AWS re:Invent

NOV. 28 – DEC. 2, 2022 | LAS VEGAS, NV

NET307-R

Become a network support expert: We break it, you fix it

Jesper Eneberg (he/him)

Global Solution Architect
Amazon Web Services

Maks Khomutskyi (he/him)

Sr. Enterprise Solution Architect
Amazon Web Services

NET307-R AWS team

Saptarshi Moitra

Abhishek Dey

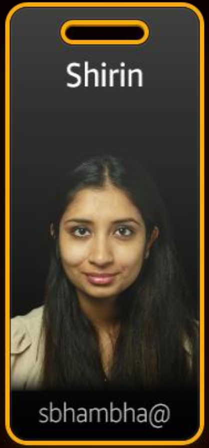
Saransh Burman

Slawek Balcerzak

Maks Khomutskyi

Jeff Klopfenstein

Victor Babasanmi



Shirin Bhambhani

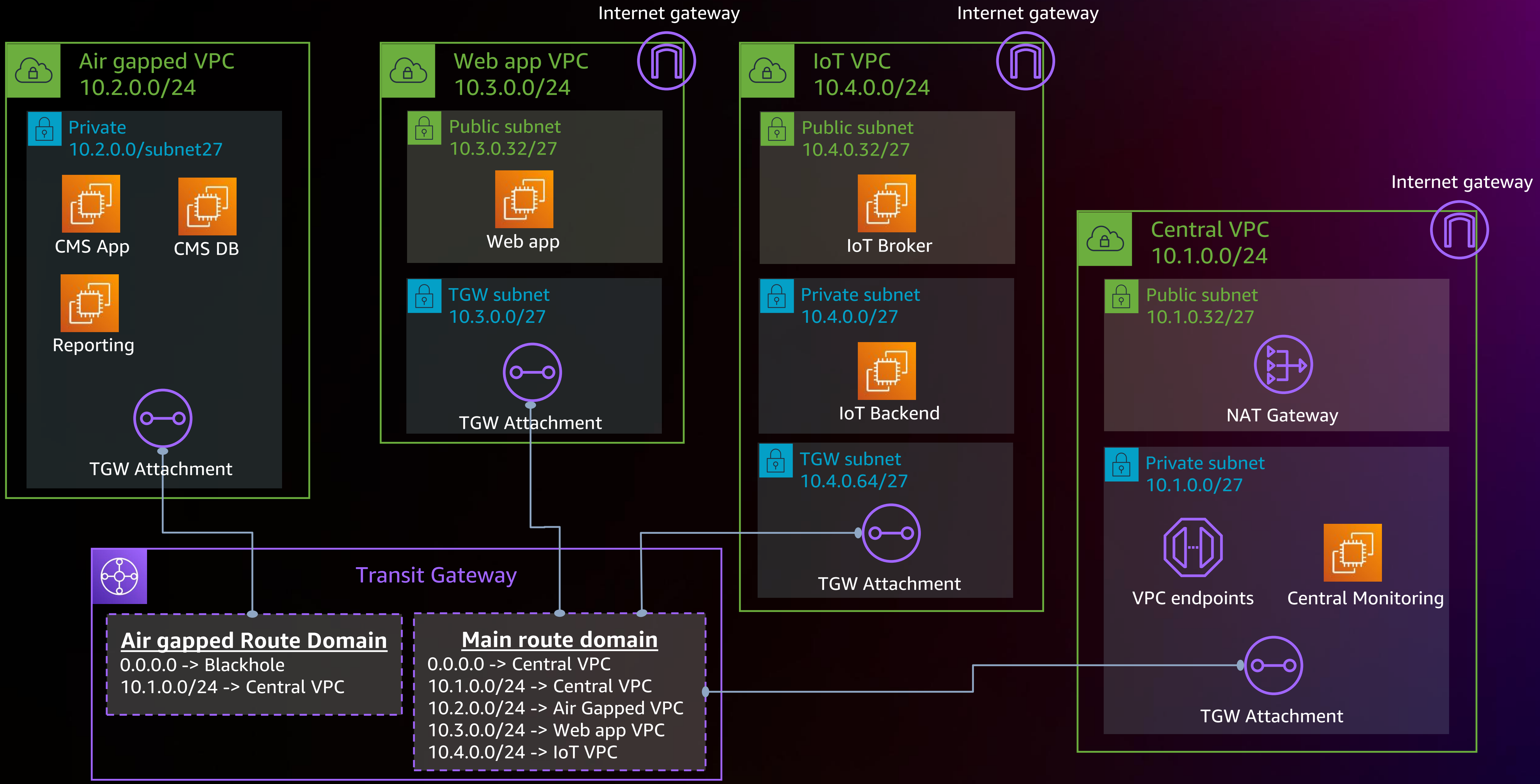
Jesper Eneberg

Sushma Nagaraj

Agenda

- What are we playing with? (Overview of the environment and services)
- How are we playing with it? (Introduction to the labs)
- Alright, so how do I get started? (Access the workshop environment)
- Fix the environment!

Lab environment



Air gapped VPC
10.2.0.0/24

Private
10.2.0.0/subnet27

CMS App

CMS DB

Reporting

TGW Attachment

Internet gateway

Web app VPC
10.3.0.0/24

Public subnet
10.3.0.32/27

Web app

TGW subnet
10.3.0.0/27

TGW Attachment

Internet gateway

IoT VPC
10.4.0.0/24

Public subnet
10.4.0.32/27

IoT Broker

Private subnet
10.4.0.0/27

IoT Backend

TGW subnet
10.4.0.64/27

TGW Attachment

Internet gateway

Central VPC
10.1.0.0/24

Public subnet
10.1.0.32/27

NAT Gateway

Private subnet
10.1.0.0/27

VPC endpoints

Central Monitoring

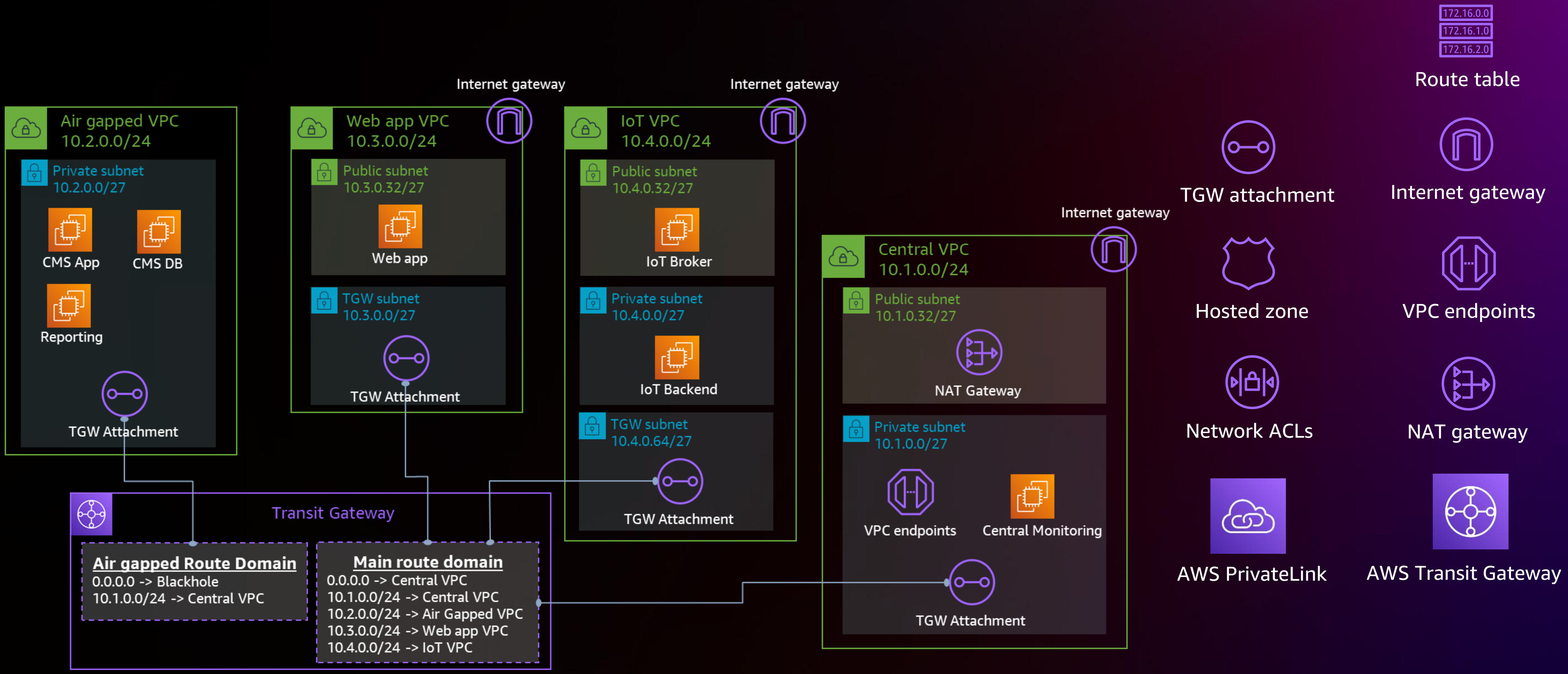
TGW Attachment

Transit Gateway

Air gapped Route Domain
0.0.0.0 -> Blackhole
10.1.0.0/24 -> Central VPC

Main route domain
0.0.0.0 -> Central VPC
10.1.0.0/24 -> Central VPC
10.2.0.0/24 -> Air Gapped VPC
10.3.0.0/24 -> Web app VPC
10.4.0.0/24 -> IoT VPC

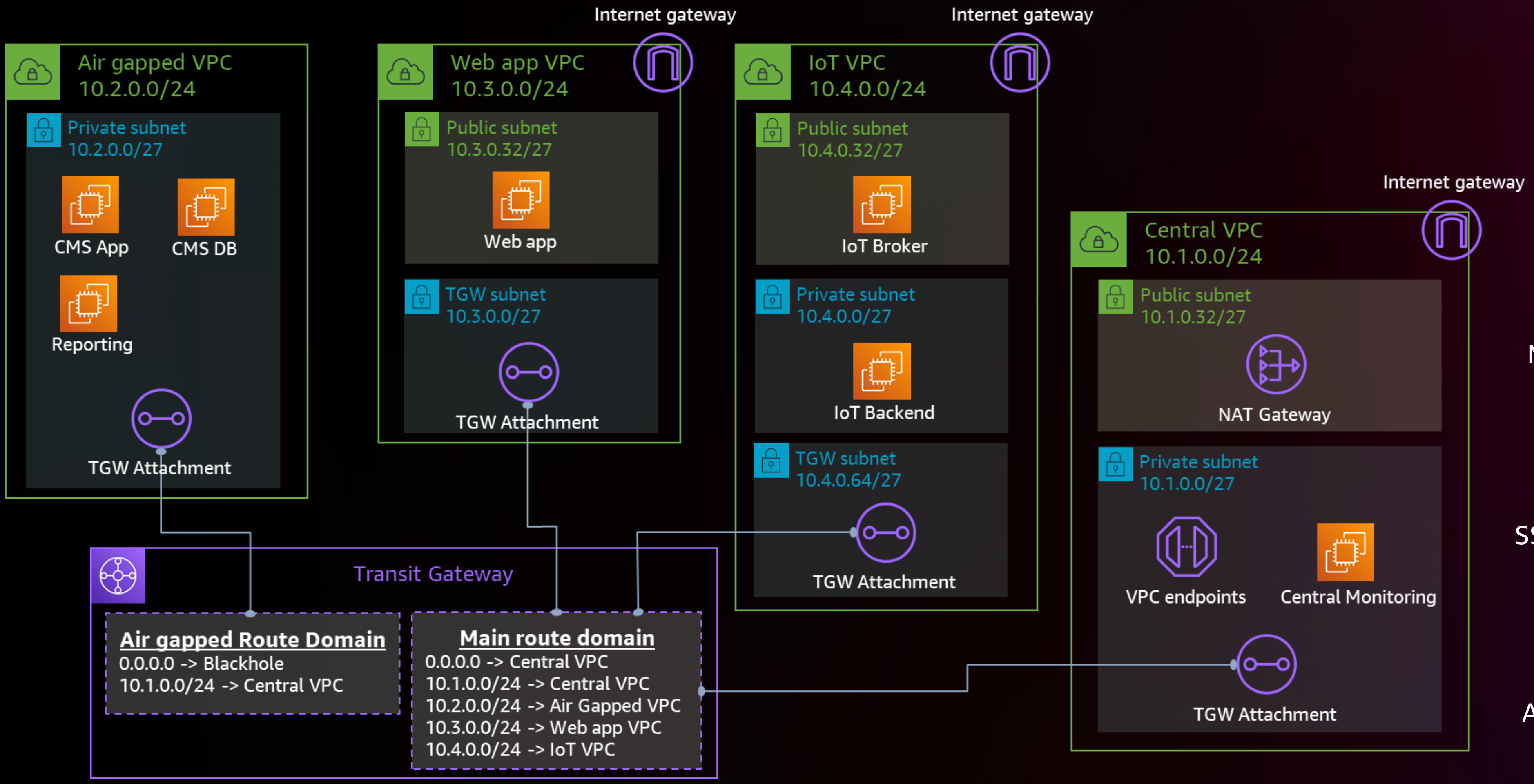
Lab environment – Issues



Air gapped Route Domain
0.0.0.0 -> Blackhole
10.1.0.0/24 -> Central VPC

Main route domain
0.0.0.0 -> Central VPC
10.1.0.0/24 -> Central VPC
10.2.0.0/24 -> Air Gapped VPC
10.3.0.0/24 -> Web app VPC
10.4.0.0/24 -> IoT VPC

Lab environment – Troubleshooting



Internet gateway

Internet gateway

Internet gateway

Air gapped VPC
10.2.0.0/24

Private subnet
10.2.0.0/27

CMS App

CMS DB

Reporting

TGW Attachment

Web app VPC
10.3.0.0/24

Public subnet
10.3.0.32/27

Web app

TGW subnet
10.3.0.0/27

TGW Attachment

IoT VPC
10.4.0.0/24

Public subnet
10.4.0.32/27

IoT Broker

Private subnet
10.4.0.0/27

IoT Backend

TGW subnet
10.4.0.64/27

TGW Attachment

Central VPC
10.1.0.0/24

Public subnet
10.1.0.32/27

NAT Gateway

Private subnet
10.1.0.0/27

VPC endpoints

Central Monitoring

TGW Attachment

Transit Gateway

Air gapped Route Domain
0.0.0.0 -> Blackhole
10.1.0.0/24 -> Central VPC

Main route domain
0.0.0.0 -> Central VPC
10.1.0.0/24 -> Central VPC
10.2.0.0/24 -> Air Gapped VPC
10.3.0.0/24 -> Web app VPC
10.4.0.0/24 -> IoT VPC

Instance logs

VPC Network Access Analyzer

AWS Systems Manager (SSM) Run Command

VPC Reachability Analyzer

SSM Session Manager

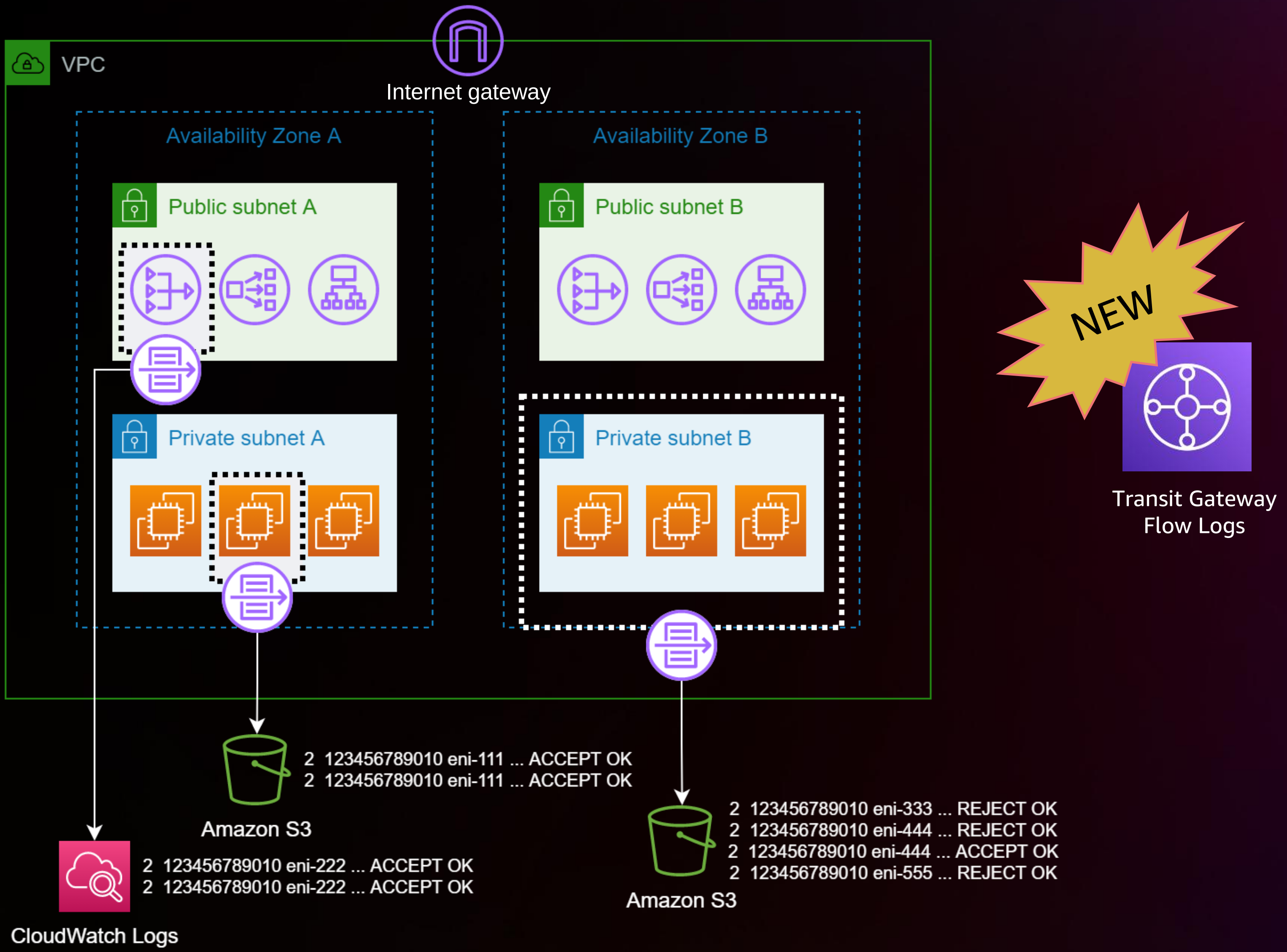
VPC and TGW flow logs

Amazon Inspector

Resolver query logging

VPC troubleshooting

FLOW LOGS



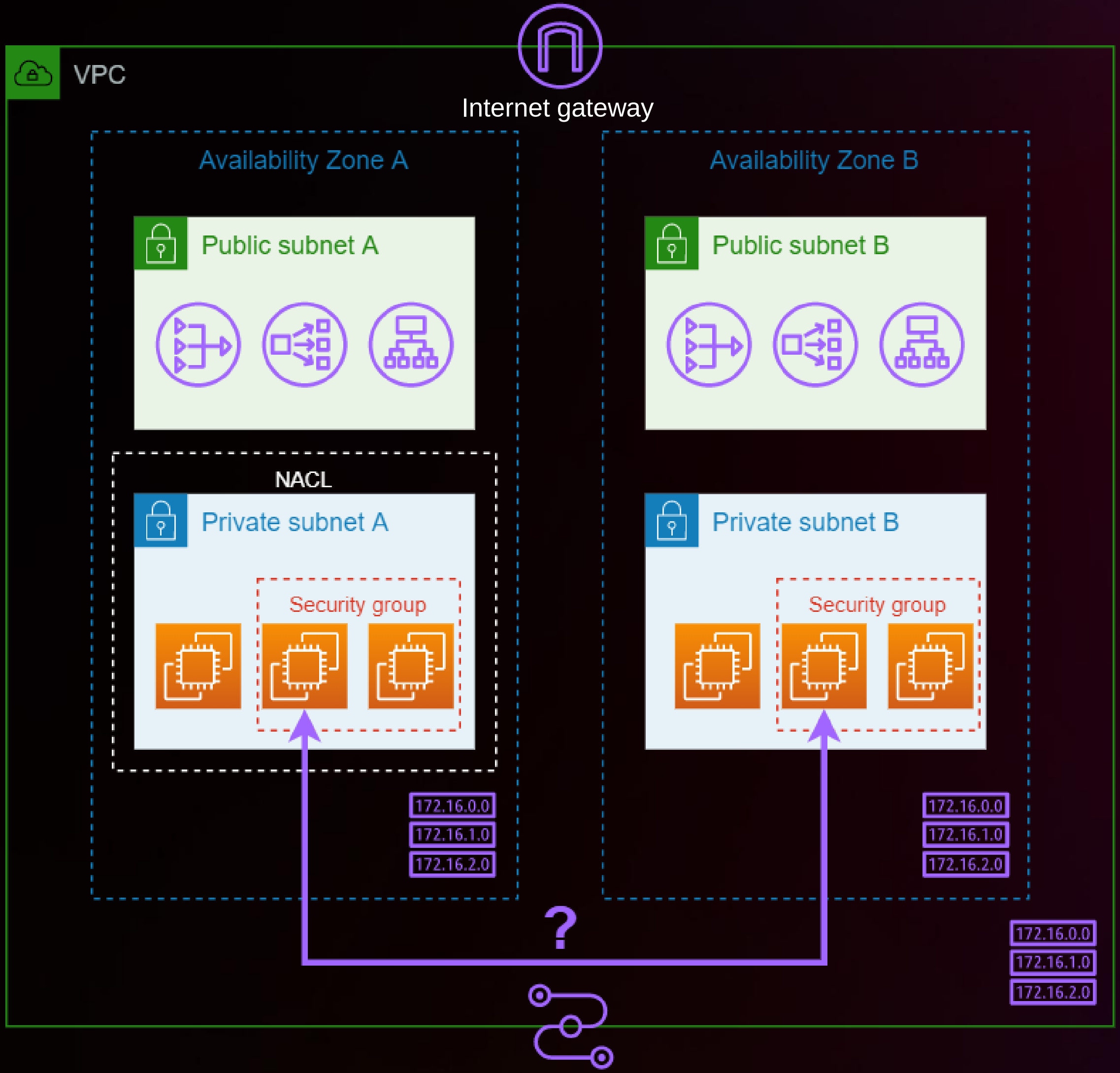
```
2  123456789010 eni-111 ... ACCEPT OK
2  123456789010 eni-111 ... ACCEPT OK
```

```
2  123456789010 eni-222 ... ACCEPT OK
2  123456789010 eni-222 ... ACCEPT OK
```

```
2  123456789010 eni-333 ... REJECT OK
2  123456789010 eni-444 ... REJECT OK
2  123456789010 eni-444 ... ACCEPT OK
2  123456789010 eni-555 ... REJECT OK
```

VPC troubleshooting

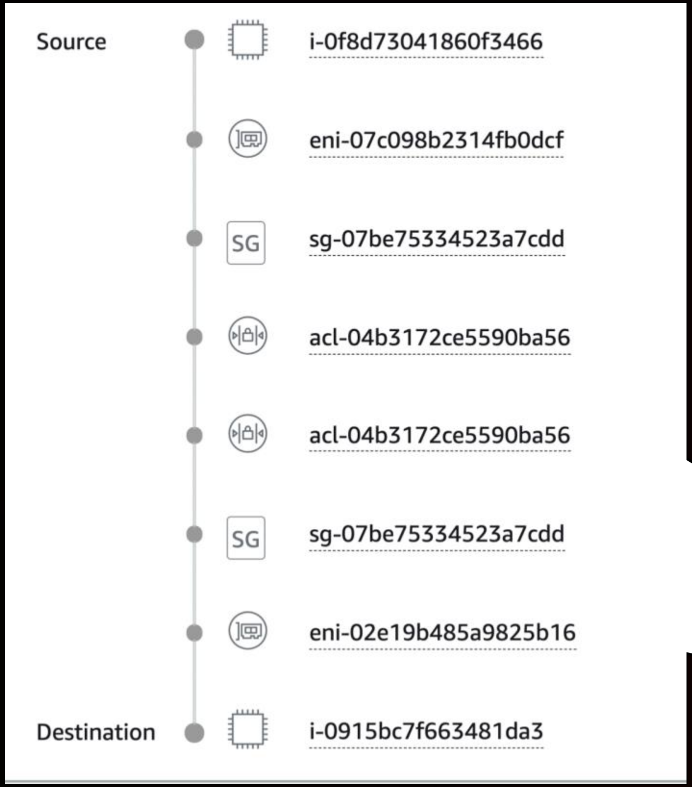
VPC REACHABILITY ANALYZER



VPC troubleshooting

VPC REACHABILITY ANALYZER

Network diagnostics tool that troubleshoots reachability between two endpoints in a VPC or within multiple VPCs



Source i-0f8d73041860f3466

eni-07c098b2314fb0dcf

SG sg-07be75334523a7cdd

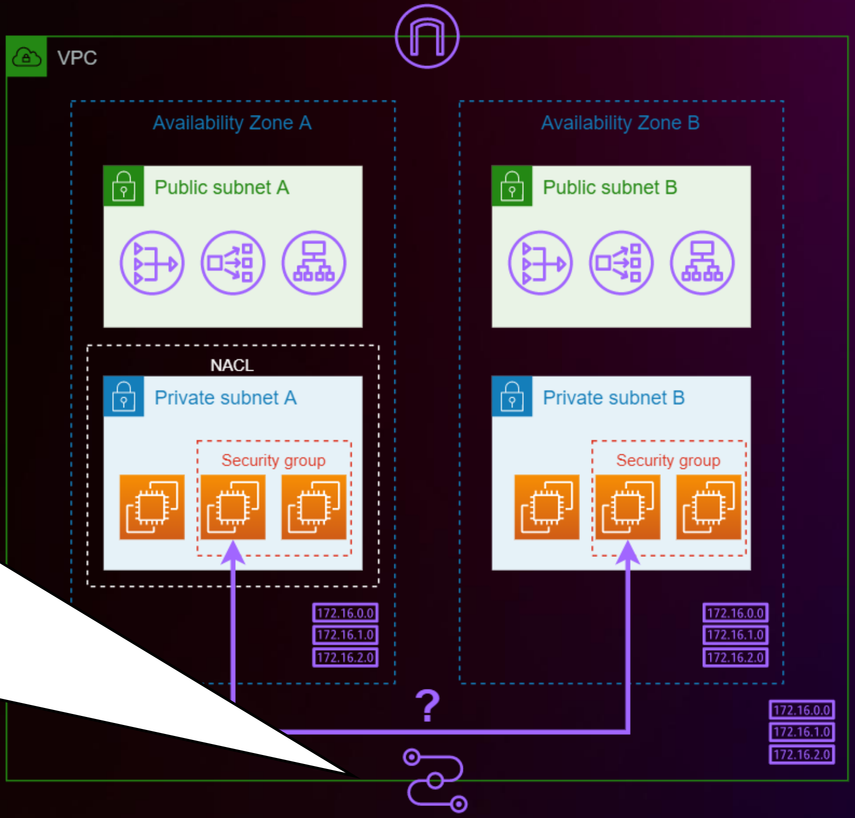
acl-04b3172ce5590ba56

acl-04b3172ce5590ba56

SG sg-07be75334523a7cdd

eni-02e19b485a9825b16

Destination i-0915bc7f663481da3

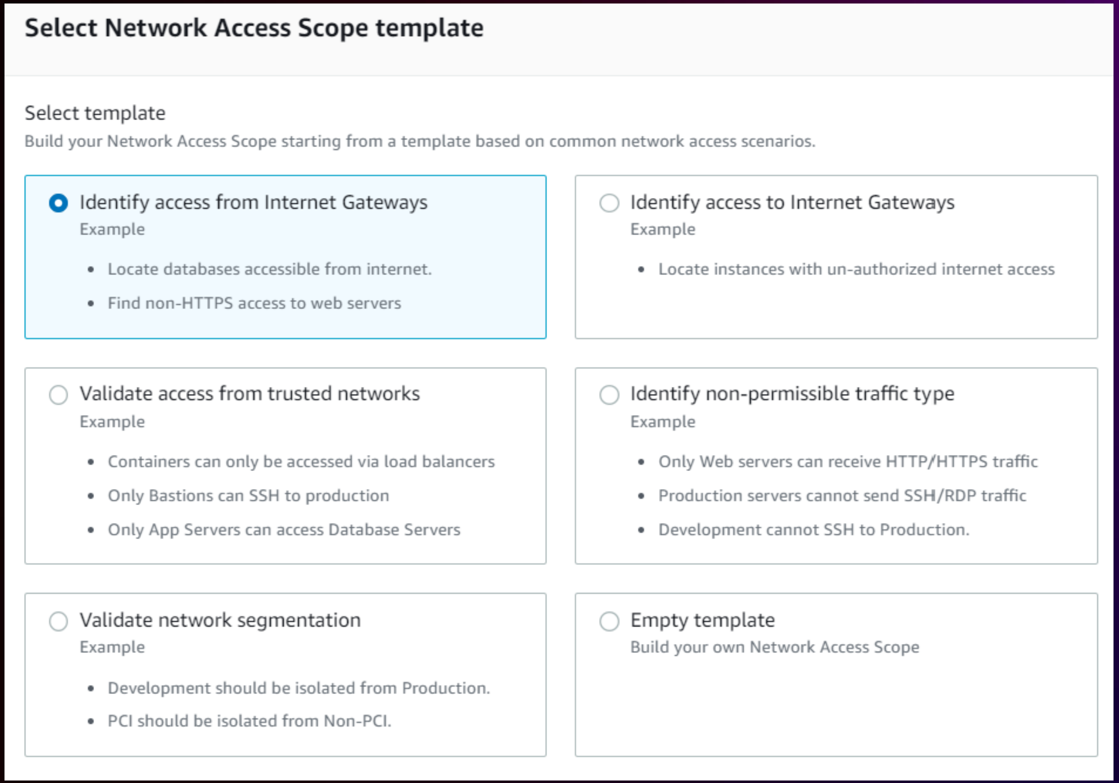


VPC troubleshooting

VPC NETWORK ACCESS ANALYZER

VPC Network Access Analyzer is a feature that identifies unintended network access to your resources on AWS

- Understand, verify, and improve your network security posture
- Demonstrate compliance
- Verify your network security posture



Select Network Access Scope template

Select template

Build your Network Access Scope starting from a template based on common network access scenarios.

● Identify access from Internet Gateways
Example
- Locate databases accessible from internet.
- Find non-HTTPS access to web servers

○ Identify access to Internet Gateways
Example
- Locate instances with un-authorized internet access

○ Validate access from trusted networks
Example
- Containers can only be accessed via load balancers
- Only Bastions can SSH to production
- Only App Servers can access Database Servers

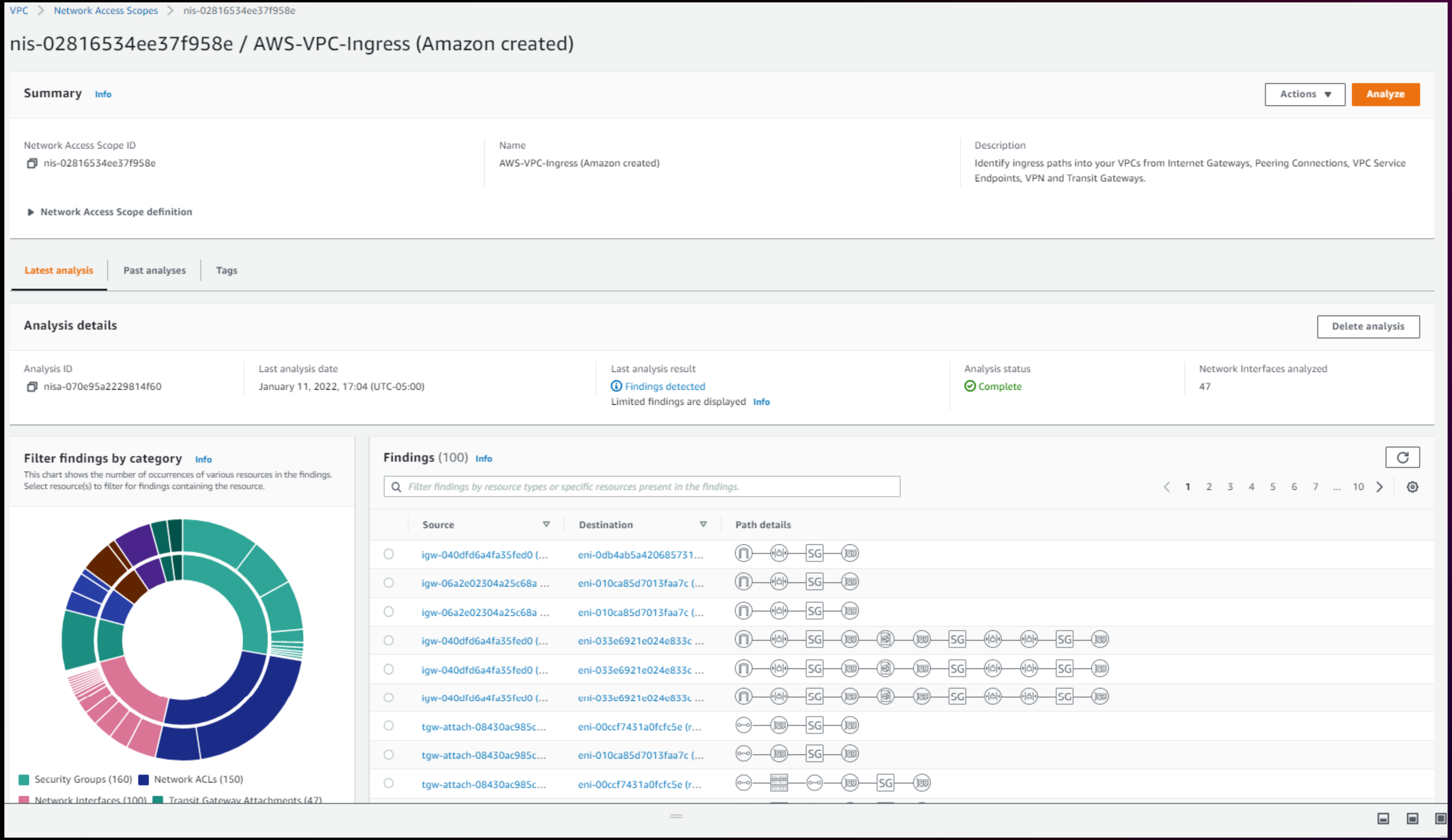
○ Identify non-permissible traffic type
Example
- Only Web servers can receive HTTP/HTTPS traffic
- Production servers cannot send SSH/RDP traffic
- Development cannot SSH to Production.

○ Validate network segmentation
Example
- Development should be isolated from Production.
- PCI should be isolated from Non-PCI.

○ Empty template
Build your own Network Access Scope

VPC troubleshooting

VPC NETWORK ACCESS ANALYZER



VPC > Network Access Scopes > nis-02816534ee37f958e

nis-02816534ee37f958e / AWS-VPC-Ingress (Amazon created)

Summary Info

Actions ▼ | Analyze

Network Access Scope ID	Name	Description
nis-02816534ee37f958e	AWS-VPC-Ingress (Amazon created)	Identify ingress paths into your VPCs from Internet Gateways, Peering Connections, VPC Service Endpoints, VPN and Transit Gateways.

▶ Network Access Scope definition

Latest analysis | Past analyses | Tags

Analysis details

Delete analysis

Analysis ID	Last analysis date	Last analysis result	Analysis status	Network Interfaces analyzed
nisa-070e95a2229814f60	January 11, 2022, 17:04 (UTC-05:00)	Findings detected Limited findings are displayed Info	✓ Complete	47

Filter findings by category Info

This chart shows the number of occurrences of various resources in the findings. Select resource(s) to filter for findings containing the resource.

🟩 Security Groups (160) 🟦 Network ACLs (150)
🟥 Network Interfaces (100) 🟩 Transit Gateway Attachments (47)

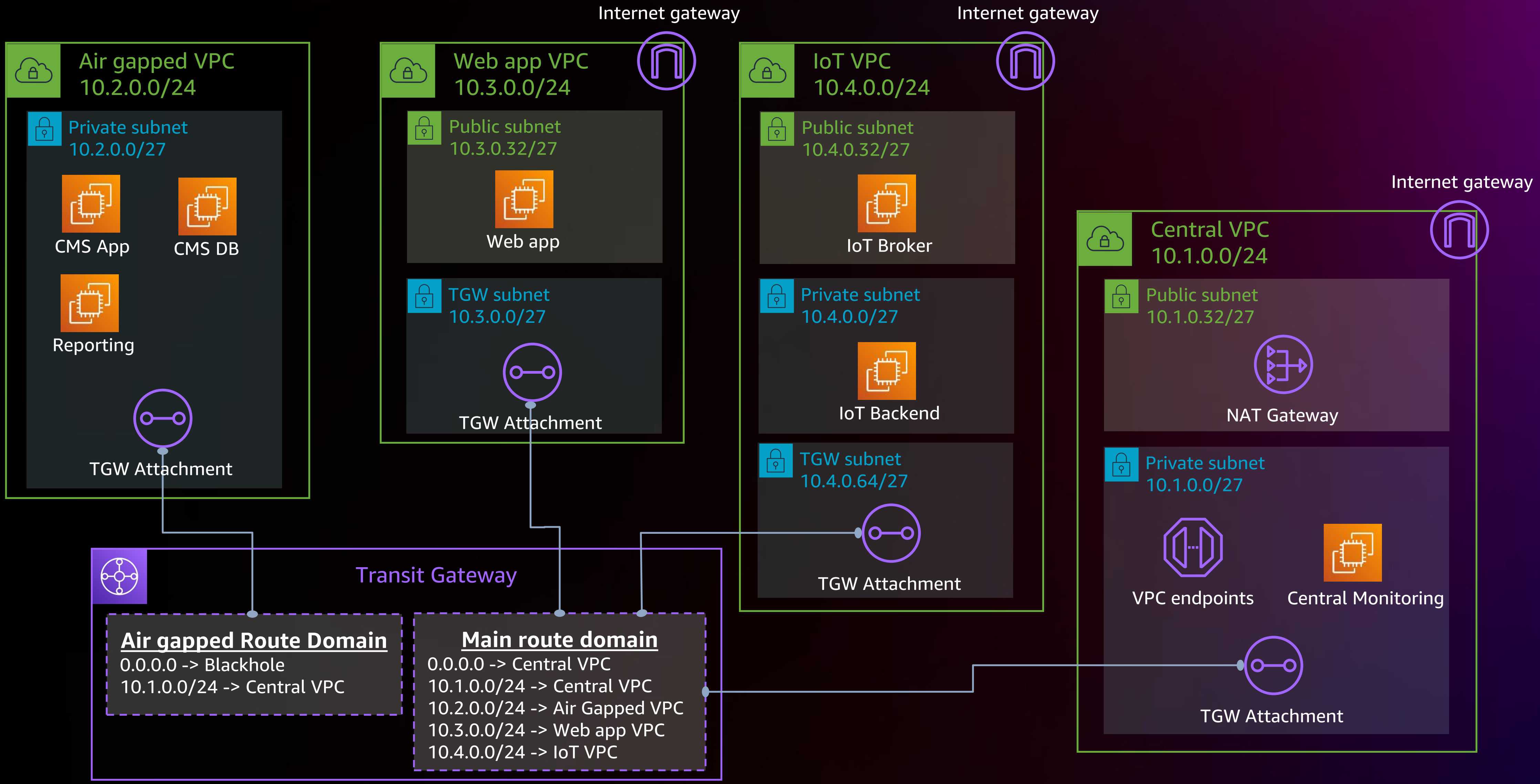
Findings (100) Info

Filter findings by resource types or specific resources present in the findings.

< 1 2 3 4 5 6 7 ... 10 >

	Source	Destination	Path details
○	igw-040dfd6a4fa35fed0 (...	eni-0db4ab5a420685731...	SG
○	igw-06a2e02304a25c68a ...	eni-010ca85d7013faa7c (...	SG
○	igw-06a2e02304a25c68a ...	eni-010ca85d7013faa7c (...	SG
○	igw-040dfd6a4fa35fed0 (...	eni-033e6921e024e833c ...	SG SG SG
○	igw-040dfd6a4fa35fed0 (...	eni-033e6921e024e833c ...	SG SG SG
○	igw-040dfd6a4fa35fed0 (...	eni-033e6921e024e833c ...	SG SG SG
○	tgw-attach-08430ac985c...	eni-00ccf7431a0fcfc5e (r...	SG
○	tgw-attach-08430ac985c...	eni-010ca85d7013faa7c (...	SG
○	tgw-attach-08430ac985c...	eni-00ccf7431a0fcfc5e (r...	SG

Lab environment



Air gapped Route Domain

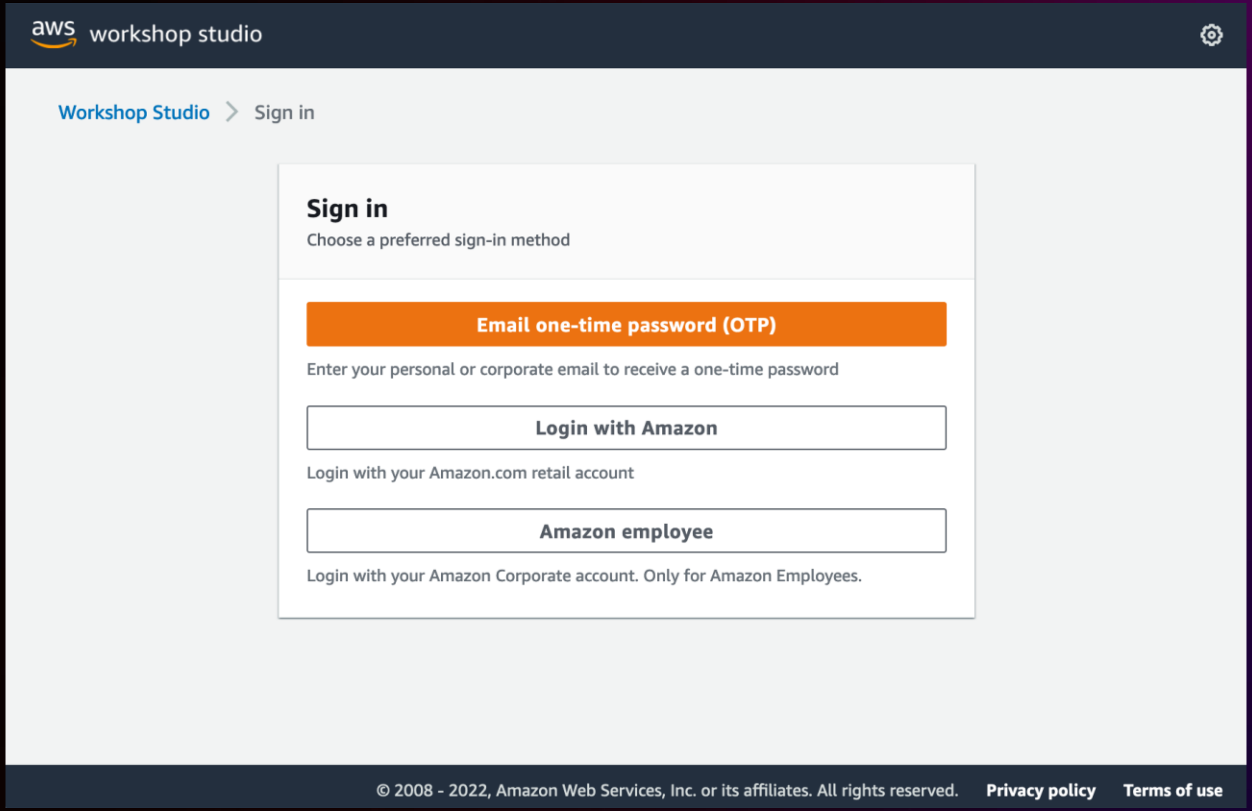
0.0.0.0 -> Blackhole
10.1.0.0/24 -> Central VPC

Main route domain

0.0.0.0 -> Central VPC
10.1.0.0/24 -> Central VPC
10.2.0.0/24 -> Air Gapped VPC
10.3.0.0/24 -> Web app VPC
10.4.0.0/24 -> IoT VPC

Step 1: Sign in via your preferred method

https://s12d.com/NET307-2022



Workshop Studio > Sign in

Sign in

Choose a preferred sign-in method

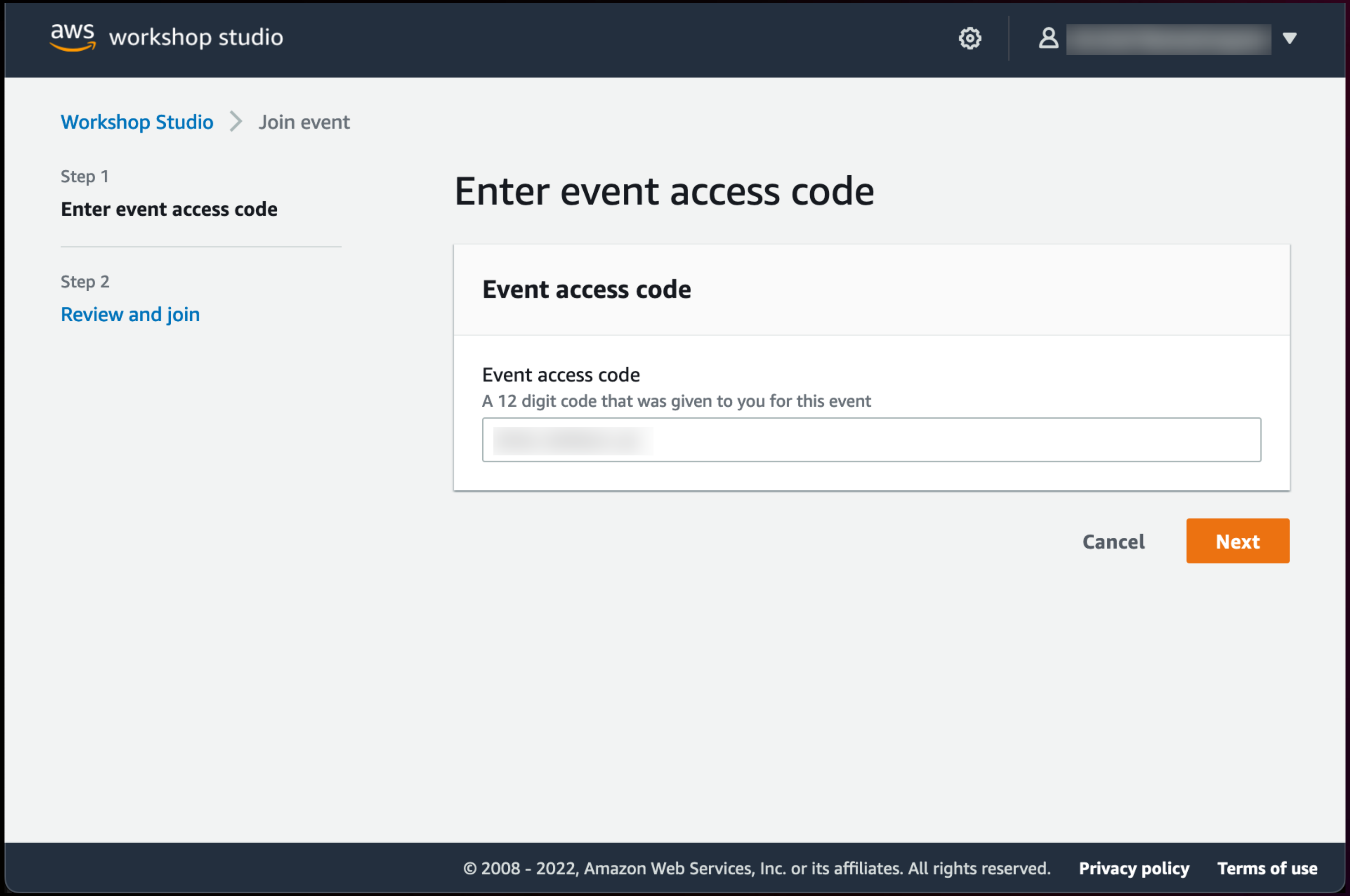
Enter your personal or corporate email to receive a one-time password

Login with your Amazon.com retail account

Login with your Amazon Corporate account. Only for Amazon Employees.

Privacy policy **Terms of use**

Step 2: Enter event access code



Workshop Studio > Join event

Step 1
Enter event access code

Step 2
Review and join

Enter event access code

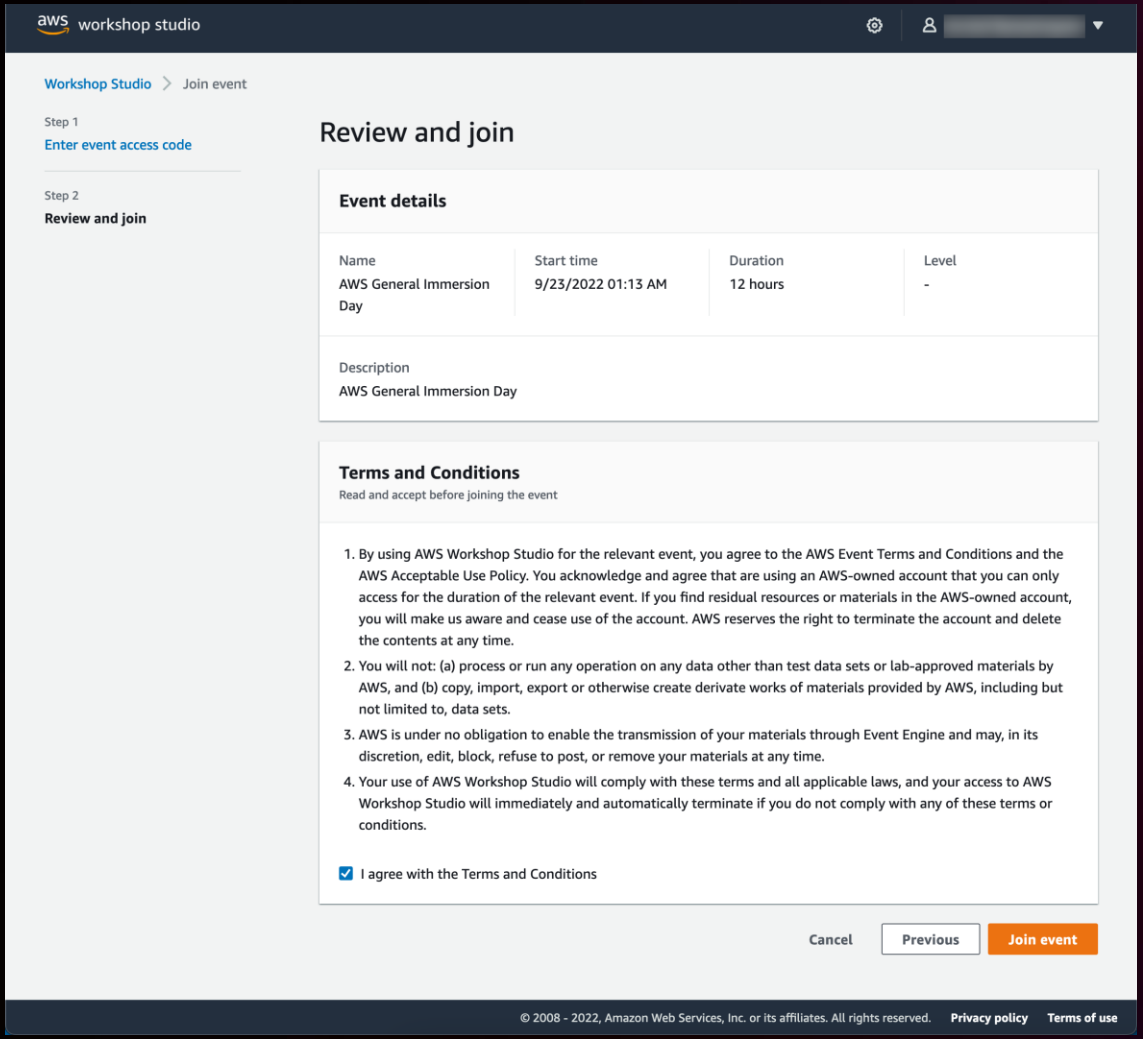
Event access code

Event access code
A 12 digit code that was given to you for this event

[redacted]

Privacy policy **Terms of use**

Step 3: Review terms and join event



Review and join

Event details

Name	Start time	Duration	Level
AWS General Immersion Day	9/23/2022 01:13 AM	12 hours	-

Description
AWS General Immersion Day

Terms and Conditions

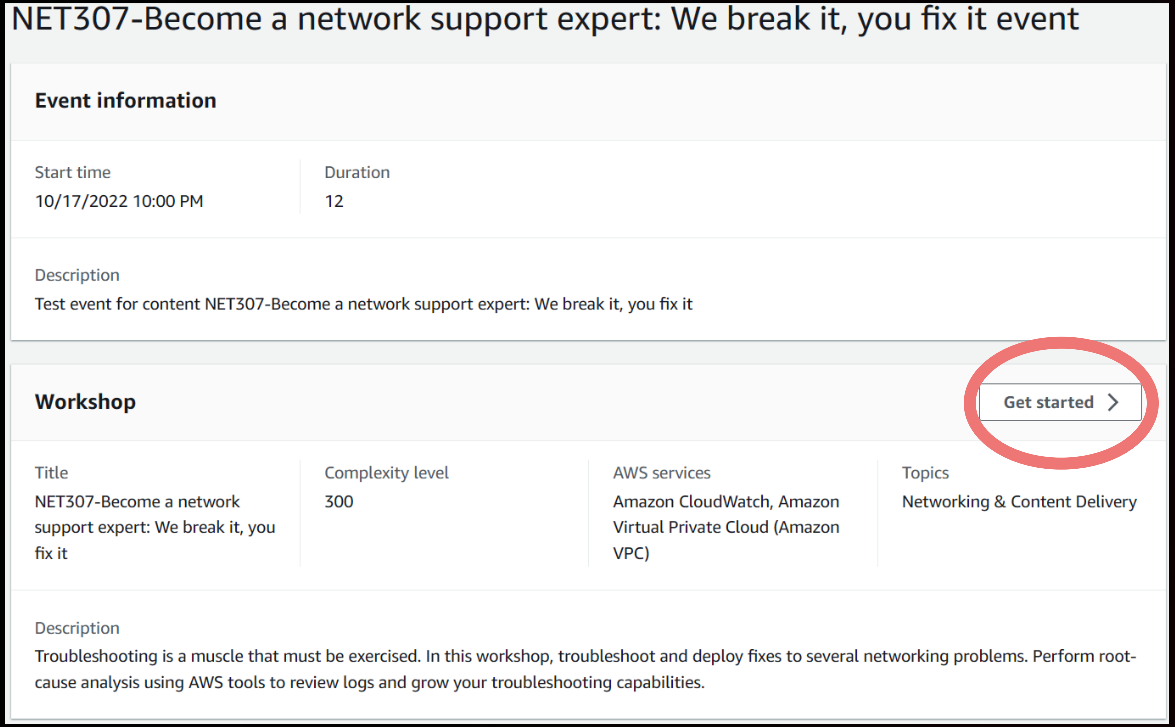
Read and accept before joining the event

1. By using AWS Workshop Studio for the relevant event, you agree to the AWS Event Terms and Conditions and the AWS Acceptable Use Policy. You acknowledge and agree that are using an AWS-owned account that you can only access for the duration of the relevant event. If you find residual resources or materials in the AWS-owned account, you will make us aware and cease use of the account. AWS reserves the right to terminate the account and delete the contents at any time.
2. You will not: (a) process or run any operation on any data other than test data sets or lab-approved materials by AWS, and (b) copy, import, export or otherwise create derivate works of materials provided by AWS, including but not limited to, data sets.
3. AWS is under no obligation to enable the transmission of your materials through Event Engine and may, in its discretion, edit, block, refuse to post, or remove your materials at any time.
4. Your use of AWS Workshop Studio will comply with these terms and all applicable laws, and your access to AWS Workshop Studio will immediately and automatically terminate if you do not comply with any of these terms or conditions.

☑ I agree with the Terms and Conditions

Cancel
Previous
Join event
© 2008 - 2022, Amazon Web Services, Inc. or its affiliates. All rights reserved.
Privacy policy
Terms of use

Step 4: Get started with the workshop



NET307-Become a network support expert: We break it, you fix it event

Event information

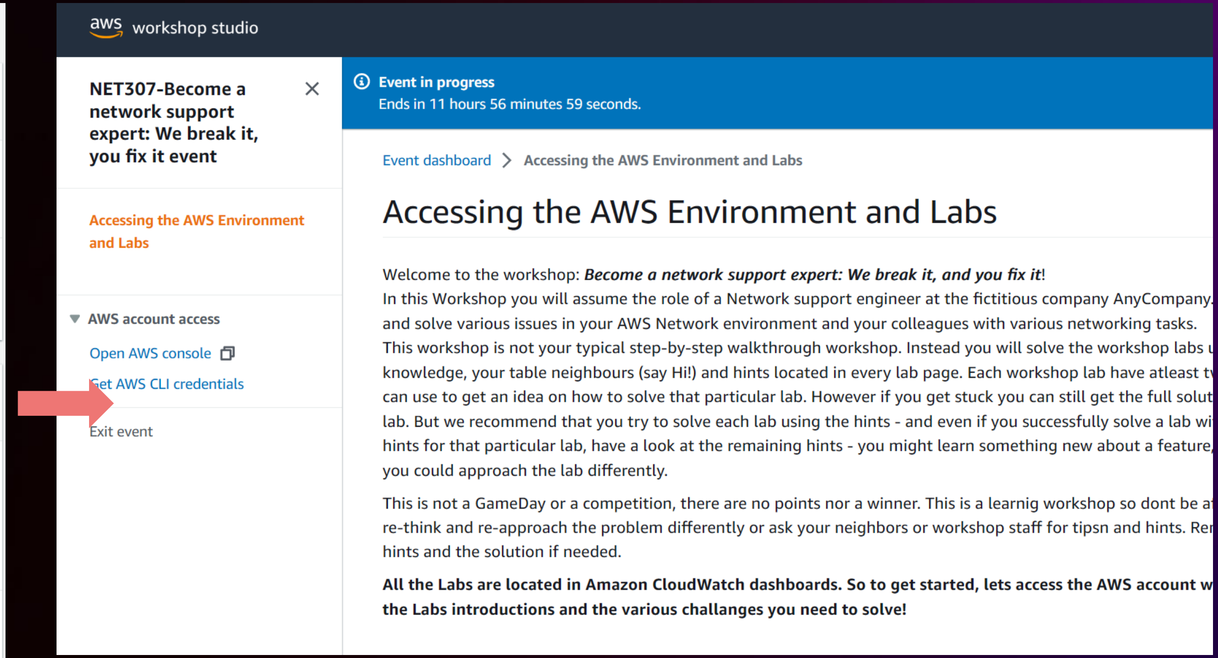
Start time	Duration
10/17/2022 10:00 PM	12

Description
Test event for content NET307-Become a network support expert: We break it, you fix it

Workshop

Title	Complexity level	AWS services	Topics
NET307-Become a network support expert: We break it, you fix it	300	Amazon CloudWatch, Amazon Virtual Private Cloud (Amazon VPC)	Networking & Content Delivery

Description
Troubleshooting is a muscle that must be exercised. In this workshop, troubleshoot and deploy fixes to several networking problems. Perform root-cause analysis using AWS tools to review logs and grow your troubleshooting capabilities.



NET307-Become a network support expert: We break it, you fix it event

Accessing the AWS Environment and Labs
AWS account access
Open AWS console
Get AWS CLI credentials
Exit event

Event in progress
Ends in 11 hours 56 minutes 59 seconds.

Event dashboard > Accessing the AWS Environment and Labs

Accessing the AWS Environment and Labs

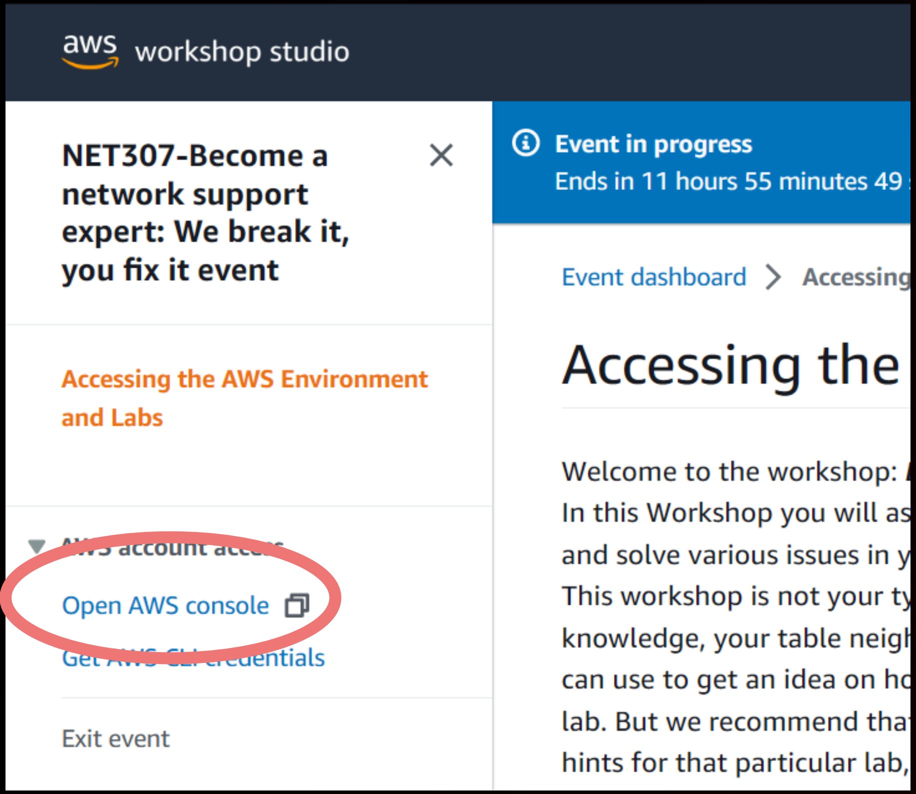
Welcome to the workshop: ***Become a network support expert: We break it, and you fix it***!
In this Workshop you will assume the role of a Network support engineer at the fictitious company AnyCompany. and solve various issues in your AWS Network environment and your colleagues with various networking tasks.
This workshop is not your typical step-by-step walkthrough workshop. Instead you will solve the workshop labs u knowledge, your table neighbours (say Hi!) and hints located in every lab page. Each workshop lab have atleast t can use to get an idea on how to solve that particular lab. However if you get stuck you can still get the full solut lab. But we recommend that you try to solve each lab using the hints - and even if you successfully solve a lab wi hints for that particular lab, have a look at the remaining hints - you might learn something new about a feature, you could approach the lab differently.

This is not a GameDay or a competition, there are no points nor a winner. This is a learnig workshop so dont be a re-think and re-approach the problem differently or ask your neighbors or workshop staff for tipsn and hints. Re hints and the solution if needed.

All the Labs are located in Amazon CloudWatch dashboards. So to get started, lets access the AWS account w the Labs introductions and the various challanges you need to solve!

Step 5: Access AWS account

Access the AWS console



aws workshop studio

NET307-Become a network support expert: We break it, you fix it event

Accessing the AWS Environment and Labs

AWS account access

Open AWS console

Get AWS CLI credentials

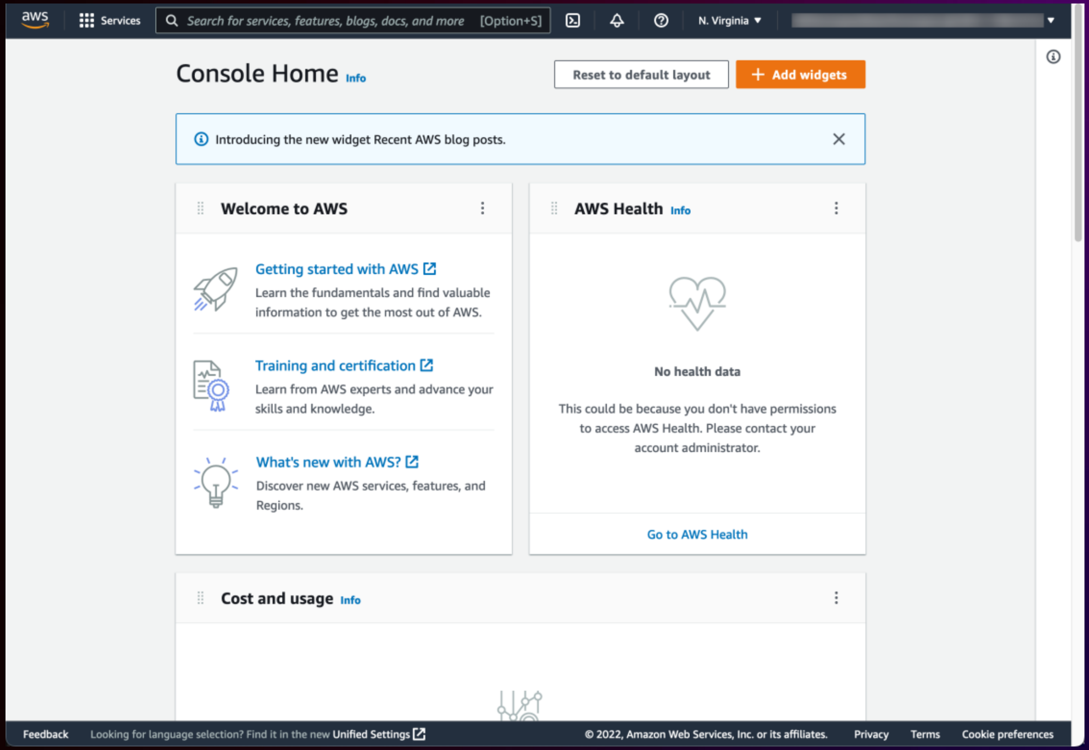
Exit event

Event in progress
Ends in 11 hours 55 minutes 49

Event dashboard > Accessing

Accessing the

Welcome to the workshop:
In this Workshop you will as
and solve various issues in y
This workshop is not your ty
knowledge, your table neigh
can use to get an idea on ho
lab. But we recommend tha
hints for that particular lab,



aws
Services
Search for services, features, blogs, docs, and more [Option+S]
N. Virginia ▾

[redacted]

Console Home Info

Reset to default layout
+ Add widgets

Introducing the new widget Recent AWS blog posts.

Welcome to AWS

Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.

Training and certification
Learn from AWS experts and advance your skills and knowledge.

What's new with AWS?
Discover new AWS services, features, and Regions.

AWS Health Info

No health data

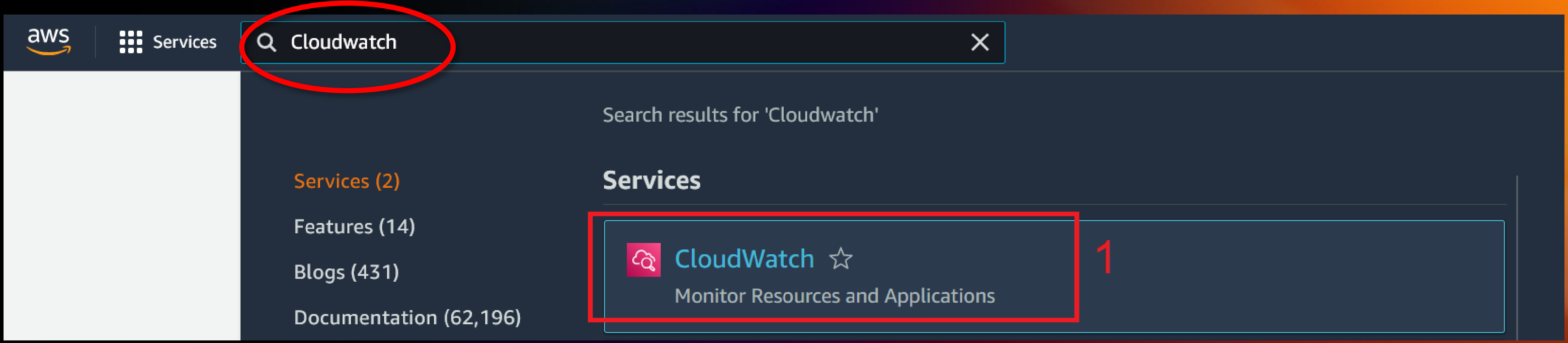
This could be because you don't have permissions to access AWS Health. Please contact your account administrator.

Go to AWS Health

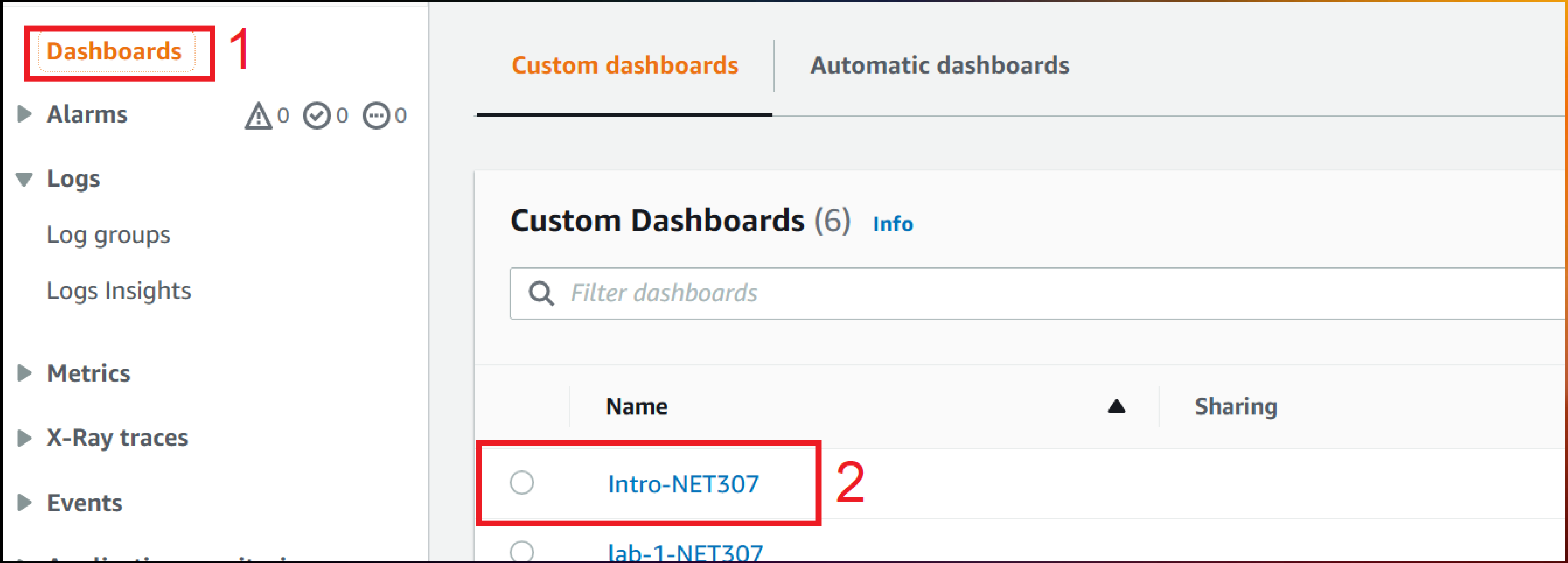
Cost and usage Info

Feedback
Looking for language selection? Find it in the new Unified Settings
© 2022, Amazon Web Services, Inc. or its affiliates.
Privacy
Terms
Cookie preferences

Step 6: Access lab instructions

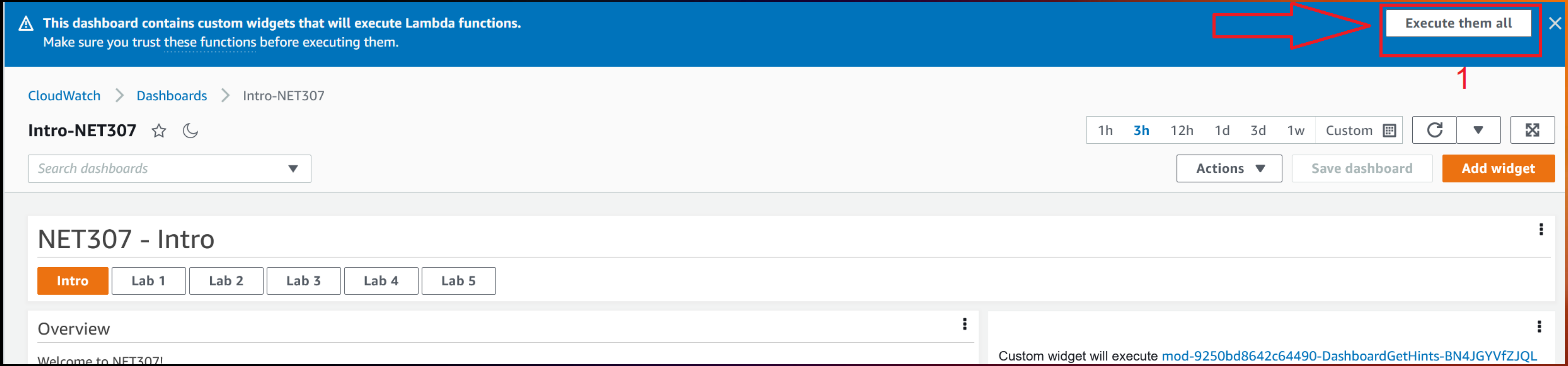


Step 7: Access lab dashboards



	Name ▲	Sharing
○	Intro-NET307	
○	lab-1-NET307	

Step 8: Enable lab dashboards



This dashboard contains custom widgets that will execute Lambda functions.
Make sure you trust these functions before executing them.

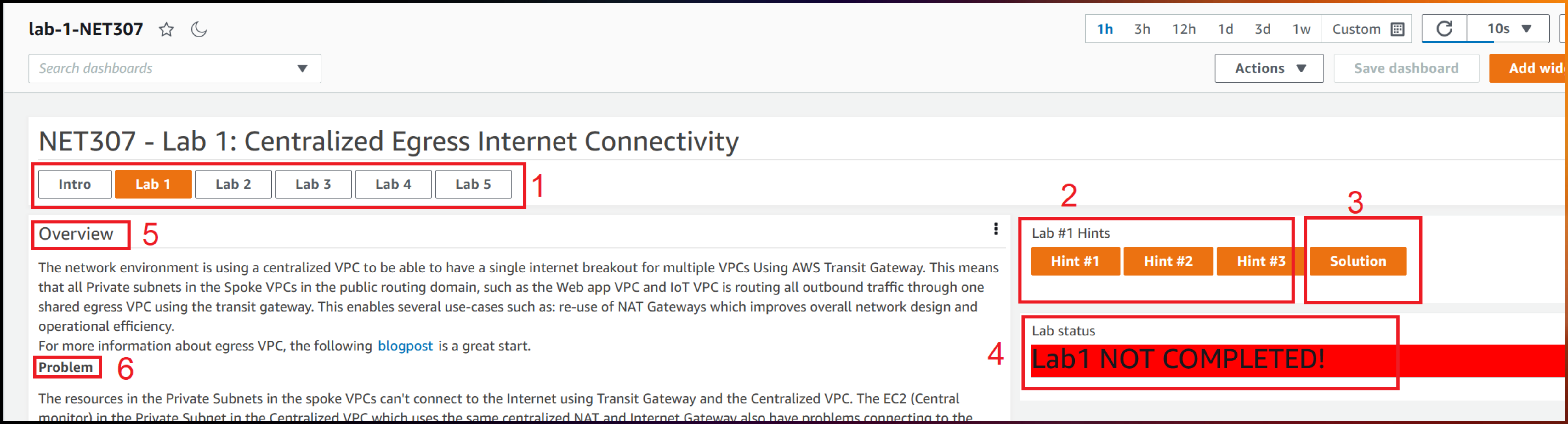
NET307 - Intro

Overview

Welcome to NET307!

Custom widget will execute mod-9250bd8642c64490-DashboardGetHints-BN4JGYVfZJQL

Lab dashboard overview



NET307 - Lab 1: Centralized Egress Internet Connectivity

Lab1 NOT COMPLETED!

Overview

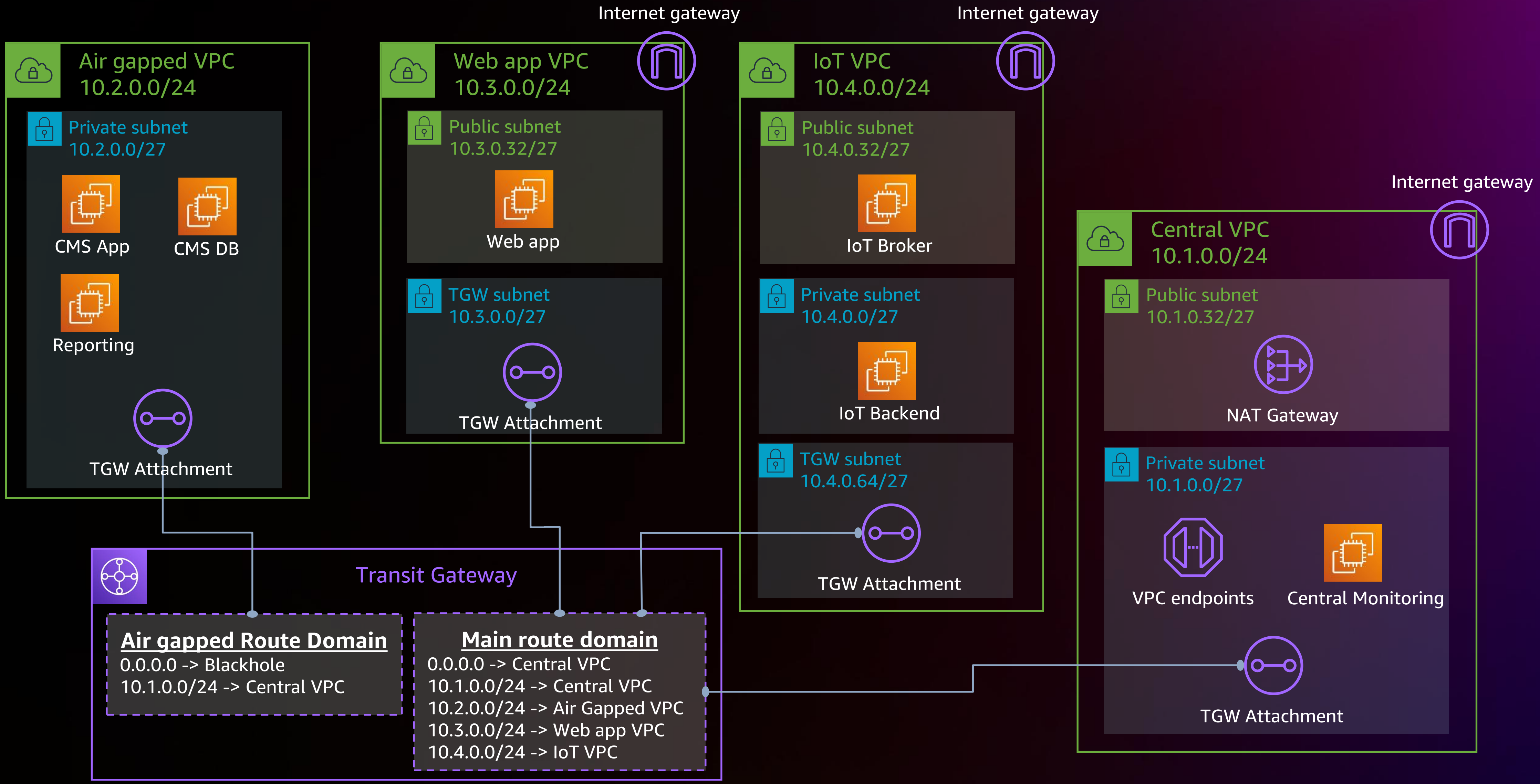
The network environment is using a centralized VPC to be able to have a single internet breakout for multiple VPCs Using AWS Transit Gateway. This means that all Private subnets in the Spoke VPCs in the public routing domain, such as the Web app VPC and IoT VPC is routing all outbound traffic through one shared egress VPC using the transit gateway. This enables several use-cases such as: re-use of NAT Gateways which improves overall network design and operational efficiency.

For more information about egress VPC, the following blogpost is a great start.

Problem

The resources in the Private Subnets in the spoke VPCs can't connect to the Internet using Transit Gateway and the Centralized VPC. The EC2 (Central monitor) in the Private Subnet in the Centralized VPC which uses the same centralized NAT and Internet Gateway also have problems connecting to the

Lab environment



Internet gateway

Internet gateway

Internet gateway

Air gapped VPC
10.2.0.0/24

Private subnet
10.2.0.0/27

CMS App

CMS DB

Reporting

TGW Attachment

Web app VPC
10.3.0.0/24

Public subnet
10.3.0.32/27

Web app

TGW subnet
10.3.0.0/27

TGW Attachment

IoT VPC
10.4.0.0/24

Public subnet
10.4.0.32/27

IoT Broker

Private subnet
10.4.0.0/27

IoT Backend

TGW subnet
10.4.0.64/27

TGW Attachment

Central VPC
10.1.0.0/24

Public subnet
10.1.0.32/27

NAT Gateway

Private subnet
10.1.0.0/27

VPC endpoints

Central Monitoring

TGW Attachment

Transit Gateway

Air gapped Route Domain
0.0.0.0 -> Blackhole
10.1.0.0/24 -> Central VPC

Main route domain
0.0.0.0 -> Central VPC
10.1.0.0/24 -> Central VPC
10.2.0.0/24 -> Air Gapped VPC
10.3.0.0/24 -> Web app VPC
10.4.0.0/24 -> IoT VPC

Thank you!

Jesper Eneberg
enebergj@amazon.com

Maks Khomutskyi
makskh@amazon.com

Please complete the session survey in the **mobile app**