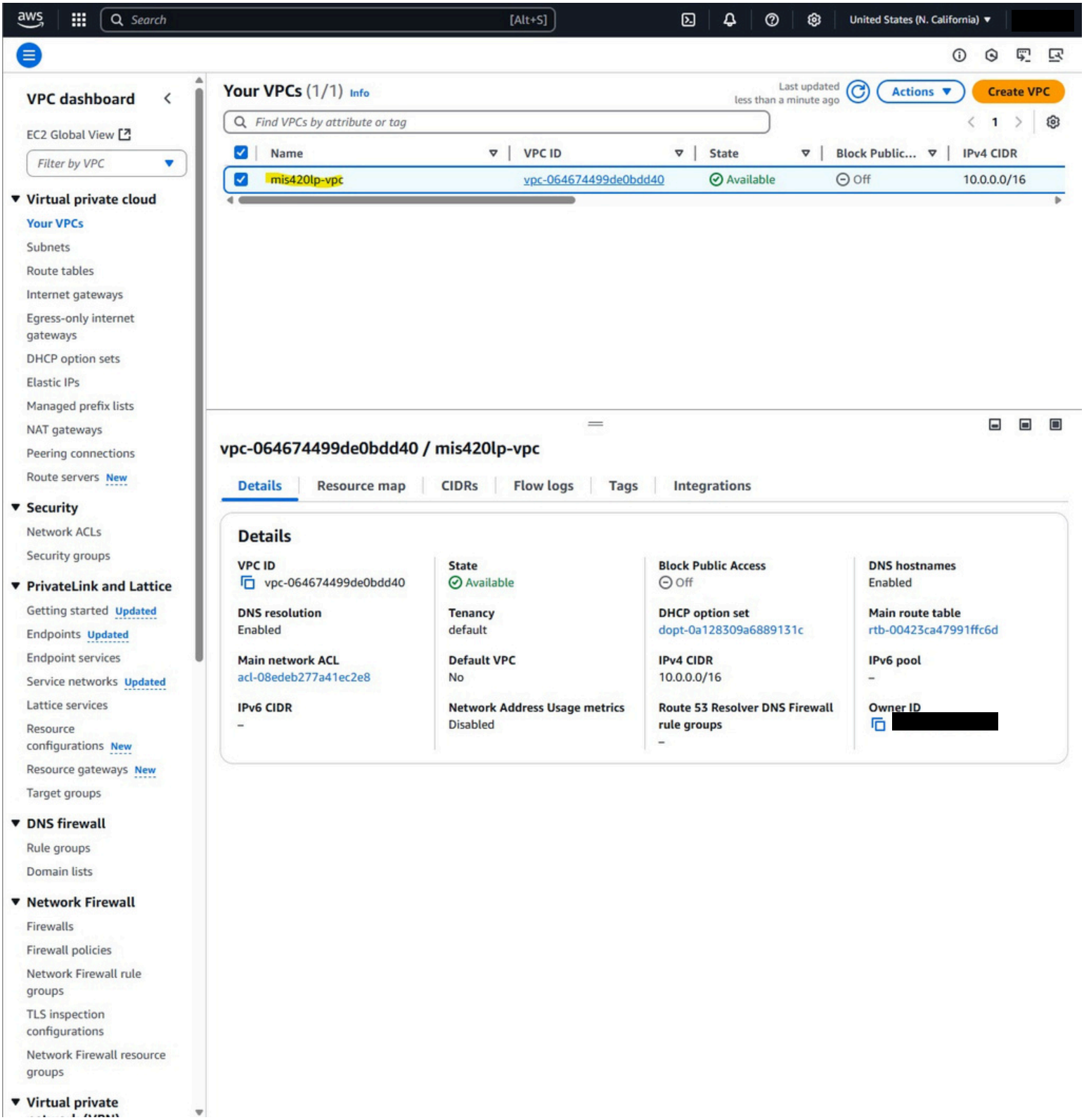
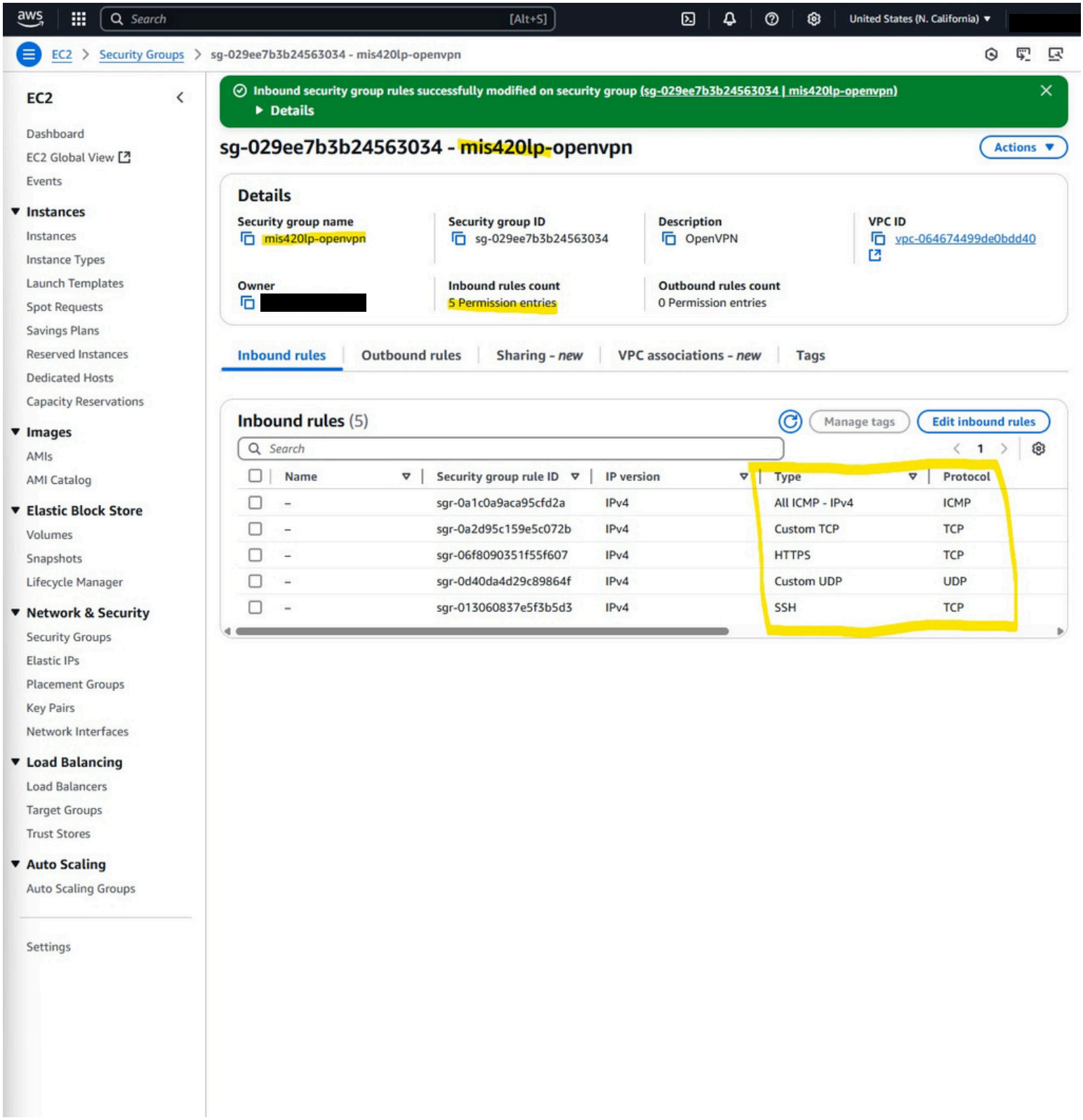
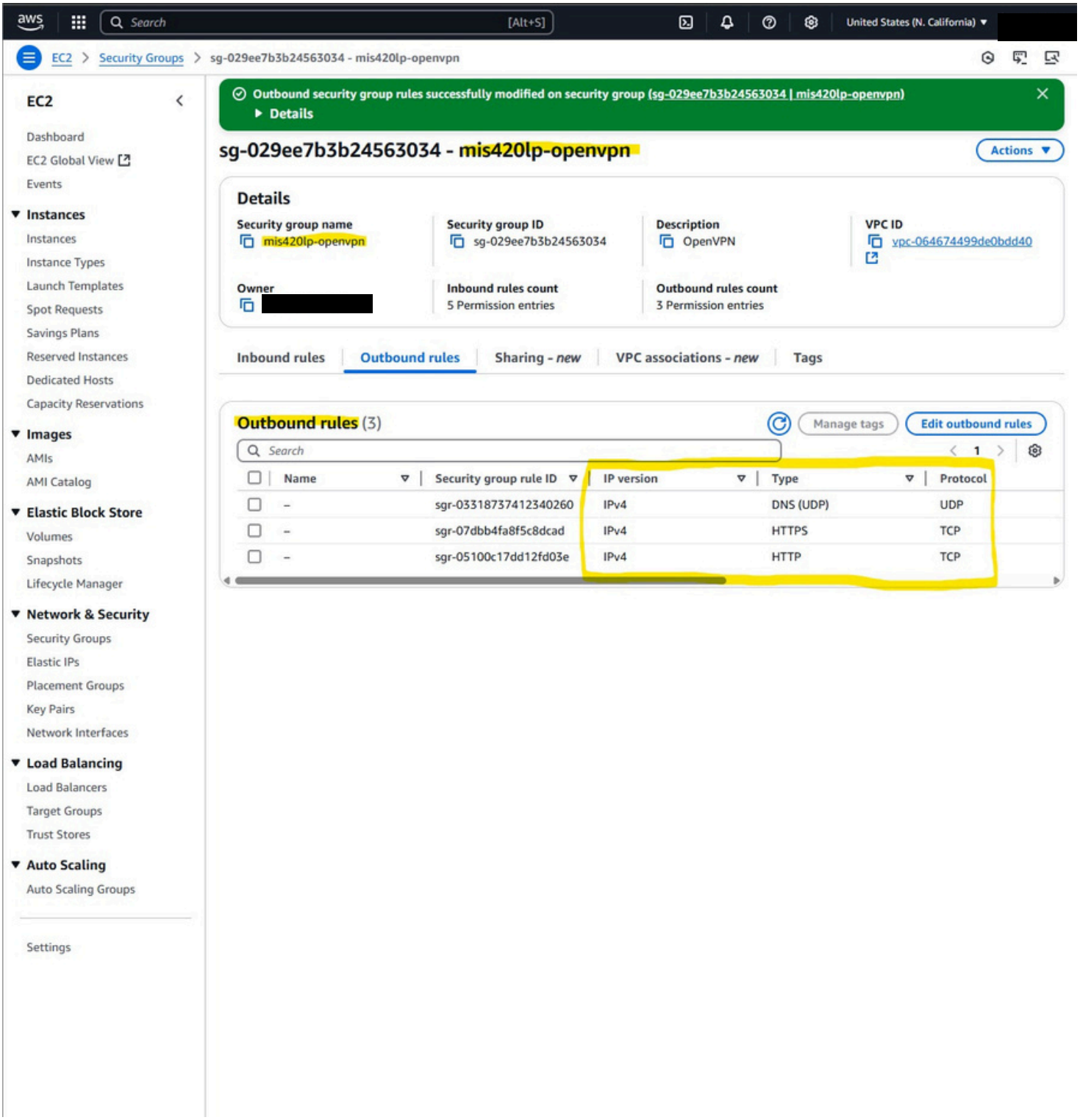
1. VPC creation for the project



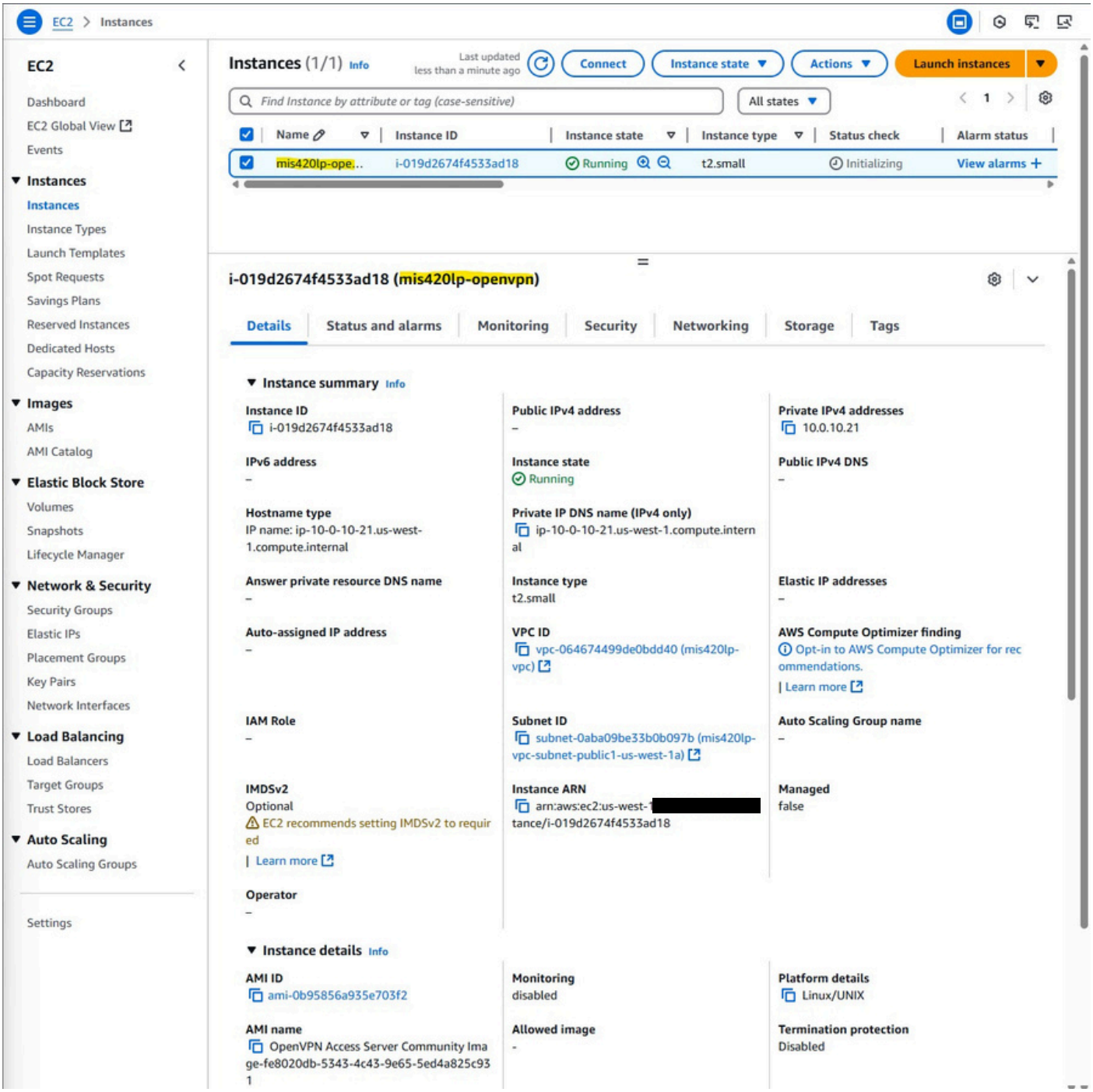
2. Security Groups for the OpenVPN EC2 instance



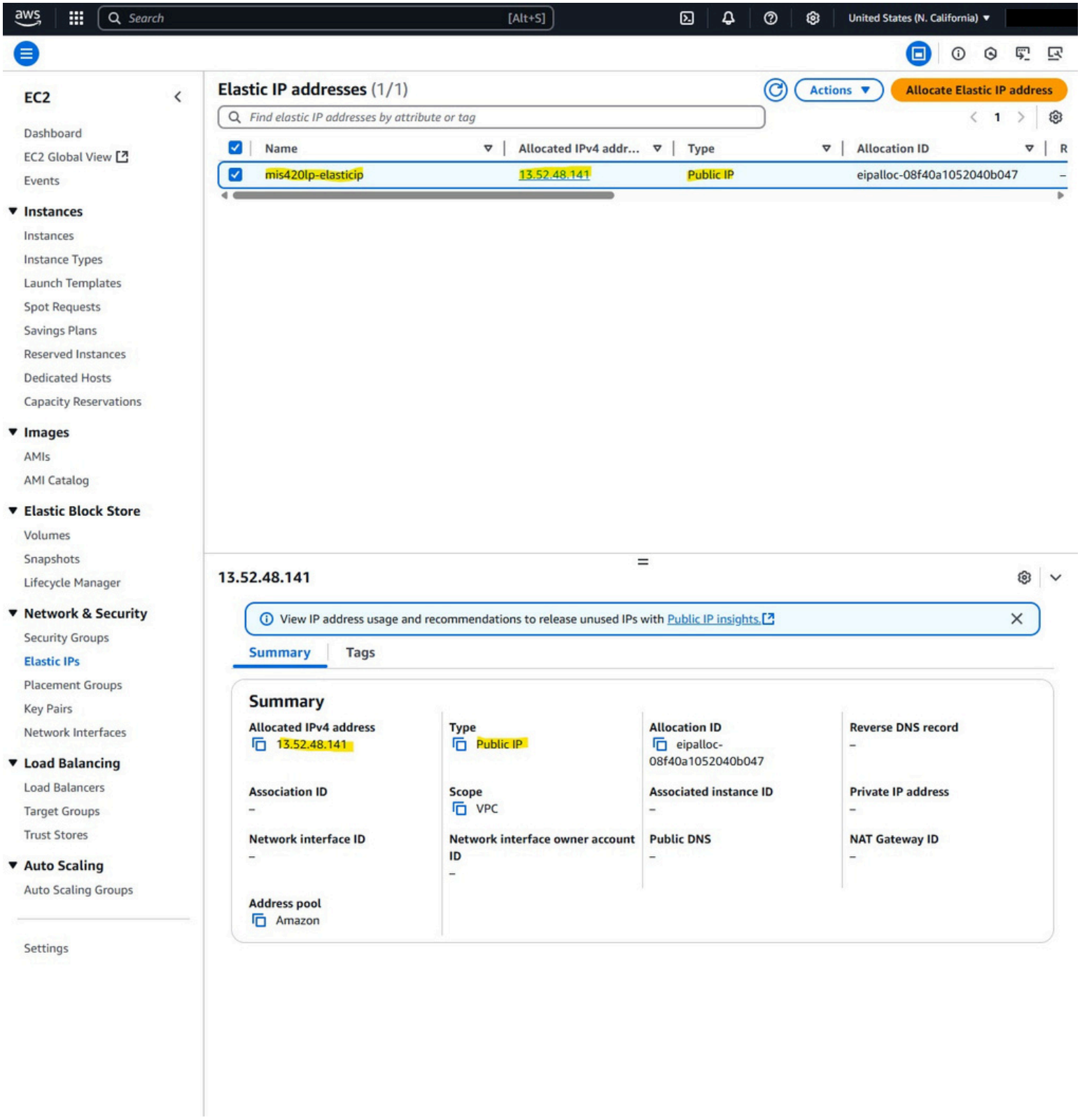
3. Creating Outbound Rules



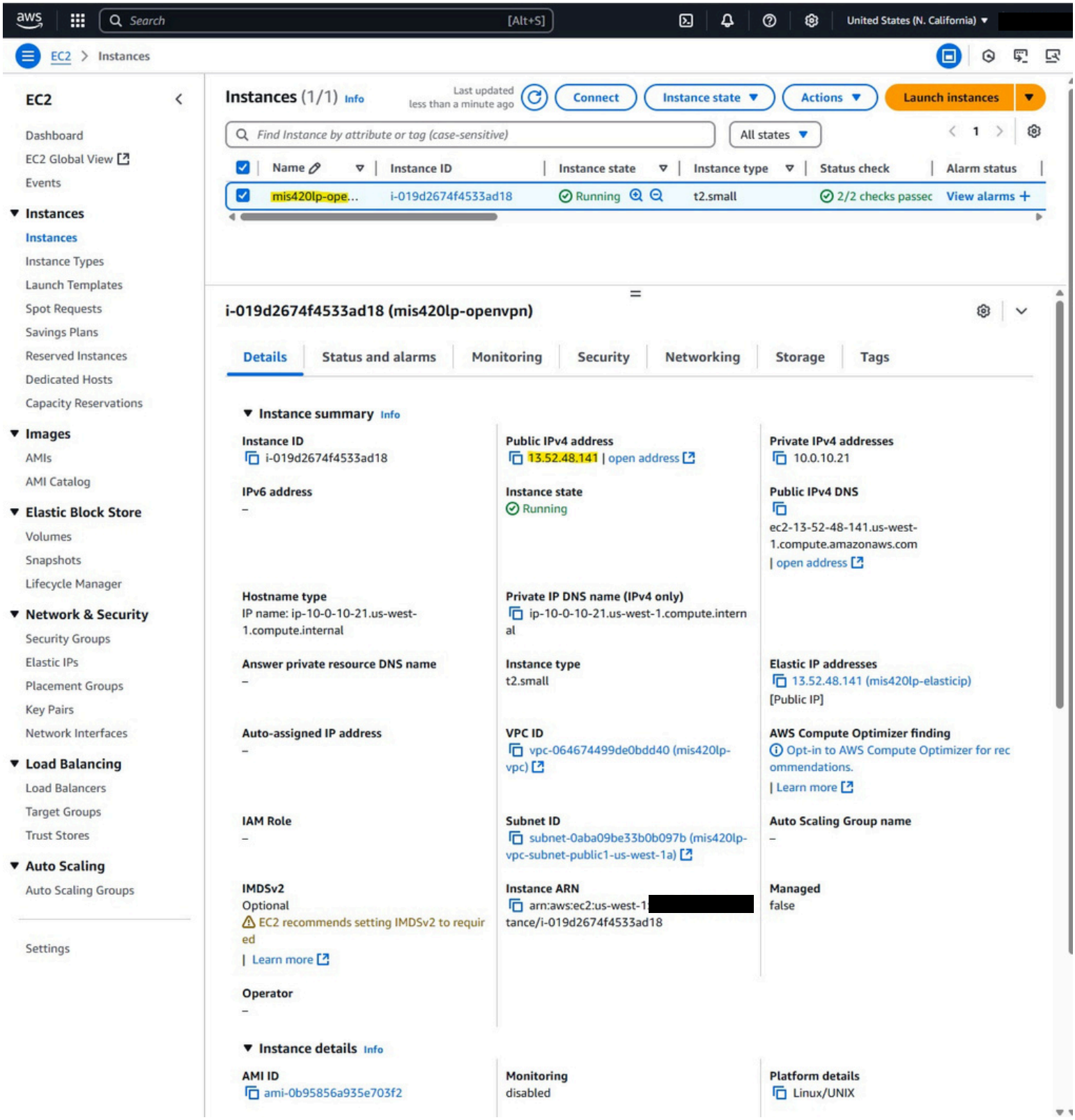
4. Creating an EC2 instance for OpenVPN



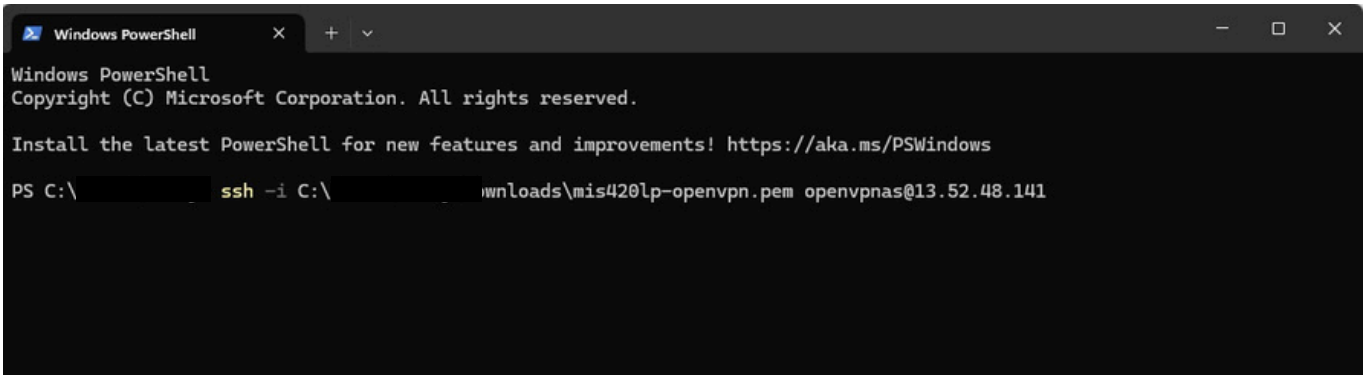
5. Creating an elastic IPv4 for the Instance

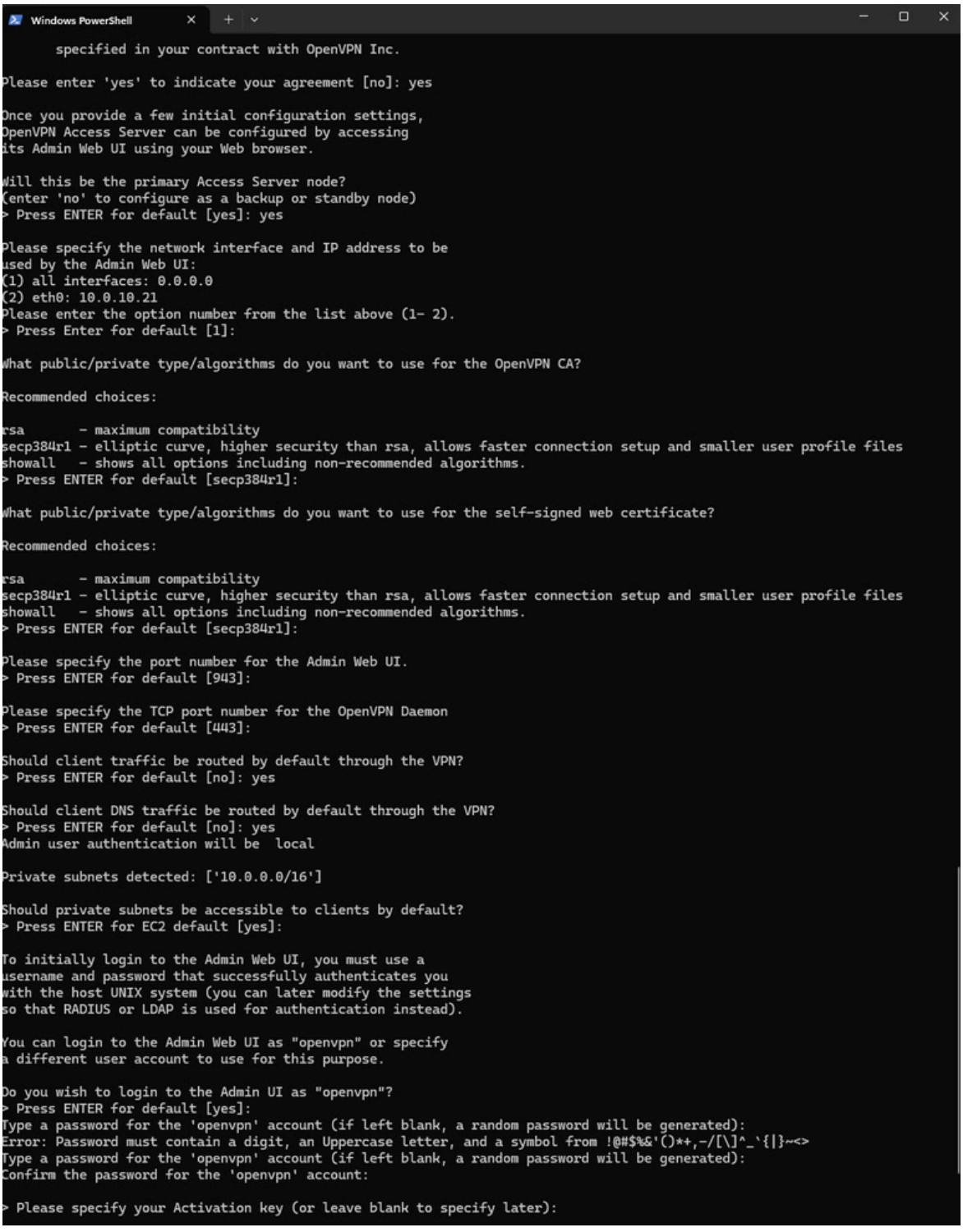


6. Associating the Elastic IP to the EC2 instance

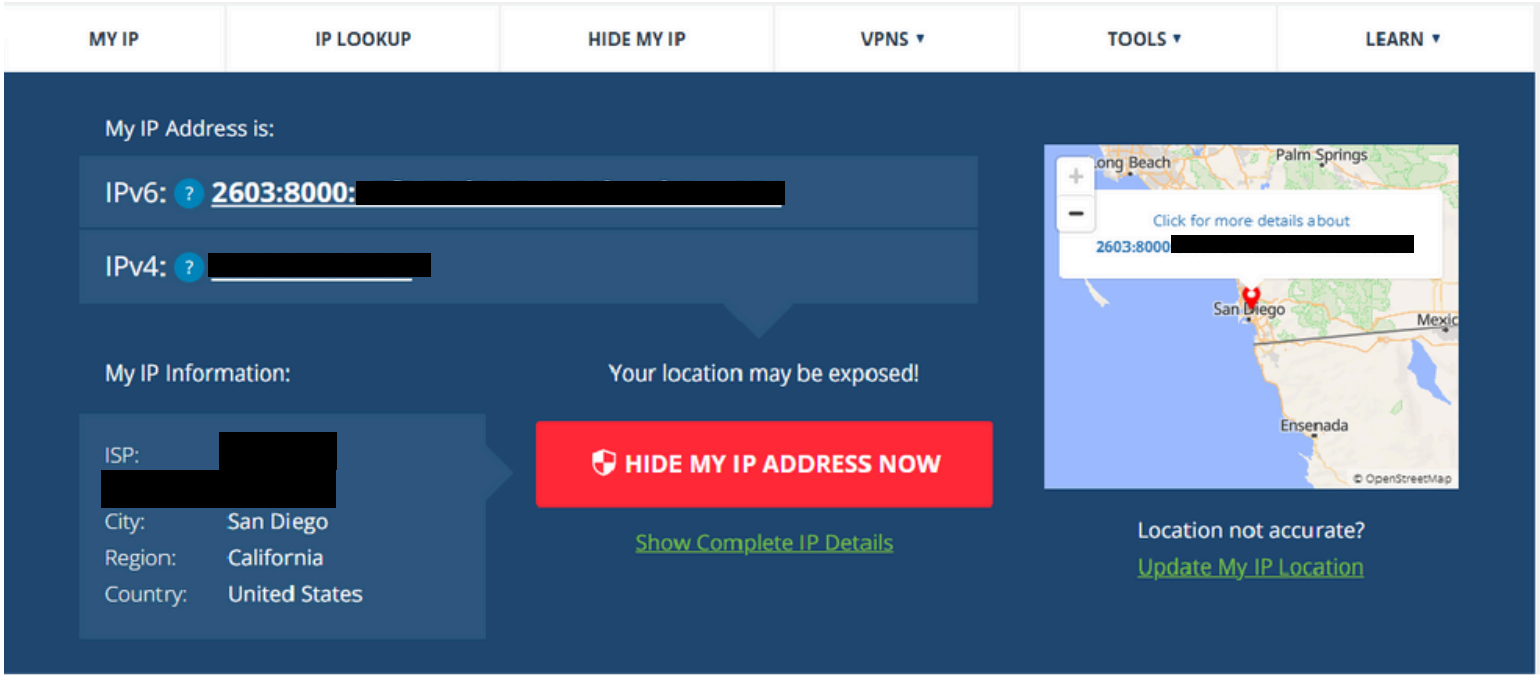


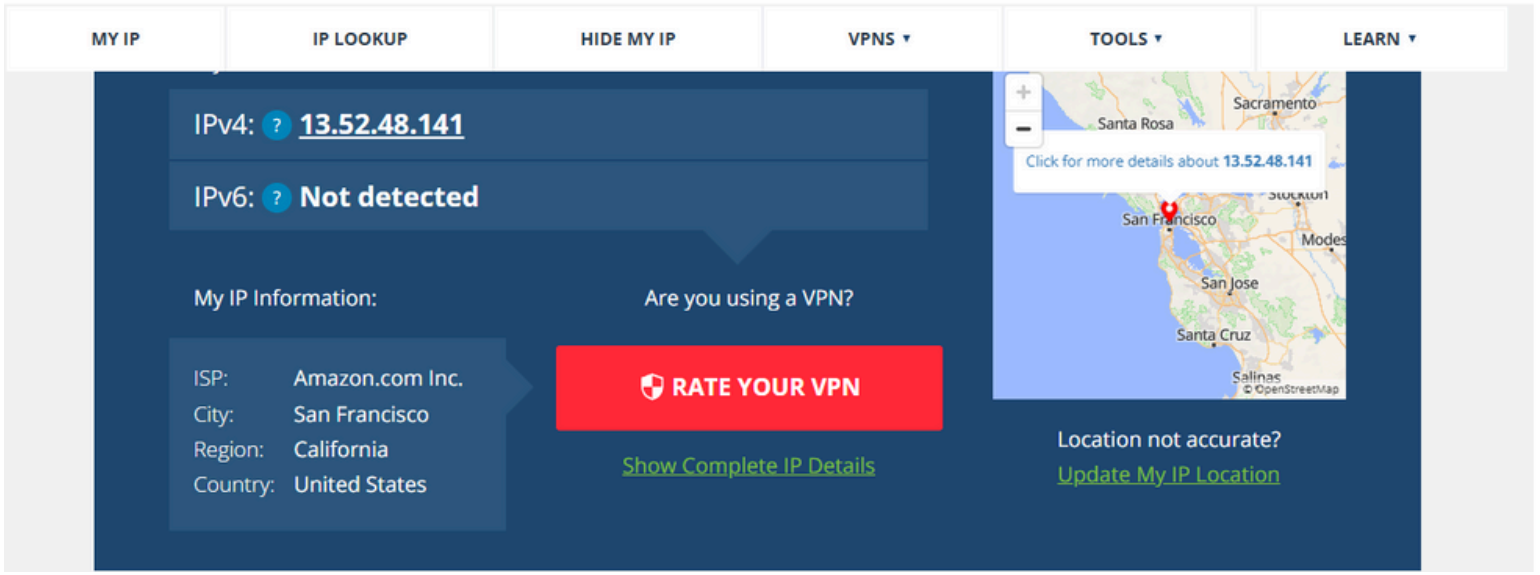
7. Connecting to the VPN with Windows Powershell for initial configuration



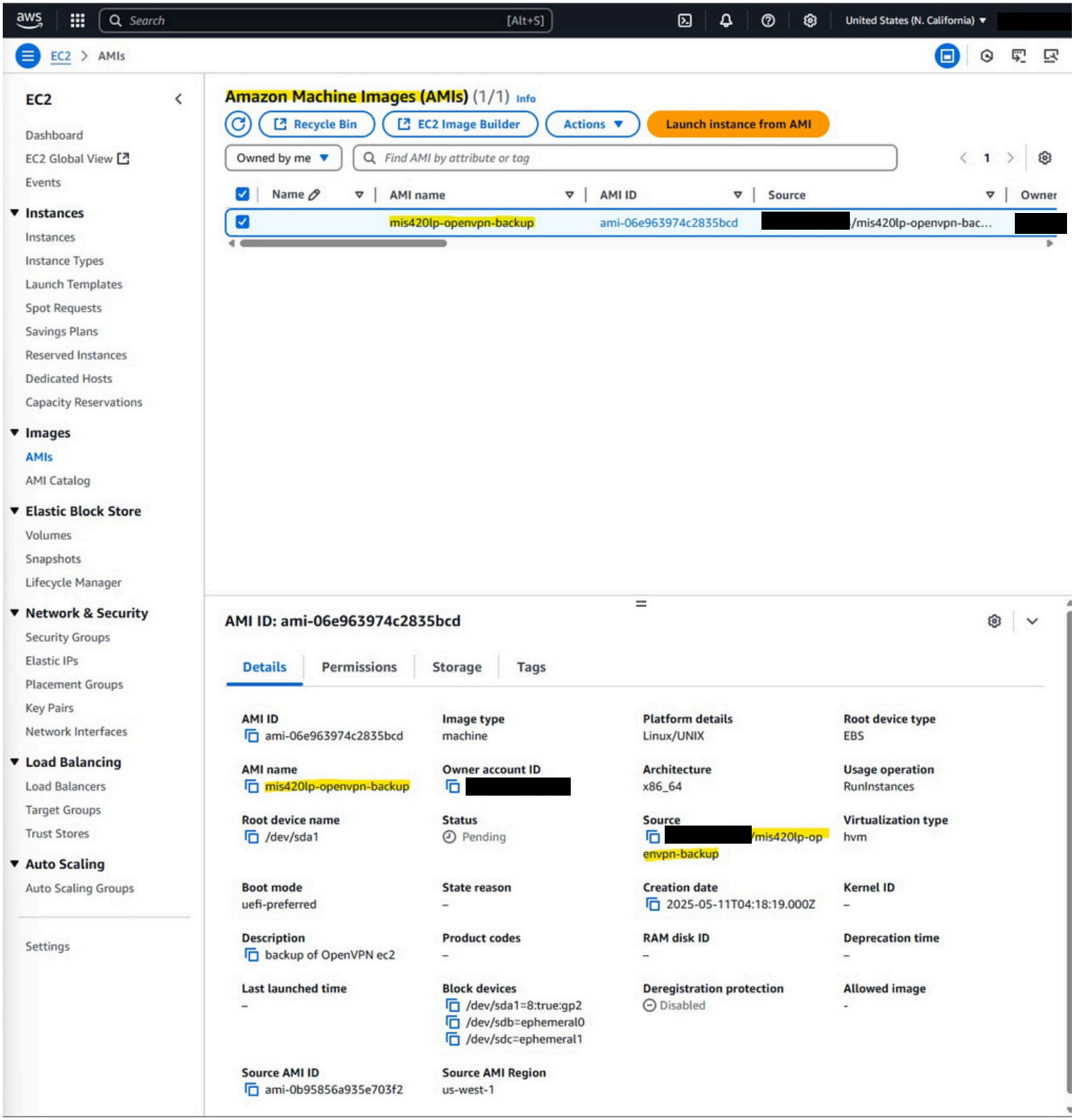


8. Computer IP before and after connecting to the VPN

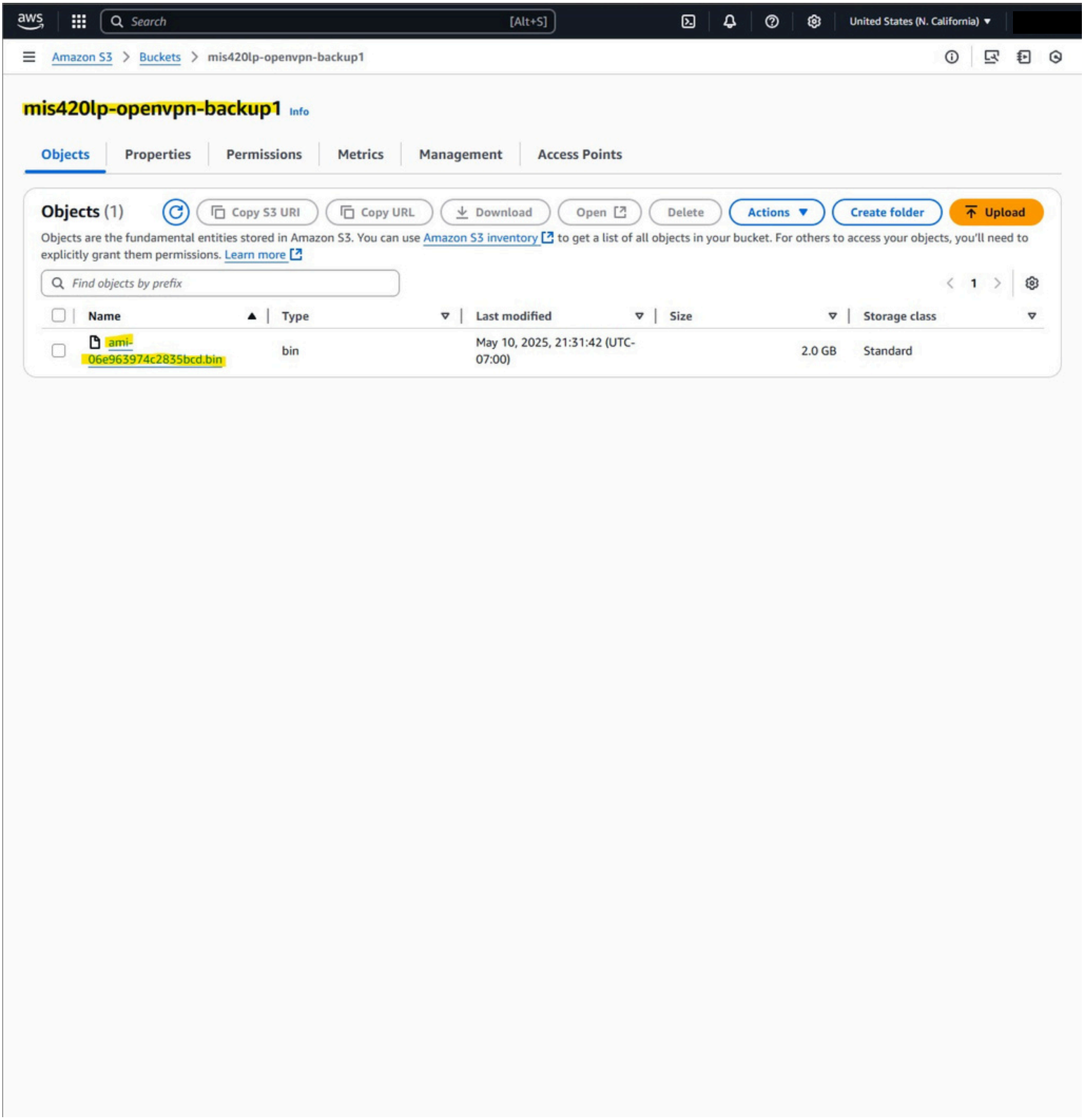




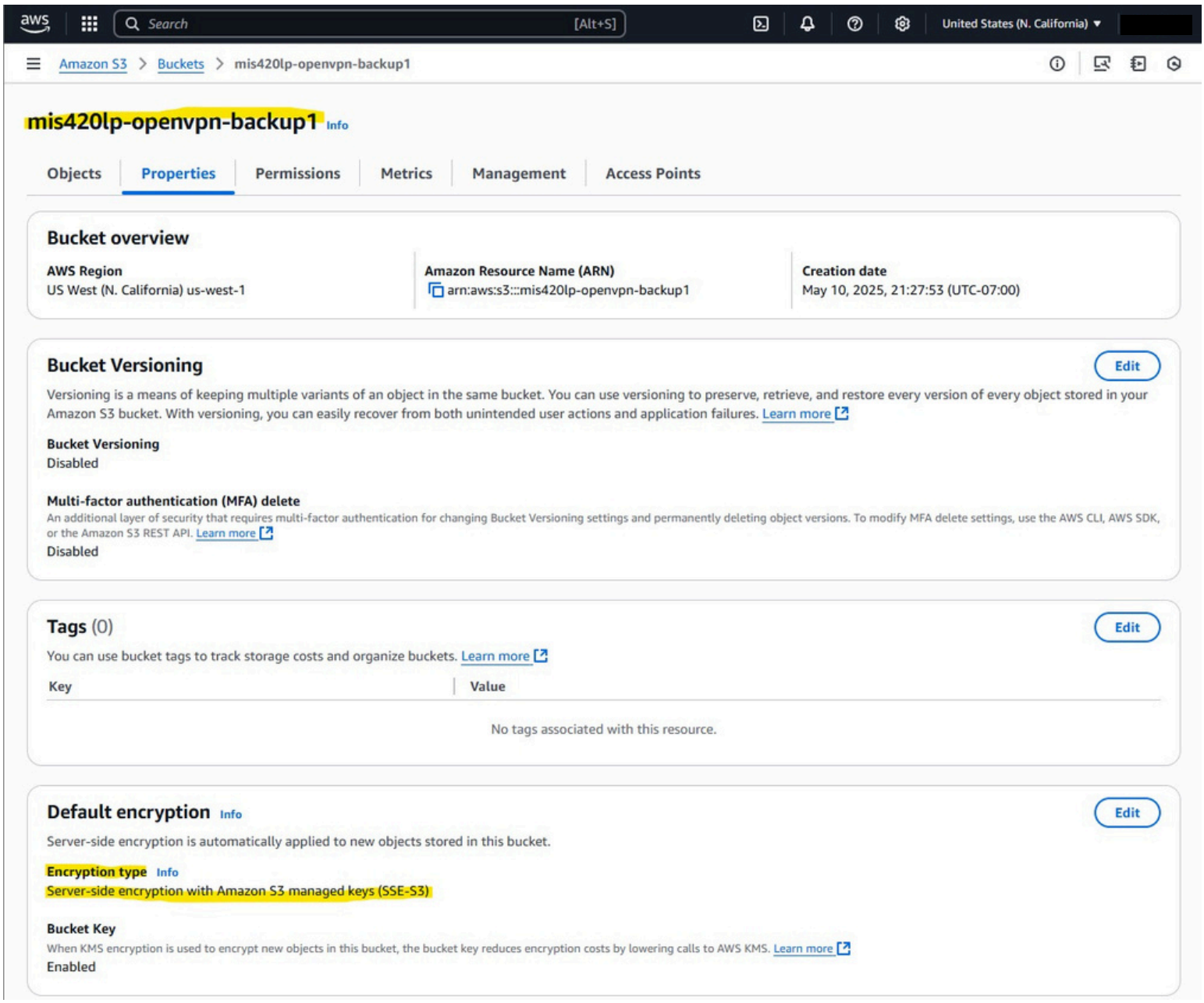
9. AMI creation for S3 bucket



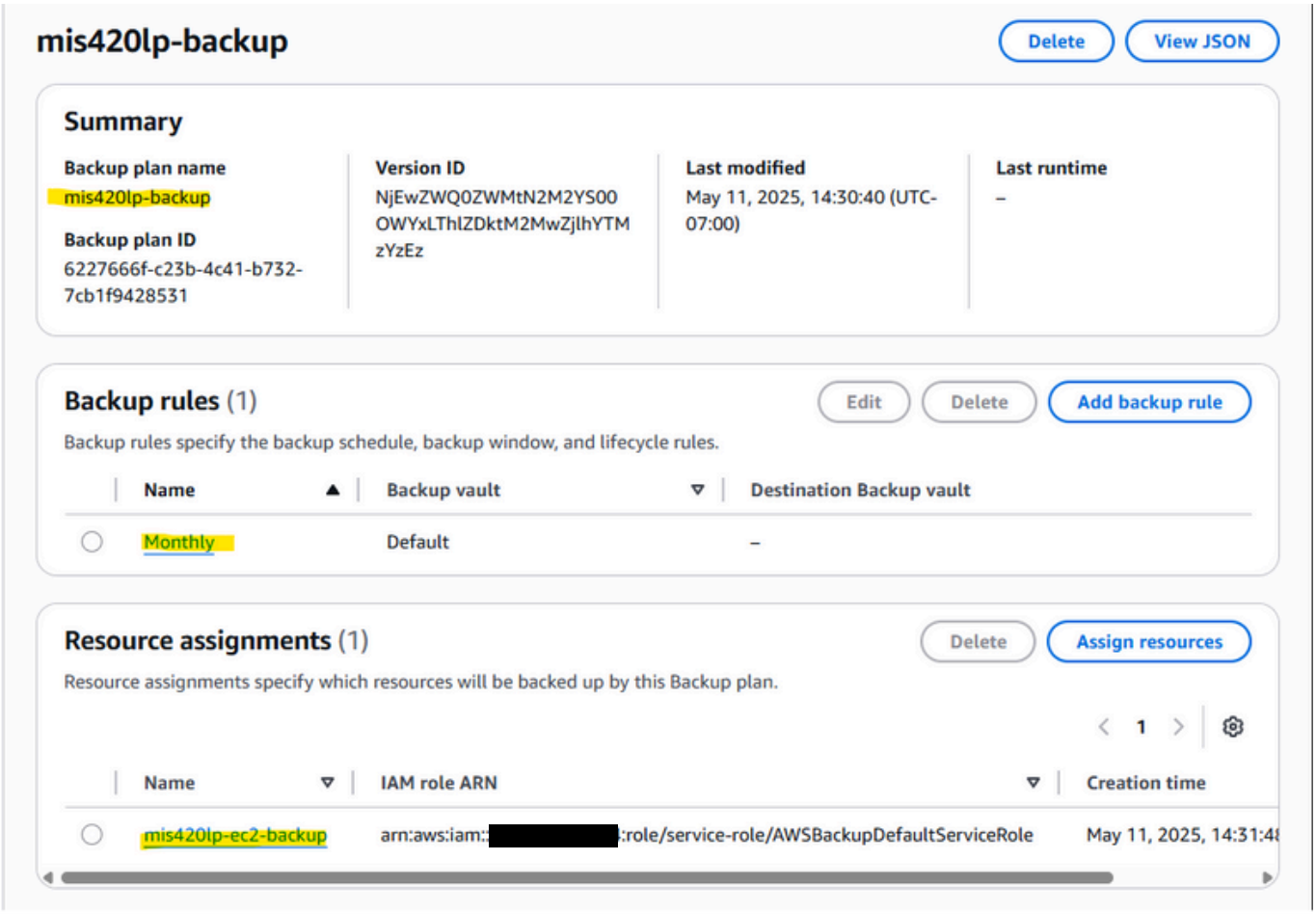
10. S3 bucket AMI storage

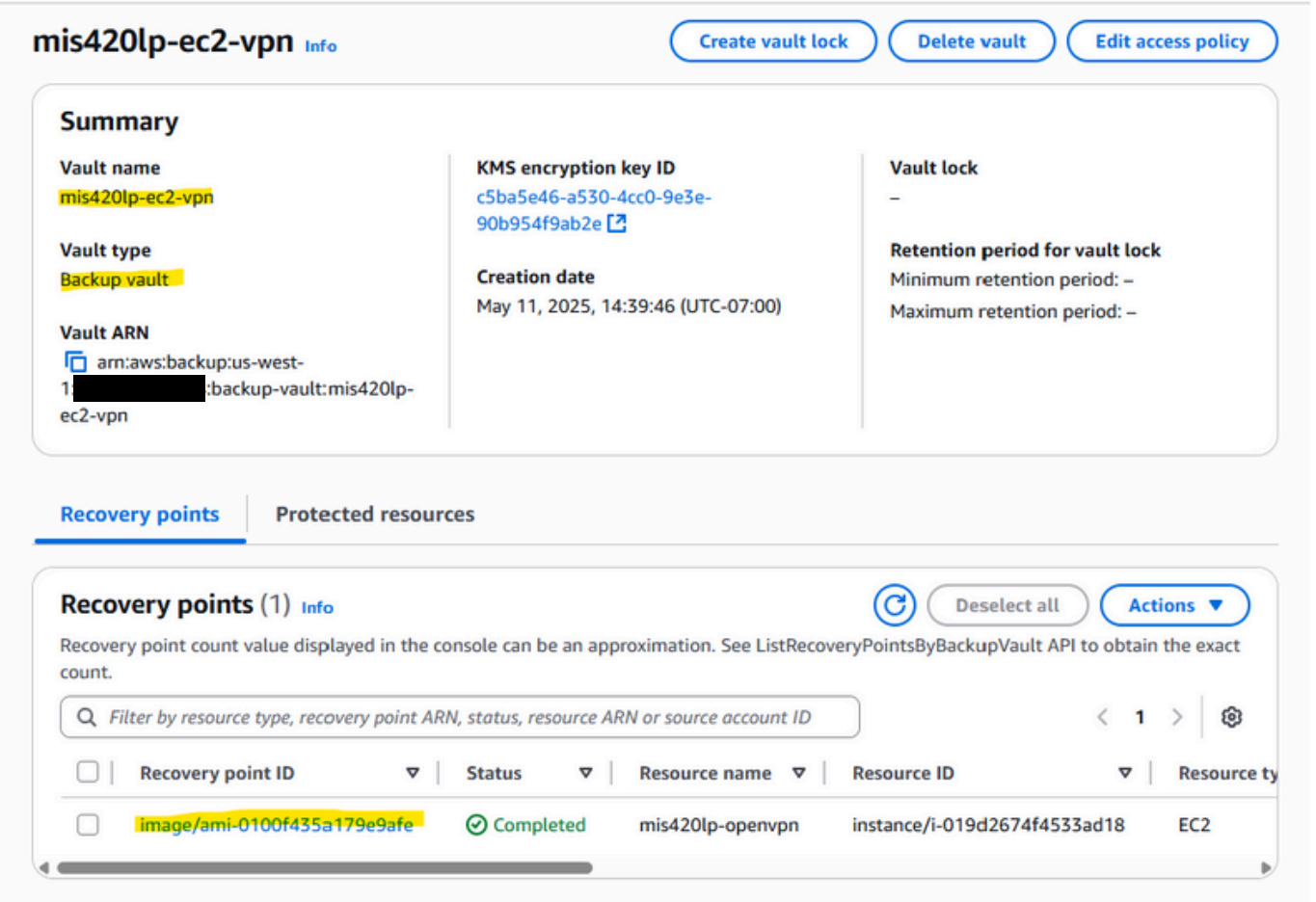


11. Bucket encryption for AMI

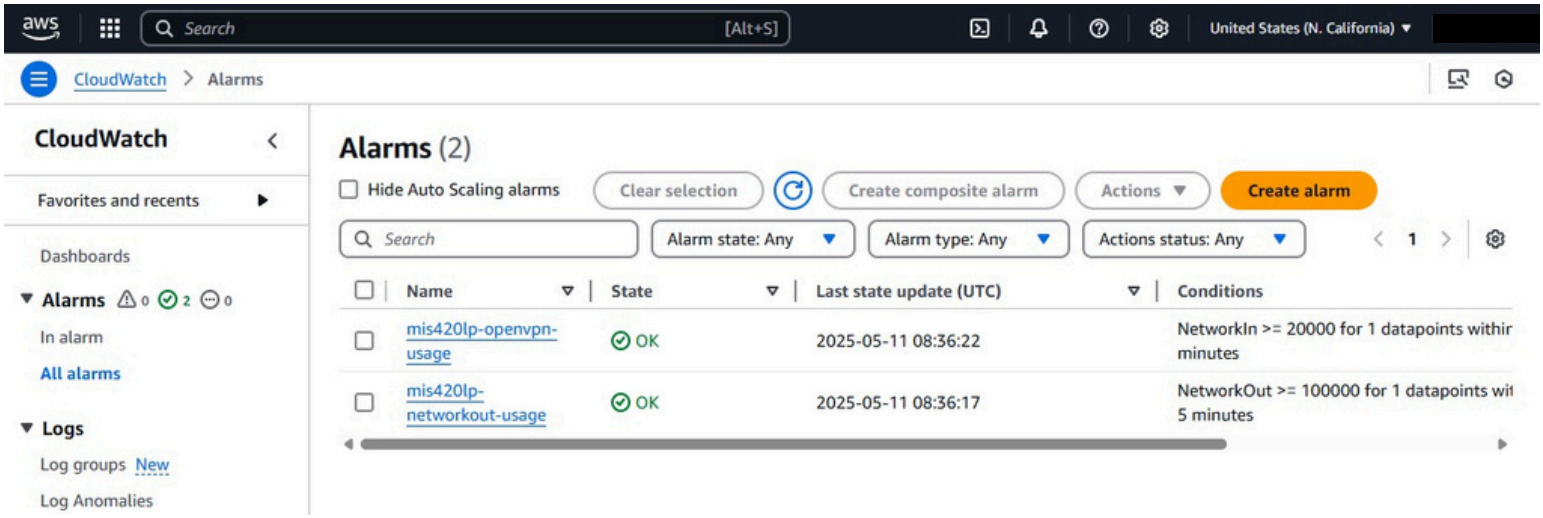


12. Backup plan and backup vault AMI

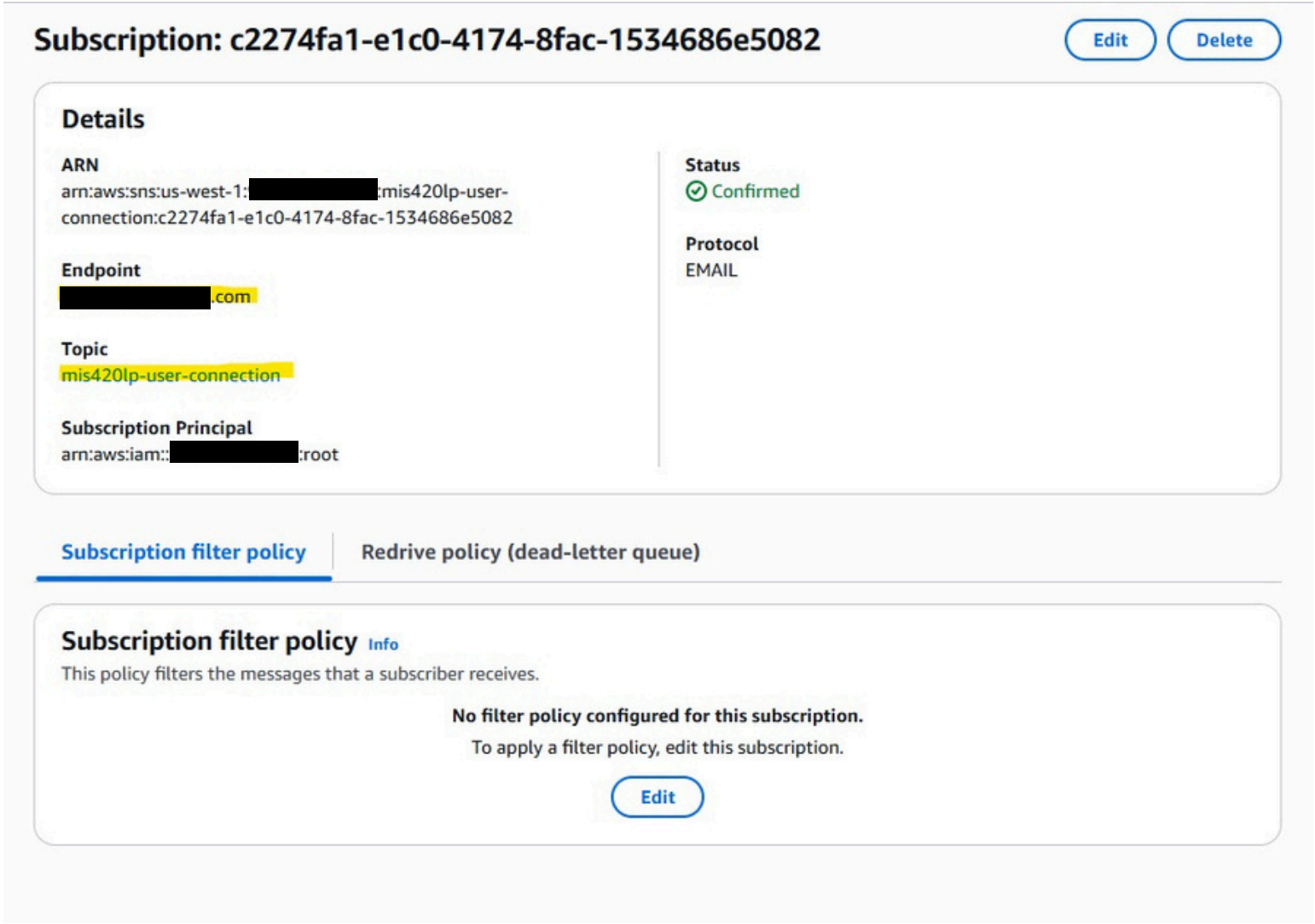




13. CloudWatch Alarms for EC2 instance traffic



14. Utilizing Amazon SNS to set email notifications



Subscription: b3857455-5af6-459f-ab3a-92885b062c09

Edit | Delete

Details

ARN
arn:aws:sns:us-west-1:[redacted]:mis420lp-networkout-usage:b3857455-5af6-459f-ab3a-92885b062c09

Endpoint
[redacted].com

Topic
mis420lp-networkout-usage

Subscription Principal
arn:aws:iam::[redacted]:root

Status
Confirmed

Protocol
EMAIL

Subscription filter policy | Redrive policy (dead-letter queue)

Subscription filter policy Info

This policy filters the messages that a subscriber receives.

No filter policy configured for this subscription.

To apply a filter policy, edit this subscription.

Edit

15. CloudWatch Notification for VPN usage

Gmail Luca <[redacted]>

ALARM: "mis420lp-openvpn-usage" in US West (N. California)

AWS Notifications <no-reply@sns.amazonaws.com> Sat, May 10, 2025 at 10:16 PM
To [redacted]

You are receiving this email because your Amazon CloudWatch Alarm "mis420lp-openvpn-usage" in the US West (N. California) region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [71043.0 (11/05/25 05:11:00)] was greater than or equal to the threshold (20000.0)." at "Sunday 11 May, 2025 05:16:22 UTC".

View this alarm in the AWS Management Console:
https://us-west-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-1#alarmsV2:alarm/mis420lp-openvpn-usage

Alarm Details:
- Name: mis420lp-openvpn-usage
- Description: Alarm on instance i-019d2674f4533ad18: Triggered when NetworkIn >= 20000 for 1 consecutive 5-minute periods.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [71043.0 (11/05/25 05:11:00)] was greater than or equal to the threshold (20000.0).
- Timestamp: Sunday 11 May, 2025 05:16:22 UTC
- AWS Account: [redacted]
- Alarm Arn: arn:aws:cloudwatch:us-west-1:[redacted]:alarm:mis420lp-openvpn-usage

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 20000.0 for at least 1 of the last 1 period(s) of 300 seconds.

Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: NetworkIn
- Dimensions: [InstanceId = i-019d2674f4533ad18]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-west-1[redacted]:mis420lp-user-connection]
- INSUFFICIENT_DATA:

Gmail Luca <[redacted]>

ALARM: "mis420lp-networkout-usage" in US West (N. California)
1 message

AWS Notifications <no-reply@sns.amazonaws.com> Sun, May 11, 2025 at 1:32 AM
To: [redacted]

You are receiving this email because your Amazon CloudWatch Alarm "mis420lp-networkout-usage" in the US West (N. California) region has entered the ALARM state, because "Threshold Crossed: 1 datapoint [1.0636053E7 (11/05/25 08:27:00)] was greater than or equal to the threshold (100000.0)." at "Sunday 11 May, 2025 08:32:17 UTC".

View this alarm in the AWS Management Console:
https://us-west-1.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-1#alarmsV2:alarm/mis420lp-networkout-usage

Alarm Details:
- Name: mis420lp-networkout-usage
- Description: Alarm on instance i-019d2674f4533ad18: Triggered when NetworkOut >= 100000 for 1 consecutive 5-minute periods.
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 datapoint [1.0636053E7 (11/05/25 08:27:00)] was greater than or equal to the threshold (100000.0).
- Timestamp: Sunday 11 May, 2025 08:32:17 UTC
- AWS Account: [redacted]
- Alarm Arn: arn:aws:cloudwatch:us-west-1[redacted]alarm:mis420lp-networkout-usage

Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanOrEqualToThreshold 100000.0 for at least 1 of the last 1 period(s) of 300 seconds.

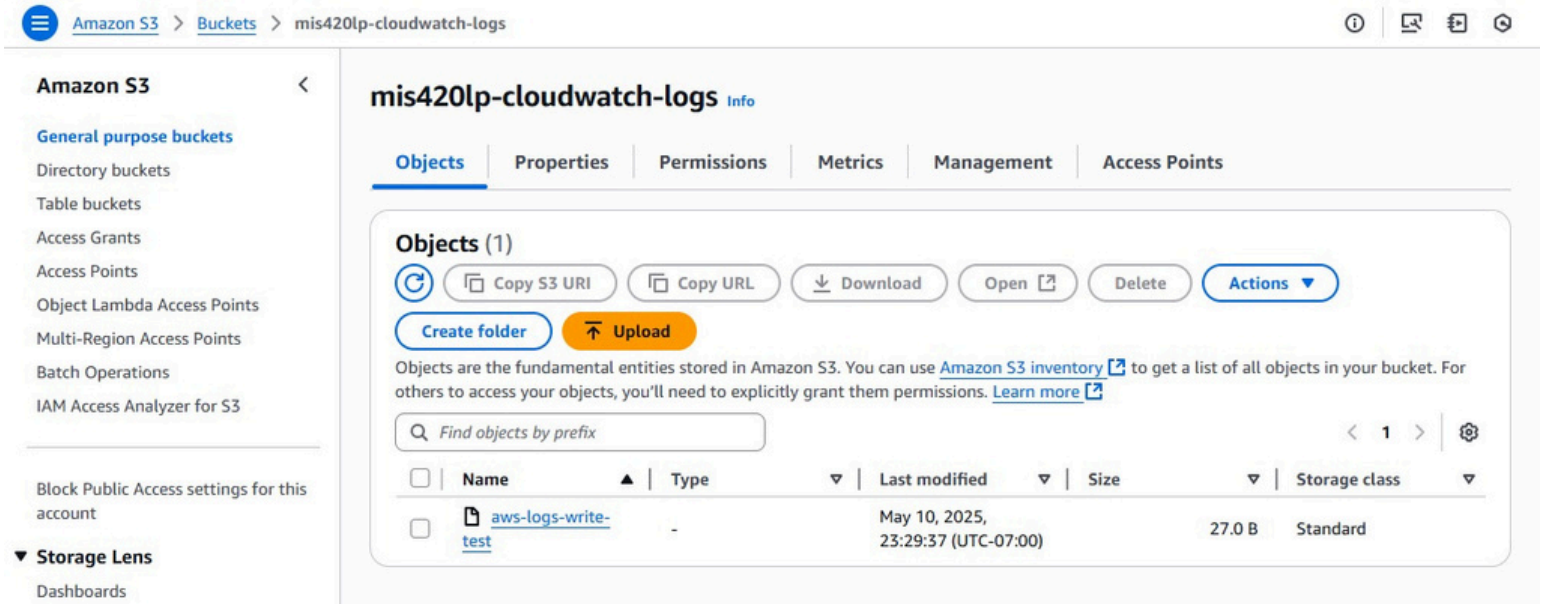
Monitored Metric:
- MetricNamespace: AWS/EC2
- MetricName: NetworkOut
- Dimensions: [InstanceId = i-019d2674f4533ad18]
- Period: 300 seconds
- Statistic: Average
- Unit: not specified

State Change Actions:
- OK:
- ALARM: [arn:aws:sns:us-west-1:[redacted]:mis420lp-networkout-usage]
- INSUFFICIENT_DATA:

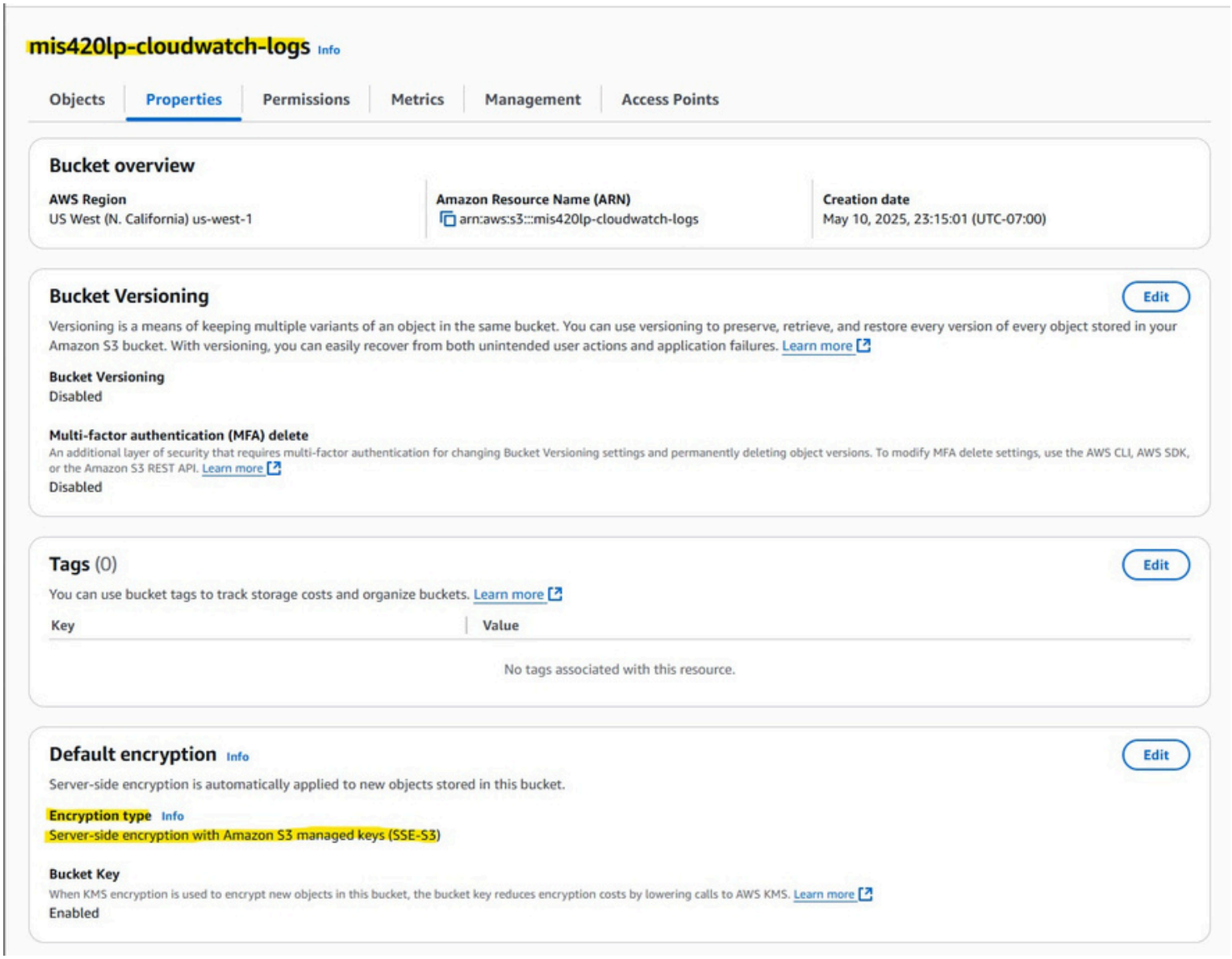
--
If you wish to stop receiving notifications from this topic, please click or visit the link below to unsubscribe:
https://sns.us-west-1.amazonaws.com/unsubscribe.html?SubscriptionArn=arn:aws:sns:us-west-1[redacted]mis420lp-networkout-usage:b3857455-5af6-459f-ab3a-92885b062c09&Endpoint=[redacted]

Please do not reply directly to this email. If you have any questions or comments regarding this email, please contact us at https://aws.amazon.com/support

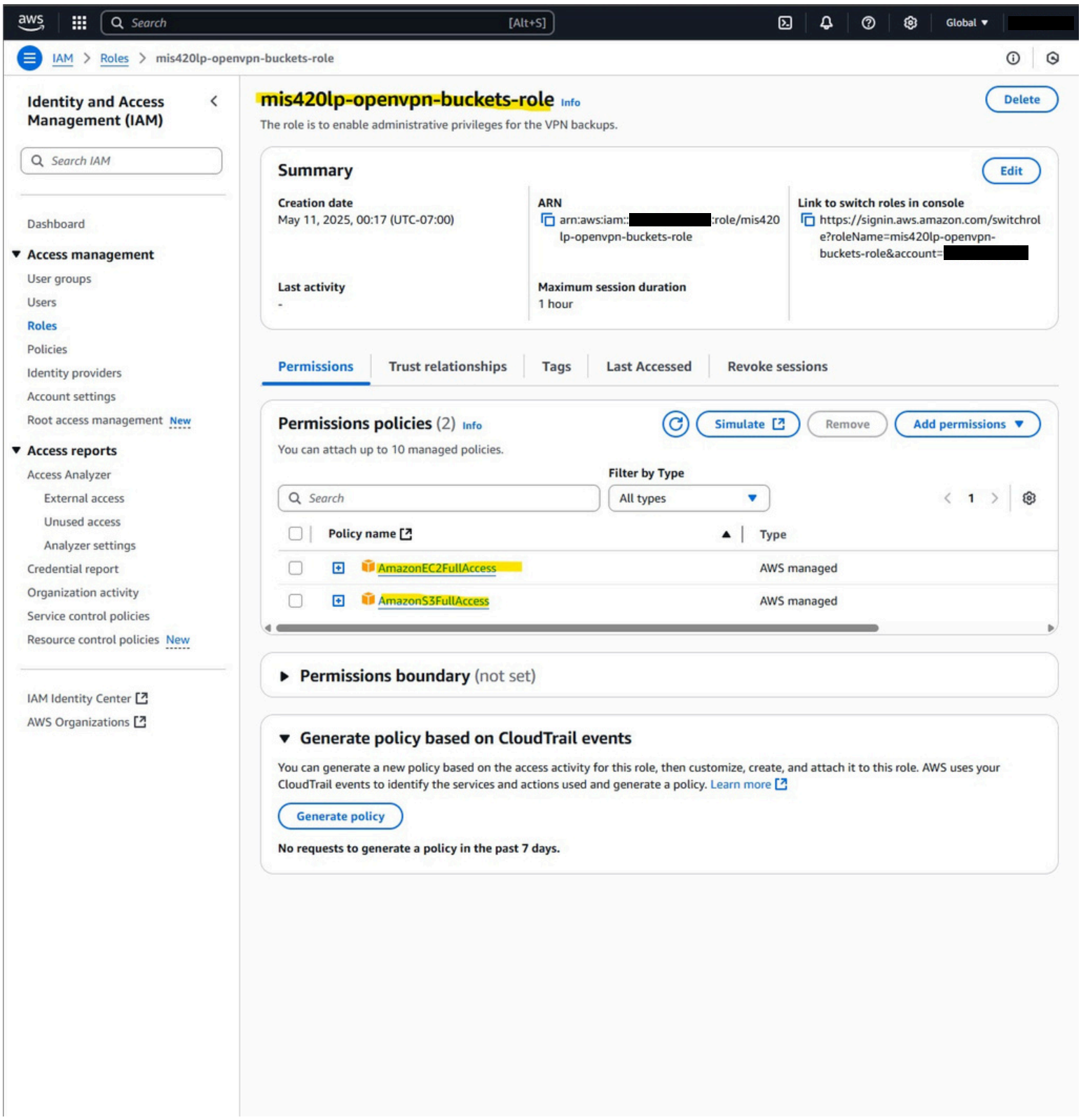
16. Logs backed up to S3 bucket



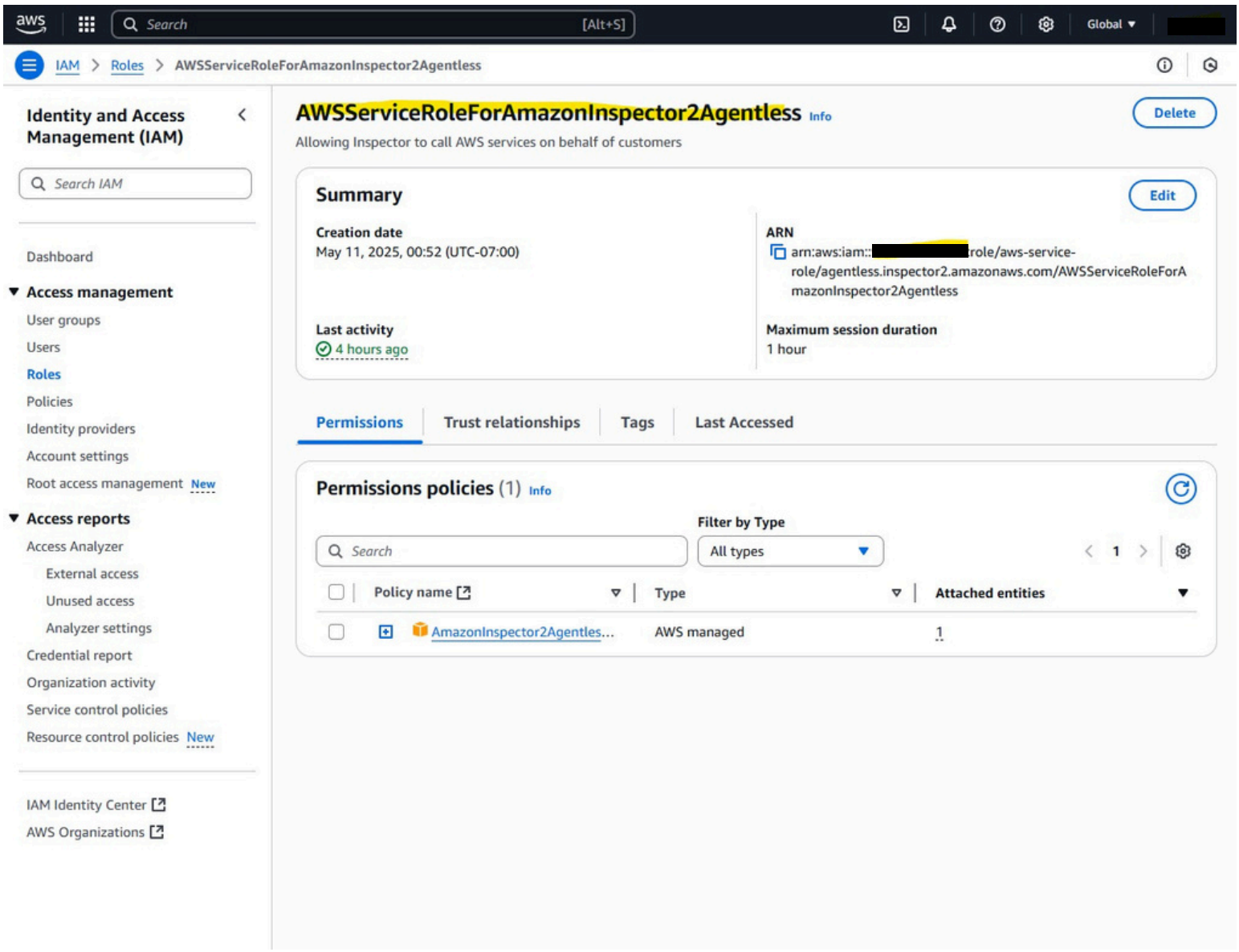
17. Bucket encryption for logs



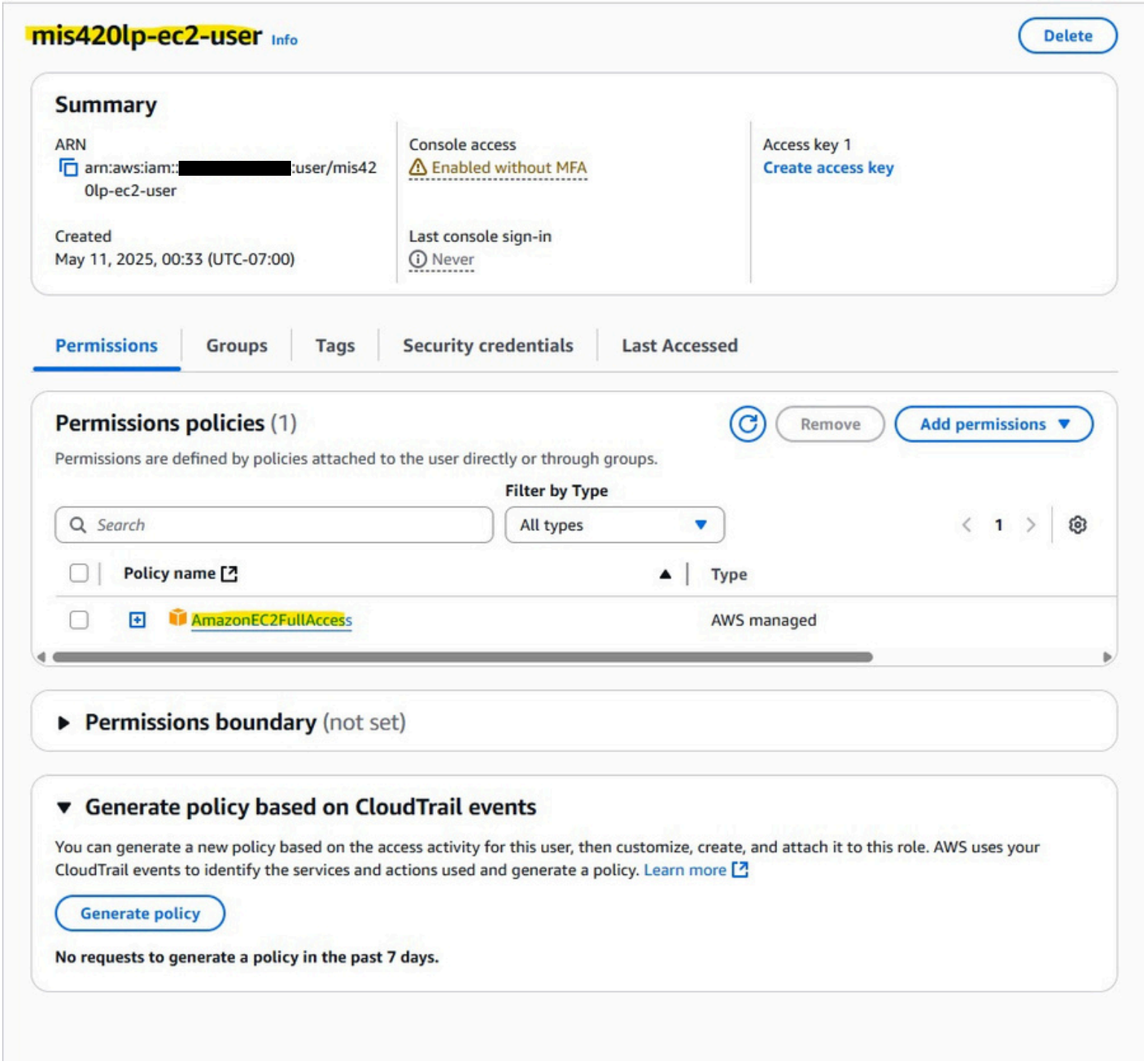
18. Role for OpenVPN buckets and instances



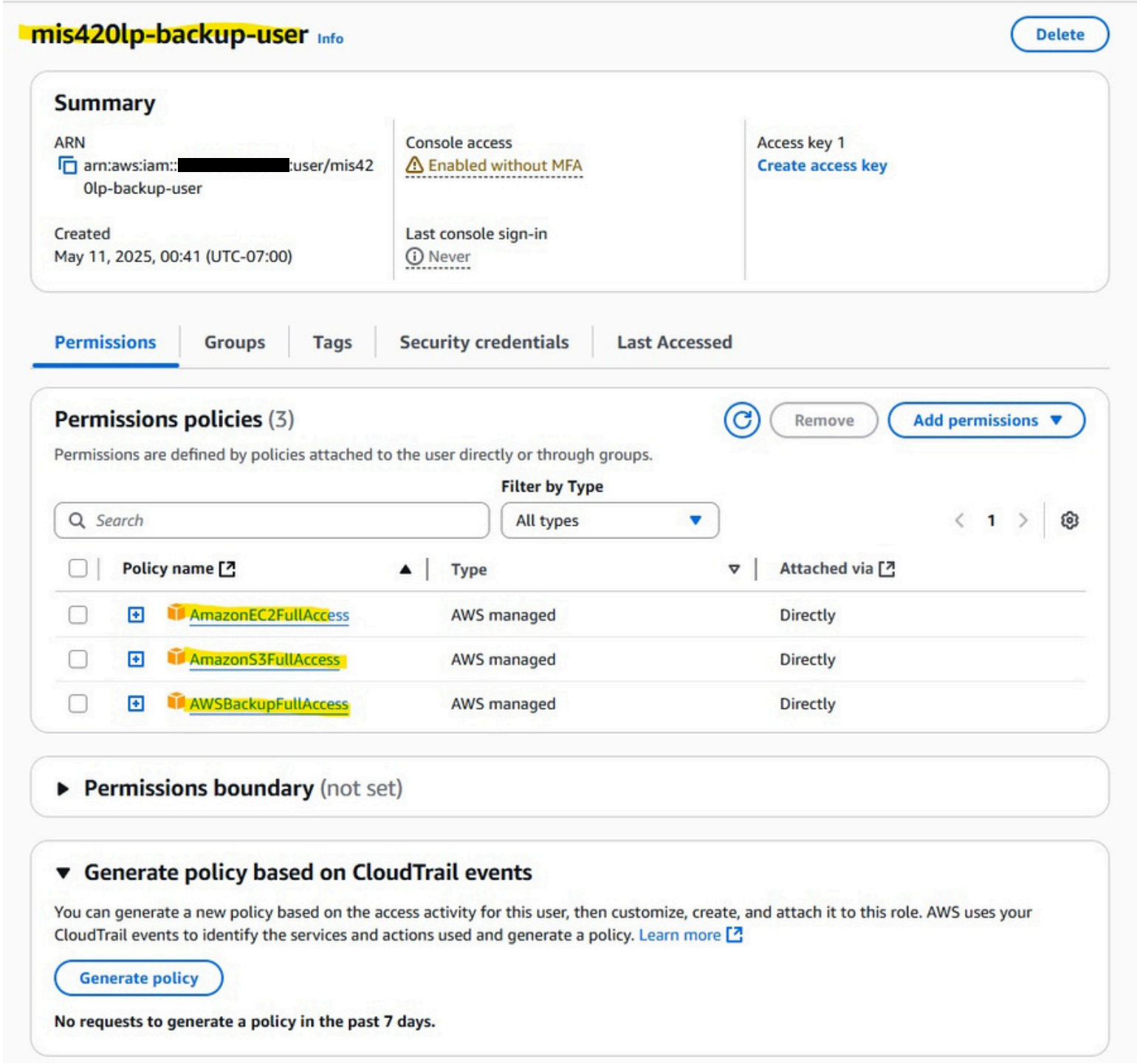
19. Role for utilizing inspector



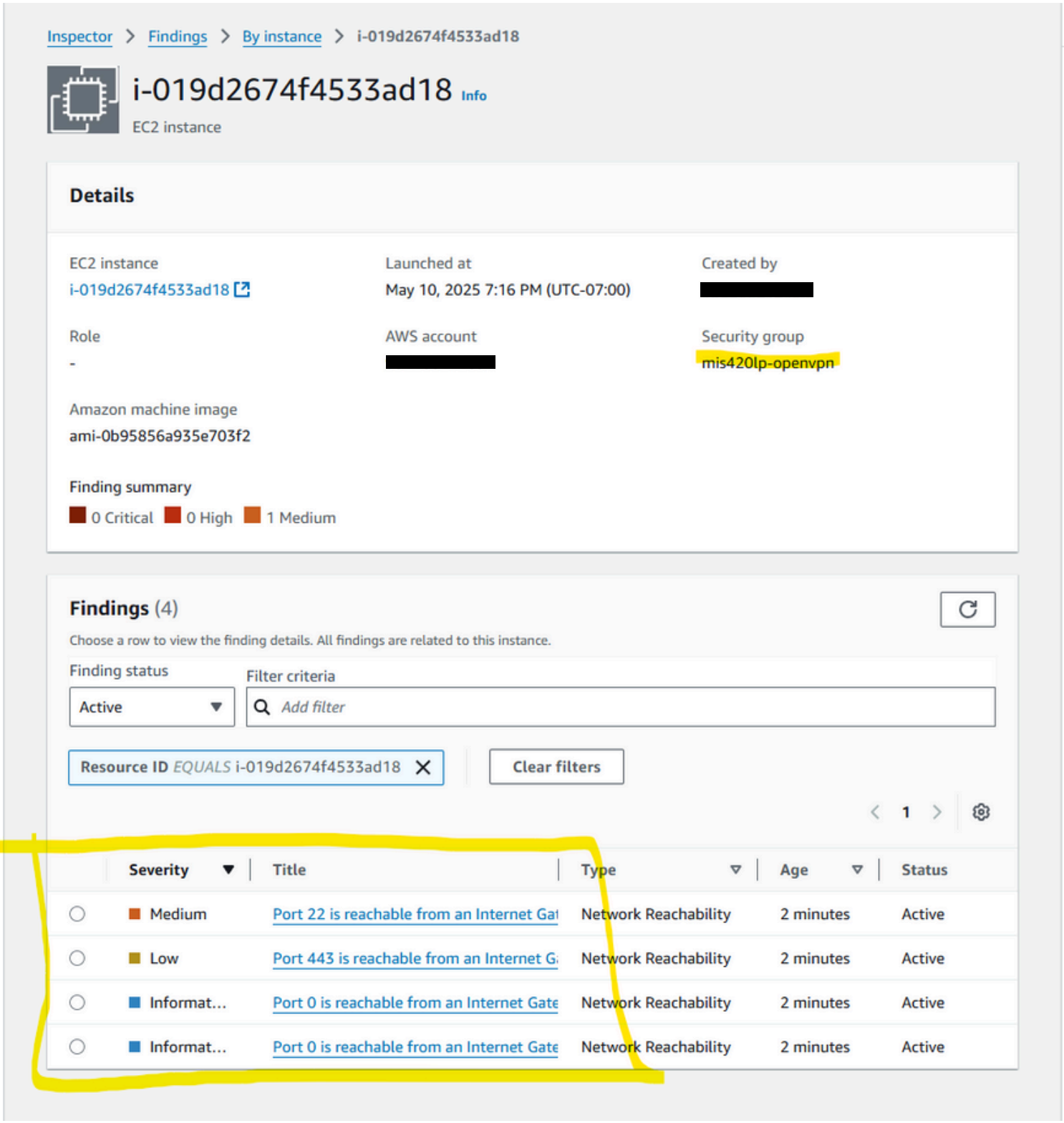
20. EC2 administrator user account



21. Account for managing backups for resources



22. Amazon Inspector EC2 scan results



i-019d2674f4533ad18 Info

EC2 instance

Details

EC2 instance
i-019d2674f4533ad18

Launched at
May 10, 2025 7:16 PM (UTC-07:00)

Created by
[redacted]

Role
-

AWS account
[redacted]

Security group
mis420lp-openvpn

Amazon machine image
ami-0b95856a935e703f2

Finding summary
20 Critical 438 High
1403 Medium

Findings (200+)

Choose a row to view the finding details. All findings are related to this instance.

Finding status: Active

Filter criteria: Add filter

Resource ID *EQUALS* i-019d2674f4533ad18 | Clear filters

1 2 3 4 5 6 7 ... >

Severity	Title	Type	Age	Status
Critical	CVE-2024-47685 - linux-image-aws	Package Vulnerability	4 minutes	Active
Critical	CVE-2024-45492 - libexpat1	Package Vulnerability	4 minutes	Active
Critical	CVE-2022-48174 - busybox-initramfs,	Package Vulnerability	4 minutes	Active
Critical	CVE-2020-27619 - python3.10, pytho	Package Vulnerability	4 minutes	Active
Critical	CVE-2024-45491 - libexpat1	Package Vulnerability	4 minutes	Active
Critical	CVE-2019-9636 - python3.10, python	Package Vulnerability	4 minutes	Active
Critical	CVE-2019-10160 - python3.10, pytho	Package Vulnerability	4 minutes	Active
Critical	CVE-2024-37371 - libgssapi-krb5-2, li	Package Vulnerability	4 minutes	Active
Critical	CVE-2022-36227 - libarchive13	Package Vulnerability	4 minutes	Active
Critical	CVE-2019-9948 - python3.10, python	Package Vulnerability	4 minutes	Active
Critical	CVE-2016-9841 - klibc-utils, libklibc	Package Vulnerability	4 minutes	Active