



# 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.

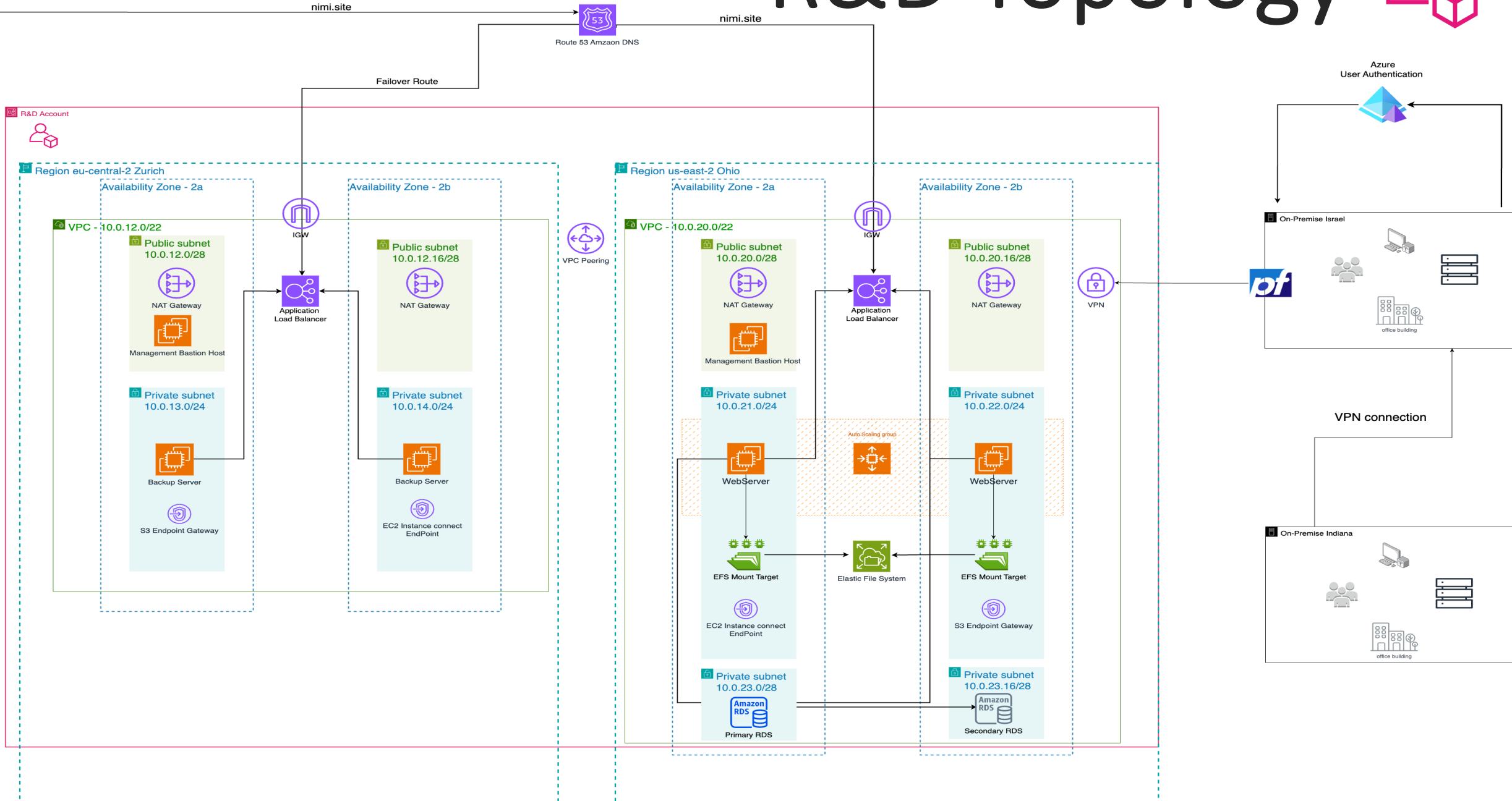
HTTPS certificate ensures encrypted connections via Load Balancer.

## Integration with On-Premises Systems:

Exclusive connection to the primary region using VPN.

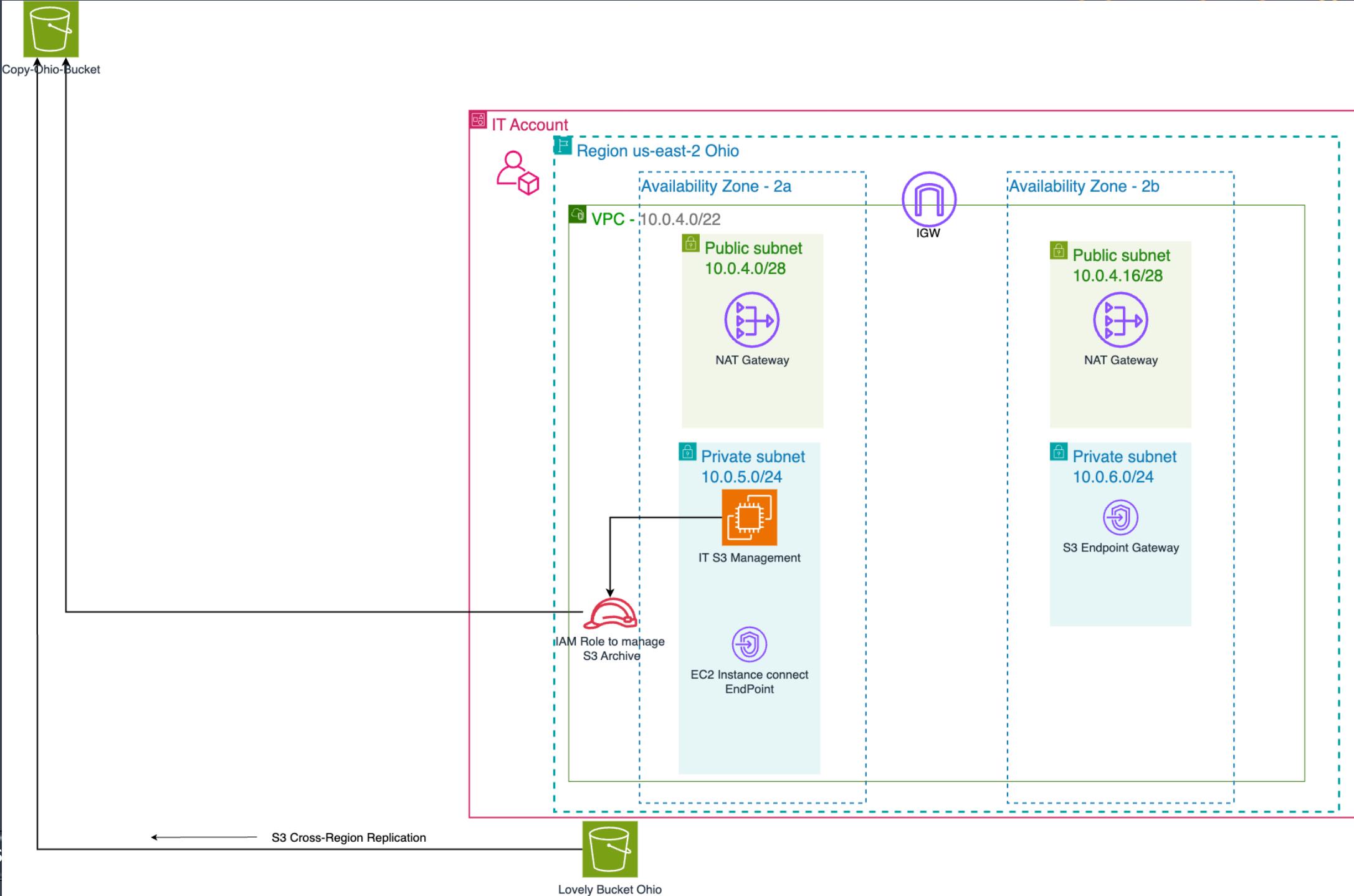
This architecture ensures high availability, scalability and security and also guaranteeing optimal resource utilization.

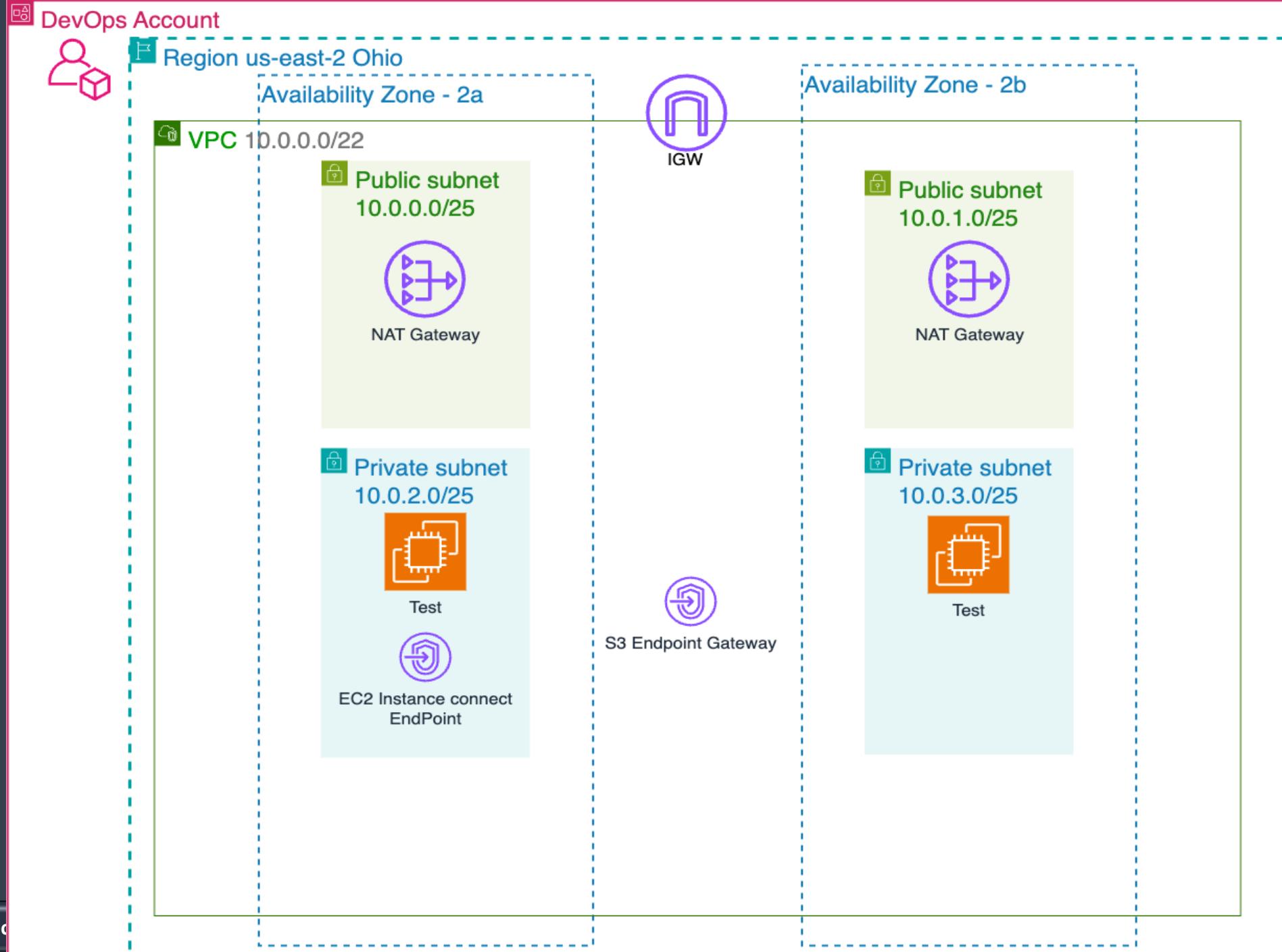
# R&D Topology





AWS - Cloud S







# 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.

Organization

Organizational units (OUs) enable you to group several accounts together and administer them as a single unit instead of one at a time.

Actions ▾

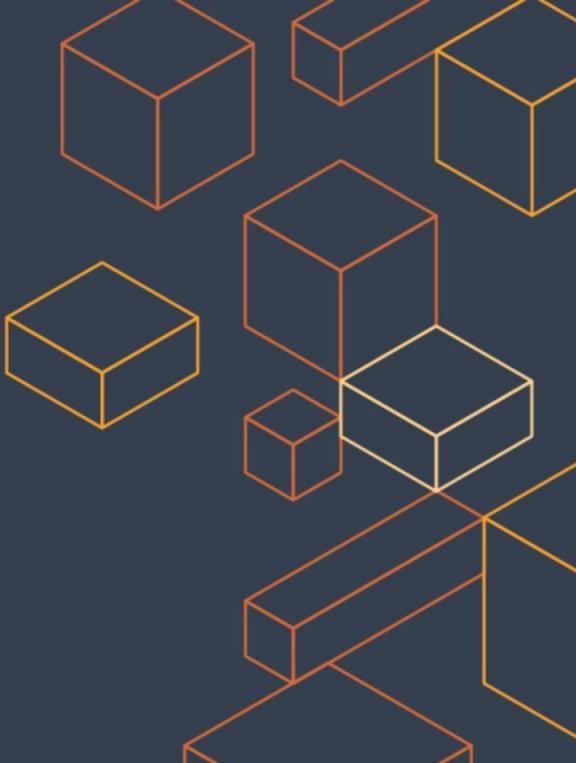
Hierarchy List

Organizational structure Account created/joined date

OU Path	Account ID	Email Address	Joined Date
Root	r-dq04		
DevOps	ou-dq04-wcw742c8		
nimatan_Development	370552112004	aws.nimatan+1@gmail.com	Joined 2023/12/01
IT	ou-dq04-vyapjx53		
nimatan_IT	520724220613	aws.nimatan@gmail.com	Joined 2023/12/01
Management	ou-dq04-ez6ywoz3		
nimatan_Management	647591616647	aws.nimatan+2@gmail.com	Joined 2023/12/01
RnD	ou-dq04-fawigqux		
nimatan_RnD	006412898784	aws.nimatan+3@gmail.com	Joined 2023/12/01

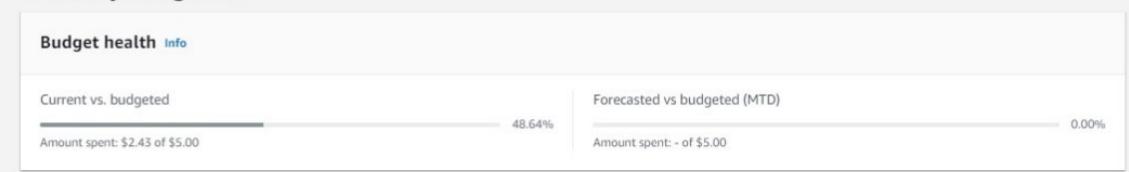


# Billing - Budget



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

## MonthlyBudget [Info](#)



[Delete](#) [Edit](#)

## Alerts [Info](#)

Thresholds	Actions
<a href="#">OK</a>	-

[View all alerts](#)

## Details

Budget name  
MonthlyBudget

Budget type  
Cost budget [Info](#)

[► Additional budget parameters](#)

Budget amount  
\$5.00

Period  
Monthly

## Budget history [Alerts](#)

### Alerts (3) [Info](#)

Review any exceeded thresholds and any pending actions below from your alerts.

[View details](#) [Delete alert](#) [Edit alerts](#)

#### Actual cost > 75%

##### Definition

When your actual cost is greater than 75% (\$3.75) of your **budgeted amount** (\$5.00), the alert threshold will be exceeded.

##### Threshold

Not exceeded

##### Actions

-

#### Forecasted cost > 100%

##### Definition

When your forecasted cost is greater than 100% (\$5.00) of your **budgeted amount** (\$5.00), the alert threshold will be exceeded.

##### Threshold

Not exceeded

##### Actions

-

#### Actual cost > 100%

##### Definition

When your actual cost is greater than 100% (\$5.00) of your **budgeted amount** (\$5.00), the alert threshold will be exceeded.

##### Threshold

Not exceeded

##### Actions

-



# 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.

The screenshot shows the AWS IAM Identity Center console for the account 'nimatan\_Management'. It includes sections for 'Overview' (Account name: nimatan\_Management, Account ID: 647591616647), 'Users and groups (6)' (selected), and 'Permission sets (3)'. The 'Assigned users and groups (6)' section lists six users, each with a blue person icon and assigned permission sets:

Username / group name	Permission sets
Dani-mgmt@awsnimatangmail.onmicrosoft.com	BillingReadOnly   Management
Yuli-Mgmt@awsnimatangmail.onmicrosoft.com	AdministratorAccess   Management
Nimi-mgmt@awsnimatangmail.onmicrosoft.com	Management
Avigail-Mgnt@awsnimatangmail.onmicrosoft.com	Management
Moses-Mgmt@awsnimatangmail.onmicrosoft.com	Management
Matan-mgmt@awsnimatangmail.onmicrosoft.com	Management

On the right side of the slide, there is a decorative graphic of interconnected 3D cubes in orange and grey.



# VPC - Peering

R&D Ohio to R&D Zurich



Peering connections (1/1) [Info](#)

Find resources by attribute or tag

Name	Peering connection ID	Status	Requester VPC	Acceptor VPC	Requester CIDRs	Acceptor CIDRs	Requester Region
Peer-RnD-Ohio	pcx-040554fc0a58cae09	Active	vpc-0e5597fc29c6e1410 / RnD...	vpc-0b91338854dba9c47	10.0.12.0/22	10.0.20.0/22	Zurich (eu-central-2)

[Create peering connection](#)

pcx-040554fc0a58cae09 / Peer-RnD-Ohio

[Details](#) [DNS](#) [Route tables](#) [Tags](#)

**Details**

Requester owner ID	Acceptor owner ID	VPC Peering connection ARN
<a href="#">006412898784</a>	<a href="#">006412898784</a>	<a href="#">arn:aws:ec2:eu-central-2:006412898784:vpc-peering-connection/pcx-040554fc0a58cae09</a>
Peering connection ID	Requester VPC	Acceptor VPC
<a href="#">pcx-040554fc0a58cae09</a>	<a href="#">vpc-0e5597fc29c6e1410 / RnD-VPC-Zurich-vpc</a>	<a href="#">vpc-0b91338854dba9c47</a>
Status	Requester CIDRs	Acceptor CIDRs
<a href="#">Active</a>	<a href="#">10.0.12.0/22</a>	<a href="#">10.0.20.0/22</a>
Expiration time	Requester Region	Acceptor Region
-	<a href="#">Zurich (eu-central-2)</a>	<a href="#">Ohio (us-east-2)</a>

AWS - Cloud Solutions Architect Project



# 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.

**Roles (18) [Info](#)**

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities such as AWS services, Lambda functions, or other AWS accounts.

**s3** X **8 matches**

<input type="checkbox"/>	<b>Role name</b>	<input type="checkbox"/>	<b>Trusted entities</b>
<input type="checkbox"/>	<a href="#">S3-Backup-Management</a>	<input type="checkbox"/>	AWS Service: ec2
<input type="checkbox"/>	<a href="#">s3crr_role_for_nimatan-bucket</a>	<input type="checkbox"/>	AWS Service: s3
<input type="checkbox"/>	<a href="#">S3PremissionIT</a>	<input type="checkbox"/>	Account: 520724220613
<input type="checkbox"/>	<a href="#">S3PremissionManagement</a>	<input type="checkbox"/>	Account: 647591616647
<input type="checkbox"/>	<a href="#">S3PremissionRnD</a>	<input type="checkbox"/>	Account: 006412898784
<input type="checkbox"/>	<a href="#">S3Premissions</a>	<input type="checkbox"/>	Account: 370552112004

[Amazon S3](#) > [Buckets](#) > nimatan-bucket

**nimatan-bucket [Info](#)**

[Objects](#) [Properties](#) [Permissions](#) [Metrics](#) [Management](#) [Access Points](#)

**Objects (4) [Info](#)**

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects.

<input type="checkbox"/>	<b>Name</b>	<input type="checkbox"/>	<b>Type</b>
<input type="checkbox"/>	DevOps/	<input type="checkbox"/>	Folder
<input type="checkbox"/>	IT/	<input type="checkbox"/>	Folder
<input type="checkbox"/>	Management/	<input type="checkbox"/>	Folder
<input type="checkbox"/>	RnD/	<input type="checkbox"/>	Folder



# R&D Related Roles

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

Policies (1163) [Info](#)  
A policy is an object in AWS that defines permissions.

Search

Policy name	Type
<a href="#">RnD_NoNetworking</a>	Customer managed
<b>RnD_NoNetworking</b>	
<pre>1 { "Version": "2012-10-17", "Statement": [ 2 { "Action": "ec2:*", "Effect": "Allow", "Resource": "*", "Condition": { "StringEquals": { "aws:RequestedRegion": "us-east-2" } } }, 3 { "Effect": "Allow", "Action": "elasticloadbalancing:*", "Resource": "*", "Condition": { "StringEquals": { "aws:RequestedRegion": "us-east-2" } } }</pre>	
<a href="#">RnD_NoNetworking_Israel</a>	Customer managed
<b>RnD_NoNetworking_Israel</b>	
<pre>1 { "Version": "2012-10-17", "Statement": [ 2 { "Action": "ec2:*", "Effect": "Allow", "Resource": "*", "Condition": { "StringEquals": { "aws:RequestedRegion": "eu-central-2" } } }</pre>	

IAM > Roles > RnD-Networking

**RnD-Networking** [Info](#)  
A role to manage RnD networking management

**Summary**

Creation date December 11, 2023, 22:41 (UTC+02:00) ARN [arn:aws:iam::006412898784:role/RnD-Networking](#)

Last activity [13 hours ago](#) Maximum session duration 1 hour

[Permissions](#) [Trust relationships](#) [Tags](#) [Access Advisor](#) [Revoke sessions](#)

**Permissions policies (1)** [Info](#)  
You can attach up to 10 managed policies.

Search Policy name Type

[NetworkAdministrator](#) AWS managed - job function

**RnD-Networking** [Info](#)  
A role to manage RnD networking management

**Summary**

Creation date December 11, 2023, 22:41 (UTC+02:00) ARN [arn:aws:iam::006412898784:role/RnD-Networking](#)

Last activity [13 hours ago](#) Maximum session duration 1 hour

[Permissions](#) [Trust relationships](#) [Tags](#) [Access Advisor](#) [Revoke sessions](#)

**Trusted entities**

Entities that can assume this role under specified conditions.

```
1 { "Version": "2012-10-17", "Statement": [ 2 { "Sid": "NetworkManagement", "Effect": "Allow", "Principal": { "AWS": [ "arn:aws:iam::370552112004:root", "arn:aws:iam::520724220613:root" ] } }, 3 { "Action": "sts:AssumeRole" } ] }
```

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.



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.

The screenshot shows the pfSense IPsec Status Overview page. It displays a table of IPsec connections. One connection is listed:

ID	Description	Local	Remote	Role	Timers	Algo	Status
con2 #4	VPN to Ohio	ID: 192.168.0.254 Host: 192.168.0.254:4500 SPI: 896f438b0c982860 NAT-T	ID: 18.220.130.51 Host: 18.220.130.51:4500 NAT-T SPI: da63b470c83a9fbf	IKEv1 Initiator	Reauth: 10524s (02:55:24)	AES_CBC (128) HMAC_SHA1_96 PRF_HMAC_SHA1 MODP_1024	Established 12805 seconds (03:33:25) ago

[Show child SA entries \(2 Connected\)](#)



The screenshot shows the AWS VPC console's VPN connections page. It lists one connection:

Name	VPN ID	State	Virtual private gateway	Transit gateway	Customer gateway	Customer gateway address	Inside IP range
VPN2TelAviv	vpn-02ba06c1211db400a	Available	vgw-012af9c1768dd3798	-	cgw-0606b20972afb20b2	43.198.224.224	IPv4

**VPN connection vpn-02ba06c1211db400a / VPN2TelAviv**

Details | **Tunnel details** | Static routes | Tags

**Tunnel state**

Tunnel number	Outside IP address	Inside IPv4 CIDR	Inside IPv6 CIDR	Status	Last status change	Details	Certificate ARN
Tunnel 1	18.220.130.51	169.254.151.92/30	-	Up	December 11, 2023, 12:42:09 (UTC+02:00)	-	-
Tunnel 2	18.221.12.51	169.254.98.0/30	-	Down	December 11, 2023, 12:27:50 (UTC+02:00)	-	-



R&D Ohio

# Security Groups

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

Security Groups (9) <a href="#">Info</a>					
<input type="text"/> Find resources by attribute or tag					
<input type="checkbox"/>	Name	▲	Security group ID	▼	Security group name
<input type="checkbox"/>	-		<a href="#">sg-0d50ad50f0f5a93b7</a>		default
<input type="checkbox"/>	-		<a href="#">sg-079d2669d221a16ce</a>		Check4FW
<input type="checkbox"/>	ALB-SG		<a href="#">sg-0e648f64960b9f893</a>		ALB-SG
<input type="checkbox"/>	AllToAll		<a href="#">sg-09a23e48c3579aa14</a>		AllToAll
<input type="checkbox"/>	Bastion-SG		<a href="#">sg-05019d1a02aa82fc6</a>		Bastion-SG
<input type="checkbox"/>	DB-SG		<a href="#">sg-0160cc0868d316824</a>		DB-SG
<input type="checkbox"/>	EFS-SG		<a href="#">sg-05a0a3fac5aaca3ca</a>		EFS-SG
<input type="checkbox"/>	VPNCheck		<a href="#">sg-0e9b61eeaec6c27ee</a>		VPNCheck
<input type="checkbox"/>	WP-SG		<a href="#">sg-02c6409c9a7f1d8b8</a>		Wordpress-SG

# aws

# S3 Copy: IT EC2 - Role Access

[Back to IT](#)

Permissions policies (1) [Info](#)  
You can attach up to 10 managed policies.

Search

Policy name [\[x\]](#)

[S3FullPremissions](#)

**S3FullPremissions**

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Sid": "S3Premission",  
6             "Effect": "Allow",  
7             "Action": [  
8                 "s3:*"  
9             ],  
10            "Resource": [  
11                "arn:aws:s3:::zurich-copy",  
12                "arn:aws:s3:::zurich-copy/*"  
13            ]  
14        }  
15    ]  
16 }
```

**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 Advisor

Trusted entities

Entities that can assume this role under specified conditions.

```
1 {  
2     "Version": "2012-10-17",  
3     "Statement": [  
4         {  
5             "Effect": "Allow",  
6             "Principal": {  
7                 "Service": "ec2.amazonaws.com"  
8             },  
9             "Action": "sts:AssumeRole"  
10        }  
11    ]  
12 }
```

**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

```
1 Version: "2012-10-17",  
2 Statement: [  
3     {  
4         Sid: "role",  
5         Effect: "Allow",  
6         Principal: {  
7             AWS: "arn:aws:iam::520724220613:role/S3-Backup-Management"  
8         },  
9         Action: "s3:*",  
10        Resource: "arn:aws:s3:::zurich-copy"  
11    },  
12    {  
13        Sid: "deny",  
14        Effect: "Deny",  
15        Principal: "*",  
16        Action: "s3:*",  
17        Resource: "arn:aws:s3:::zurich-copy",  
18        Condition: {  
19            StringNotEquals: {  
20                aws:PrincipalArn: "arn:aws:iam::520724220613:root"  
21            }  
22        }  
23    }  
24 }  
25 ]  
26 }
```



# 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.

The screenshot displays the AWS S3 Bucket Configuration interface. It includes three main sections: Object Lock, Bucket Versioning, and Replication rules.

**Object Lock**:  
Enabled  
Default retention  
Automatically protect new objects put into this bucket from being deleted or overwritten.  
Enabled

**Bucket Versioning**:  
Versioning is a means of keeping multiple variants of user actions and application failures. [Learn more](#)  
Bucket Versioning can't be suspended  
Bucket Versioning  
Enabled

**Replication rules (1)**:  
Use replication rules to define options you want Amazon S3 to apply during replication such as server-side encryption, replica ownership, transitioning replicas to another storage class, and more. [Learn more](#)  
View details | Edit rule | Delete | Actions ▾ | Create replication rule

Replication rule name	Status	Destination bucket	Destination Region	Priority	Scope	Storage class	Replica owner	Replication Time Control	KMS-encrypted objects (SSE-KMS or DSSE-KMS)	Replica modification sync
Zurich replication	Enabled	s3://zurich-copy	Europe (Zurich) eu-central-2	0	Entire bucket	Same as source	Same as source	Disabled	Do not replicate	Disabled



# Your attention is greatly appreciated.

Matan Alon & Nimrod Meshulam