Trustsoft
Cloud Operations Partner

Terraform AWS Infrastructure

Trustsoft Internship Project

2.5.2025

Maksym Suvorov

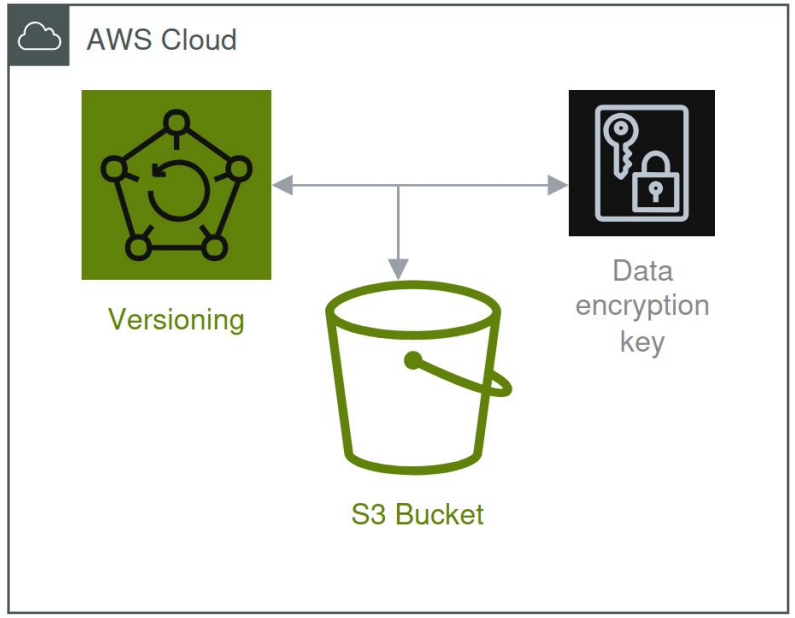
Trustsoft
Cloud Operations Partner

Agenda

1. **Diagram**
2. **IaC**

Trustsoft
Cloud Operations Partner

Remote Backend

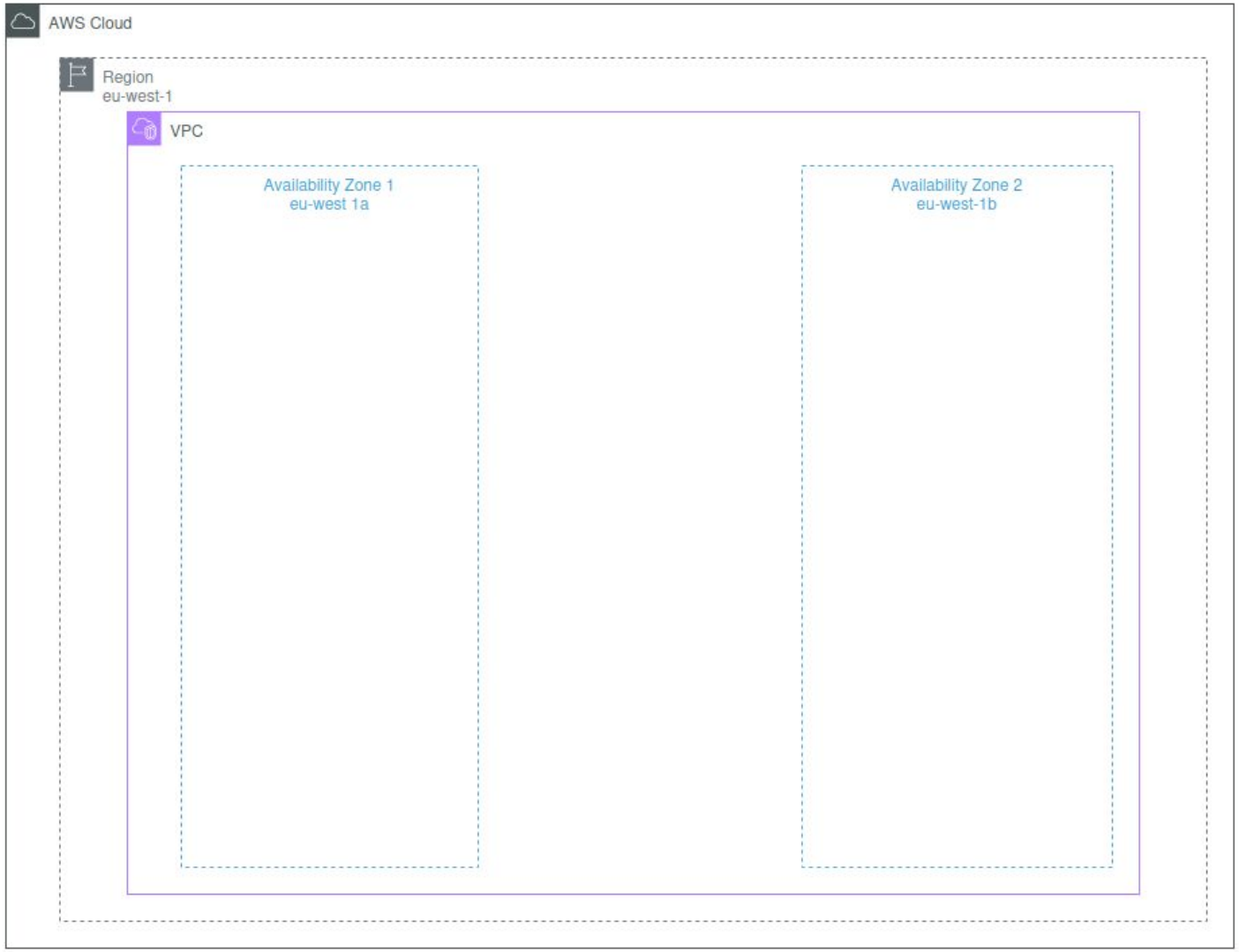


Trustsoft
Cloud Operations Partner

Region

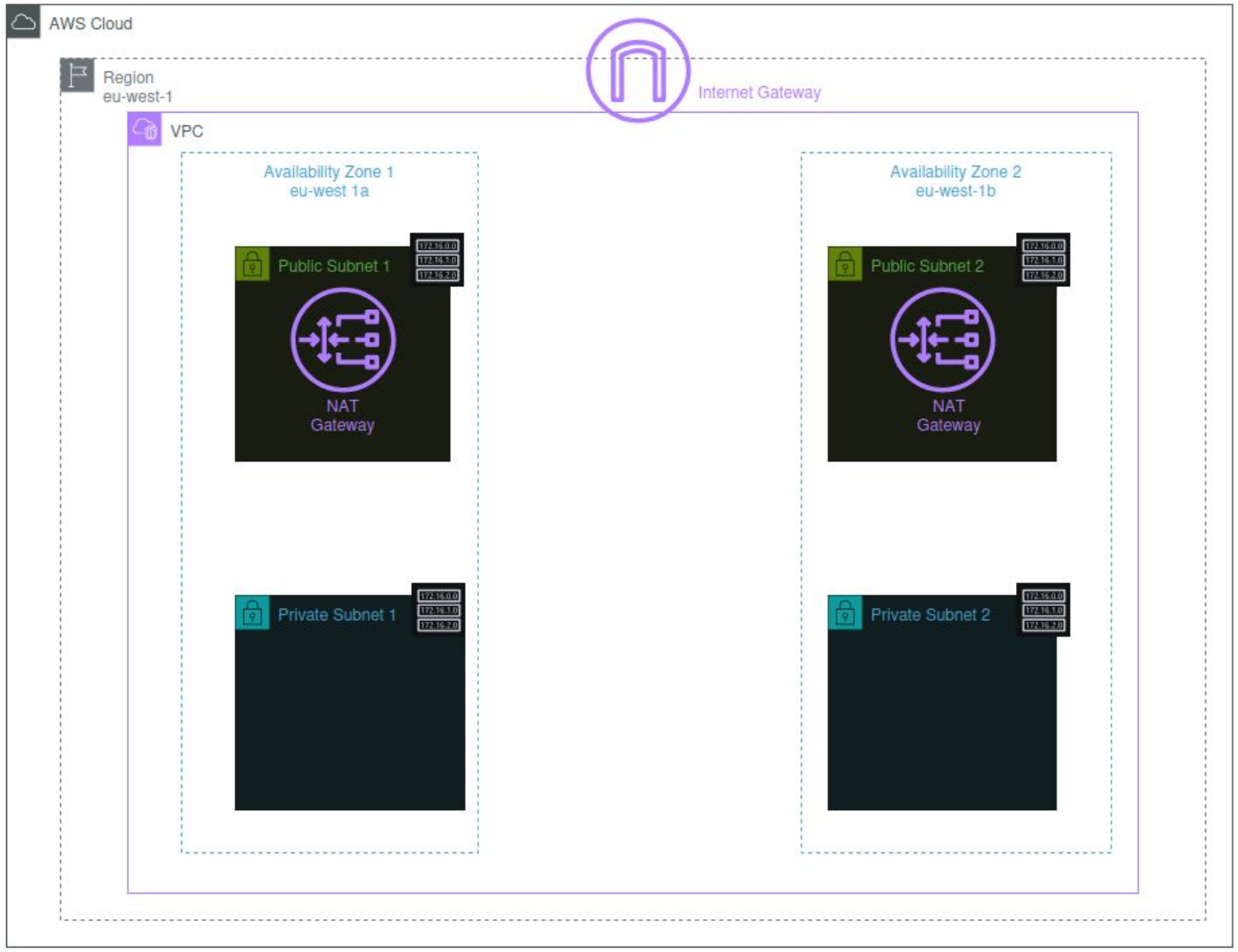
Trustsoft
Cloud Operations Partner

VPC



Trustsoft
Cloud Operations Partner

Networking



1. Public Route Table (`public_subnet_rt`)

- **Associated with:**
  - `public_subnet_1` (AZ-1)
  - `public_subnet_2` (AZ-2)
- **Routes:**

Destination	Target	Purpose
`0.0.0.0/0`	Internet Gateway	Allows inbound Internet traffic to ALB, NAT GWs
`local`	`-` (VPC router)	Enables inside-VPC communication

2. Private Route Table AZ-1 (`private_subnet_rt_1`)

- **Associated with:**
  - `private_subnet_1` (AZ-1)
- **Routes:**

Destination	Target	Purpose
`0.0.0.0/0`	NAT Gateway 1 (`nat_gw_1`)	Allows EC2 in private subnet to reach Internet
`local`	`-` (VPC router)	Enables inside-VPC communication

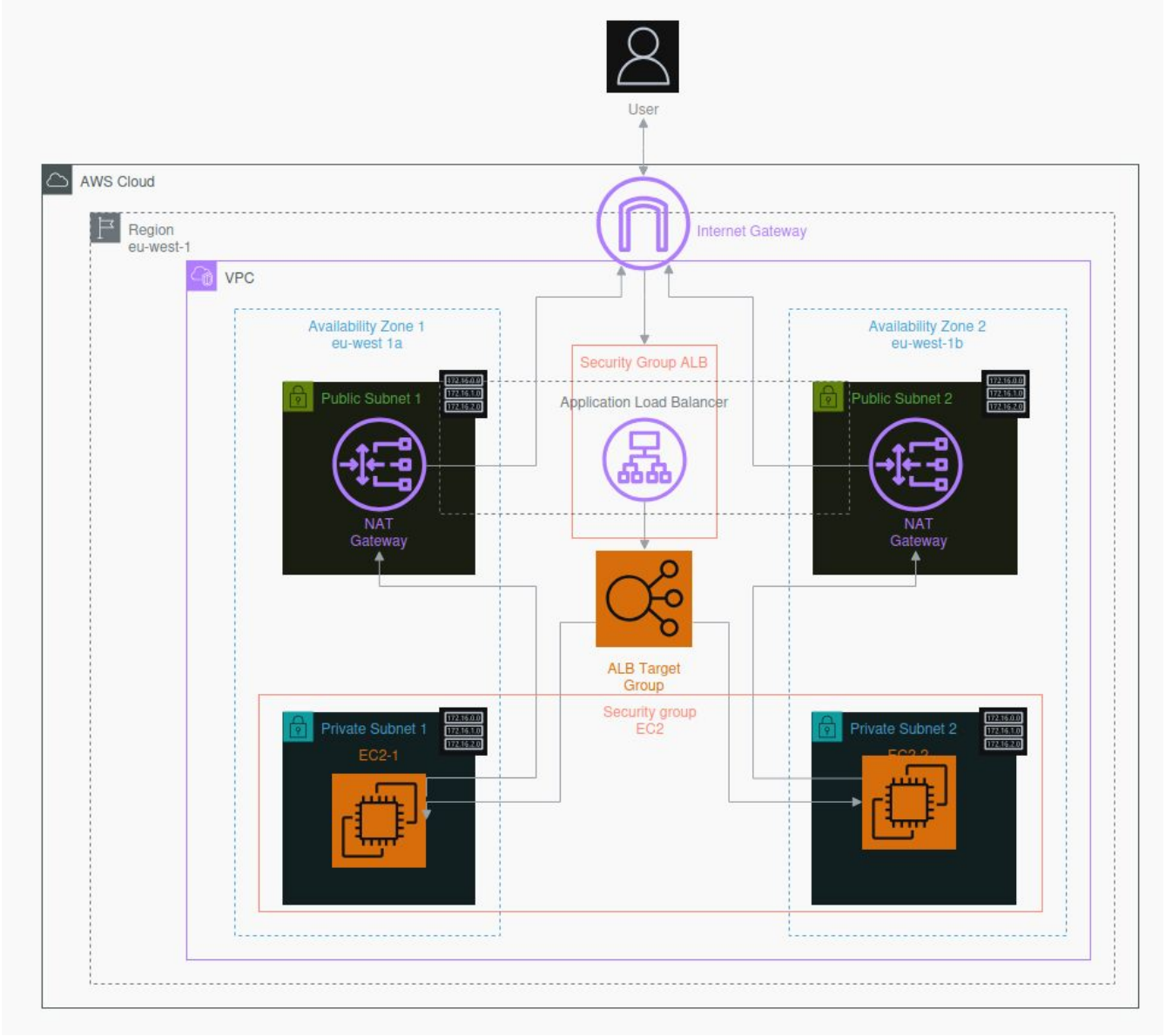
3. Private Route Table AZ-2 (`private_subnet_rt_2`)

- **Associated with:**
  - `private_subnet_2` (AZ-2)
- **Routes:**

Destination	Target	Purpose
`0.0.0.0/0`	NAT Gateway 2 (`nat_gw_2`)	Allows EC2 in private subnet to reach Internet
`local`	`-` (VPC router)	Enables inside-VPC communication

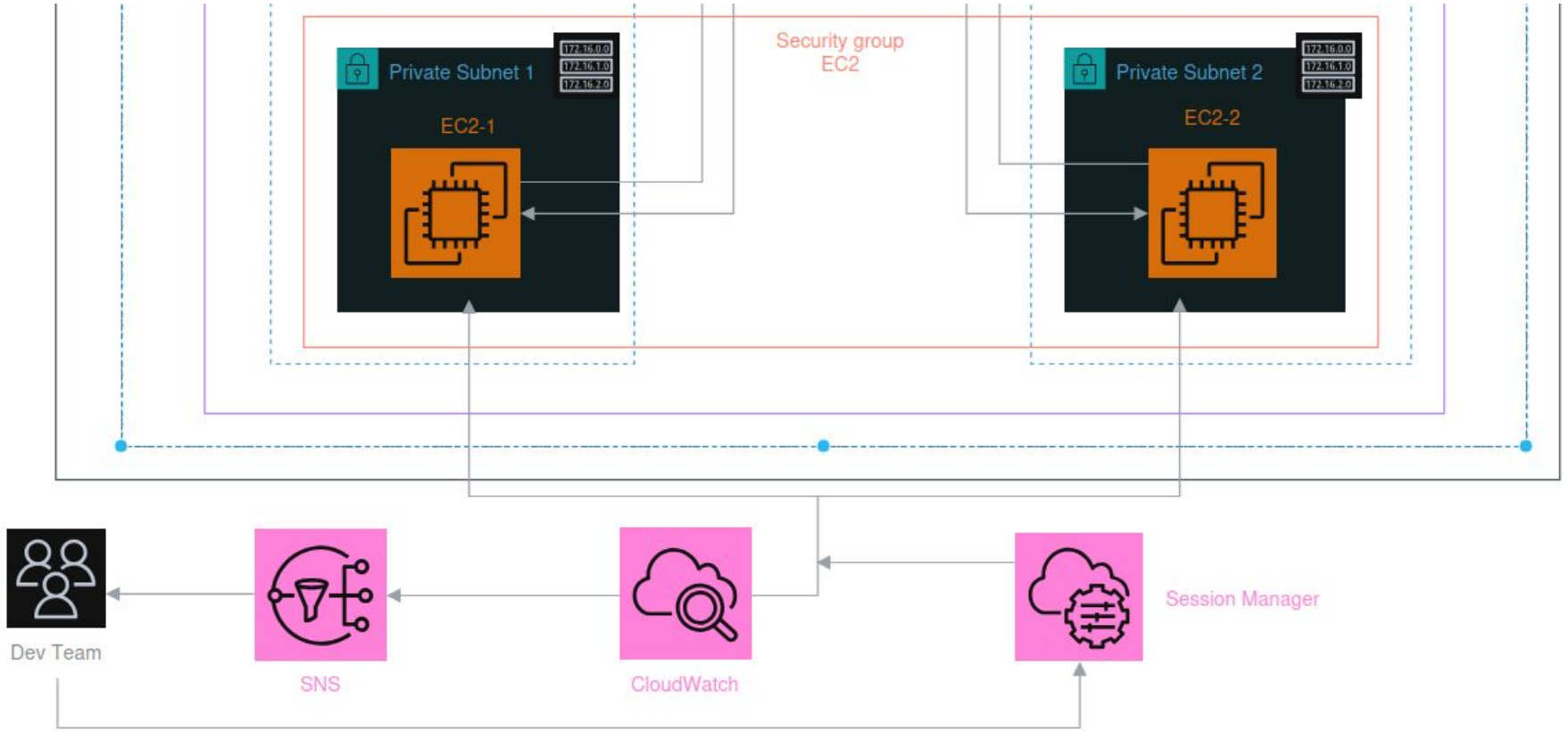
Trustsoft
Cloud Operations Partner

Compute & Load-Balancing



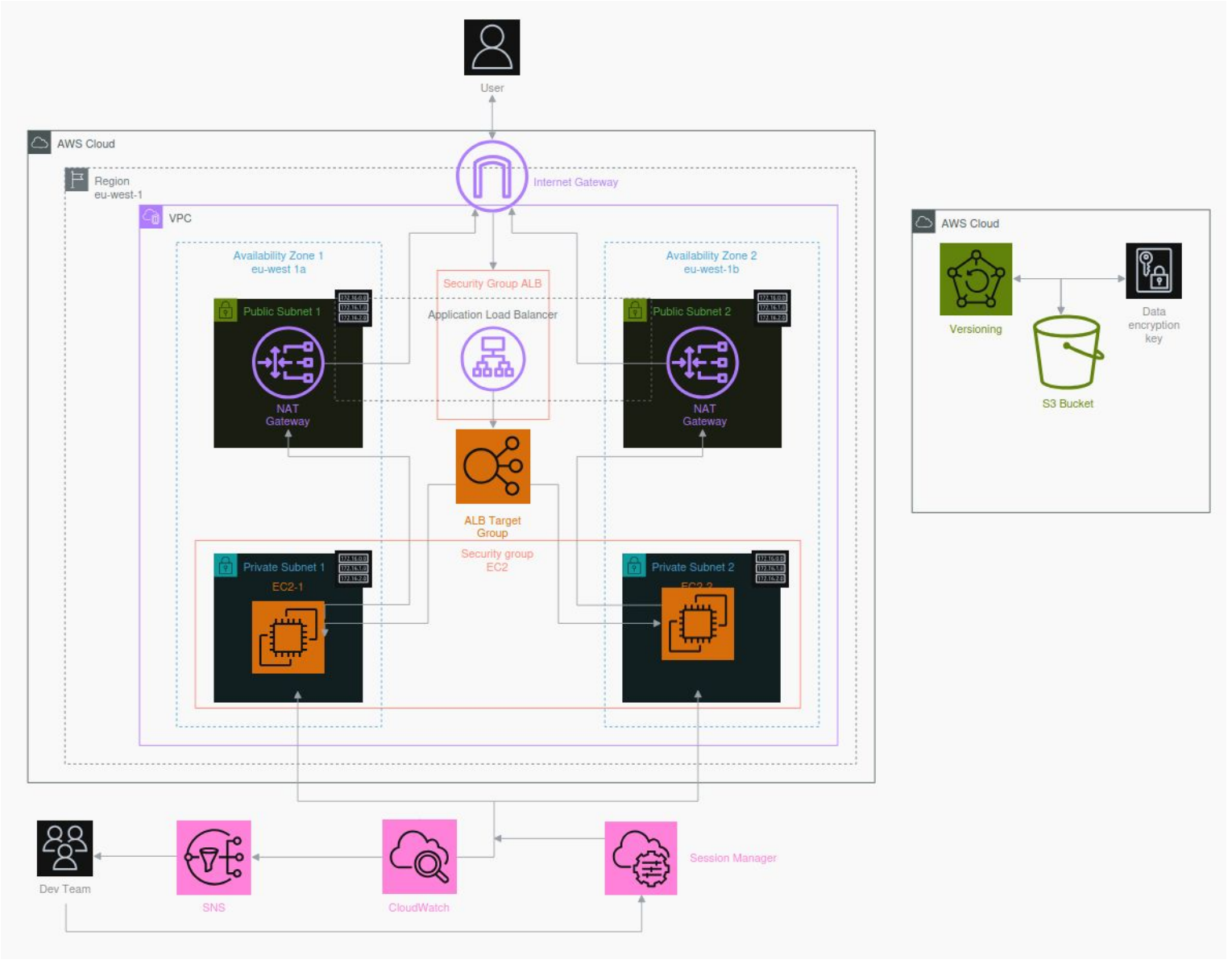
Trustsoft
Cloud Operations Partner

Monitoring



Trustsoft
Cloud Operations Partner

Diagram Overview



Trustsoft
Cloud Operations Partner

Agenda

1. **Diagram**
2. **IaC**

Trustsoft
Cloud Operations Partner

Iac Structure

```
├── backend.tf                # Remote backend configuration (S3 + DynamoDB)
├── versions.tf               # Terraform & provider version constraints
├── variables.tf              # Root-module input variable definitions
├── outputs.tf                # Root-module outputs that expose module results
├── main.tf                   # Calls all child modules
├── bootstrap/                # Create backend infrastructure (S3 bucket, DynamoDB, KMS)
│   └── backend-setup.tf      # Resources for S3, DynamoDB, KMS key
├── modules/                  # Reusable modules, each with its own variables/outputs
│   ├── networking/           # Module for VPC, subnets, IGW, NAT, route tables
│   │   ├── main.tf
│   │   ├── variables.tf      # Inputs: vpc_cidr, subnet CIDRs, AZs
│   │   └── outputs.tf        # Outputs: vpc_id, subnet IDs, igw_id, nat_gw_ids, rt_ids
│   ├── security/             # Module for security groups (ALB & EC2)
│   │   ├── main.tf
│   │   ├── variables.tf      # Inputs: vpc_id, alb_cidr_blocks
│   │   └── outputs.tf        # Outputs: alb_sg_id, ec2_sg_id
│   ├── iam/                  # Module for IAM roles & instance profiles
│   │   ├── main.tf
│   │   ├── variables.tf
│   │   └── outputs.tf        # Outputs: role_arn, instance_profile
│   ├── compute/              # Module for EC2 instances
│   │   ├── main.tf
│   │   ├── variables.tf      # Inputs: ami_id, instance_type, subnet_ids, SGs, iam_instance_profile, user_data_file
│   │   └── outputs.tf        # Outputs: instance_ids, private_ips
│   ├── alb/                  # Module for Application Load Balancer & target group
│   │   ├── main.tf
│   │   ├── variables.tf      # Inputs: vpc_id, public_subnet_ids, security_group_id, target_ids
│   │   └── outputs.tf        # Outputs: alb_dns_name, target_group_arn
│   └── monitoring/           # Module for CloudWatch alarms & SNS notifications
│       ├── main.tf
│       ├── variables.tf      # Inputs: instance_ids, email_addresses
│       └── outputs.tf        # Outputs: sns_topic_arn
├── scripts/                  # Helper scripts and user_data files
└──── userdata.sh             # Bootstraps EC2 with Web Server and SSM
```

Trustsoft
Cloud Operations Partner

Demonstration 1

Outputs

```
alb_dns_name = "lb-internship-maksym-1646098265.eu-west-1.elb.amazonaws.com"
```

```
instance_ips = [
  "10.0.11.123",
  "10.0.12.167",
]
```

Demonstration

Hello from EC2 instance ip-10-0-11-123.eu-west-1.compute.internal

Hello from EC2 instance ip-10-0-12-167.eu-west-1.compute.internal

Trustsoft
Cloud Operations Partner

Demonstration 2

variables.tf

```
variable "email_addresses" {  1 usage   Maksym Suvorov
  description = "List of email addresses to receive CloudWatch alarm notifications"
  type        = list(string)
  default = ["maksym.suvorov@trustsoft.eu"]
}
```

Demonstration

Trustsoft
Cloud Operations Partner

Questions & Answers

Thank you for your attention

Trustsoft
Cloud Operations Partner

Zurich, Switzerland • **Prague,** Czechia • **London,** United Kingdom