was updated. Lifecycle rule "my_rule" was successfully added.

It may take some time for the configuration to be updated. Press the refresh button if changes to the rule are not displayed.

Amazon S3 > Buckets > andre429bucket > Lifecycle configuration

Lifecycle configuration Info

To manage your objects so that they are stored cost effectively throughout their lifecycle, configure their lifecycle. A lifecycle configuration is a set of rules that define actions that Amazon S3 applies to a group of objects. Lifecycle rules run once per day.

Lifecycle rules (1)

Use lifecycle rules to define actions you want Amazon S3 to take during an object's lifetime such as transitioning objects to another storage class, archiving them, or deleting them after a specified period of time. [Learn more](#)

Actions	Create lifecycle rule					
<input type="button" value="View details"/>	<input type="button" value="Edit"/>	<input type="button" value="Delete"/>	<input type="button" value="Actions ▾"/>	<input type="button" value="Create lifecycle rule"/>		
<input type="text" value="Find lifecycle rules by name"/>						
Lifecycle rule name	Status	Scope	Current version actions	Noncurrent versions actions	Expired object delete markers	Incomplete multipart uploads
my_rule	Enabled	Entire bucket	Transition to Glacier Instant Retrieval	-	-	-

Configuring a backup tool to auto backup the instance- AWS Backup Service

AWS Backup

Backup vaults (2) Info

Backup vaults are containers where your backups are stored. You can have one default vault or multiple vaults where backups can be stored.

Backup vault name	Vault lock status	Recovery points	KMS encryption key ID
Default	-	1	430a03fd-af4c-4d02-a96b-741b136595bd
my_backup_plan_vault	-	0	430a03fd-af4c-4d02-a96b-741b136595bd

Create backup vault

CloudWatch CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

AWS Backup

Summary

Backup plan name	Version ID	Last modified	Last runtime
my_backup_plan	YTQwMGVim2EtOTM3Ny00MDc4LWI1YjYtMmNkYTkyOWMxZGJj	May 8, 2023, 20:22:29 (UTC-07:00)	May 8, 2023, 22:00:14 (UTC-07:00)
Backup plan ID			
c759c1c2-c641-489f-8f9f-e5ee3b7e5daf			

Backup rules (3)

Backup rules specify the backup schedule, backup window, and lifecycle rules.

Name	Backup vault	Destination Backup vault
DailyBackups	Default	-
MonthlyBackups	Default	-
WeeklyBackups	my_backup_plan_vault	-

Resource assignments (2)

Resource assignments specify which resources will be backed up by this Backup plan.

Name	IAM role ARN	Creation time
mis_resource	arn:aws:iam::844137130423:role/service-role/AWSBackupDefaultServiceRole	May 8, 2023, 20:26:22 (UTC-07:00)
primary_backup_plan	arn:aws:iam::844137130423:role/service-role/AWSBackupDefaultServiceRole	May 8, 2023, 20:38:09 (UTC-07:00)

CloudWatch CloudShell Feedback Language © 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Creating IAM users with the permissions/policies

IAM Management Console

ec2access_andre

Summary

ARN arn:aws:iam::844137130423:user/ec2access_andre	Console access Enabled without MFA	Access key 1 Not enabled
Created May 09, 2023, 18:15 (UTC-07:00)	Last console sign-in Never	Access key 2 Not enabled

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (1)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonEC2FullAccess	AWS managed	Directly

S3access_andre

Summary

ARN arn:aws:iam::844137130423:user/S3access_andre	Console access Enabled without MFA	Access key 1 Not enabled
Created May 09, 2023, 18:17 (UTC-07:00)	Last console sign-in Never	Access key 2 Not enabled

Permissions Groups Tags Security credentials Access Advisor

Permissions policies (3)

Permissions are defined by policies attached to the user directly or through groups.

Policy name	Type	Attached via
AmazonInspector2FullAccess	AWS managed	Directly
AmazonS3FullAccess	AWS managed	Directly
AWSBackupServiceRolePolicyForS...	AWS managed	Directly

Screenshot of the AWS IAM Management Console showing the 'Users' page. The left sidebar shows 'Identity and Access Management (IAM)' with 'Users' selected. The main content area shows two users: 'ec2access_andre' and 'S3access_andre'. Both users have 'None' for Groups, Last activity, and MFA. Their Password age is '3 minutes ago' and Active key age is '-'. A search bar at the top says 'Find users by username or access key'.

Configuring a vulnerability scanner - Inspector - REPORT

Screenshot of the AWS Amazon Inspector console showing the 'Findings' page. The left sidebar shows 'Findings' with a 'Severity Filter' set to 'Medium'. The main content area displays three findings:

	Severity	Date	Finding	Target	Template
<input type="checkbox"/>	Medium	Yesterday at...	On instance i-0b0b5f8c493886260, TCP port 22 which is associated with 'SSH' is reac...	Assessment-Targe...	Assessment-
<input type="checkbox"/>	Low	Yesterday at...	On instance i-0b0b5f8c493886260, TCP port 443 which is associated with 'HTTPS' is ...	Assessment-Targe...	Assessment-
<input type="checkbox"/>	Informational	Yesterday at...	Aggregate network exposure: On instance i-0b0b5f8c493886260, ports are reachable f...	Assessment-Targe...	Assessment-

The status bar at the bottom right shows 'Max records per page: 25' and a note to 'refresh browser to reflect change'.