# Capstone Project

Created by Keegan Barbosa, Adeel Awan, and Robin Gaudreau


# I.Our Team

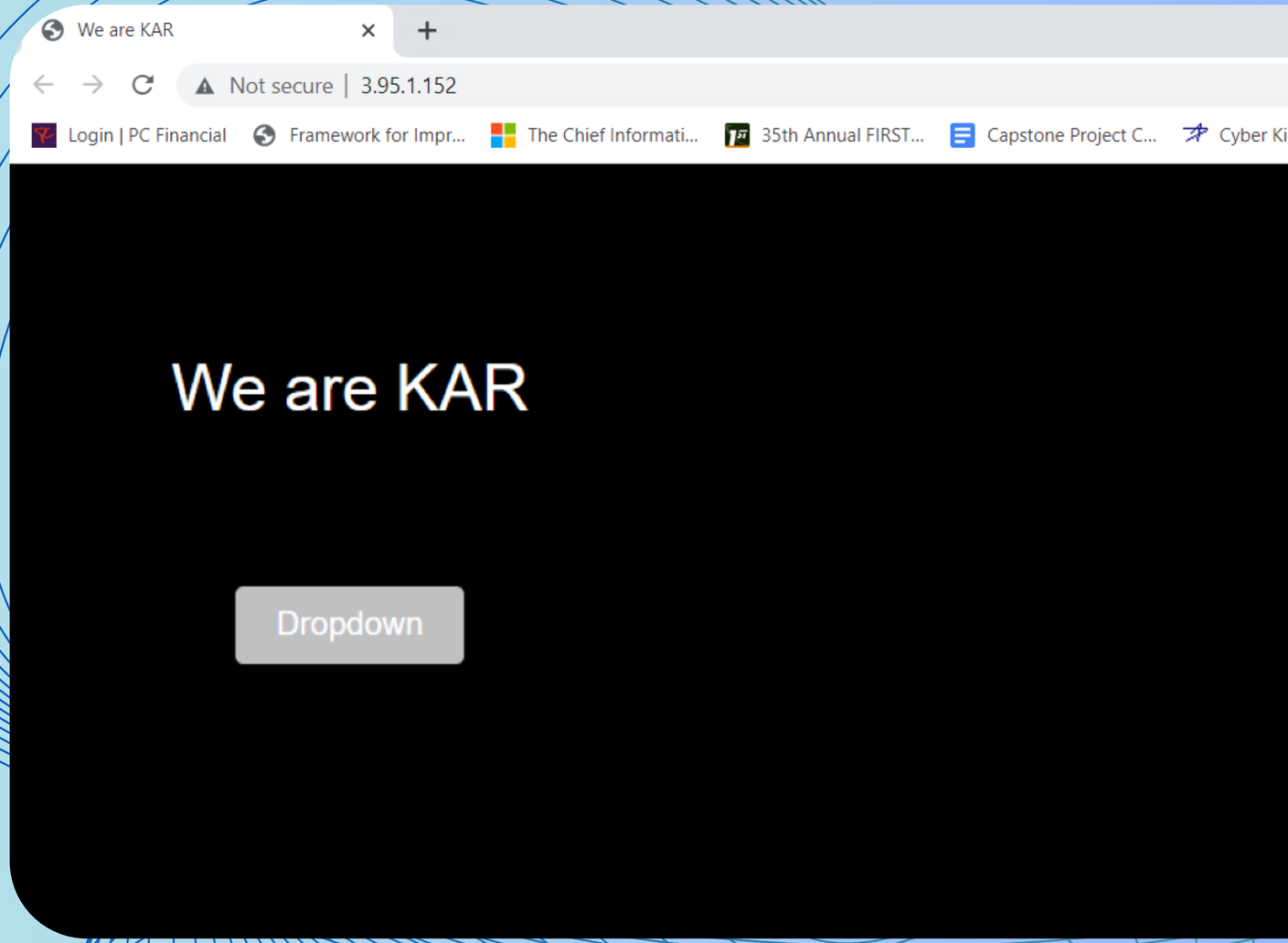
Keegan

Adeel

Robin

# 2.KAR App

a KAR dealership, where your future vehicle awaits you.

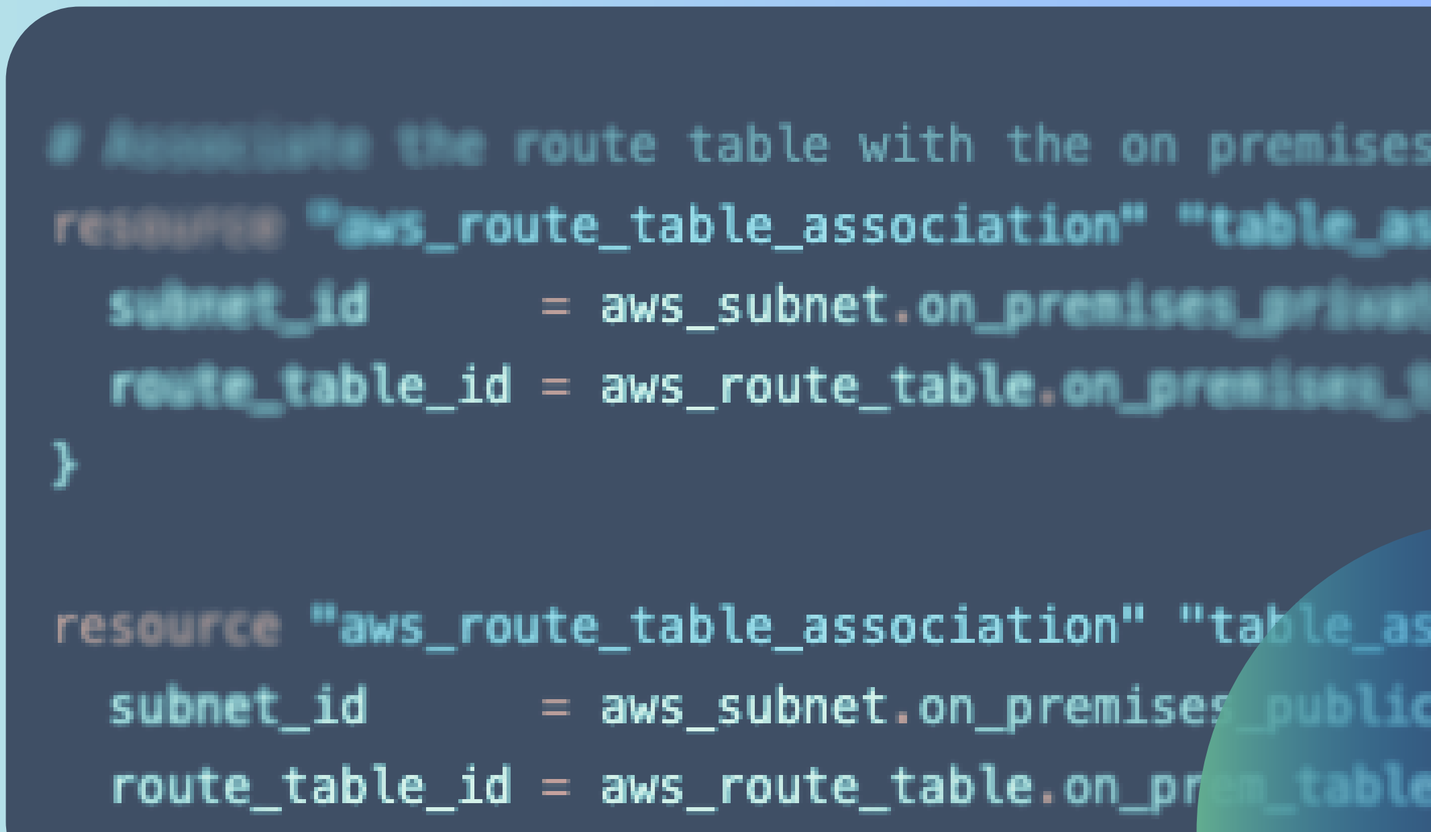


# 3.Infrastructure as Code

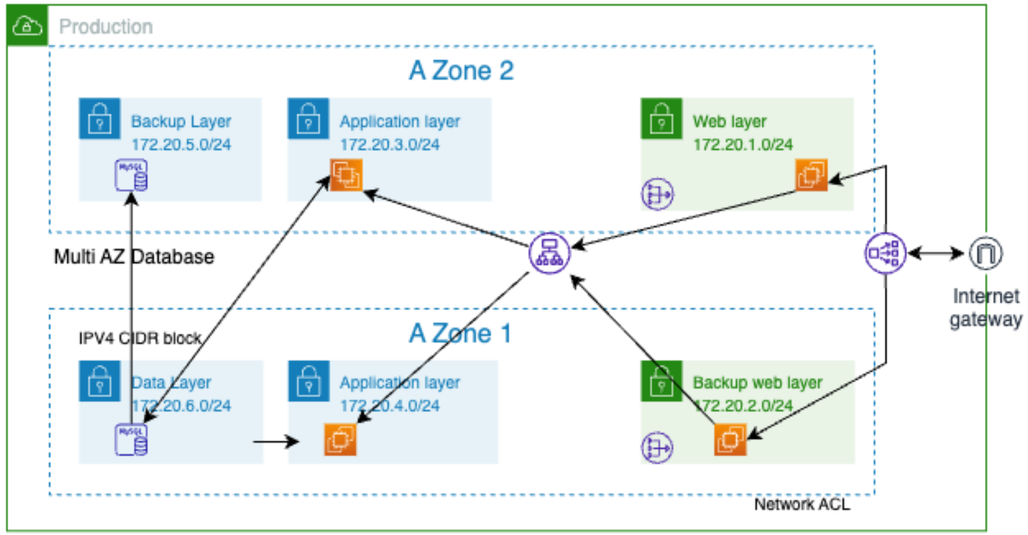
Terraform used to deploy and develop infrastructure

Benefits:

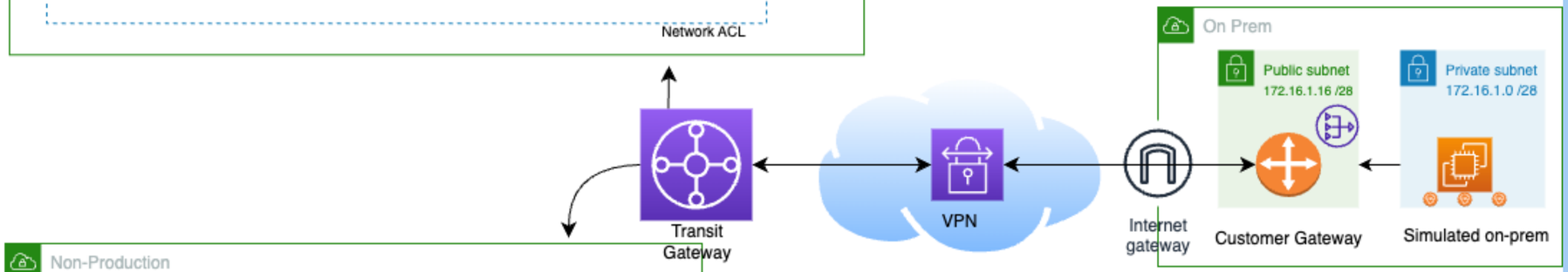
- Agility
- Consistency
- Versioning
- Collaboration
- Documentation

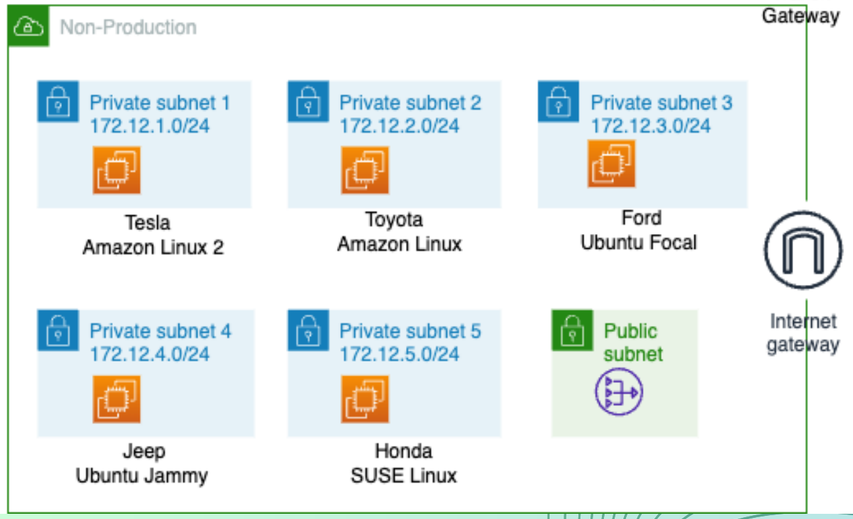


# 4.Architechture




| Transit Gateway Connectivity | | | |
|---|---|---|---|
| Environtments | Production | Non-prod | On-prem |
| Production | Internal restrictions | No connection | Through VPN |
| Non-prod | No connection | None | Through VPN |
| On-prem | Through VPN | Through VPN | LAN |



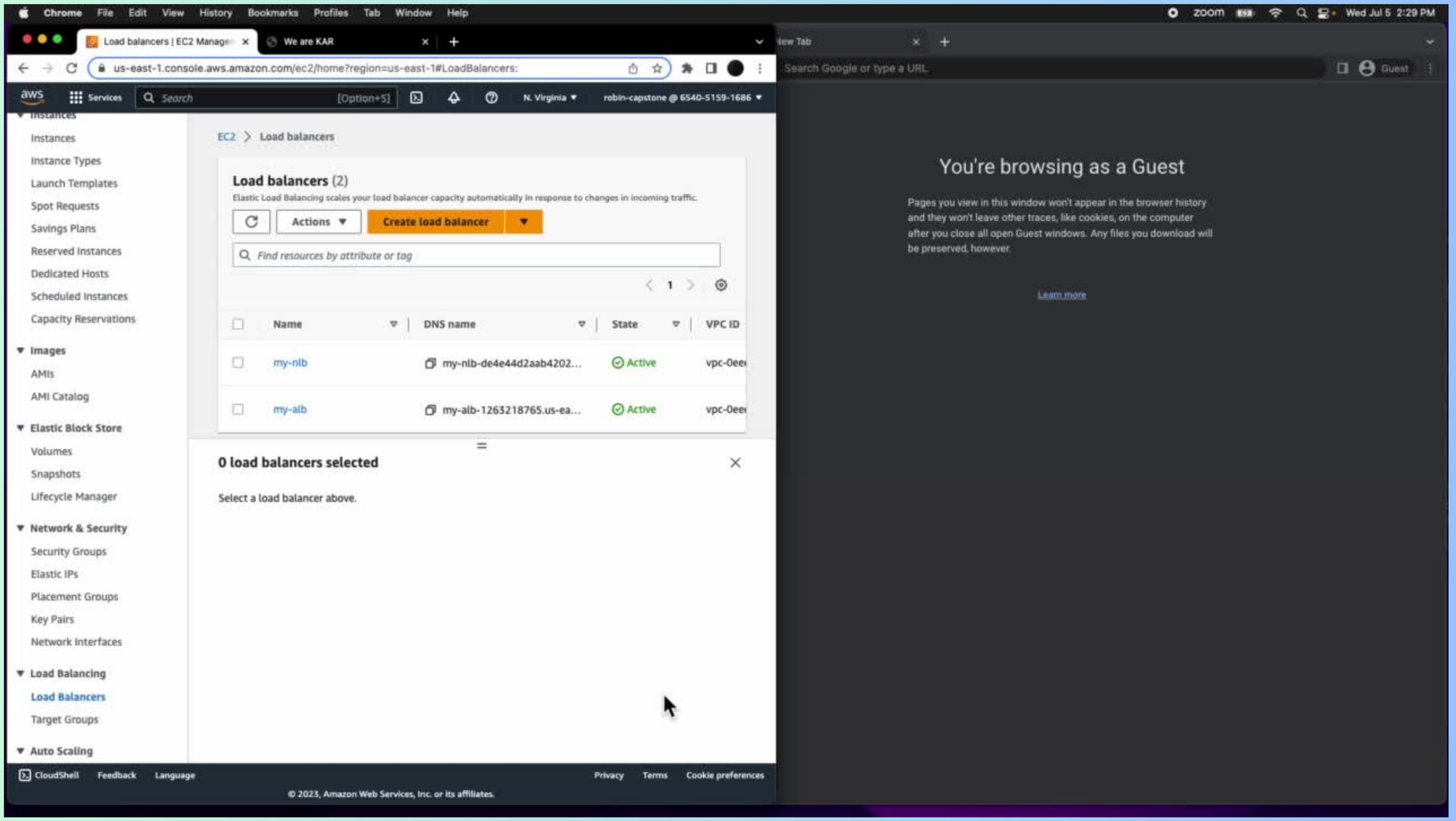

| VPC CIDR blocks |
|---|
| Production: 172.20.0.0/20 |
| Non-prod: 172.12.0.0/20 |
| On-prem: 172.16.1.0/20 |

Production environment

Non-Production environment

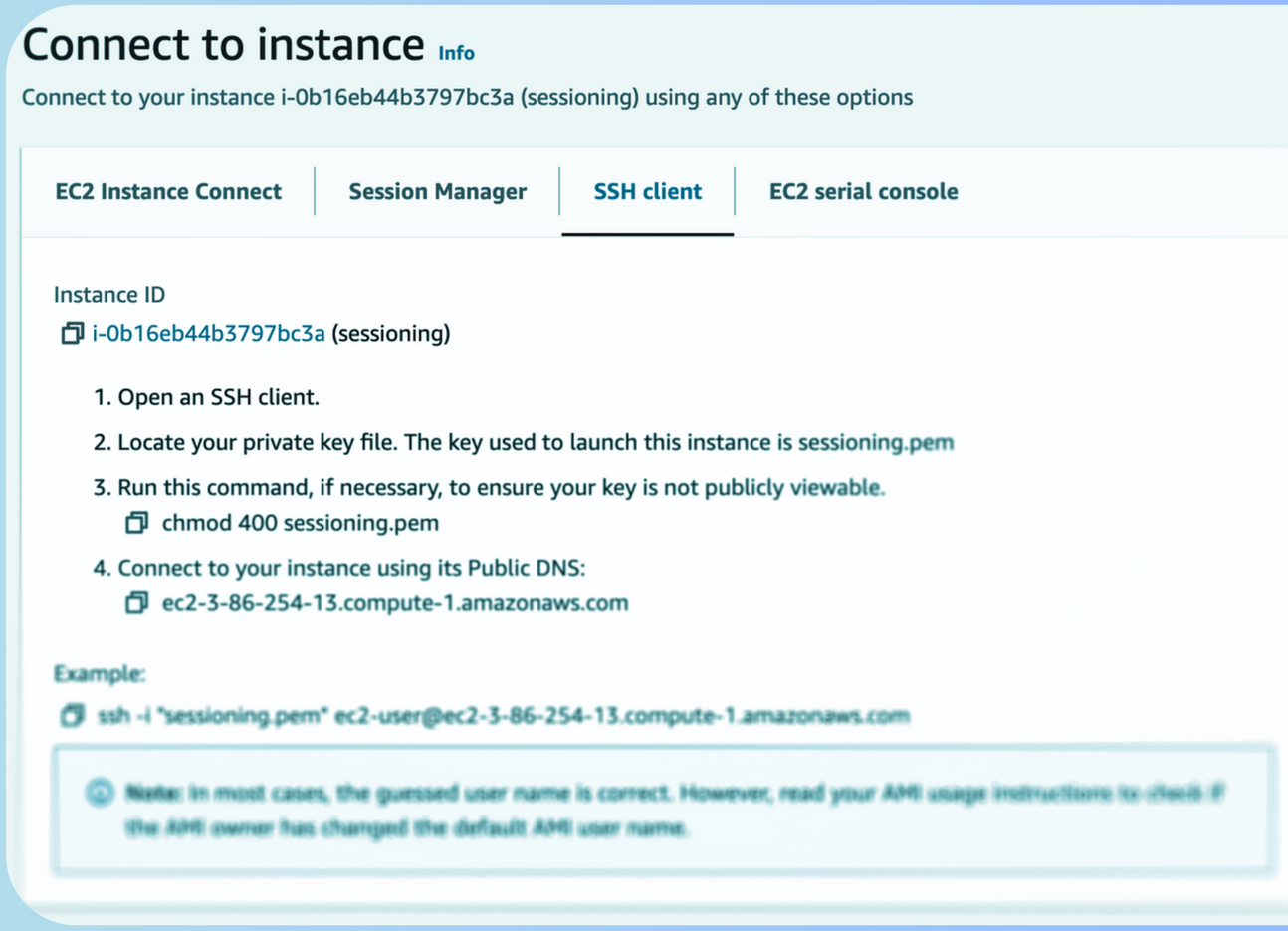
Simulated on-prem

Transit Gateway connectivity


Chrome File Edit View History Bookmarks Profiles Tab Window Help
Wed Jul 5 2:29 PM
Load balancers | EC2 Manage
We are KAR
us-east-1.console.aws.amazon.com/ec2/home?region=us-east-1#LoadBalancers:
Search Google or type a URL
Guest
aws
Services
Search
[Option+S]
N. Virginia
robin-capstone @ 6540-5159-1686
Instances
Instance Types
Launch Templates
Spot Requests
Savings Plans
Reserved Instances
Dedicated Hosts
Scheduled Instances
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
Auto Scaling
EC2 > Load balancers
Load balancers (2)
Elastic Load Balancing scales your load balancer capacity automatically in response to changes in incoming traffic.
Actions
Create load balancer
Find resources by attribute or tag
Name
DNS name
State
VPC ID
my-nlb
my-nlb-de4e44d2aab4202...
Active
my-alb
my-alb-1263218765.us-ea...
Active
0 load balancers selected
Select a load balancer above.
CloudShell
Feedback
Language
Privacy
Terms
Cookie preferences
© 2023, Amazon Web Services, Inc. or its affiliates.
You're browsing as a Guest
Pages you view in this window won't appear in the browser history and they won't leave other traces, like cookies, on the computer after you close all open Guest windows. Any files you download will be preserved, however.
Learn more

# 5.SSH vs SSM

AWS service used to access our on-premises environment securely.




Advantages:

- Starting with Security
- Centralized Access Control
- Auditing and Logging


# 6.Zero Trust

**Guiding security principle that assumes no inherent trust.**

**Pillars:**

- **Least privilege**
- **Assuming breach**
- **Always verify**

AWS Network Manager

- Connectivity
  - Global Networks
  - Settings
  - Shared by me
    - Attachments
    - Peerings
- Monitoring and troubleshooting
  - Reachability Analyzer

Network Manager > Reachability Analyzer

VPC Reachability Analyzer now supports analyses across multiple accounts in your AWS Organization. Learn more

VPC Reachability Analyzer now also supports analyses through Gateway Load Balancers, AWS Network Firewall and AWS PrivateLink, and analyses based on Destination IP address.

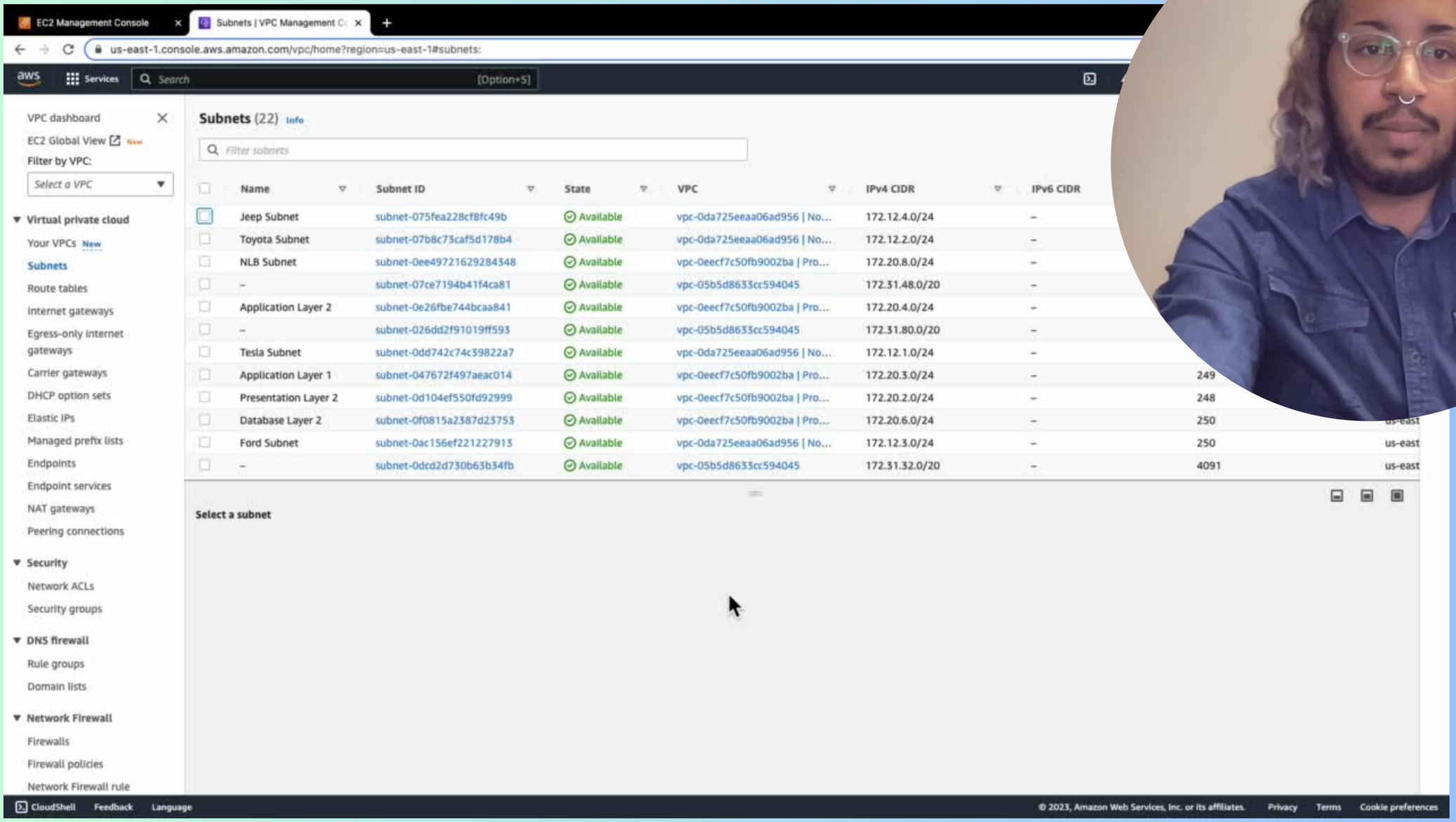
**Paths** (3) Info

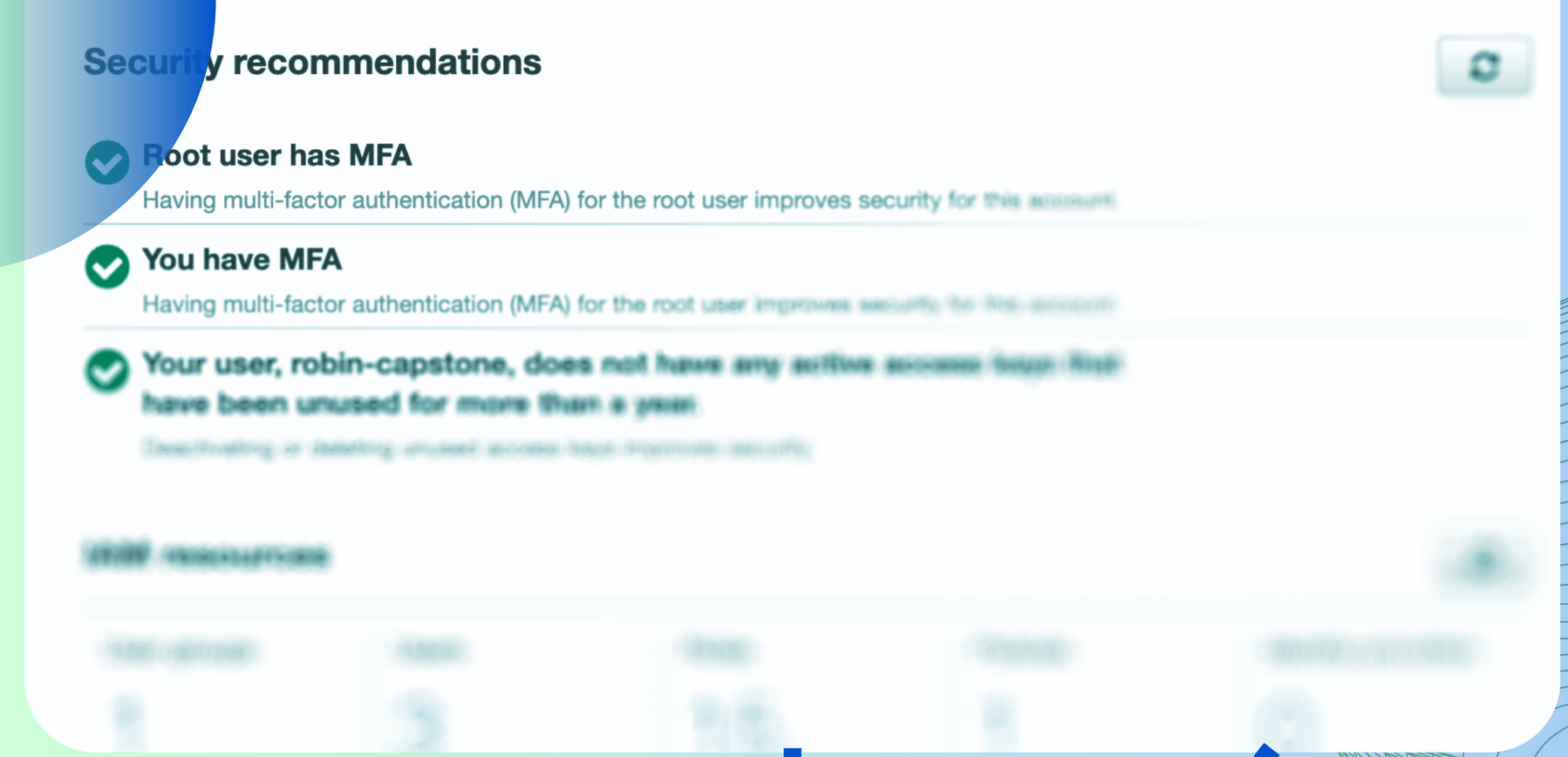
Actions | Create and analyze path

Filter paths

1

| Name | Path ID | Reachability status |
|---|---|---|
| non-prod-to-prod | nip-05dc8144af270af01 | Not reachable |
| on-prod-to-prod | nip-0fcf1413806f30c2a | Reachable |
| non-prod to on-prem | nip-019c4fe599c5db0b5 | Reachable |


EC2 Management Console
Subnets | VPC Management C
us-east-1.console.aws.amazon.com/vpc/home?region=us-east-1#subnets:
aws
Services
Search
[Option+S]
VPC dashboard
EC2 Global View
New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
Carrier gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Firewall policies
Network Firewall rule
Subnets (22) Info
Filter subnets
Name
Subnet ID
State
VPC
IPv4 CIDR
IPv6 CIDR
Jeep Subnet subnet-075fea228cf8fc49b Available vpc-0da725eeaa06ad956 | No... 172.12.4.0/24 –
Toyota Subnet subnet-07b8c73caf5d178b4 Available vpc-0da725eeaa06ad956 | No... 172.12.2.0/24 –
NLB Subnet subnet-0ee49721629284348 Available vpc-0eecf7c50fb9002ba | Pro... 172.20.8.0/24 –
– subnet-07ce7194b41f4ca81 Available vpc-05b5d8633cc594045 172.31.48.0/20 –
Application Layer 2 subnet-0e26fbe744bcaa841 Available vpc-0eecf7c50fb9002ba | Pro... 172.20.4.0/24 –
– subnet-026dd2f91019ff593 Available vpc-05b5d8633cc594045 172.31.80.0/20 –
Tesla Subnet subnet-0dd742c74c39822a7 Available vpc-0da725eeaa06ad956 | No... 172.12.1.0/24 –
Application Layer 1 subnet-047672f497aeac014 Available vpc-0eecf7c50fb9002ba | Pro... 172.20.3.0/24 – 249
Presentation Layer 2 subnet-0d104ef550fd92999 Available vpc-0eecf7c50fb9002ba | Pro... 172.20.2.0/24 – 248
Database Layer 2 subnet-0f0815a2387d23753 Available vpc-0eecf7c50fb9002ba | Pro... 172.20.6.0/24 – 250
Ford Subnet subnet-0ac156ef221227913 Available vpc-0da725eeaa06ad956 | No... 172.12.3.0/24 – 250 us-east
– subnet-0dcd2d730b63b34fb Available vpc-05b5d8633cc594045 172.31.32.0/20 – 4091 us-east
Select a subnet
CloudShell
Feedback
Language
© 2023, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences




# 7.MFA and Securing the Root

Minimal use of the root account

DUO mobile MFA app


# 7.MFA and Securing the Root

IAM > Users

## Users (10) Info

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

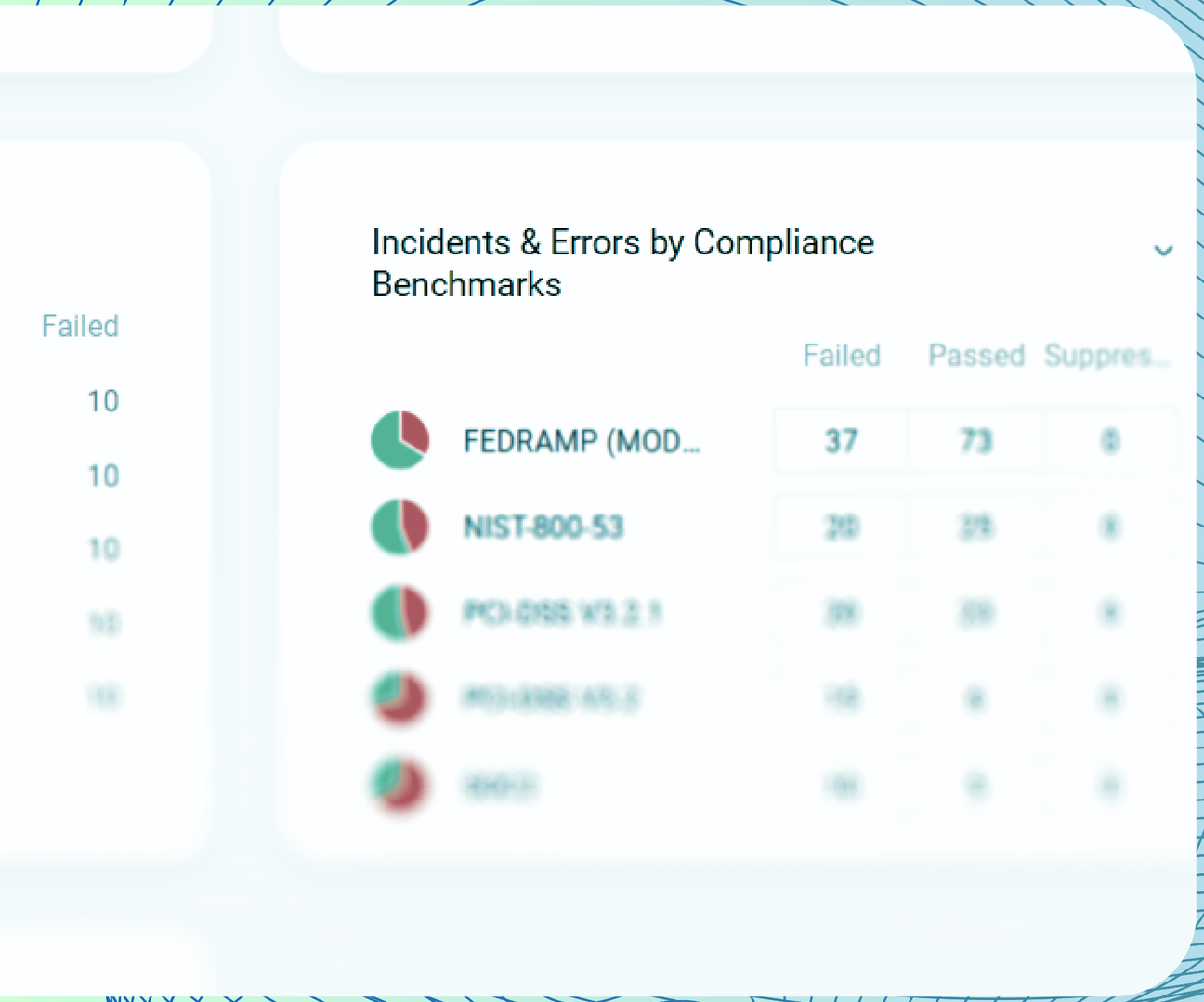
| User name | Path | Groups | Last activity | Password | |
|---|---|---|---|---|---|
| adeel_awan | / | admins | 29 days ago | 29 days ag | |
| Database_access | / | Database_admin | Never | None | |
| Ford_driver | / | Non-prod-users | Never | None | - |
| Honda_driver | / | Non-prod-users | Never | None | - |
| Jeep_driver | / | Non-prod-users | Never | None | - |
| keegan_dasilva_barbosa | / | admins | 29 days ago | 29 days ago | - |
| Network_admin | / | Network_admin | Never | None | - |
| robin_gaudreau | / | admins | 12 minutes ago | 29 days ago | 18 days ago |
| Tesla_driver | / | Non-prod-users | Never | None | - |
| Toyota_driver | / | Non-prod-users | Never | None | - |

# 9.Jump Server: Theoretical Concerns

Project restriction

Access to private data through public IP

Not compatible with Zero Trust



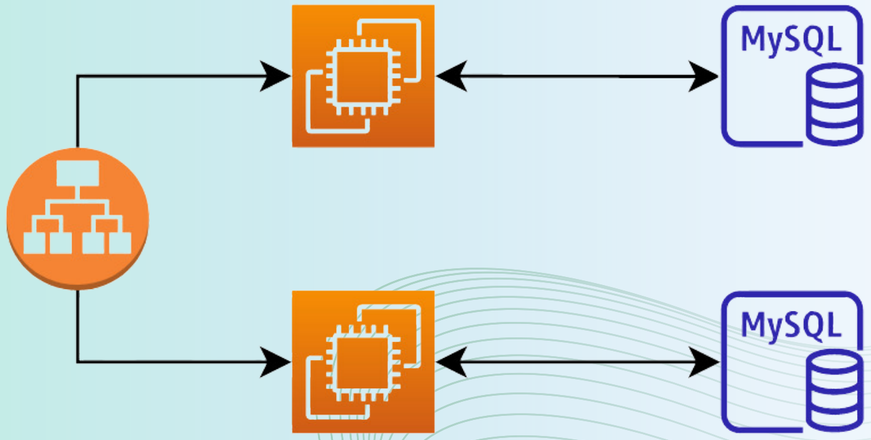

# IO. Assessing Vulnerabilities

Tenable VM Scans

AWS Config and Inspector

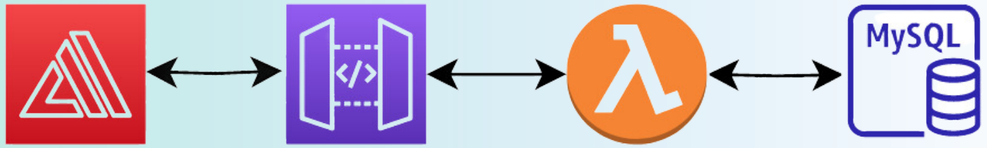
Bridgecrew

# Possible Solutions



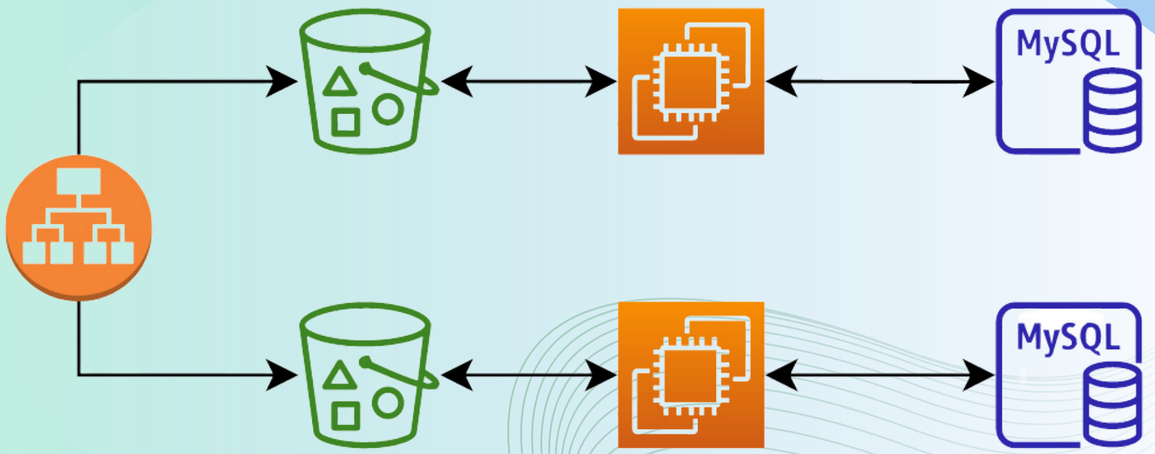

Reverse Proxy

# Possible Solutions




Going Serverless

# Possible Solutions




Static on Buckets

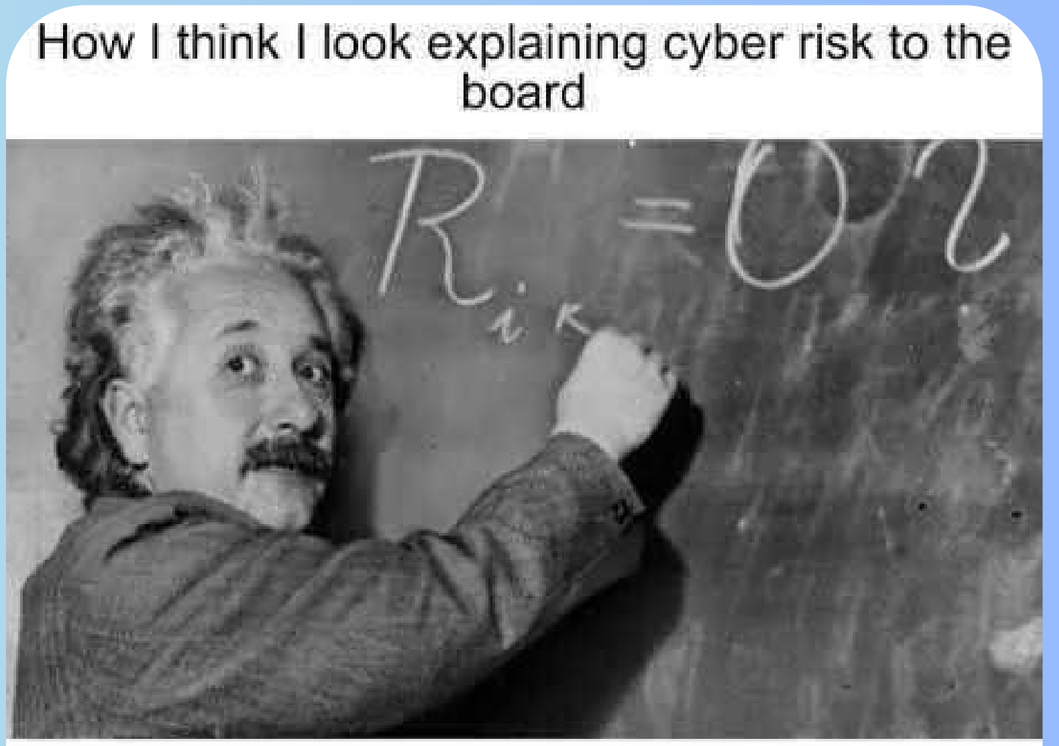
# Thank you

Keegan

Adeel

Robin

Scan this code to download our full report.




Some images within were created using Canva AI, and are included for aesthetic purposes only.