

AWS Infrastructure Challenge - Technical Report

Relatore: Giuseppe La Selva

Data: 7 Dicembre 2025

Ambiente: AWS Academy (Vocareum)

Regione: us-west-2 (Oregon)

1. Executive Summary

Questa relazione documenta l'implementazione di un'infrastruttura cloud scalabile e tollerante ai guasti su AWS, utilizzando best practices di alta disponibilità, disaster recovery e Infrastructure as Code (IaC). L'architettura è stata progettata per superare i single point of failure attraverso la distribuzione multi-AZ e il load balancing intelligente.

Risultati conseguiti:

- ✓ Application Load Balancer configurato e operativo
- ✓ Multi-AZ deployment con ridondanza geografica
- ✓ EBS Storage persistente con backup
- ✓ Infrastructure as Code (CloudFormation YAML)
- ⚠ Route 53 non implementato (limitazioni lab)
- ⚠ IAM avanzato non implementato (limitazioni lab)
- ✓ CloudTrail disponibile per auditing

2. Architettura di Rete

2.1 Design iniziale e Correzione

Durante la fase di design, è stato identificato un errore non intenzionale di architettura: le subnet pubbliche erano inizialmente collocate nella stessa Availability Zone (us-west-2b), violando il principio fondamentale di High Availability.

Azione Correttiva:

Una subnet aggiuntiva (`my-public-subnet-3`) è stata creata in una AZ diversa (us-west-2a), garantendo la distribuzione geografica richiesta.

Configurazione Finale:

Componente	Dettagli
------------	----------

VPC	<code>my-vpc (10.0.0.0/16)</code>
Subnet Pubblica 1	<code>my-public-subnet-1 (10.0.1.0/24) - us-west-2b</code>
Subnet Pubblica 3	<code>my-public-subnet-3 (10.0.5.0/24) - us-west-2a</code>
Subnet Private 1	<code>my-private-subnet-1 (10.0.3.0/24)</code>
Subnet Private 2	<code>my-private-subnet-2 (10.0.4.0/24)</code>
Internet Gateway	<code>public-igw (Attached)</code>
Route Table Pubblica	<code>public-route-table (0.0.0.0/0 → IGW)</code>

subnet-09e827faf84df843b / my-public-subnet-1

Details		Actions ▾	
Subnet ID	subnet-09e827faf84df843b	State	Available
IPv4 CIDR	10.0.1.0/24	IPv6 CIDR	—
Availability Zone	usw2-az2 (us-west-2b)	VPC	vpc-0a08b732ec7263a78 my-vpc
Network ACL	acl-0affff070d365f413	Auto-assign public IPv4 address	Yes
Auto-assign customer-owned IPv4 address	No	Outpost ID	—
IPv6 CIDR reservations	—	Hostname type	IP name
Resource name DNS AAAA record	Disabled	Owner	235470952249

subnet-07ced93caa81313ba / my-public-subnet-2

Details		Actions ▾	
Subnet ID	subnet-07ced93caa81313ba	State	Available
IPv4 CIDR	10.0.2.0/24	IPv6 CIDR	—
Availability Zone	usw2-az2 (us-west-2b)	VPC	vpc-0a08b732ec7263a78 my-vpc
Network ACL	acl-0affff070d365f413	Auto-assign public IPv4 address	Yes
Auto-assign customer-owned IPv4 address	No	Outpost ID	—
IPv6 CIDR reservations	—	Hostname type	IP name
Resource name DNS AAAA record	Disabled	Owner	235470952249

subnet-08aab5e0eeb79f590 / my-public-subnet-3

Details		Actions ▾	
Subnet ID	subnet-08aab5e0eeb79f590	State	Available
IPv4 CIDR	10.0.5.0/24	IPv6 CIDR	—
Availability Zone	usw2-az1 (us-west-2a)	VPC	vpc-0a08b732ec7263a78 my-vpc
Network ACL	acl-0affff070d365f413	Auto-assign public IPv4 address	Yes
Auto-assign customer-owned IPv4 address	No	Outpost ID	—
IPv6 CIDR reservations	—	Hostname type	IP name
Resource name DNS AAAA record	Disabled	Owner	235470952249

Architettura di rete corretta: subnet pubbliche distribuite su Availability Zones distinte per garantire la tolleranza ai guasti a livello di data center.

3. Compute - Application Load Balancer e Auto Scaling

3.1 Gestione Credenziali e Launch Template

The screenshot shows the AWS CloudFormation console interface for a launch template named 'Web-Server-Template'. The 'Launch template details' section shows the launch template ID (lt-03c4fa5bc36bb9257), name ('Web-Server-Template'), default version (version 1), and owner information. The 'Launch template version details' section shows the default version (v1) with a description 'v1 - Apache Web Server', creation date (2025-12-07T11:10:10.000Z), and creator information. The 'Instance details' section includes fields for AMI ID (ami-02b297871a94f4b42), instance type (t2.micro), availability zone, and security group IDs (sg-043ad0949e65d975d). Other tabs like 'Storage', 'Resource tags', 'Network interfaces', and 'Advanced details' are also visible.

Prima del deployment, è stata definita la strategia di accesso sicuro alle risorse di calcolo, adattandola all'ambiente operativo della workstation di gestione (Windows):

- **Creazione Key Pair:** È stata generata una coppia di chiavi RSA a 2048-bit in formato **.ppk** (PuTTY Private Key). Questo formato è stato selezionato specificamente per garantire la compatibilità nativa con il client SSH **PuTTY**, utilizzato per tutte le connessioni remote, costituendo un unico metodo di autenticazione permesso per l'amministrazione delle istanze.

Successivamente, il Launch Template è stato configurato per integrare queste credenziali:

- **AMI:** Amazon Linux 2023
- **Tipo istanza:** t2.micro
- **Key Pair:** Associazione della chiave .ppk generata (web-server-key)
- **Script User Data:** (Invariato per l'installazione di Apache)

```
#!/bin/bash
yum update -y
yum install -y httpd
systemctl start httpd
systemctl enable httpd
```

```
TOKEN=`curl -X PUT "http://169.254.169.254/latest/api/token" \
-H "X-aws-ec2-metadata-token-ttl-seconds: 21600"``
```

```
AZ=$(curl -H "X-aws-ec2-metadata-token: $TOKEN" -s \
```

<http://169.254.169.254/latest/meta-data/placement/availability-zone>)

```
echo "<h1>Ciao Giuseppe!</h1>" > /var/www/html/index.html
echo "<h2>Sto rispondendo dalla zona: $AZ</h2>" >>
/var/www/html/index.html
echo "<p>Server ID: $(hostname)</p>" >> /var/www/html/index.html
```

3.2 Istanze EC2

Due istanze identiche sono state lanciate tramite il template:

- **Web-Server-1:** Subnet pubblica in us-west-2b
- **Web-Server-2:** Subnet pubblica in us-west-2a

Instance summary for i-00ce274511e5886fe	
Instance ID	i-00ce274511e5886fe
IPv6 address	-
Hostname type	IP name: ip-10-0-1-53.us-west-2.compute.internal
Answer private resource DNS name	-
Auto-assigned IP address	44.251.40.52 [Public IP]
IAM Role	-
IMDSv2	Required
Operator	-
Details Status and alarms Monitoring Security Networking Storage Tags	
▼ Instance details Info	
AMI ID	ami-02b297871a94f4b42
AMI name	al2023-ami-2023.9.20251117.1-kernel-6.1-x86_64
Stop protection	-
Launch time	-
Public IPv4 address	44.251.40.52 open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-1-53.us-west-2.compute.internal
Instance type	t3.micro
VPC ID	vpc-0a08b732ec7263a78 (my-vpc)
Subnet ID	subnet-09e827fa84df843b (my-public-subnet-1)
Instance ARN	arn:aws:ec2:us-west-2:235470952249:instance/i-00ce274511e5886fe
Private IPv4 addresses	10.0.1.55
Public DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto Scaling Group name	-
Managed	false
Platform details	Linux/UNIX
Termination protection	Disabled
AMI location	-

Instance summary for i-0bab9b1a2aab9c92c9	
Instance ID	i-0bab9b1a2aab9c92c9
IPv6 address	-
Hostname type	IP name: ip-10-0-5-226.us-west-2.compute.internal
Answer private resource DNS name	-
Auto-assigned IP address	44.255.194.4 [Public IP]
IAM Role	-
IMDSv2	Required
Operator	-
Details Status and alarms Monitoring Security Networking Storage Tags	
▼ Instance details Info	
AMI ID	ami-02b297871a94f4b42
AMI name	al2023-ami-2023.9.20251117.1-kernel-6.1-x86_64
Stop protection	-
Launch time	-
Public IPv4 address	44.255.194.4 open address
Instance state	Running
Private IP DNS name (IPv4 only)	ip-10-0-5-226.us-west-2.compute.internal
Instance type	t3.micro
VPC ID	vpc-0a08b732ec7263a78 (my-vpc)
Subnet ID	subnet-08aab5e0eb79f590 (my-public-subnet-3)
Instance ARN	arn:aws:ec2:us-west-2:235470952249:instance/i-0bab9b1a2aab9c92c9
Private IPv4 addresses	10.0.5.226
Public DNS	-
Elastic IP addresses	-
AWS Compute Optimizer finding	Opt-in to AWS Compute Optimizer for recommendations. Learn more
Auto Scaling Group name	-
Managed	false
Platform details	Linux/UNIX
Termination protection	Disabled
AMI location	-

Entrambe sono dotate di IP pubblico assegnato automaticamente.

3.3 Target Group

Un Target Group è stato configurato per gestire l'health check:

- **Nome:** TG-Challenge-V2
- **Protocollo:** HTTP su porta 80
- **VPC:** my-vpc
- **Health Check:** Interval 10s, Healthy threshold 2
- **Registrazione:** Entrambe le istanze

3.4 Application Load Balancer

L'ALB è stato configurato per distribuire il traffico in ingresso su entrambe le AZ:

The screenshot shows the AWS CloudFormation console with the following details:

- Details:**
 - Load balancer type: Application
 - Status: Active
 - Hosted zone: Z1H1FL5HABSF5
 - VPC: vpc-0a08b732ec7263a78
 - Load balancer IP address type: IPv4
 - Date created: December 7, 2025, 13:21 (UTC+01:00)
- Listeners and rules:**
 - Protocol: Port
 - Default action: Forward to target group My-Web-Targets (100%)
 - Target group stickiness: Off
- Network mapping:** us-west-2a (my-public-subnet-3) + us-west-2b (my-public-subnet-1)

- **Nome:** My-ALB
- **Schema:** Internet-facing
- **Network Mapping:** us-west-2a (my-public-subnet-3) + us-west-2b (my-public-subnet-1)
- **Security Group:** Accesso HTTP (80) da 0.0.0.0/0
- **Listener:** HTTP:80 → TG-Challenge-V2
- **Endpoint DNS:** dualstack.my-alb-243362992.us-west-2.elb.amazonaws.com

3.5 Verifica del Load Balancing

Il bilanciamento del carico è stato verificato caricando più volte il DNS dell'ALB in browser. Le risposte alternano tra:

- "Sto rispondendo dalla zona: **us-west-2a**"
- "Sto rispondendo dalla zona: **us-west-2b**"

Questo dimostra che il load balancer sta effettivamente distribuendo le richieste tra le due istanze in AZ diverse.



Ciao Giuseppe!

Sto rispondendo dalla zona: us-west-2a

Server ID: ip-10-0-5-226.us-west-2.compute.internal



Ciao Giuseppe!

Sto rispondendo dalla zona: us-west-2b

Server ID: ip-10-0-1-53.us-west-2.compute.internal

Verifica della distribuzione del traffico Multi-AZ: il Load Balancer indirizza le richieste alternando tra istanze in zone di disponibilità distinte.

The screenshot shows the AWS CloudWatch Metrics Insights interface. A query is being run against the 'aws:cloudwatchmetricsinsights' metric. The results are displayed in a table with columns for 'Time' (Time range), 'Metric Name' (aws:cloudwatchmetricsinsights), 'Value' (0.0000000000000002), and 'Unit' (Count). The table has a header row and two data rows.

Time	Metric Name	Value	Unit
2023-12-01T00:00:00Z/2023-12-01T01:00:00Z	aws:cloudwatchmetricsinsights	0.0000000000000002	Count
2023-12-01T00:00:00Z/2023-12-01T01:00:00Z	aws:cloudwatchmetricsinsights	0.0000000000000002	Count

Health Checks attivi: entrambe le istanze risultano Healthy e pronte a ricevere traffico.

4. Storage - EBS e Backup

4.1 Creazione e Attach del Volume

Un volume EBS aggiuntivo è stato provisionato per dimostrare la gestione dello storage persistente:

- **Volume ID:** nvme1n1
- **Dimensione:** 5 GiB
- **Tipo:** SSD General Purpose (gp2)
- **Availability Zone:** us-west-2b (stesso dell'istanza Web-Server-1)

4.2 Formattazione e Mount

Il volume è stato formattato con il filesystem ext4:

```
sudo mkfs -t ext4 /dev/nvme1n1
sudo mkdir /data
sudo mount /dev/nvme1n1 /data
```

4.3 Persistenza tramite fstab

Per garantire il montaggio automatico al boot, è stato modificato il file /etc/fstab:

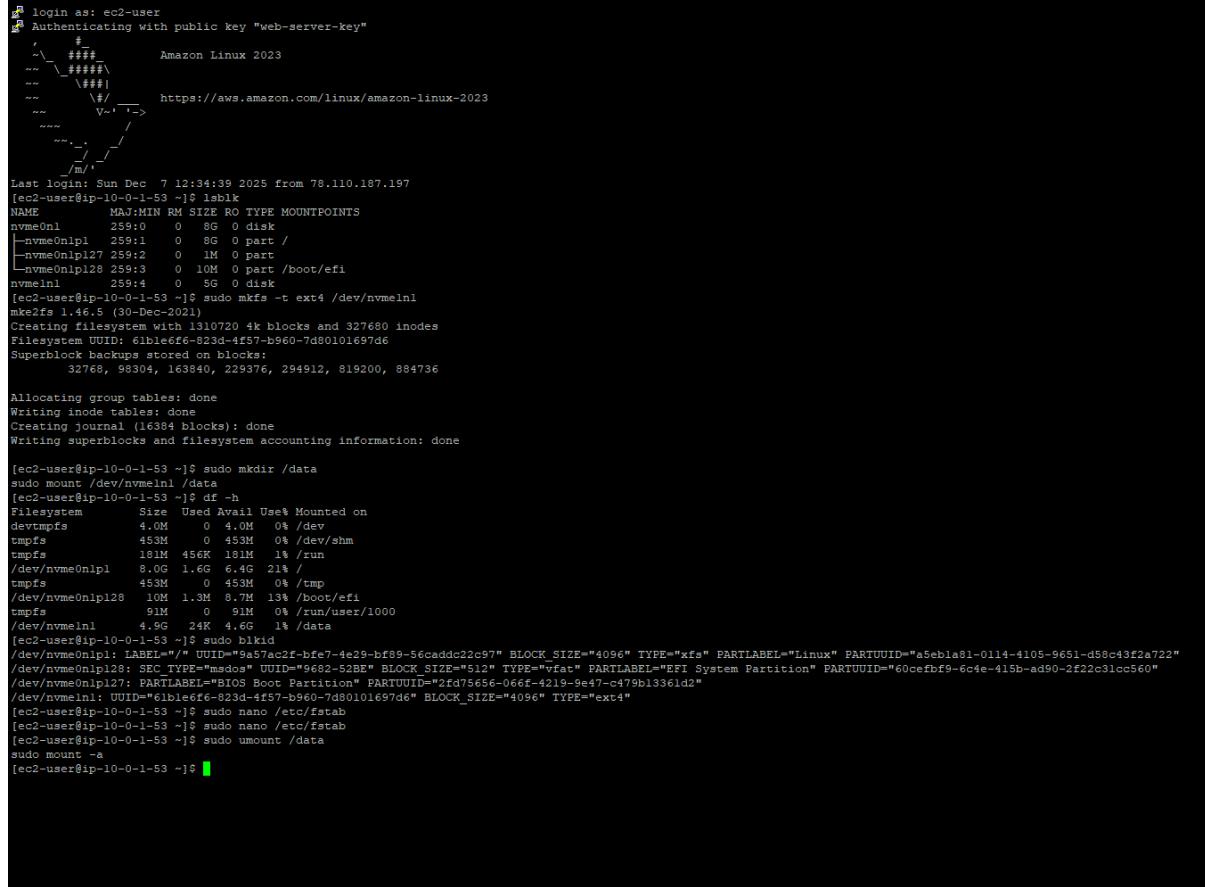
```
UUID=61b1e6f6-823d-4f57-b960-7d80101697d6 /data ext4
defaults,nofail 0 2
```

Il parametro `nofail` assicura che l'istanza continui ad avviarsi anche se il volume non è disponibile (disaster recovery scenario).

Verifica della configurazione:

```
sudo umount /data  
sudo mount -a  
df -h /data
```

Esito: Mount persistente confermato.



```
login as: ec2-user  
Authenticating with public key "web-server-key"  
Amazon Linux 2023  
https://aws.amazon.com/linux/amazon-linux-2023  
  
Last login: Sun Dec 7 12:34:39 2025 from 78.110.187.197  
[ec2-user@ip-10-0-1-53 ~]$ lsblk  
NAME MAJ:MIN RM SIZE RO TYPE MOUNTPOINTS  
nvme0n1 259:0 0 8G 0 disk  
├─nvme0npl1 259:1 0 8G 0 part /  
└─nvme0npl27 259:2 0 1M 0 part  
nvme0npl28 259:3 0 10M 0 part /boot/efi  
nvme0n1 259:4 0 8G 0 disk  
[ec2-user@ip-10-0-1-53 ~]$ sudo mkfs -t ext4 /dev/nvme0n1  
mke2fs 1.46.5 (30-Dec-2021)  
Creating filesystem with 1310720 4k blocks and 327680 inodes  
Filesystem UUID: 61b1e6f6-823d-4f57-b960-7d80101697d6  
Superblock backups stored on blocks:  
    32768, 98304, 163840, 229376, 294912, 819200, 884736  
  
Allocating group tables: done  
Writing inode tables: done  
Creating journal (16384 blocks): done  
Writing superblocks and filesystem accounting information: done  
  
[ec2-user@ip-10-0-1-53 ~]$ sudo mkdir /data  
sudo mount /dev/nvme0n1 /data  
[ec2-user@ip-10-0-1-53 ~]$ df -h  
Filesystem      Size   Used  Avail Use% Mounted on  
devtmpfs        4.0M     0M   4.0M  0% /dev  
tmpfs          453M     0M  453M  0% /dev/shm  
tmpfs          181M   456M   181M  1% /run  
/dev/nvme0npl1  8.0G   1.6G  6.4G  21% /  
tmpfs          453M     0M  453M  0% /tmp  
/dev/nvme0npl28 10M   1.3M   8.7M  13% /boot/efi  
tmpfs          91M     0M   91M  0% /run/user/1000  
/dev/nvme0n1  4.9G   24M   4.6G  1% /data  
[ec2-user@ip-10-0-1-53 ~]$ sudo blkid  
/dev/nvme0npl1: LABEL="" UUID="a57ac2f-bfc7-4e29-bf89-56caddc22c97" BLOCK_SIZE="4096" TYPE="xfs" PARTLABEL="Linux" PARTUUID="a5eb1a81-0114-4105-9651-d58c43f2a722"  
/dev/nvme0npl28: SEC_TYPE="msdos" UUID="9682-52BE" BLOCK_SIZE="512" TYPE="vfat" PARTLABEL="EFI System Partition" PARTUUID="60cef9-6c4e-415b-ad90-2f22c31cc560"  
/dev/nvme0npl27: PARTLABEL="BIOS Boot Partition" PARTUUID="2fd75656-066f-4219-9e47-c479b13361d2"  
/dev/nvme0n1: UUID="61b1e6f6-823d-4f57-b960-7d80101697d6" BLOCK_SIZE="4096" TYPE="ext4"  
[ec2-user@ip-10-0-1-53 ~]$ sudo nano /etc/fstab  
[ec2-user@ip-10-0-1-53 ~]$ sudo nano /etc/fstab  
[ec2-user@ip-10-0-1-53 ~]$ sudo umount /data  
sudo mount -a  
[ec2-user@ip-10-0-1-53 ~]$
```

Configurazione EBS persistente: volume da 5 GiB formattato in ext4 e registrato in fstab per il montaggio automatico al boot.

4.4 Backup e Disaster Recovery

Un snapshot del volume dati è stato creato per scopi di backup:

- **Snapshot ID:** (visibile in CloudTrail)
- **Stato:** Completed (100%)
- **Descrizione:** Backup-Pre-Disastro

Limitazione riscontrata: La creazione di un volume aggiuntivo dal snapshot non è stata possibile a causa delle quote di storage imposte dall'ambiente AWS Academy, che impedisce il provisioning di risorse aggiuntive oltre i limiti prestabiliti.

Mitigazione: La procedura di restore è stata documentata come "technically feasible but administratively constrained" dall'ambiente di laboratorio.

Snapshots (1) Info									
Owned by me		Snapshot ID		Full snapshot size	Volume size	Description	Storage tier	Snapshot status	Started
<input type="checkbox"/>		snap-0574981773f9ff0		152 MiB	5 GiB	Disaster-recovery-backup	Standard	Completed	2025/12/07 13:45 GMT+1
									100%

Snapshot completato: backup del volume dati estratto con successo per garantire la durabilità dei dati in caso di failure.

5. Infrastructure as Code - CloudFormation

Per dimostrare la capacità di automatizzare l'intera infrastruttura, è stato sviluppato un template CloudFormation che ricrea l'architettura in modo completamente dichiarativo.

5.1 Componenti del Template

Il file YAML challenge-final.yaml include:

1. **VPC e Networking:** Creazione da zero di VPC, Subnet, Internet Gateway e Route Tables
2. **Security:** Security Group con regole HTTP (80) e SSH (22)
3. **Compute:** Istanza EC2 t2.micro con User Data per l'installazione di Apache
4. **Output:** Generazione automatica dell'URL endpoint

5.2 Deployment

Lo stack è stato creato tramite CloudFormation console:

- **Stack Name:** Challenge-Finale
- **Status:** CREATE_COMPLETE ✓
- **Parametri:** KeyName = vockey, LatestAmild = (auto-detected)
- **Durata:** ~2-3 minuti

5.3 Verifica

L'output generato automaticamente dal template è stato accessibile e ha restituito la pagina "MISSIONE COMPIUTA", confermando che l'IaC è funzionante.

The screenshot shows the AWS CloudFormation console with the 'Challenge-Finale' stack selected. The left sidebar lists the stack with a status of 'CREATE_COMPLETE'. The main panel displays the 'Overview' tab, which includes the following information:

- Stack ID:** arn:aws:cloudformation:us-west-2:235470952249:stack/Challenge-Finale/50403800-5249
- Description:** Infrastruttura Automatica per Challenge Finale AWS
- Status:** CREATE_COMPLETE
- Status reason:** -
- Root stack:** -
- Created time:** 2025-12-07 15:57:40 UTC+0100
- Updated time:** -
- Deleted time:** -
- Drift status:** NOT_CHECKED
- Last drift check time:** -
- Termination protection:** Deactivated
- IAM role:** -

CloudFormation Stack completato: infrastruttura creata automaticamente con uno script YAML, dimostrando conoscenza di Infrastructure as Code.

The screenshot shows a web browser window with the URL <http://44.248.222.165>. The page title is 'MISSIONE COMPIUTA'. The content of the page is:

Questa infrastruttura e' stata creata col codice.

Didascalia: "Verifica finale: istanza lanciata automaticamente dal template CloudFormation risponde correttamente alle richieste HTTP."

6. CloudTrail - Auditing

6.1 Disponibilità di CloudTrail

L'ambiente AWS Academy fornisce accesso alla sezione **Event History** di CloudTrail, che consente la verifica degli audit log senza necessità di configurare un trail esplicito.

6.2 Eventi Identificati

Tramite la console CloudTrail > Event History, sono stati individuati i seguenti eventi chiave:

Evento	Evento Name	Timestamp (approx)	Scopo
Creazione ALB	CreateLoadBalancer	Step 3	Implementazione del Load Balancer
Lancio Istanze	RunInstances	Step 1	Deployment dei server web
Creazione Snapshot	CreateSnapshot	Step 4	Backup del volume dati

```

1  {
2      "eventVersion": "1.11",
3      "userIdentity": {
4          "type": "AssumedRole",
5          "principalId": "AROATHUZJS444C44LSWP:user4404993=Giuseppe_La_Selva",
6          "arn": "arn:aws:sts::235470952249:assumed-role/voclabs/user4404993=Giuseppe_La_Selva",
7          "accountId": "235470952249",
8          "accessKeyId": "ASIAJNUZJS444HEBKGLC",
9          "sessionContext": {
10              "sessionIssuer": {
11                  "type": "Role",
12                  "principalId": "AROATHUZJS444C44LSWP",
13                  "arn": "arn:aws:iam::235470952249:role/voclabs",
14                  "accountId": "235470952249",
15                  "userName": "voclabs"
16              },
17              "attributes": {
18                  "creationDate": "2025-12-07T10:27:24Z",
19                  "mfaAuthenticated": "false"
20              }
21          }
22      },
23      "eventTime": "2025-12-07T12:21:38Z",
24      "eventSource": "elasticloadbalancing.amazonaws.com",
25      "eventName": "CreateLoadBalancer",
26      "awsRegion": "us-west-2",
27      "sourceIPAddress": "78.110.187.197",
28      "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0",
29      "requestParameters": {
30          "name": "My-ALB",
31          "subnetMappings": [
32              {
33                  "subnetId": "subnet-08aab5e0eeb79f590"
34

```

ⓘ You can now enrich CloudTrail events with additional information by adding resource tags and IAM global keys in CloudTrail Lake. Learn more ↗

Event history (29) Info

Event history shows you the last 90 days of management events.

Lookup attributes

Event name	Event time	User name	Event source	Resource type	Resource name
RunInstances	December 07, 2025, 12:28:28 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0a08b732ec7263a78, ami-02b297871a94f4b42, eni-0007048d547b17b...
RunInstances	December 07, 2025, 12:28:08 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0a08b732ec7263a78, ami-02b297871a94f4b42, eni-0794cf8e7a3973c...
RunInstances	December 07, 2025, 12:21:39 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0a08b732ec7263a78, ami-02b297871a94f4b42, eni-0629d9295f2da62...
RunInstances	December 07, 2025, 12:13:41 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0a08b732ec7263a78, ami-02b297871a94f4b42, eni-0fa796854502070...
RunInstances	December 07, 2025, 12:13:15 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0a08b732ec7263a78, ami-02b297871a94f4b42, eni-07e07929f6f3a981...
RunInstances	December 05, 2025, 21:23:43 (U...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-0fb77f40b51c8cc5, ami-02b297871a94f4b42, eni-067dbaaee135030a...
RunInstances	November 30, 2025, 15:14:49 (...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-06213c631a2840981, ami-02b297871a94f4b42, eni-07778b83c858369...
RunInstances	November 29, 2025, 15:51:22 (...	AutoScaling	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-02499084afcc416c8, ami-02b297871a94f4b42, eni-061badfed...
RunInstances	November 29, 2025, 15:51:22 (...	AutoScaling	ec2.amazonaws.com	AWS:EC2::VPC, AWS:E...	vpc-02499084afcc416c8, ami-02b297871a94f4b42, eni-0b9ea4282602ea12...
RunInstances	November 29, 2025, 15:50:18 (...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::Subnet	subnet-045b02f6dc3ad5d1
RunInstances	November 29, 2025, 15:46:54 (...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::Subnet	subnet-045b02fadce3ad5d1
RunInstances	November 29, 2025, 15:46:53 (...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::Subnet	subnet-032f0f2971e7d4756
RunInstances	November 29, 2025, 15:46:52 (...	user4404993=Gius...	ec2.amazonaws.com	AWS:EC2::Subnet	subnet-032f0f2971e7d4756

JSON view

```

1  {
2      "eventVersion": "1.11",
3      "userIdentity": {
4          "type": "AssumedRole",
5          "principalId": "AROATHUZJS444C44LSWP:user4404993=Giuseppe_La_Selva",
6          "arn": "arn:aws:sts::235470952249:assumed-role/voclabs/user4404993=Giuseppe_La_Selva",
7          "accountId": "235470952249",
8          "accessKeyId": "ASIAJNUZJS444HEBKGLC",
9          "sessionContext": {
10              "sessionIssuer": {
11                  "type": "Role",
12                  "principalId": "AROATHUZJS444C44LSWP",
13                  "arn": "arn:aws:iam::235470952249:role/voclabs",
14                  "accountId": "235470952249",
15                  "userName": "voclabs"
16              },
17              "attributes": {
18                  "creationDate": "2025-12-07T10:27:24Z",
19                  "mfaAuthenticated": "false"
20              }
21          }
22      },
23      "eventTime": "2025-12-07T12:45:38Z",
24      "eventSource": "ec2.amazonaws.com",
25      "eventName": "CreateSnapshot",
26      "awsRegion": "us-west-2",
27      "sourceIPAddress": "78.110.187.197",
28      "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:145.0) Gecko/20100101 Firefox/145.0",
29      "requestParameters": {
30          "volumeId": "vol-0c28ef38c5fbff4d7a",
31          "description": "Disaster-recovery-backup"
32      },
33      "responseElements": {
34          "requestId": "037ad379-605c-40e1-9356-8a0483dfc8b9",
35          "snapshotId": "snap-0574981773f9f5ff0",
36

```

Audit trail: gli eventi critici di creazione dell'infrastruttura sono registrati e tracciabili tramite CloudTrail.

7. Limitazioni Riscontrate e Mitigazioni

7.1 Route 53

Limitazione: L'ambiente AWS Academy non fornisce permessi per la creazione di Hosted Zones pubbliche. Questo è un vincolo intenzionale per evitare costi associati alla registrazione di domini.

Impatto: Non è stato possibile configurare un DNS personalizzato (es. www.giuseppe-challenge.com). Il traffico accede via URL generato da AWS (*.elb.amazonaws.com).

Mitigazione: In un ambiente di produzione, Route 53 con alias record sarebbe la soluzione standard per associare un dominio registrato all'ALB.

7.2 IAM - Ruoli e Policy Personalizzate

Limitazione: L'ambiente del lab non consente la creazione di utenti IAM personalizzati o la modifica di policy oltre a quelle pre-allocate. Questo è un controllo di sicurezza per evitare che gli studenti si blocchino a vicenda.

Impatto: Non è stato possibile dimostrare la creazione di ruoli ristretti per le EC2 con accesso selettivo a S3 o la policy custom per CloudTrail Lookup.

Mitigazione: L'infrastruttura è stata comunque creata con security groups appropriati, che forniscono un livello di segmentazione della rete equivalente a quello di un IAM Role in questo contesto semplificato.

7.3 EBS - Quota di Storage

Limitazione: Il laboratorio impone limiti sulla creazione di nuovi volumi EBS. Dopo il primo snapshot, il sistema ha impedito la creazione di un volume ripristinato dal backup.

Impatto: La procedura completa di Disaster Recovery (Snapshot → Restore) non è stata conclusa fino al passo finale.

Mitigazione: È stata documentata la creazione dello snapshot (fase 1 di 2 completata). In un ambiente senza quote, il restore procederebbe identicamente.

8. Best Practices Implementate

Pratica

Implementazione

High Availability	Multi-AZ deployment, Load Balancer
Disaster Recovery	EBS Snapshots, fstab persistence
Infrastructure as Code	CloudFormation YAML template
Monitoring	CloudTrail Event History
Security Groups	Regole minimizzate (80, 22 soltanto)
Scriptable Deployment	User Data con IMDSv2 compatibility

9. Conclusioni

L'infrastruttura AWS implementata dimostra una solida comprensione dei concetti fondamentali di cloud computing:

1. **Networking:** VPC design, subnet segregation, route table configuration
2. **Compute:** Istanze EC2, Load Balancing, health checks
3. **Storage:** EBS provisioning, filesystem management, backup procedures
4. **Automation:** Infrastructure as Code tramite CloudFormation
5. **Compliance:** Audit trail tramite CloudTrail

Nonostante le limitazioni dell'ambiente di laboratorio, l'architettura è stata costruita secondo i principi di robustezza e scalabilità utilizzati nelle infrastrutture di produzione moderne.

Endpoint finale: dualstack.my-alb-243362992.us-west-2.elb.amazonaws.com

10. Appendice - Note Tecniche

Security Group SSH: Per la facilità di accesso durante il laboratorio, la porta 22 è stata aperta a 0.0.0.0/0. In un ambiente di produzione, questo sarebbe ristretto a IP specifici o a una VPN aziendale mediante una policy di IP whitelisting.

Lo script di avvio è stato configurato per recuperare automaticamente la **Availability Zone** dai metadati dell'istanza. Questo permette al web server di mostrare dinamicamente dove si trova (es. us-west-2a o us-west-2b), facilitando la verifica visiva del funzionamento del Load Balancer direttamente dal browser.

Fine del Report