AWS - Associate Architect Final Project

Matan and Nimrod

Architecture Overview

Welcome to our AWS architecture overview, meticulously crafted for reliability, scalability and security. Our setup spans across multiple regions connected via VPC peering, ensuring seamless data flow and high availability.

Key Highlights:

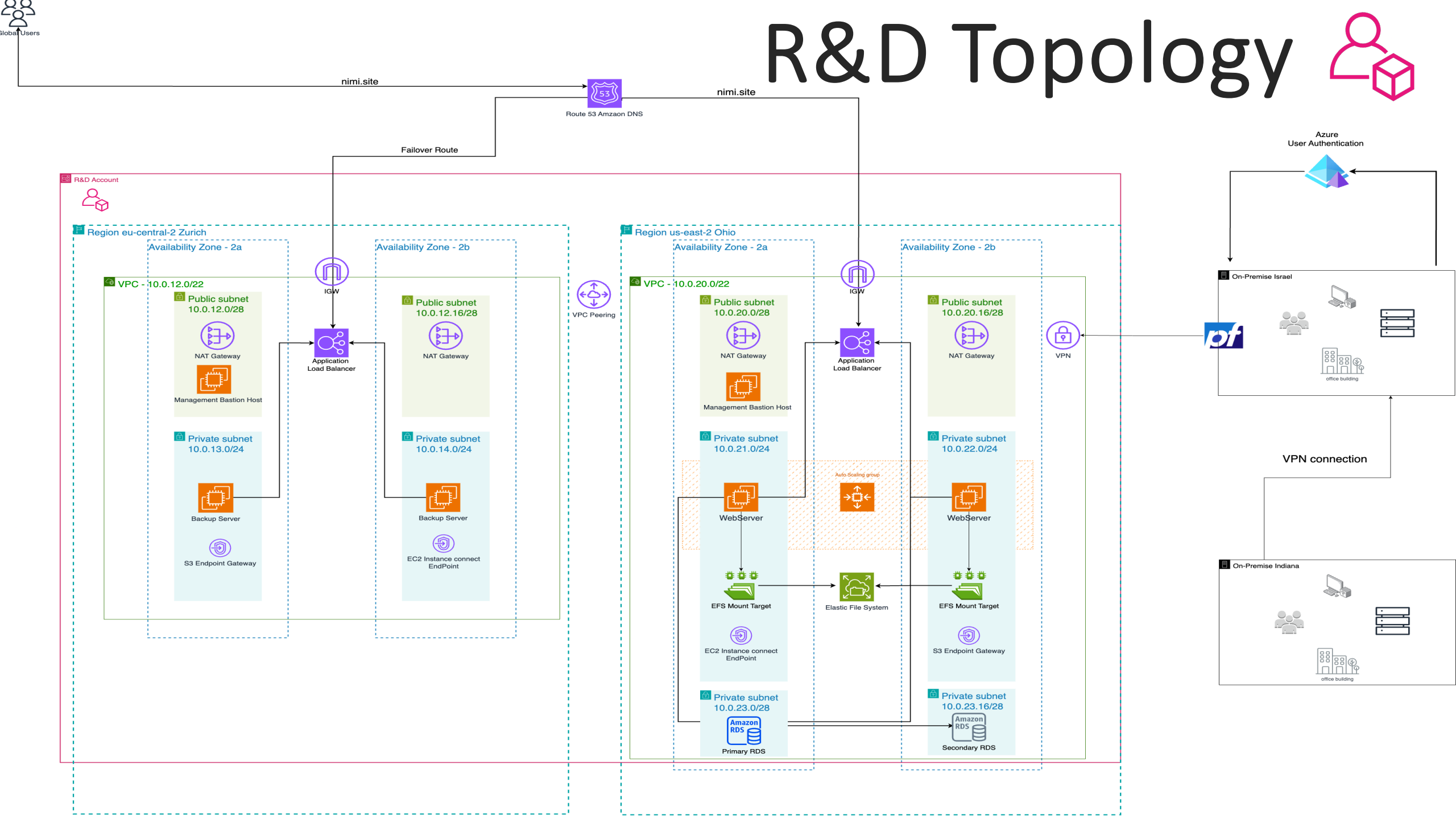
Multi-Region Infrastructure: Two regions managed by R&D, with a backup architecture for redundancy.
Public Subnets: Bastion hosts and NAT Gateways for secure access to private assets.
Private Subnets: Houses WordPress infrastructure with ALB for optimized performance.
WordPress: Utilizes EFS for a shared content folder and RDS for HA and storage scalability.
Auto Scaling: Integrates Route 53 to route traffic seamlessly to the Auto Scaling Group, ensuring the ability to meet varying demands effectively.
Failover Management: Routing managed by Route 53 to a secondary region setup with local databases.
Provisioning and Authentication: Azure Entra ID Integration.

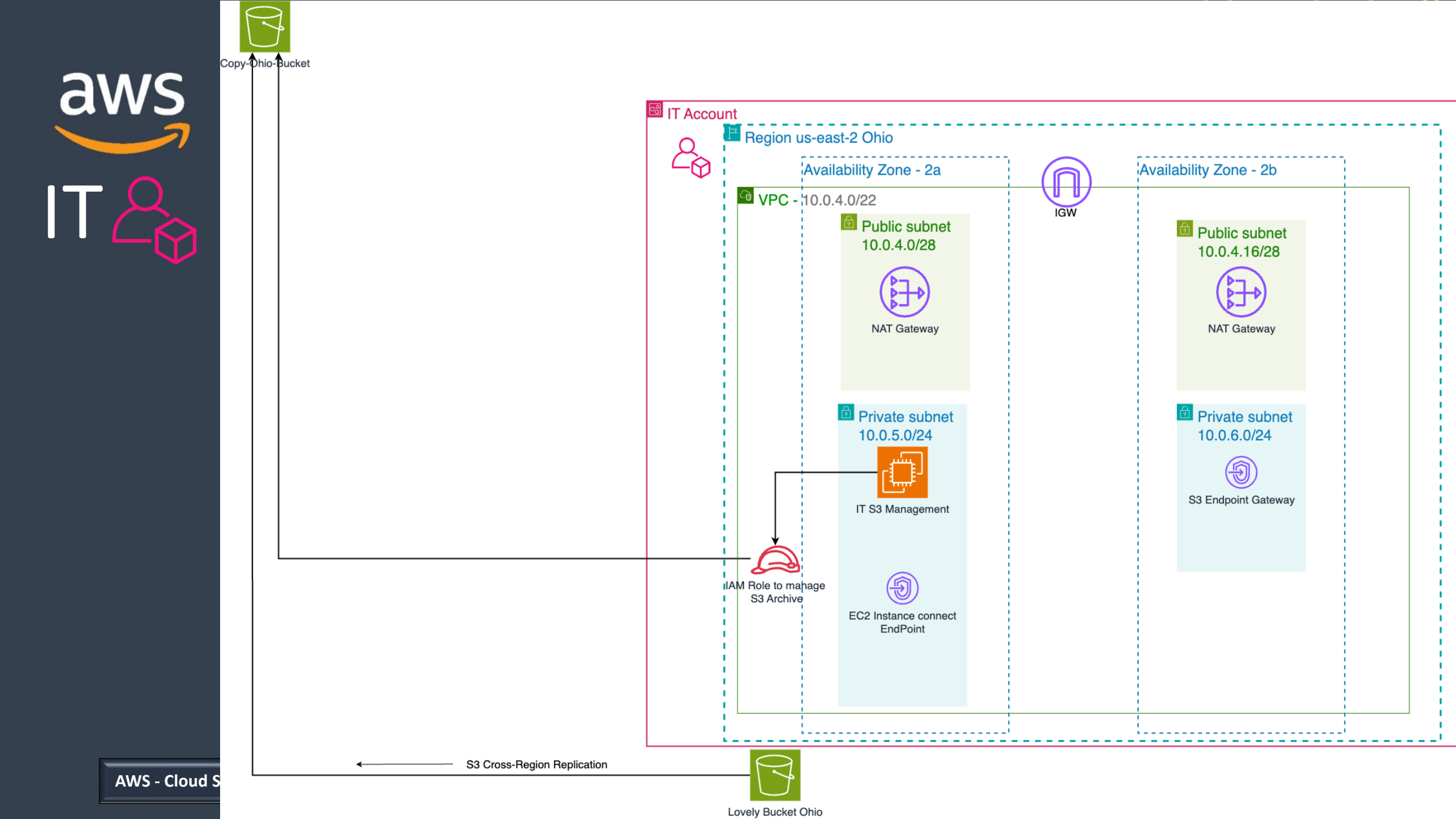
Advanced Configurations:

Leverages S3 and EC2 endpoints for cost management and secure connections.
HTTPS certificate ensures encrypted connections via Load Balancer.
Integration with On-Premises Systems:
Exclusive connection to the primary region using VPN.

This architecture ensures high availability, scalability and security and also guaranteeing optimal resource utilization.

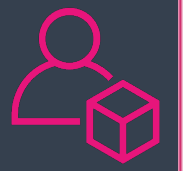
R&D Topology

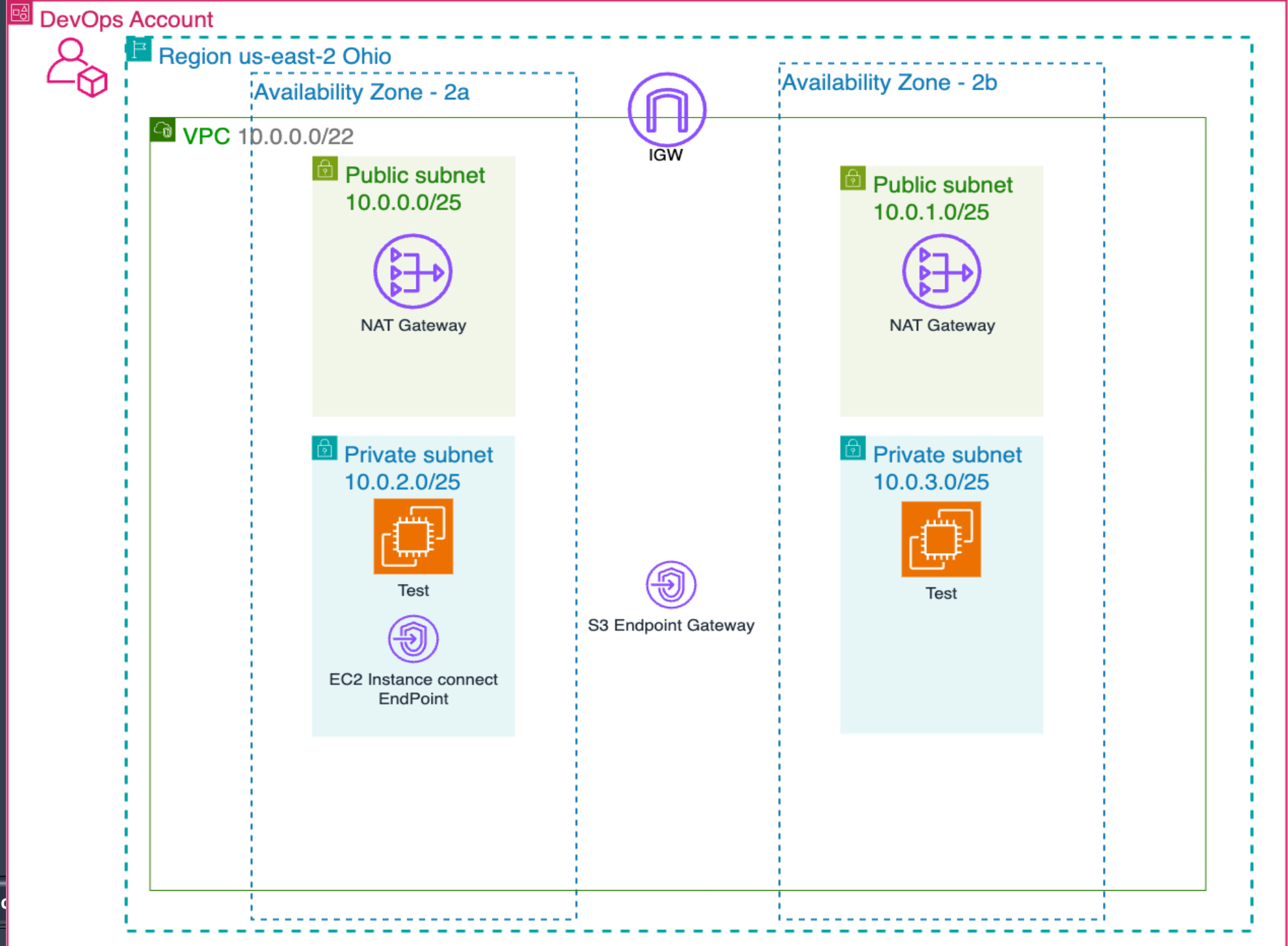

Global Users
nimi.site
Route 53 Amzaon DNS
nimi.site
Failover Route
R&D Account
Region eu-central-2 Zurich
Availability Zone - 2a
Availability Zone - 2b
VPC - 10.0.12.0/22
IGW
Public subnet
10.0.12.0/28
NAT Gateway
Management Bastion Host
Application
Load Balancer
Public subnet
10.0.12.16/28
NAT Gateway
Private subnet
10.0.13.0/24
Backup Server
S3 Endpoint Gateway
Private subnet
10.0.14.0/24
Backup Server
EC2 Instance connect
EndPoint
VPC Peering
Region us-east-2 Ohio
Availability Zone - 2a
Availability Zone - 2b
VPC - 10.0.20.0/22
IGW
Public subnet
10.0.20.0/28
NAT Gateway
Management Bastion Host
Application
Load Balancer
Public subnet
10.0.20.16/28
NAT Gateway
VPN
Private subnet
10.0.21.0/24
WebServer
Auto-Scaling group
Private subnet
10.0.22.0/24
WebServer
EFS Mount Target
Elastic File System
EFS Mount Target
EC2 Instance connect
EndPoint
S3 Endpoint Gateway
Private subnet
10.0.23.0/28
Amazon
RDS
Primary RDS
Private subnet
10.0.23.16/28
Amazon
RDS
Secondary RDS
Azure
User Authentication
On-Premise Israel
office building
VPN connection
On-Premise Indiana
office building


Copy-Ohio-Bucket
IT Account
Region us-east-2 Ohio
Availability Zone - 2a
Availability Zone - 2b
VPC - 10.0.4.0/22
IGW
Public subnet
10.0.4.0/28
NAT Gateway
Public subnet
10.0.4.16/28
NAT Gateway
Private subnet
10.0.5.0/24
IT S3 Management
IAM Role to manage
S3 Archive
EC2 Instance connect
EndPoint
Private subnet
10.0.6.0/24
S3 Endpoint Gateway
S3 Cross-Region Replication
Lovely Bucket Ohio

aws

DevOps

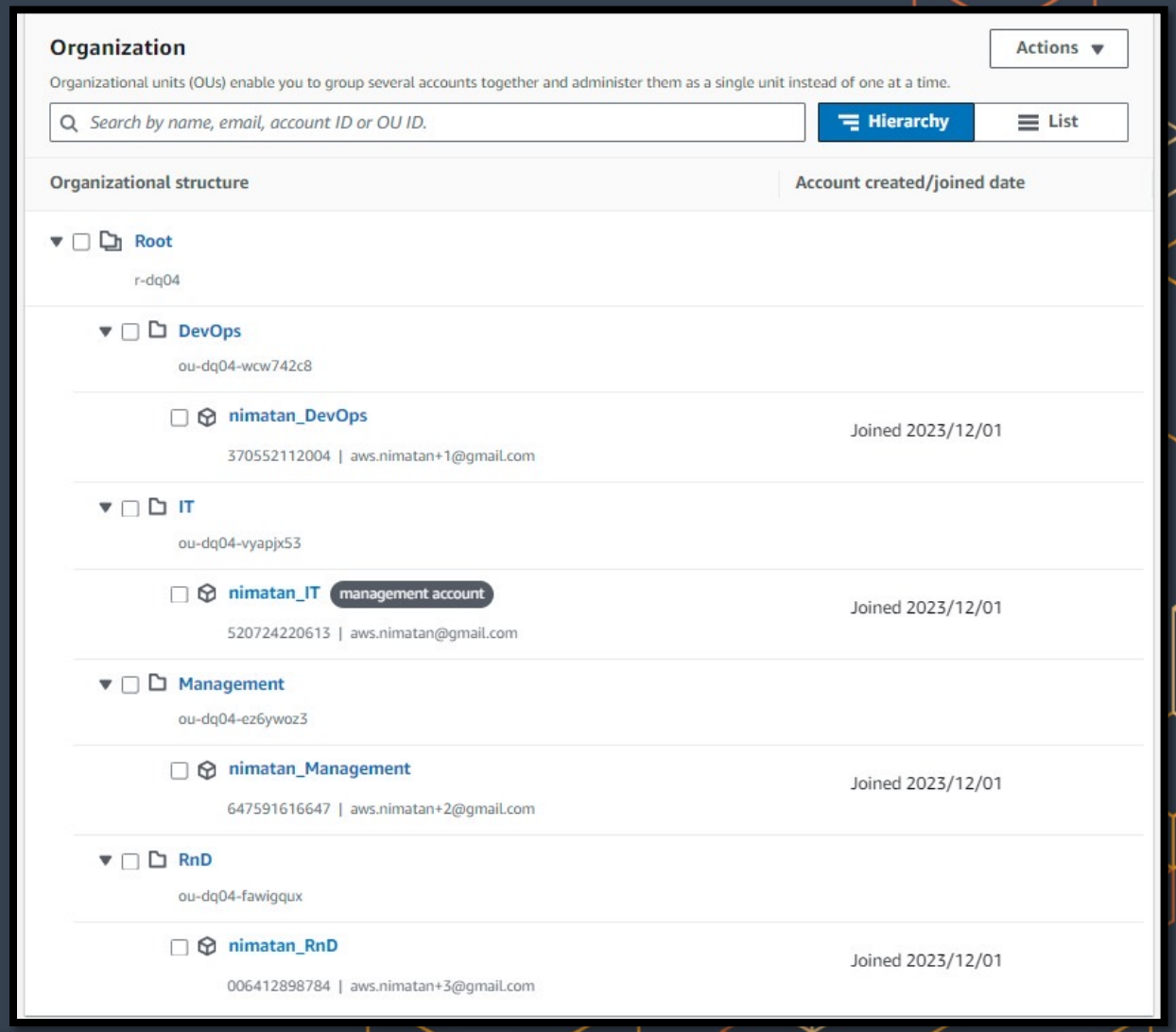



DevOps Account
Region us-east-2 Ohio
Availability Zone - 2a
Availability Zone - 2b
VPC 10.0.0.0/22
IGW
Public subnet
10.0.0.0/25
NAT Gateway
Public subnet
10.0.1.0/25
NAT Gateway
Private subnet
10.0.2.0/25
Test
EC2 Instance connect
EndPoint
S3 Endpoint Gateway
Private subnet
10.0.3.0/25
Test

Organization

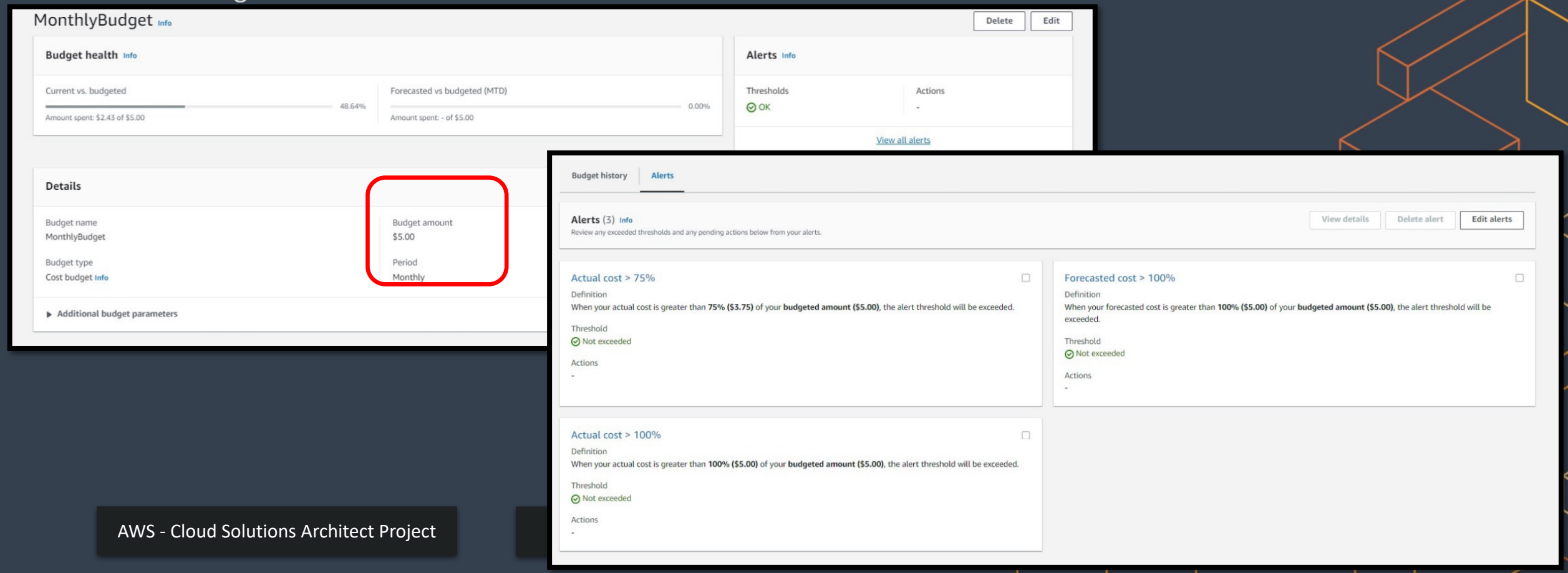
Accounts Segregation: Each organizational unit (OU) is segregated using distinct accounts.

- Users are assigned to respective accounts based on their organizational affiliation.
- Accounts are restricted via **SCPs**, employing "deny" policies on all services in regions except those actively utilized by the organization.



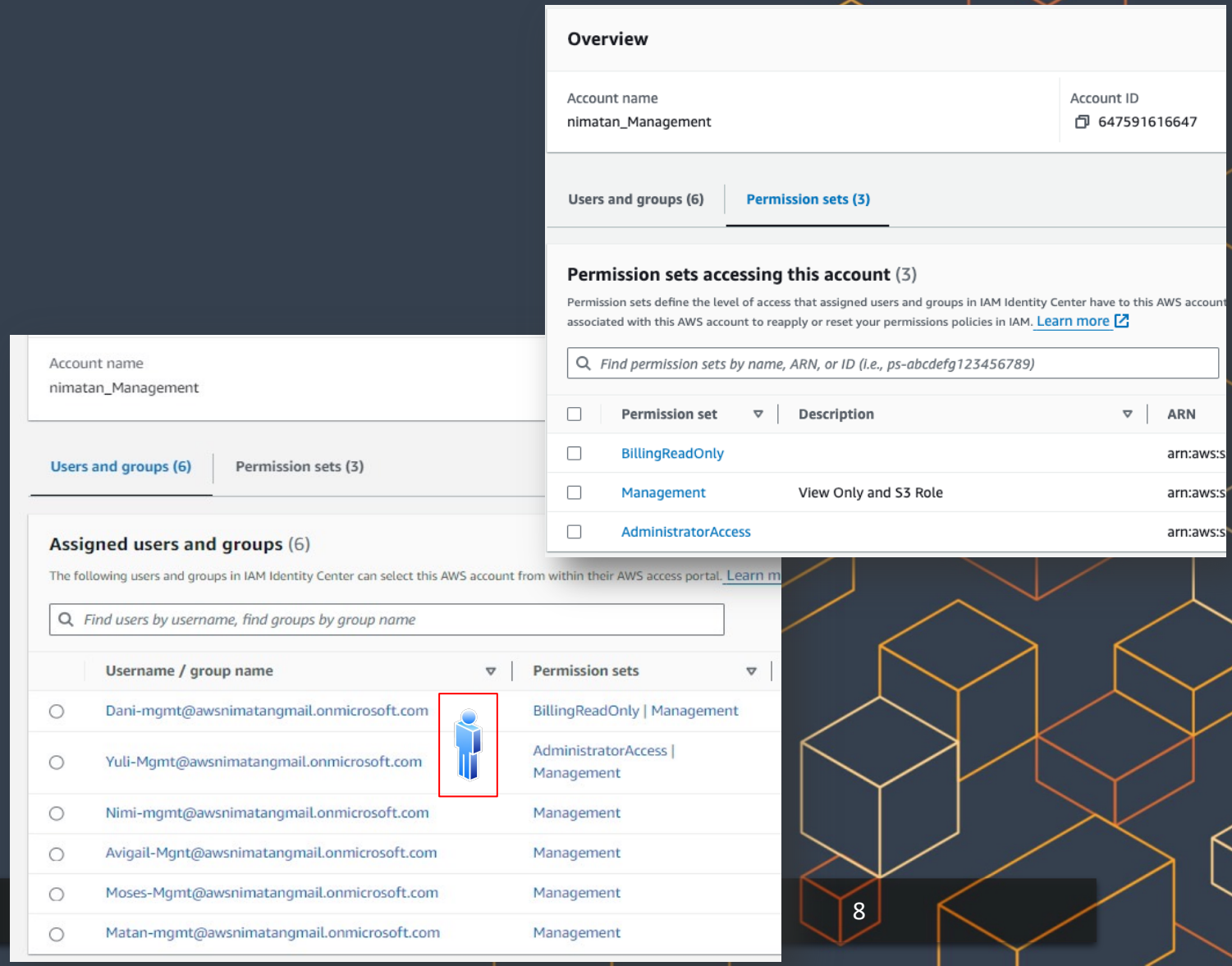
Billing - Budget

- Monthly budgets are allocated for effective financial control.
- Alarms are set to monitor and alert regarding budget thresholds, ensuring proactive financial management.



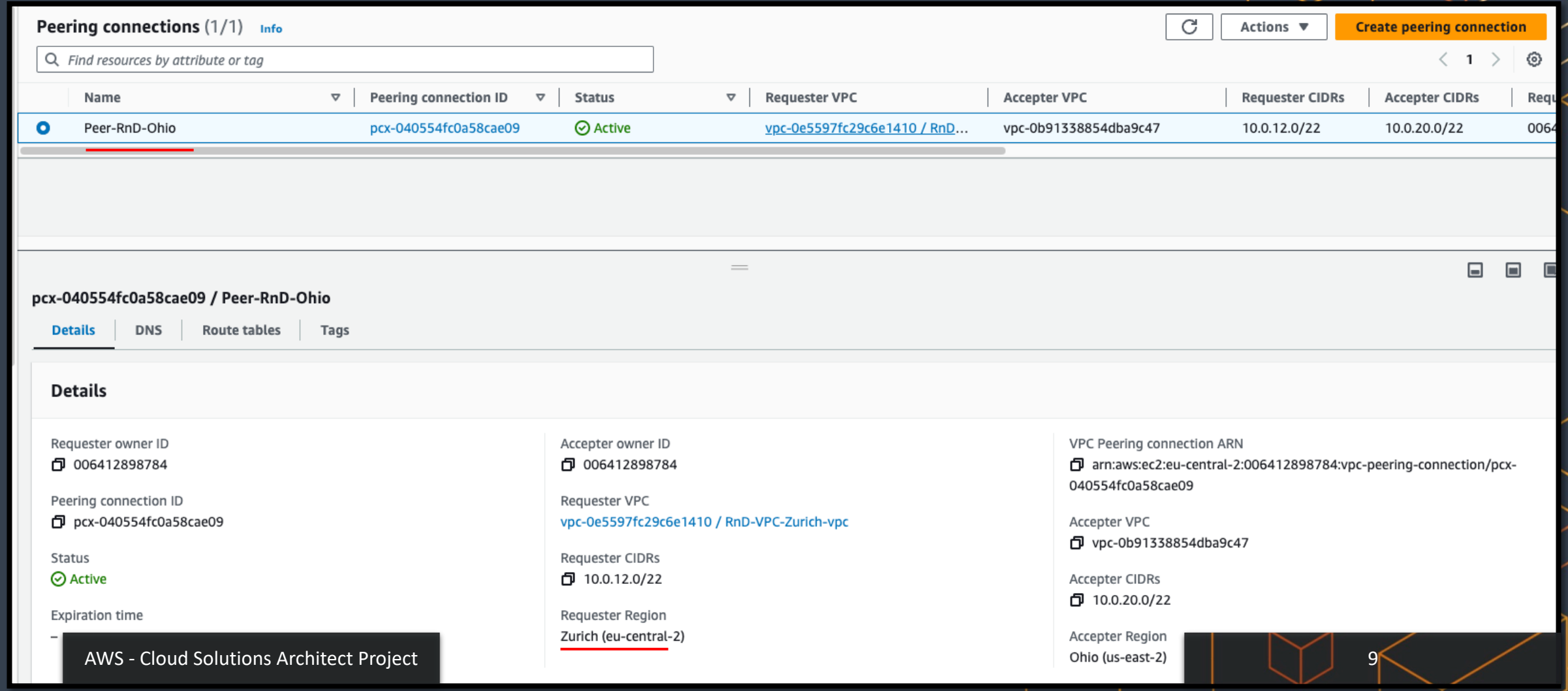
Users & Roles

- Users authentication Managed via **Azure Entra ID** for standardized, secure sign-ins.
- **User Provisioning** Exclusively conducted through Azure Entra ID, granting access via '**AWS Connect User.'**
- Users utilize **Single Sign-On** (SSO) with Microsoft Authenticator for centralized system entry.
- Access Control: Users assigned unique permission sets for precise segregation of access rights within the organizational infrastructure.



VPC - Peering

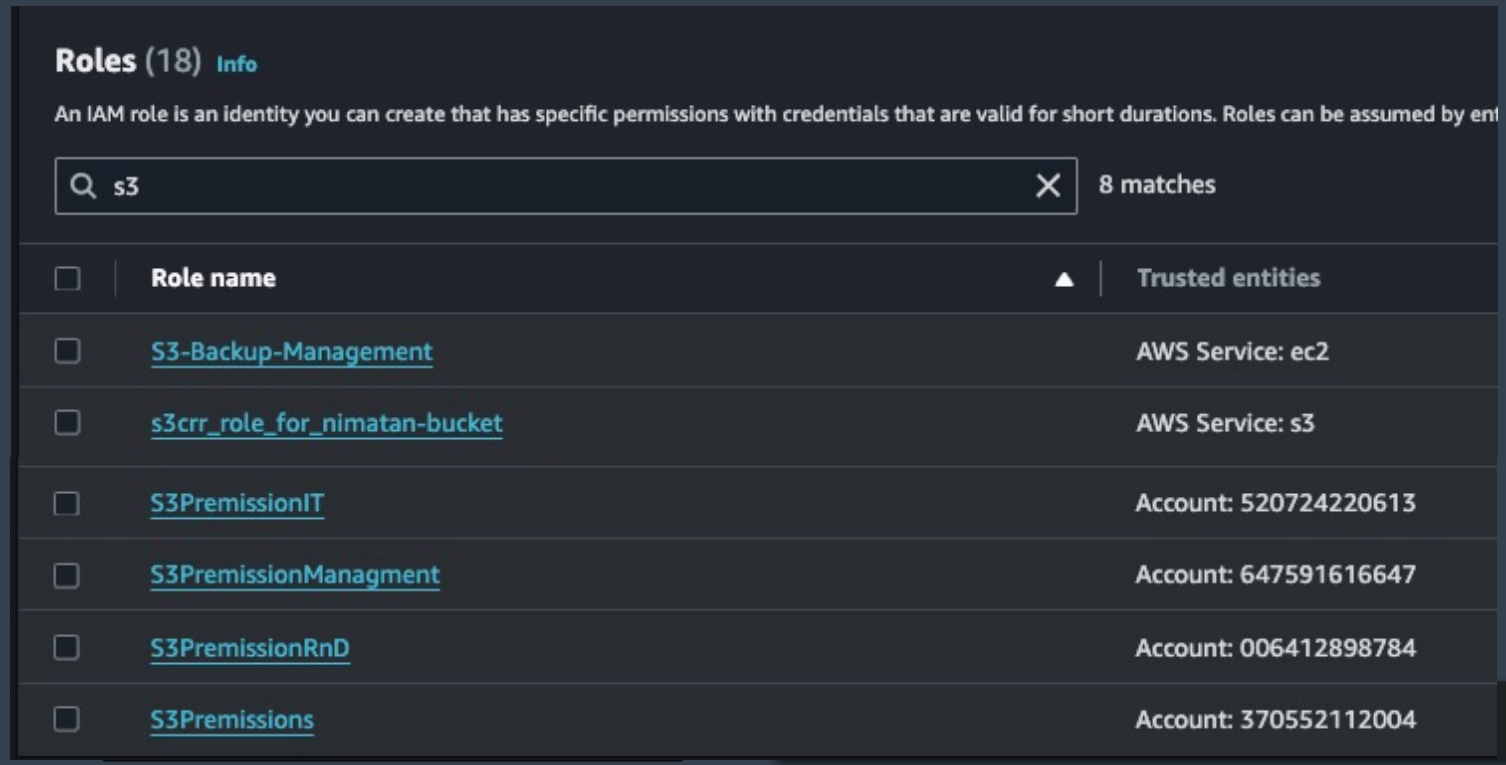
R&D Ohio to R&D Zurich

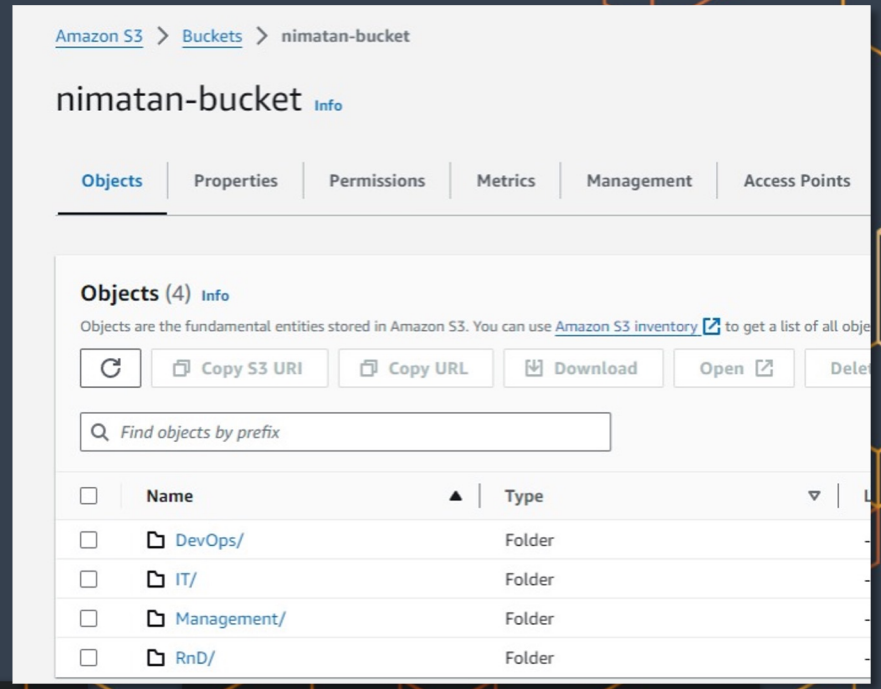


Roles

Enable secure user access within each OU to their specific folders in a shared S3 bucket.

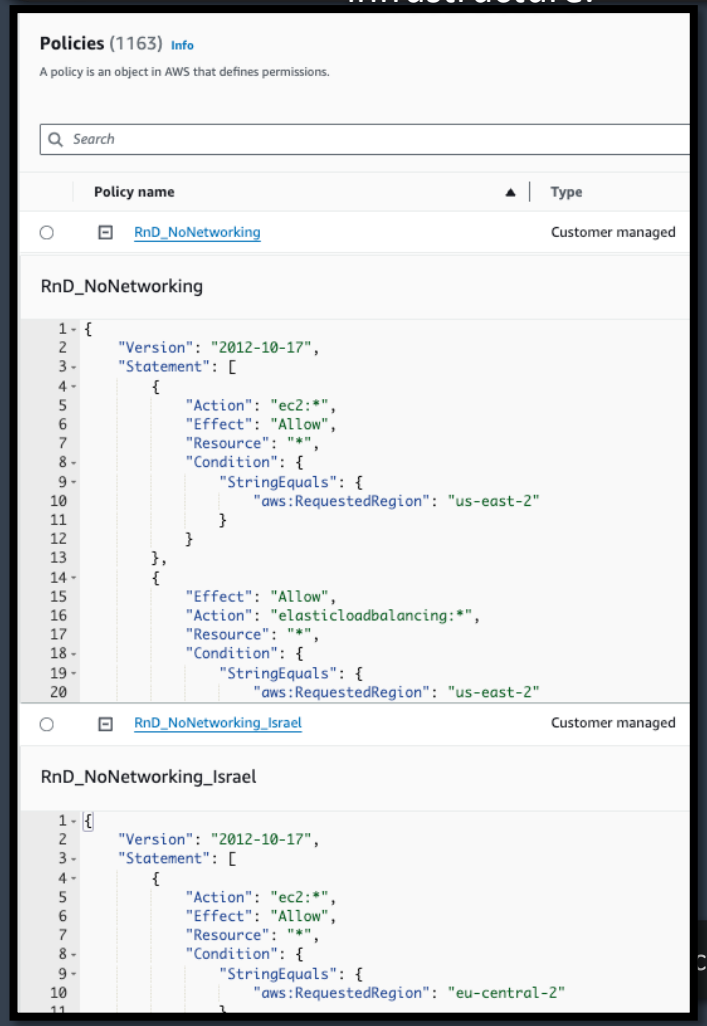
- Created unique S3 roles for each OU.
- Granular permissions tailored to restrict access to designated folders in the shared S3 bucket.
- Enhanced security: Users confined to their folders, reducing data exposure.

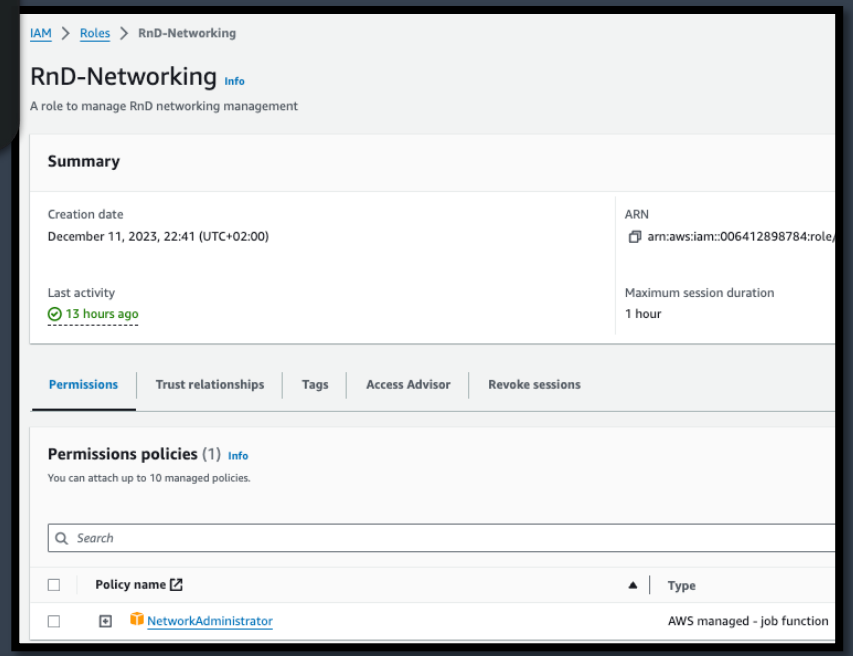


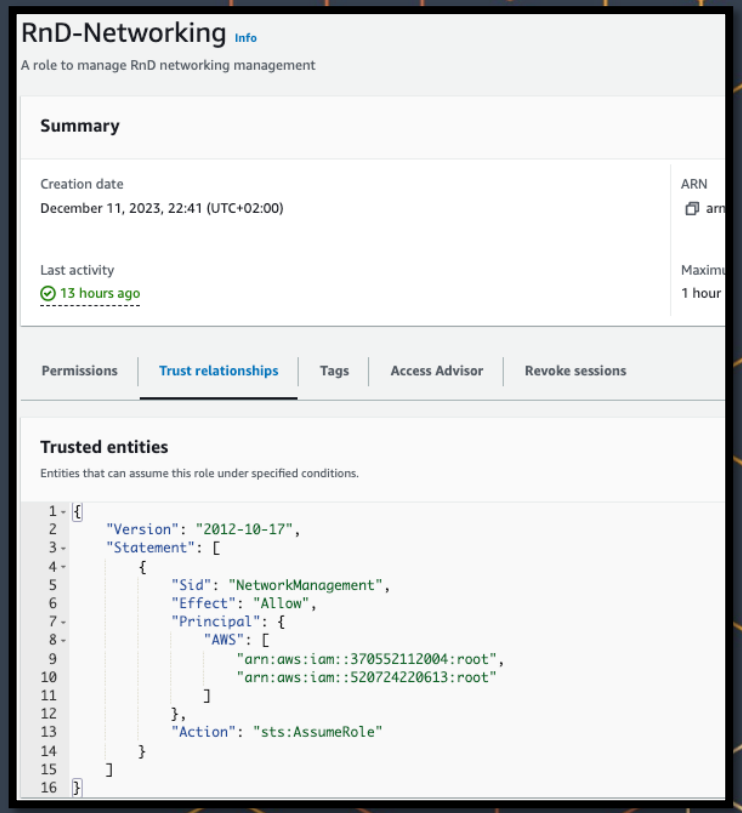


R&D Related Roles

Preventing Unintended Network Modifications: Ensuring stability and security by restricting unauthorized changes to the network infrastructure.







Only IT and DevOps can assume roles for specific network configuration tasks, such as modifying subnets or adjusting VPC settings.

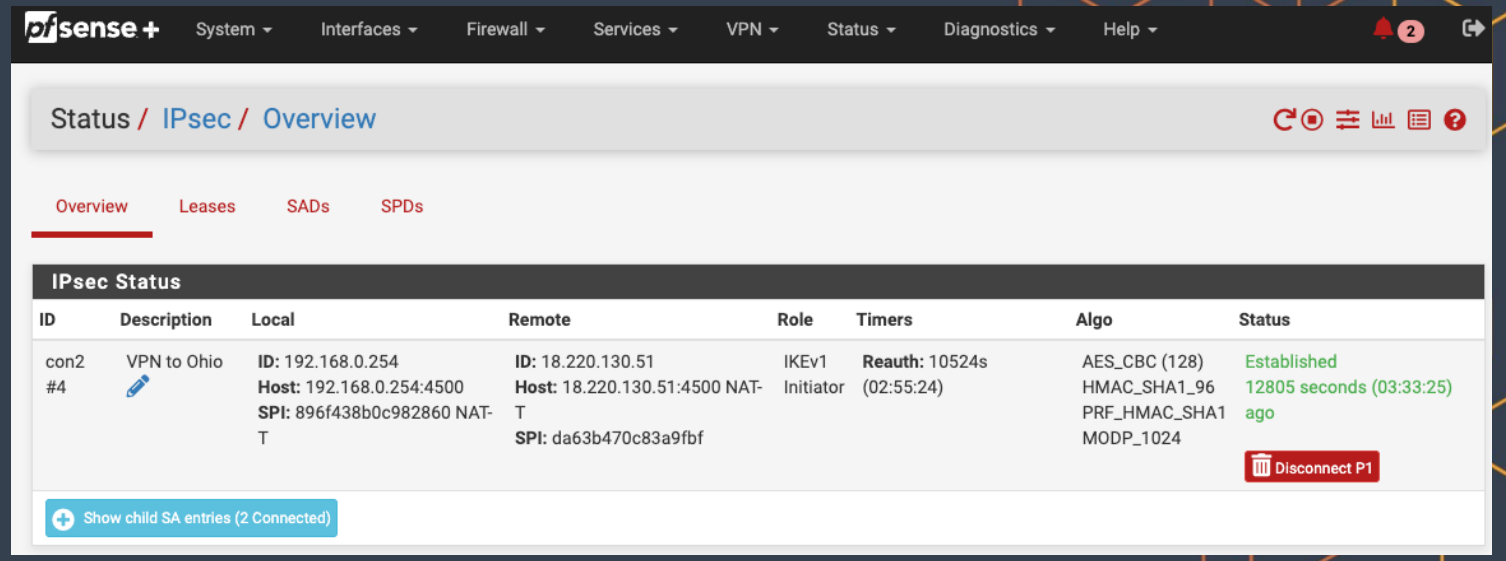
Defined trust relationships necessary to assume the role for network-related tasks.

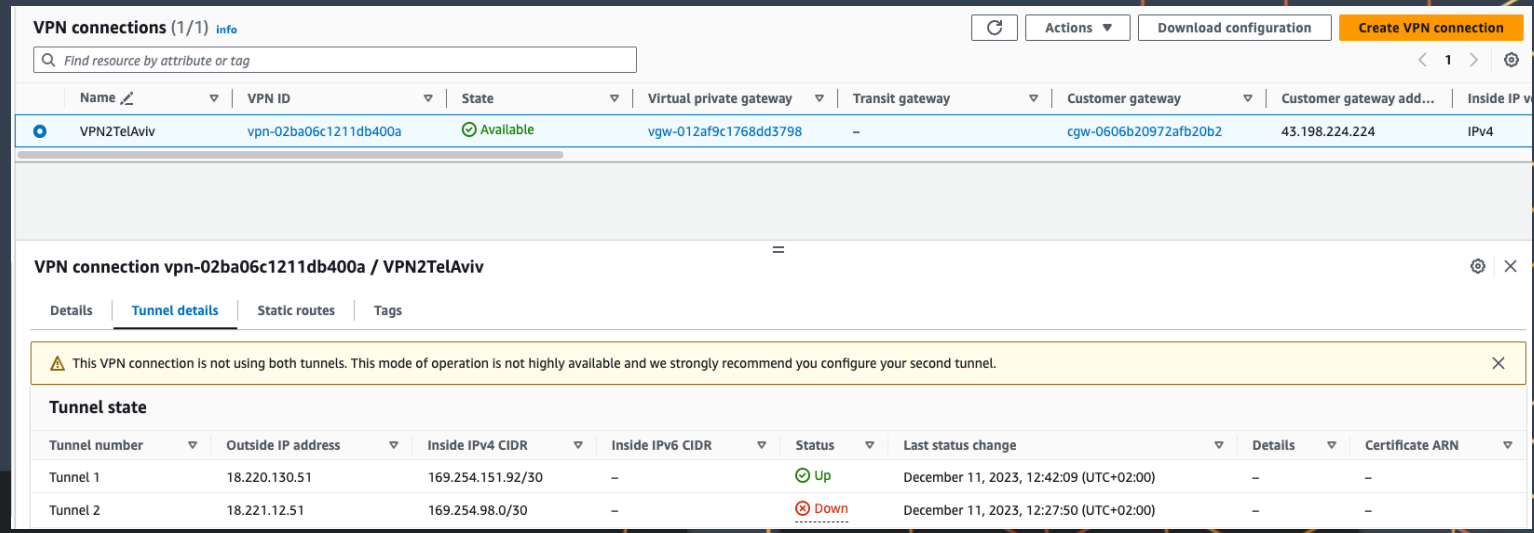
VPN

Establish a secure connection between AWS and On-Premises Network using AWS site to site VPN and pfSense firewall.

AWS Setup:
Utilized AWS Virtual Private Gateway.
Configured Customer Gateway to correspond with on-premises network settings.

On-Premises Infrastructure:
Implemented pfSense as the VPN gateway on the on-premises side.
Configured settings to match AWS VPN specifications.

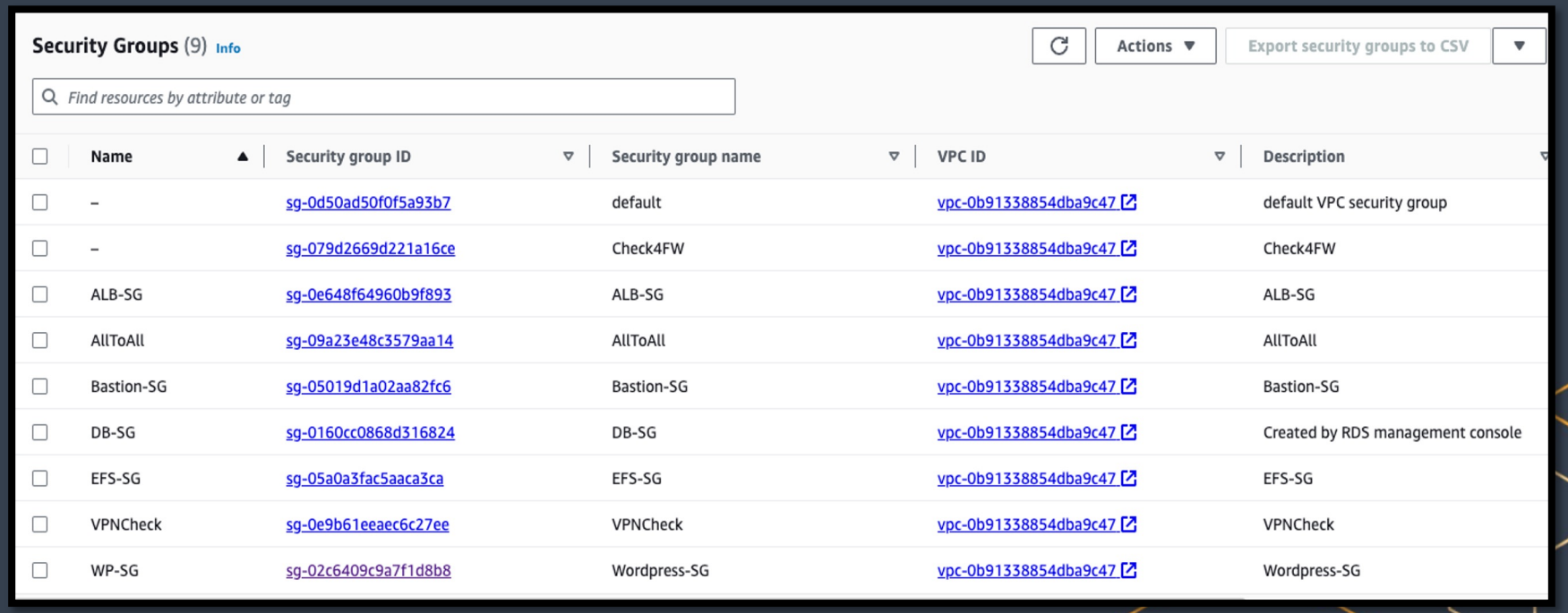




Security Groups

Access to resources is controlled by security groups to prevent unauthorized communications and access through non-compliant and insecure protocols.

R&D Ohio



Security Groups (9) Info

Actions | Export security groups to CSV

Find resources by attribute or tag

Name	Security group ID	Security group name	VPC ID	Description
-	sg-0d50ad50f0f5a93b7	default	vpc-0b91338854dba9c47	default VPC security group
-	sg-079d2669d221a16ce	Check4FW	vpc-0b91338854dba9c47	Check4FW
ALB-SG	sg-0e648f64960b9f893	ALB-SG	vpc-0b91338854dba9c47	ALB-SG
AllToAll	sg-09a23e48c3579aa14	AllToAll	vpc-0b91338854dba9c47	AllToAll
Bastion-SG	sg-05019d1a02aa82fc6	Bastion-SG	vpc-0b91338854dba9c47	Bastion-SG
DB-SG	sg-0160cc0868d316824	DB-SG	vpc-0b91338854dba9c47	Created by RDS management console
EFS-SG	sg-05a0a3fac5aaca3ca	EFS-SG	vpc-0b91338854dba9c47	EFS-SG
VPNCheck	sg-0e9b61eeaec6c27ee	VPNCheck	vpc-0b91338854dba9c47	VPNCheck
WP-SG	sg-02c6409c9a7f1d8b8	Wordpress-SG	vpc-0b91338854dba9c47	Wordpress-SG

S3 Copy: IT EC2 - Role Access

Back to IT

Permissions policies (1) Info

You can attach up to 10 managed policies.

Search

Policy name
S3FullPremissions

S3FullPremissions

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "S3Premission",
            "Effect": "Allow",
            "Action": [
                "s3:*"
            ],
            "Resource": [
                "arn:aws:s3:::zurich-copy",
                "arn:aws:s3:::zurich-copy/*"
            ]
        }
    ]
}
```

S3-Backup-Management Info

Allows EC2 instances to manage S3 Back-up

Summary

Creation date
December 06, 2023, 13:48 (UTC+02:00)

Last activity
1 hour ago

Permissions | Trust relationships | Tags | Access Adviso

Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "ec2.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

Bucket policy

The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies do

Bucket ARN
arn:aws:s3:::zurich-copy

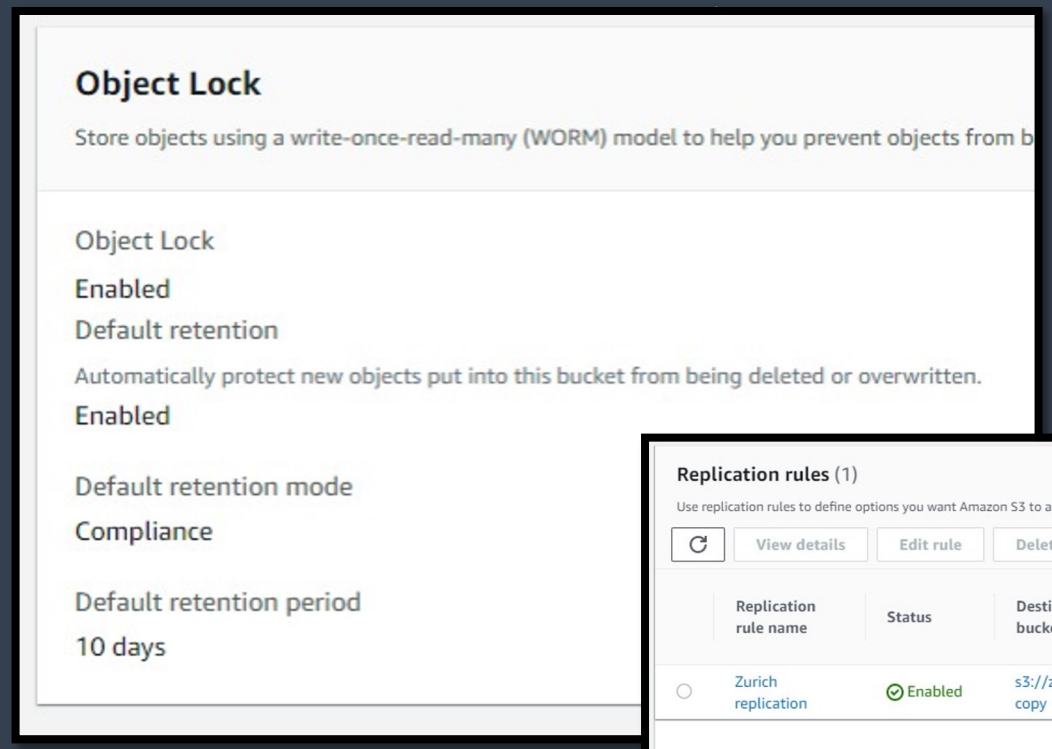
Policy

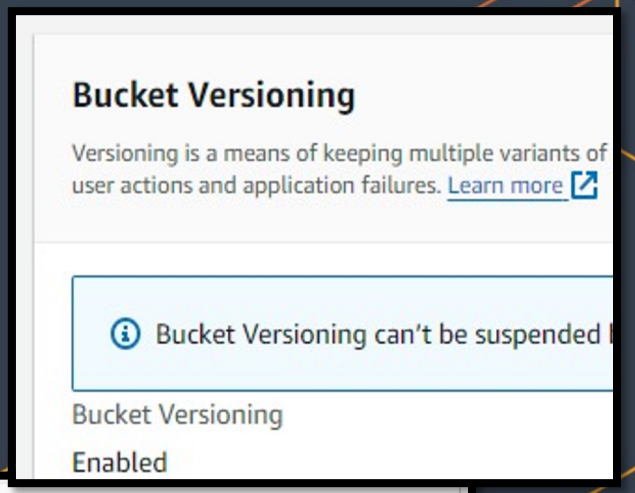
```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "role",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::520724220613:role/S3-Backup-Management"
            },
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::zurich-copy"
        },
        {
            "Sid": "deny",
            "Effect": "Deny",
            "Principal": "*",
            "Action": "s3:*",
            "Resource": "arn:aws:s3:::zurich-copy",
            "Condition": {
                "StringNotEquals": {
                    "aws:PrincipalArn": "arn:aws:iam::520724220613:root"
                }
            }
        }
    ]
}
```

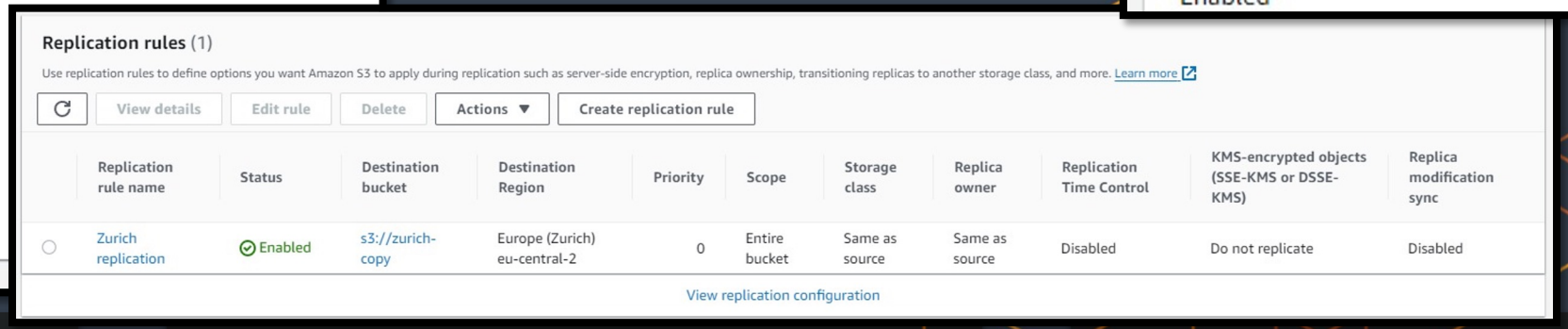
S3 -Configuration

•**Bucket Versioning, Object Lock, and Retention:** Implemented to prevent unintended data loss and ensure data integrity.

•**Cross-Region Replication:** Establishes redundancy by replicating data to a backup bucket in a different region, ensuring resilience against failures.







Your attention is greatly appreciated.

Matan Alon & Nimrod Meshulam