

1. VPC creation for the project

Screenshot of the AWS VPC dashboard showing the creation of a new VPC named "mis420lp-vpc".

The VPC details page shows the following configuration:

VPC ID	Name	State	Block Public Access	DNS hostnames
vpc-064674499de0bdd40	mis420lp-vpc	Available	Off	Enabled
CIDR	Tenancy	DHCP option set	Main route table	
10.0.0.0/16	default	dopt-0a128309a6889131c	rtb-00423ca47991ffc6d	
Default VPC	IPv4 CIDR	IPv6 pool	Owner ID	
No	10.0.0.0/16	-	[REDACTED]	
IPv6 CIDR	Network Address Usage metrics	Route 53 Resolver DNS Firewall rule groups		
-	Disabled	-		

2. Security Groups for the OpenVPN EC2 instance

Screenshot of the AWS EC2 Security Groups page showing the configuration for the security group sg-029ee7b3b24563034.

Success Message: Inbound security group rules successfully modified on security group (sg-029ee7b3b24563034 | mis420lp-openvpn)

Security Group Details:

- Security group name: mis420lp-openvpn
- Security group ID: sg-029ee7b3b24563034
- Description: OpenVPN
- VPC ID: vpc-064674499de0bdd40
- Owner: [REDACTED]
- Inbound rules count: 5 Permission entries
- Outbound rules count: 0 Permission entries

Inbound Rules (5):

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-0a1c0a9aca95cf2a	IPv4	All ICMP - IPv4	ICMP
-	sgr-0a2d95c159e5c072b	IPv4	Custom TCP	TCP
-	sgr-0f8090351f55f607	IPv4	HTTPS	TCP
-	sgr-0d40da4d29c89864f	IPv4	Custom UDP	UDP
-	sgr-013060837e5f3b5d3	IPv4	SSH	TCP

Actions: Manage tags, Edit inbound rules.

Left Sidebar:

- EC2
- Dashboard
- EC2 Global View
- Events
- Instances
 - Instances
 - Instance Types
 - Launch Templates
 - Spot Requests
 - Savings Plans
 - Reserved Instances
 - Dedicated Hosts
 - Capacity Reservations
- Images
 - AMIs
 - AMI Catalog
- Elastic Block Store
 - Volumes
 - Snapshots
 - Lifecycle Manager
- Network & Security
 - Security Groups
 - Elastic IPs
 - Placement Groups
 - Key Pairs
 - Network Interfaces
- Load Balancing
 - Load Balancers
 - Target Groups
 - Trust Stores
- Auto Scaling
 - Auto Scaling Groups
- Settings

3. Creating Outbound Rules

The screenshot shows the AWS EC2 Security Groups interface. A success message at the top right indicates that outbound security group rules were successfully modified on security group sg-029ee7b3b24563034 | mis420lp-openvpn.

Details

Security group name mis420lp-openvpn	Security group ID sg-029ee7b3b24563034	Description OpenVPN	VPC ID vpc-064674499de0bdd40
Owner [REDACTED]	Inbound rules count 5 Permission entries	Outbound rules count 3 Permission entries	

Outbound rules (3)

Name	Security group rule ID	IP version	Type	Protocol
-	sgr-03318737412340260	IPv4	DNS (UDP)	UDP
-	sgr-07dbb4fa8f5c8dcad	IPv4	HTTPS	TCP
-	sgr-05100c17dd12fd03e	IPv4	HTTP	TCP

A yellow box highlights the last three columns of the Outbound rules table: IP version, Type, and Protocol.

4. Creating an EC2 instance for OpenVPN

5. Creating an elastic IPv4 for the Instance

The screenshot shows the AWS EC2 console with the 'Elastic IP addresses' page open. The left sidebar is collapsed, and the main content area displays the following information:

Elastic IP addresses (1/1)

Name	Allocated IPv4 addr...	Type	Allocation ID
mis420lp-elasticip	13.52.48.141	Public IP	eipalloc-08f40a1052040b047

Summary

Allocated IPv4 address	Type	Allocation ID	Reverse DNS record
13.52.48.141	Public IP	eipalloc-08f40a1052040b047	-
Association ID	Scope	Associated instance ID	Private IP address
-	VPC	-	-
Network interface ID	Network interface owner account ID	Public DNS	NAT Gateway ID
-	-	-	-
Address pool	Amazon		

6. Associating the Elastic IP to the EC2 instance

The screenshot shows the AWS EC2 Instances page. On the left, a navigation pane lists various services: EC2, Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups, Elastic IPs, Placement Groups, Key Pairs, Network Interfaces), Load Balancing (Load Balancers, Target Groups, Trust Stores), and Auto Scaling (Auto Scaling Groups, Settings). The main content area displays the 'Instances (1/1)' section. A search bar at the top allows finding instances by attribute or tag. Below it, a table lists one instance: 'mis420lp-ope...' (Instance ID: i-019d2674f4533ad18), which is 'Running' (t2.small, 2/2 checks passed). The instance details page for 'i-019d2674f4533ad18 (mis420lp-openvpn)' is shown, with tabs for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. The Details tab is selected, showing sections for Instance summary, Hostname type, Answer private resource DNS name, Auto-assigned IP address, IAM Role, IMDSv2, Operator, and Instance details. The IMDSv2 section includes a note from EC2 recommending its use.

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

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\ ssh -i C:\Downloads\mis420lp-openvpn.pem openvpn@13.52.48.141

specified in your contract with OpenVPN Inc.

Please enter 'yes' to indicate your agreement [no]: yes

Once you provide a few initial configuration settings,
OpenVPN Access Server can be configured by accessing
its Admin Web UI using your Web browser.

Will this be the primary Access Server node?
(enter 'no' to configure as a backup or standby node)
> Press ENTER for default [yes]: yes

Please specify the network interface and IP address to be
used by the Admin Web UI:
(1) all interfaces: 0.0.0.0
(2) eth0: 10.0.10.21
Please enter the option number from the list above (1- 2).
> Press Enter for default [1]: 1

What public/private type/algorithms do you want to use for the OpenVPN CA?

Recommended choices:

rsa      - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall  - shows all options including non-recommended algorithms.
> Press ENTER for default [secp384r1]: secp384r1

What public/private type/algorithms do you want to use for the self-signed web certificate?

Recommended choices:

rsa      - maximum compatibility
secp384r1 - elliptic curve, higher security than rsa, allows faster connection setup and smaller user profile files
showall  - shows all options including non-recommended algorithms.
> Press ENTER for default [secp384r1]: secp384r1

Please specify the port number for the Admin Web UI.
> Press ENTER for default [943]: 943

Please specify the TCP port number for the OpenVPN Daemon
> Press ENTER for default [443]: 443

Should client traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes

Should client DNS traffic be routed by default through the VPN?
> Press ENTER for default [no]: yes
Admin user authentication will be local

Private subnets detected: ['10.0.0.0/16']

Should private subnets be accessible to clients by default?
> Press ENTER for EC2 default [yes]: yes

To initially login to the Admin Web UI, you must use a
username and password that successfully authenticates you
with the host UNIX system (you can later modify the settings
so that RADIUS or LDAP is used for authentication instead).

You can login to the Admin Web UI as "openvpn" or specify
a different user account to use for this purpose.

Do you wish to login to the Admin UI as "openvpn"?
> Press ENTER for default [yes]: yes

Type a password for the 'openvpn' account (if left blank, a random password will be generated):
Error: Password must contain a digit, an Uppercase letter, and a symbol from !@#$%^&()**+,~/[\]^_`{|}~<>
Type a password for the 'openvpn' account (if left blank, a random password will be generated):
Confirm the password for the 'openvpn' account:

> Please specify your Activation key (or leave blank to specify later):
```

8. Computer IP before and after connecting to the VPN

MY IP IP LOOKUP HIDE MY IP VPNS ▾ TOOLS ▾ LEARN ▾

My IP Address is:

IPv6: ? **2603:8000**: [REDACTED]

IPv4: ? [REDACTED]

My IP Information:

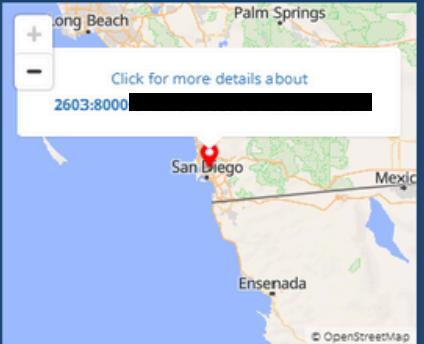
ISP: [REDACTED]

City: San Diego
Region: California
Country: United States

Your location may be exposed!

HIDE MY IP ADDRESS NOW

Show Complete IP Details

 Click for more details about 2603:8000 [REDACTED]
© OpenStreetMap

Location not accurate?
[Update My IP Location](#)

MY IP IP LOOKUP HIDE MY IP VPNS ▾ TOOLS ▾ LEARN ▾

IPv4: ? **13.52.48.141**

IPv6: ? Not detected

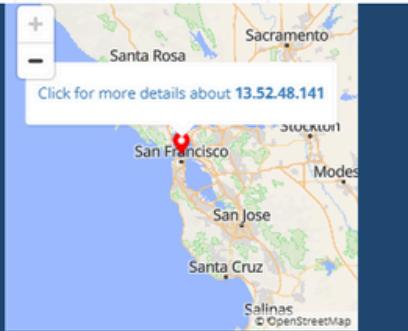
My IP Information:

ISP: Amazon.com Inc.
City: San Francisco
Region: California
Country: United States

Are you using a VPN?

RATE YOUR VPN

Show Complete IP Details

 Click for more details about 13.52.48.141 [REDACTED]
© OpenStreetMap

Location not accurate?
[Update My IP Location](#)

9. AMI creation for S3 bucket

The screenshot shows the AWS EC2 console with the 'AMIs' section selected. On the left, a sidebar lists various EC2 services: Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (selected), and AMIs. The main content area displays the 'Amazon Machine Images (AMIs) (1/1)' page. A table lists one AMI entry:

Name	AMI name	AMI ID	Source	Owner
mis420lp-openvpn-backup	ami-06e963974c2835bcd	[REDACTED]	/mis420lp-openvpn-bac...	[REDACTED]

Below this, a detailed view for the selected AMI (AMI ID: ami-06e963974c2835bcd) is shown. The 'Details' tab is active, displaying the following information:

AMI ID	Image type	Platform details	Root device type
ami-06e963974c2835bcd	machine	Linux/UNIX	EBS

AMI name: mis420lp-openvpn-backup
Owner account ID: [REDACTED]
Architecture: x86_64
Usage operation: RunInstances
Root device name: /dev/sda1
Status: Pending
Source: [REDACTED] /mis420lp-openvpn-backup
Virtualization type: hvm
Boot mode: uefi-preferred
State reason: -
Creation date: 2025-05-11T04:18:19.000Z
Kernel ID: -
Description: backup of OpenVPN ec2
Product codes: -
RAM disk ID: -
Deprecation time: -
Last launched time: -
Block devices:

- /dev/sda1=8:true:gp2
- /dev/sdb=ephemeral0
- /dev/sdc=ephemeral1

Deregistration protection: Disabled
Allowed image: -
Source AMI ID: ami-0b95856a935e703f2
Source AMI Region: us-west-1

10. S3 bucket AMI storage

The screenshot shows the AWS S3 console interface. At the top, there's a navigation bar with the AWS logo, a search bar, and a "United States (N. California)" dropdown. Below the navigation bar, the path "Amazon S3 > Buckets > mis420lp-openvpn-backup1" is displayed. The main title "mis420lp-openvpn-backup1" is followed by a "Info" link. A horizontal menu bar below the title includes "Objects", "Properties", "Permissions", "Metrics", "Management", and "Access Points".

The "Objects" tab is selected, showing a list of objects. There is one object listed:

Name	Type	Last modified	Size	Storage class
ami-06e963974c2835bcd.bin	bin	May 10, 2025, 21:31:42 (UTC-07:00)	2.0 GB	Standard

Below the table, there are several action buttons: "Copy S3 URI", "Copy URL", "Download", "Open", "Delete", "Actions", "Create folder", and "Upload". A note at the top of the object list states: "Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)".

11. Bucket encryption for AMI

The screenshot shows the AWS S3 Bucket Properties page for the bucket 'mis420lp-openvpn-backup1'. The top navigation bar includes the AWS logo, a search bar, and a 'Search' button. The region is set to 'United States (N. California)'. The main content area has tabs for 'Objects', 'Properties' (which is selected), 'Permissions', 'Metrics', 'Management', and 'Access Points'. The 'Properties' tab contains sections for 'Bucket overview', 'Bucket Versioning', 'Multi-factor authentication (MFA) delete', 'Tags (0)', and 'Default encryption'.

Bucket overview

AWS Region US West (N. California) us-west-1	Amazon Resource Name (ARN) arn:aws:s3:::mis420lp-openvpn-backup1	Creation date May 10, 2025, 21:27:53 (UTC-07:00)
---	---	---

Bucket Versioning Edit

Versioning is a means of keeping multiple variants of an object in the same bucket. You can use versioning to preserve, retrieve, and restore every version of every object stored in your Amazon S3 bucket. With versioning, you can easily recover from both unintended user actions and application failures. [Learn more](#)

Bucket Versioning
Disabled

Multi-factor authentication (MFA) delete
An additional layer of security that requires multi-factor authentication for changing Bucket Versioning settings and permanently deleting object versions. To modify MFA delete settings, use the AWS CLI, AWS SDK, or the Amazon S3 REST API. [Learn more](#)

Disabled

Tags (0) Edit

You can use bucket tags to track storage costs and organize buckets. [Learn more](#)

Key	Value
No tags associated with this resource.	

Default encryption Edit

Server-side encryption is automatically applied to new objects stored in this bucket.

Encryption type Info
Server-side encryption with Amazon S3 managed keys (SSE-S3)

Bucket Key
When KMS encryption is used to encrypt new objects in this bucket, the bucket key reduces encryption costs by lowering calls to AWS KMS. [Learn more](#)

Enabled

12. Backup plan and backup vault AMI

mis420lp-backup

[Delete](#)[View JSON](#)

Summary

Backup plan name

mis420lp-backup

Version ID

NjEwZWQ0ZWMTN2M2YS00
OWYxLThlZDktM2MwZjhYTM
zYzEz

Last modified

May 11, 2025, 14:30:40 (UTC-
07:00)

Last runtime

-

Backup plan ID

6227666f-c23b-4c41-b732-
7cb1f9428531

Backup rules (1)

[Edit](#)[Delete](#)[Add backup rule](#)

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

Name

▲

Backup vault

▼

Destination Backup vault

 Monthly

Default

-

Resource assignments (1)

[Delete](#)[Assign resources](#)

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

< 1 > ⚙

Name

▼

IAM role ARN

▼

Creation time

 mis420lp-ec2-backup

arn:aws:iam:[REDACTED]:role/service-role/AWSBackupDefaultServiceRole May 11, 2025, 14:31:48

mis420lp-ec2-vpn [Info](#)

[Create vault lock](#)[Delete vault](#)[Edit access policy](#)

Summary

Vault name

mis420lp-ec2-vpn

KMS encryption key ID

c5ba5e46-a530-4cc0-9e3e-
90b954f9ab2e ↗

Vault type

Backup vault

Creation date

May 11, 2025, 14:39:46 (UTC-07:00)

Vault lock

-

Retention period for vault lock

Minimum retention period: -

Maximum retention period: -

Vault ARN

arn:aws:backup:us-west-
1:[REDACTED]:backup-vault:miss420lp-
ec2-vpn[Recovery points](#)[Protected resources](#)

Recovery points (1) [Info](#)

[Deselect all](#)[Actions ▾](#)

Recovery point count value displayed in the console can be an approximation. See ListRecoveryPointsByBackupVault API to obtain the exact count.

 Filter by resource type, recovery point ARN, status, resource ARN or source account ID

< 1 > ⚙

 Recovery point ID

▼

Status

▼

Resource name

▼

Resource ID

▼

Resource ty

 image/ami-0100f435a179e9afe Completed

mis420lp-openvpn

instance/i-019d2674f4533ad18

EC2

13. CloudWatch Alarms for EC2 instance traffic

The screenshot shows the AWS CloudWatch Alarms page. On the left, there's a navigation sidebar with 'CloudWatch' selected. Under 'Alarms', there are links for 'In alarm' and 'All alarms'. Below that is a 'Logs' section with 'Log groups' and 'Log Anomalies'. The main area is titled 'Alarms (2)' and lists two alarms:

Name	State	Last state update (UTC)	Conditions
mis420lp-openvpn-usage	OK	2025-05-11 08:36:22	NetworkIn >= 20000 for 1 datapoints within minutes
mis420lp-networkout-usage	OK	2025-05-11 08:36:17	NetworkOut >= 100000 for 1 datapoints within 5 minutes

14. Utilizing Amazon SNS to set email notifications

Subscription: c2274fa1-e1c0-4174-8fac-1534686e5082

Edit

Delete

Details

ARN

arn:aws:sns:us-west-1:██████████:mis420lp-user-connection:c2274fa1-e1c0-4174-8fac-1534686e5082

Endpoint

██████████.com

Topic

mis420lp-user-connection

Subscription Principal

arn:aws:iam:██████████: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

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



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: [Instanceld = 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:



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: [Instanceld = 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=\[REDACTED\]](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

The screenshot shows the Amazon S3 console with the path: Amazon S3 > Buckets > mis420lp-cloudwatch-logs. The left sidebar includes sections for General purpose buckets, Storage Lens, and Dashboards. The main content area displays the 'mis420lp-cloudwatch-logs' bucket with one object listed: 'aws-logs-write-test'. The object was last modified on May 10, 2025, at 23:29:37 (UTC-07:00), has a size of 27.0 B, and is stored in the Standard storage class.

Name	Type	Last modified	Size	Storage class
aws-logs-write-test	-	May 10, 2025, 23:29:37 (UTC-07:00)	27.0 B	Standard

17. Bucket encryption for logs

The screenshot shows the 'Properties' tab for the 'mis420lp-cloudwatch-logs' bucket. It includes sections for Bucket overview, Bucket Versioning, Multi-factor authentication (MFA) delete, Tags (0), and Default encryption. The Bucket Overview section shows the AWS Region as US West (N. California) us-west-1, the ARN as arn:aws:s3:::mis420lp-cloudwatch-logs, and the Creation date as May 10, 2025, 23:15:01 (UTC-07:00). The Bucket Versioning section indicates it is disabled. The MFA delete section also indicates it is disabled. The Tags section shows no tags associated with the resource. The Default encryption section indicates server-side encryption is automatically applied to new objects stored in this bucket, using SSE-S3 encryption type and an enabled Bucket Key.

Key	Value
No tags associated with this resource.	

18. Role for OpenVPN buckets and instances

The screenshot shows the AWS IAM Roles page. On the left, a sidebar navigation includes 'Identity and Access Management (IAM)', 'Dashboard', 'Access management' (with 'Roles' selected), 'Policies', 'Identity providers', 'Account settings', 'Root access management', and 'Access reports'. Below these are links for 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', 'Organization activity', 'Service control policies', and 'Resource control policies'. At the bottom of the sidebar are links for 'IAM Identity Center' and 'AWS Organizations'.

The main content area displays the 'mis420lp-openvpn-buckets-role' configuration. The role's ARN is listed as `arn:aws:iam:█████████████████████:role/mis420lp-openvpn-buckets-role`. The 'Summary' section shows the creation date as May 11, 2025, 00:17 (UTC-07:00), and the last activity as '-' with a maximum session duration of 1 hour. An 'Edit' button is available in the top right corner of the summary box. A 'Link to switch roles in console' is provided with the URL `https://signin.aws.amazon.com/switchrole?roleName=mis420lp-openvpn-buckets-role&account=█████████████████████`.

The 'Permissions' tab is selected, showing two attached policies: `AmazonEC2FullAccess` and `AmazonS3FullAccess`, both of which are AWS managed policies. There are buttons for 'Simulate', 'Remove', and 'Add permissions'. A 'Permissions boundary (not set)' section is shown below the policy list.

A 'Generate policy based on CloudTrail events' section is present, with a note that no requests have been made in the past 7 days. A 'Generate policy' button is available in this section.

19. Role for utilizing inspector

The screenshot shows the AWS IAM Roles page. The left sidebar includes sections for Identity and Access Management (IAM), Access management, Access reports, and other AWS services like IAM Identity Center and AWS Organizations. The main content area displays the details of a role named "AWSServiceRoleForAmazonInspector2Agentless".

AWSServiceRoleForAmazonInspector2Agentless Info

Allowing Inspector to call AWS services on behalf of customers

Summary

Creation date: May 11, 2025, 00:52 (UTC-07:00)

Last activity: 4 hours ago

ARN: arn:aws:iam::██████████:role/aws-service-role/agentless.inspector2.amazonaws.com/AWSServiceRoleForAmazonInspector2Agentless

Maximum session duration: 1 hour

Permissions Trust relationships Tags Last Accessed

Permissions policies (1) Info

Filter by Type: All types

Policy name	Type	Attached entities
AmazonInspector2Agentless...	AWS managed	1

20. EC2 administrator user account

mis420lp-ec2-user [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::██████████:user/mis420lp-ec2-user	Console access Enabled without MFA	Access key 1 Create access key
Created May 11, 2025, 00:33 (UTC-07:00)	Last console sign-in Never	

Permissions [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

Permissions policies (1) [Edit](#) [Remove](#) [Add permissions ▾](#)

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

Filter by Type	
Search	All types
<input type="checkbox"/> Policy name <input type="text"/>	Type
<input type="checkbox"/> AmazonEC2FullAccess	AWS managed

1

▶ **Permissions boundary (not set)**

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more ↗](#)

[Generate policy](#)

No requests to generate a policy in the past 7 days.

21. Account for managing backups for resources

mis420lp-backup-user [Info](#) [Delete](#)

Summary

ARN arn:aws:iam::[REDACTED]:user/mis420lp-backup-user	Console access Enabled without MFA	Access key 1 Create access key
Created May 11, 2025, 00:41 (UTC-07:00)	Last console sign-in Never	

Permissions [Groups](#) [Tags](#) [Security credentials](#) [Last Accessed](#)

Permissions policies (3) [C](#) [Remove](#) [Add permissions ▾](#)

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

Filter by Type			
<input type="text"/> Search	All types	< 1 >	
<input type="checkbox"/> Policy name	Type		Attached via
<input type="checkbox"/> AmazonEC2FullAccess	AWS managed		Directly
<input type="checkbox"/> AmazonS3FullAccess	AWS managed		Directly
<input type="checkbox"/> AWSBackupFullAccess	AWS managed		Directly

▶ **Permissions boundary (not set)**

▼ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this user, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. [Learn more](#)

[Generate policy](#)

No requests to generate a policy in the past 7 days.

22. Amazon Inspector EC2 scan results

Inspector > Findings > By instance > i-019d2674f4533ad18



i-019d2674f4533ad18 [Info](#)

EC2 instance

Details

EC2 instance

i-019d2674f4533ad18 [Edit](#)

Launched at

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

Created by

[REDACTED]

Role

-

AWS account

Security group

mis420lp-openvpn

Amazon machine image

ami-0b95856a935e703f2

Finding summary

■ 0 Critical ■ 0 High ■ 1 Medium

Findings (4)

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 [X](#)

[Clear filters](#)

< 1 > [⚙️](#)

	Severity	Title	Type	Age	Status
○	■ Medium	Port 22 is reachable from an Internet Ga	Network Reachability	2 minutes	Active
○	■ Low	Port 443 is reachable from an Internet G	Network Reachability	2 minutes	Active
○	■ Informat...	Port 0 is reachable from an Internet Gate	Network Reachability	2 minutes	Active
○	■ Informat...	Port 0 is reachable from an Internet Gate	Network Reachability	2 minutes	Active



i-019d2674f4533ad18 Info

EC2 instance

Details

EC2 instance
i-019d2674f4533ad18 CopyLaunched at
May 10, 2025 7:16 PM (UTC-07:00)Created by
[REDACTED]Role
- [REDACTED]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

Filter criteria

Active

Resource ID EQUALS i-019d2674f4533ad18 X< 1 2 3 4 5 6 7 ... > ⚙

	Severity ▾	Title	Type	Age ▾	Status
<input type="radio"/>	■ Critical	CVE-2024-47685 - linux-image-aws	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2024-45492 - libexpat1	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2022-48174 - busybox-initramfs,	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2020-27619 - python3.10, python	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2024-45491 - libexpat1	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2019-9636 - python3.10, python	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2019-10160 - python3.10, python	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2024-37371 - libgssapi-krb5-2, lib	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2022-36227 - libarchive13	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2019-9948 - python3.10, python	Package Vulnerability	4 minutes	Active
<input type="radio"/>	■ Critical	CVE-2016-9841 - klibc-utils, libklibc	Package Vulnerability	4 minutes	Active