AWS re:Invent

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

SEC204-R

Analyze your network using Amazon VPC Network Access Analyzer

Suresh Patnam
Principal Solutions Architect
Amazon Web Services

Tom Santuccio
Solutions Architect
Amazon Web Services

Akshay Karanth
Sr. Solutions Architect
Amazon Web Services

Ruchi Mishra
Solutions Architect
Amazon Web Services

Ramesh Adabala
Sr. Leader Solutions Architect
Amazon Web Services

Agenda

1. What is Network Access Analyzer?
2. Why do you need Network Access Analyzer?
3. Network Access Analyzer example use cases
4. How to get started
5. Q&A
6. Hands-on workshop

What is Network Access Analyzer?

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

- Helps understand, verify, and improve your network security posture
- Helps demonstrate compliance
- Takes advantage of our automated reasoning technology that already powers AWS Identity and Access Management (IAM) Access Analyzer, VPC Reachability Analyzer, Amazon Inspector Network Reachability, and other provable security tools
- You pay $0.002 for each Elastic Network Interface (ENI) analyzed as part of an assessment

Why do you need Network Access Analyzer?

- Tedious and ineffective network control validation
- Audit is time-consuming
- Network controls need to evolve
- Improving agility between operations and development teams

Network Access Analyzer example use cases

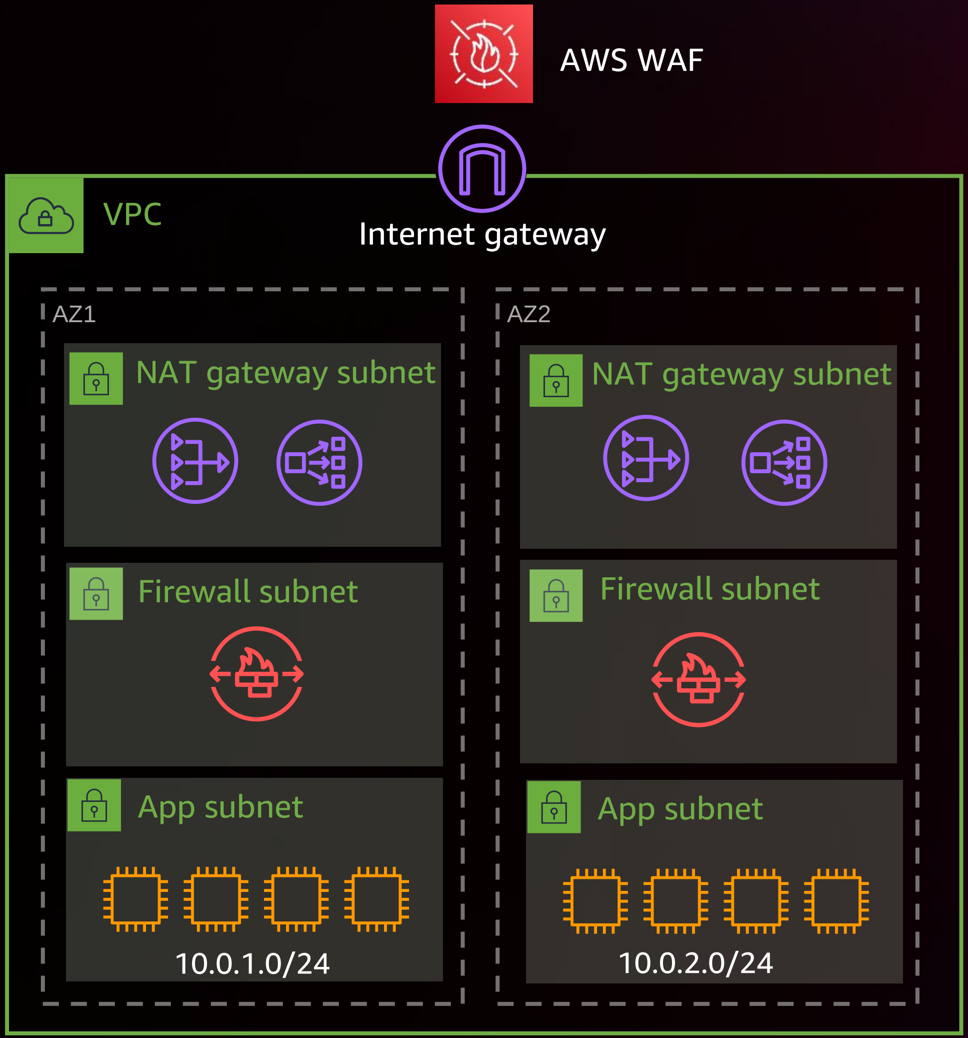
Network Access Analyzer can help you verify the following sample use cases

1. Internet accessibility
2. Network segmentation
3. Trusted network paths (OSI layer 3)
4. Trusted network access (OSI layer 4)

Supported resources
and limitations

Use case 1: Internet accessibility to resources in VPCs

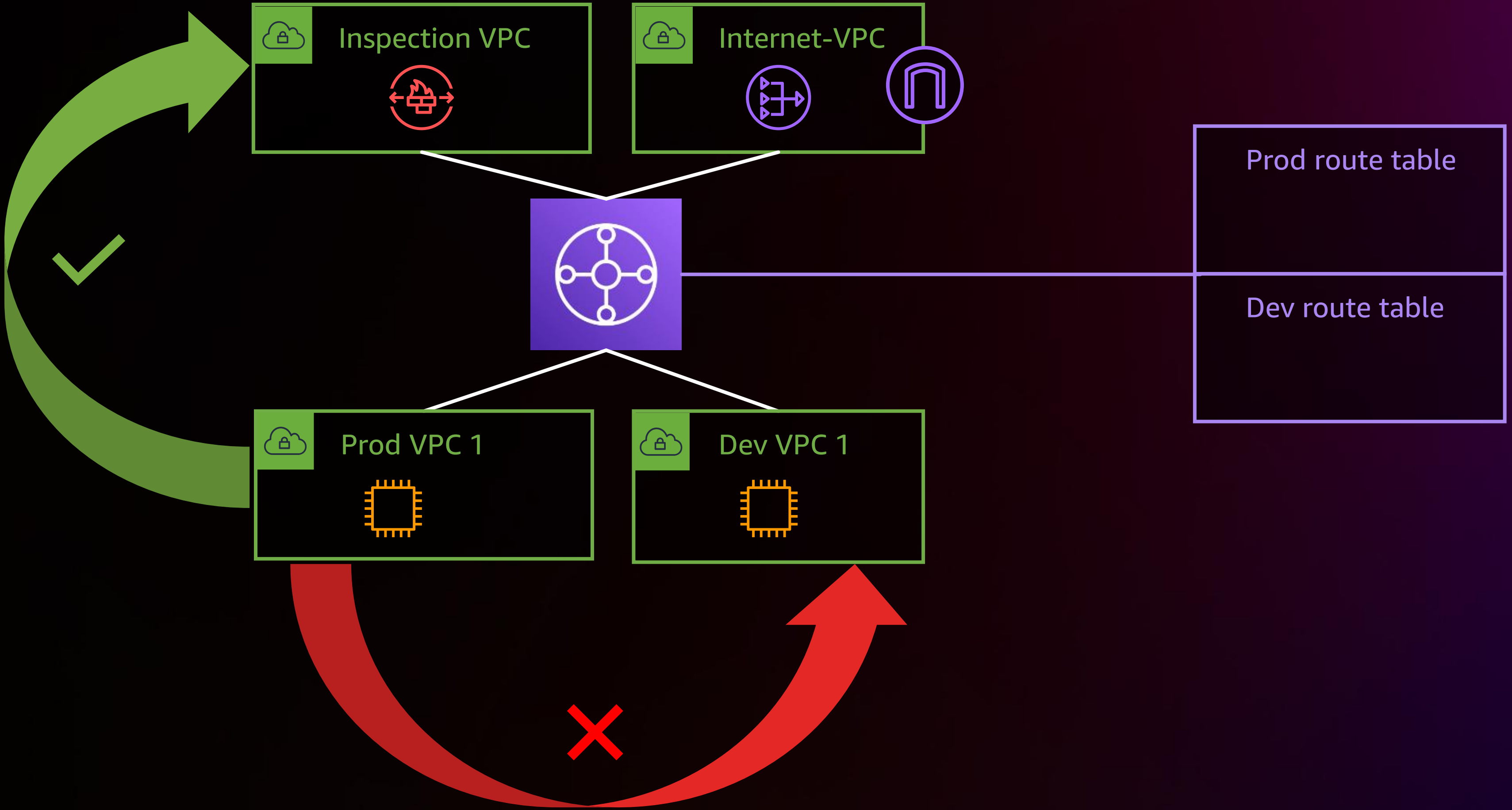
"How is my application accessible from the internet?"



Use case 2: AWS Transit Gateway network segmentation

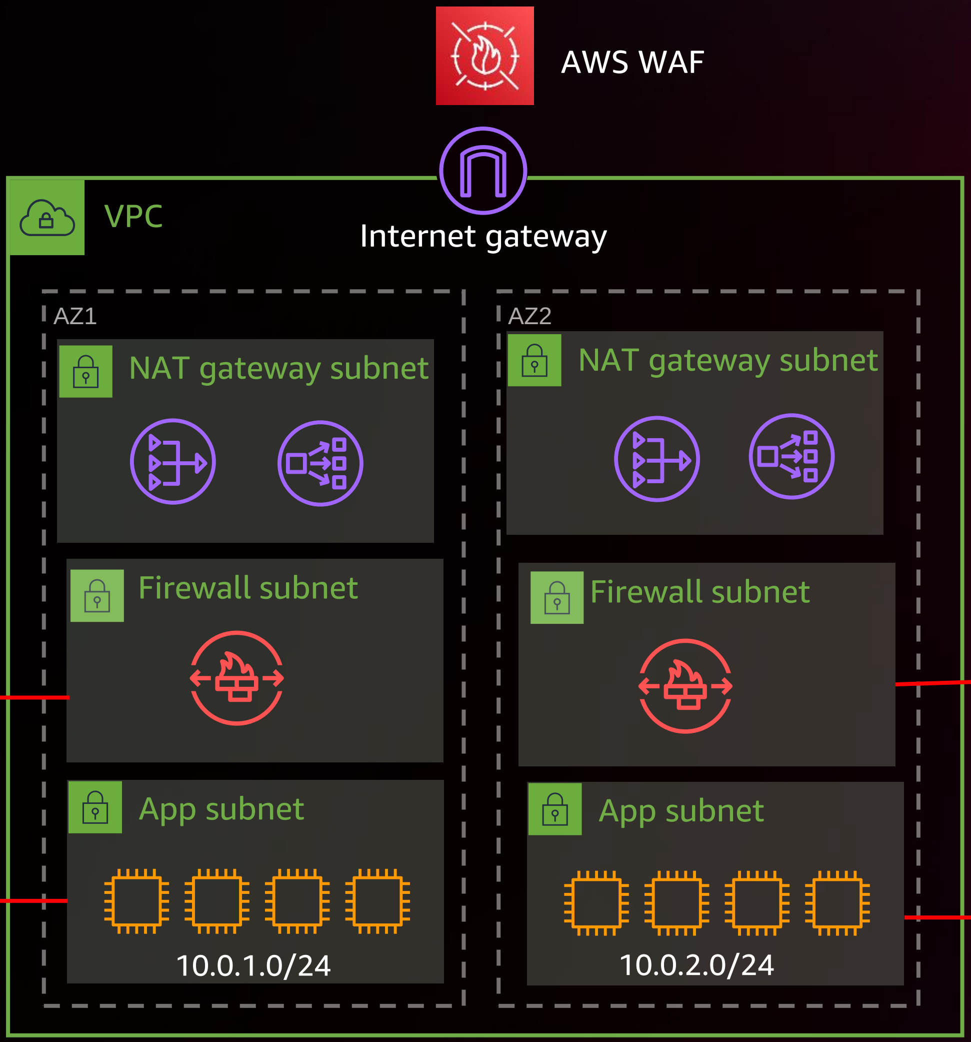
“Prod and Dev VPCs need to be isolated from each other”

“Prod VPC can communicate with Inspection VPC”



Use case 3: Security controls (e.g., firewall/NAT-GW) in path

“My application should access the internet only via AWS Network Firewall”



Destination	Target
0.0.0.0/0	nat-354ea5

!

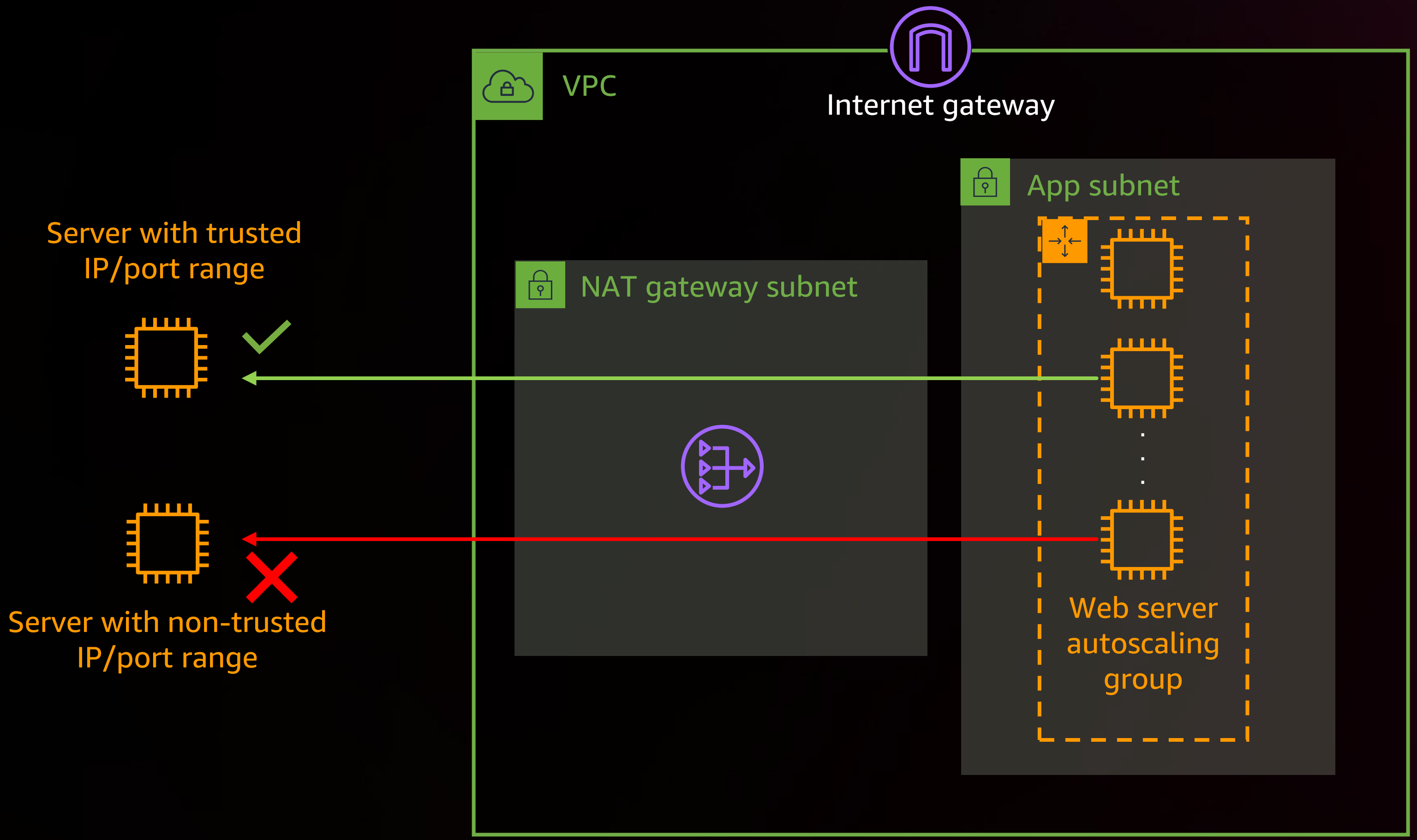
Destination	Target
0.0.0.0/0	igw-34ee85

Destination	Target
0.0.0.0/0	nat-34eea5

Destination	Target
0.0.0.0/0	vpce-343fe4

Use case 4: Access to trusted CIDRs and ports

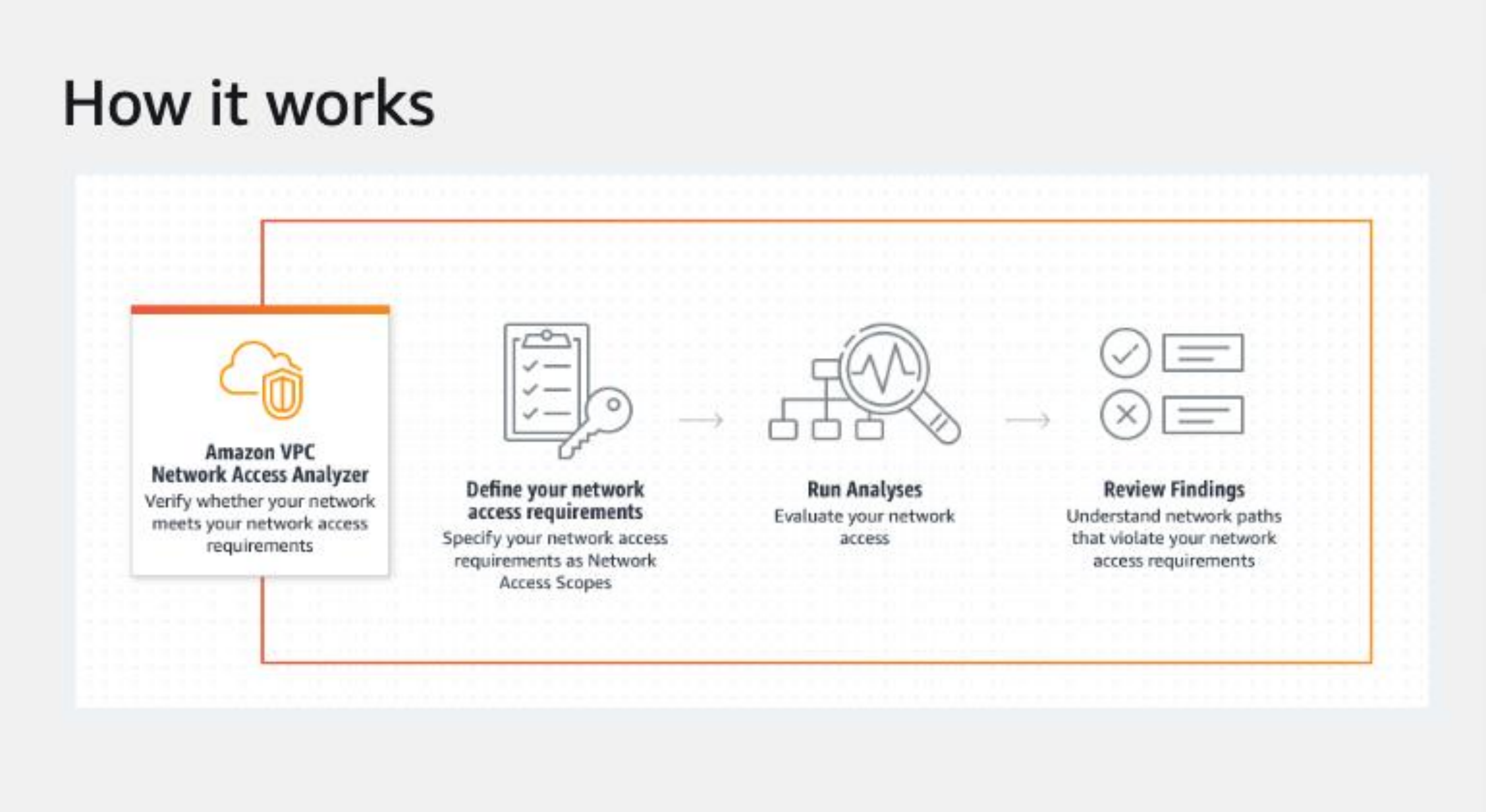
“My application instances can only download updates from trusted IP range and port”


VPC
Internet gateway
App subnet
Server with trusted IP/port range
NAT gateway subnet
Web server autoscaling group
Server with non-trusted IP/port range

AWS Network Firewall domain rule

Amazon Route 53 Resolver DNS Firewall

How Network Access Analyzer works



How it works

Amazon VPC Network Access Analyzer
Verify whether your network meets your network access requirements

Define your network access requirements
Specify your network access requirements as Network Access Scopes

→

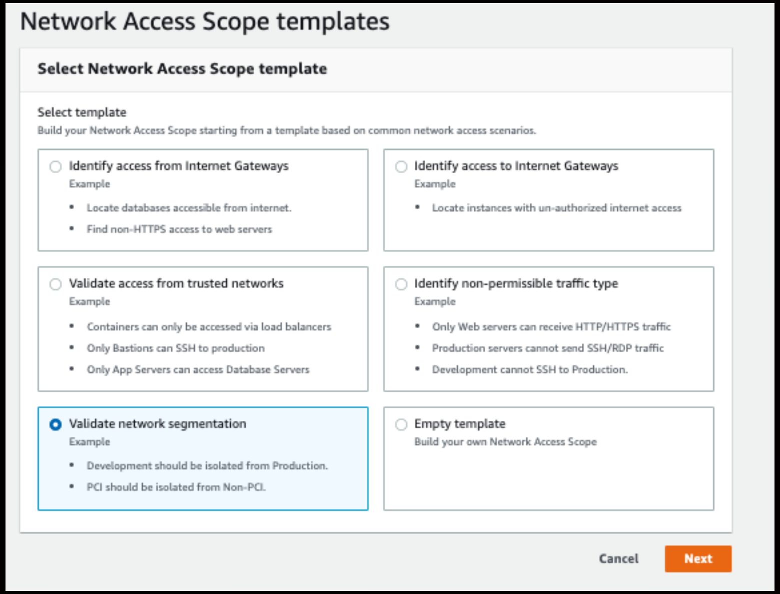
Run Analyses
Evaluate your network access

→

Review Findings
Understand network paths that violate your network access requirements

How Network Access Analyzer works: Define your requirements

Console



Network Access Scope templates

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

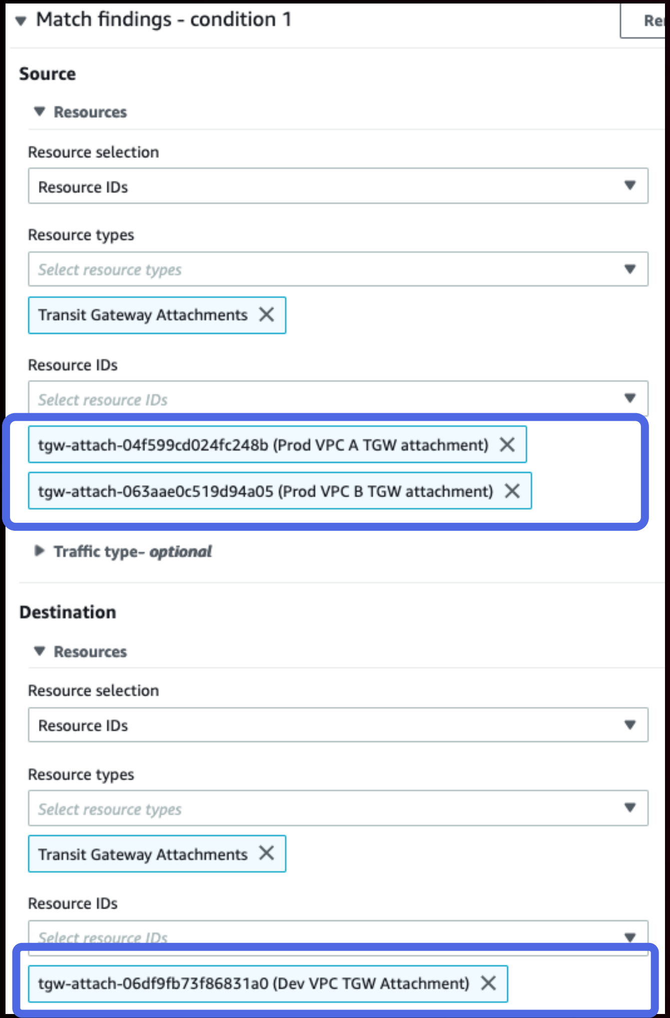
○ Identify access to Internet Gateways
Example
- Locate instances with un-authorized internet access

○ 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



▼ Match findings - condition 1

Source

▼ Resources

Resource selection: Resource IDs ▼

Resource types: Select resource types ▼

Transit Gateway Attachments ✕

Resource IDs: Select resource IDs ▼

tgw-attach-04f599cd024fc248b (Prod VPC A TGW attachment) ✕

tgw-attach-063aae0c519d94a05 (Prod VPC B TGW attachment) ✕

▶ Traffic type- *optional*

Destination

▼ Resources

Resource selection: Resource IDs ▼

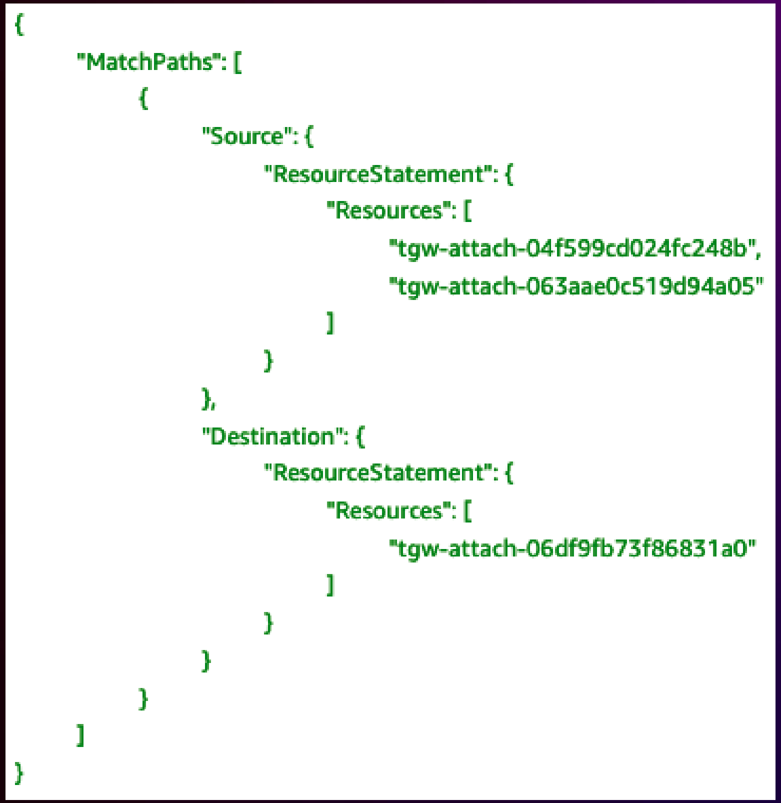
Resource types: Select resource types ▼

Transit Gateway Attachments ✕

Resource IDs: Select resource IDs ▼

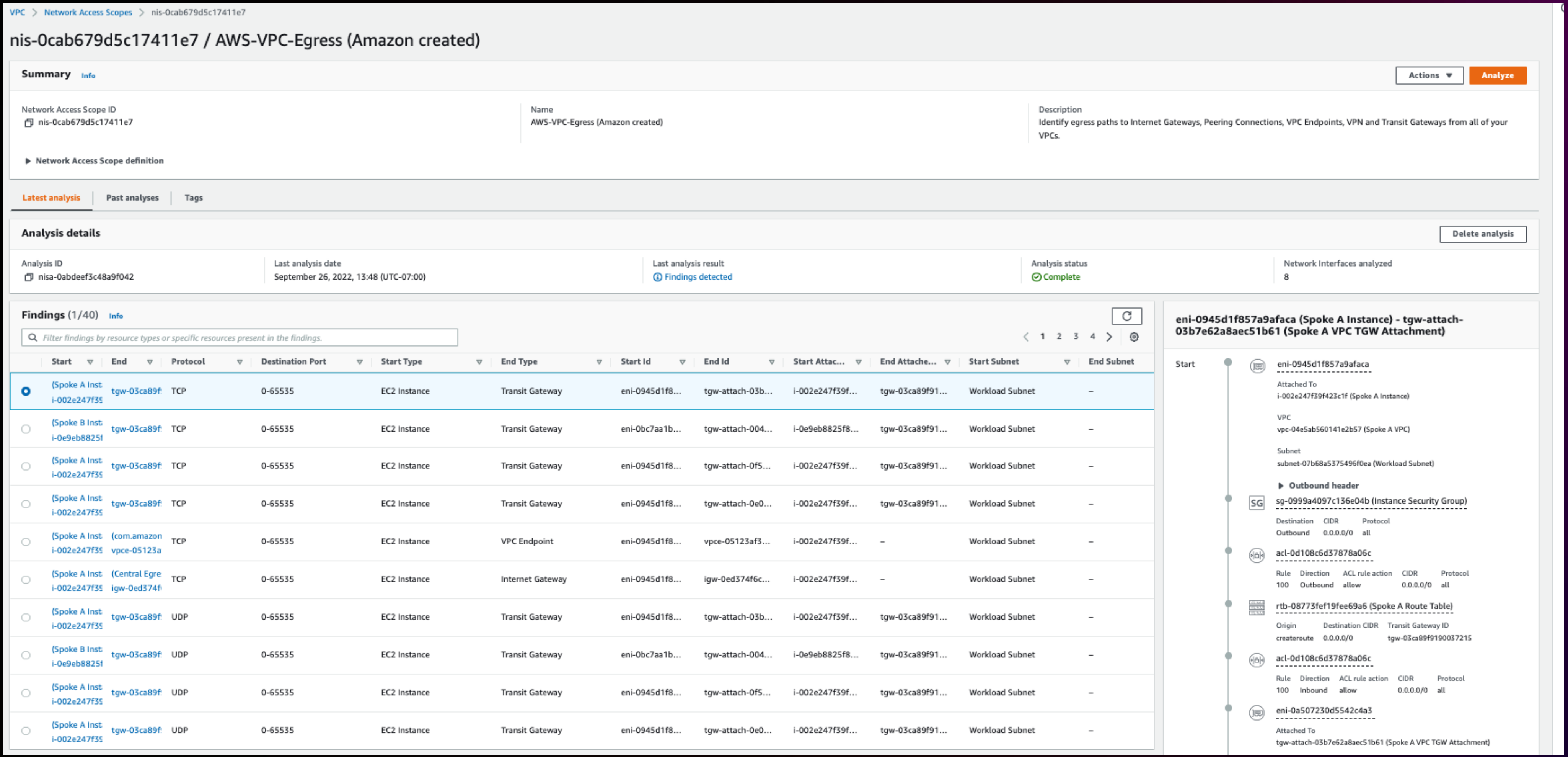
tgw-attach-06df9fb73f86831a0 (Dev VPC TGW Attachment) ✕

JSON



```
{
    "MatchPaths": [
        {
            "Source": {
                "ResourceStatement": {
                    "Resources": [
                        "tgw-attach-04f599cd024fc248b",
                        "tgw-attach-063aae0c519d94a05"
                    ]
                }
            },
            "Destination": {
                "ResourceStatement": {
                    "Resources": [
                        "tgw-attach-06df9fb73f86831a0"
                    ]
                }
            }
        }
    ]
}
```

How Network Access Analyzer works: Run analysis and review findings



VPC > Network Access Scopes > nis-0cab679d5c17411e7

nis-0cab679d5c17411e7 / AWS-VPC-Egress (Amazon created)

Summary Info

Network Access Scope ID
nis-0cab679d5c17411e7

Name
AWS-VPC-Egress (Amazon created)

Description
Identify egress paths to Internet Gateways, Peering Connections, VPC Endpoints, VPN and Transit Gateways from all of your VPCs.

▶ Network Access Scope definition

Analysis details

Analysis ID
nisa-0abdeef3c48a9f042

Last analysis date
September 26, 2022, 13:48 (UTC-07:00)

Last analysis result
Findings detected

Analysis status
Complete

Network Interfaces analyzed
8

Findings (1/40) Info

Filter findings by resource types or specific resources present in the findings.
< 1 2 3 4 >

	Start	End	Protocol	Destination Port	Start Type	End Type	Start Id	End Id	Start Attac...	End Attache...	Start Subnet	End Subnet
●	(Spoke A Inst i-002e247f39	tgw-03ca89f!	TCP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-03b...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke B Inst i-0e9eb8825f	tgw-03ca89f!	TCP	0-65535	EC2 Instance	Transit Gateway	eni-0bc7aa1b...	tgw-attach-004...	i-0e9eb8825f8...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	tgw-03ca89f!	TCP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-0f5...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	tgw-03ca89f!	TCP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-0e0...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	(com.amazon vpce-05123a	TCP	0-65535	EC2 Instance	VPC Endpoint	eni-0945d1f8...	vpce-05123af3...	i-002e247f39f...	–	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	(Central Egre igw-0ed374f	TCP	0-65535	EC2 Instance	Internet Gateway	eni-0945d1f8...	igw-0ed374f6c...	i-002e247f39f...	–	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	tgw-03ca89f!	UDP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-03b...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke B Inst i-0e9eb8825f	tgw-03ca89f!	UDP	0-65535	EC2 Instance	Transit Gateway	eni-0bc7aa1b...	tgw-attach-004...	i-0e9eb8825f8...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	tgw-03ca89f!	UDP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-0f5...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–
○	(Spoke A Inst i-002e247f39	tgw-03ca89f!	UDP	0-65535	EC2 Instance	Transit Gateway	eni-0945d1f8...	tgw-attach-0e0...	i-002e247f39f...	tgw-03ca89f91...	Workload Subnet	–

eni-0945d1f857a9afaca (Spoke A Instance) - tgw-attach-03b7e62a8aec51b61 (Spoke A VPC TGW Attachment)

Start

eni-0945d1f857a9afaca

Attached To
i-002e247f39f423c1f (Spoke A Instance)

VPC
vpc-04e5ab560141e2b57 (Spoke A VPC)

Subnet
subnet-07b68a5375496f0ea (Workload Subnet)

▶ Outbound header

SG sg-0999a4097c136e04b (Instance Security Group)

Destination	CIDR	Protocol
Outbound	0.0.0.0/0	all

acl-0d108c6d37878a06c

Rule	Direction	ACL rule action	CIDR	Protocol
100	Outbound	allow	0.0.0.0/0	all

rtb-08773fef19fee69a6 (Spoke A Route Table)

Origin	Destination CIDR	Transit Gateway ID
createroute	0.0.0.0/0	tgw-03ca89f9190037215

acl-0d108c6d37878a06c

Rule	Direction	ACL rule action	CIDR	Protocol
100	Inbound	allow	0.0.0.0/0	all

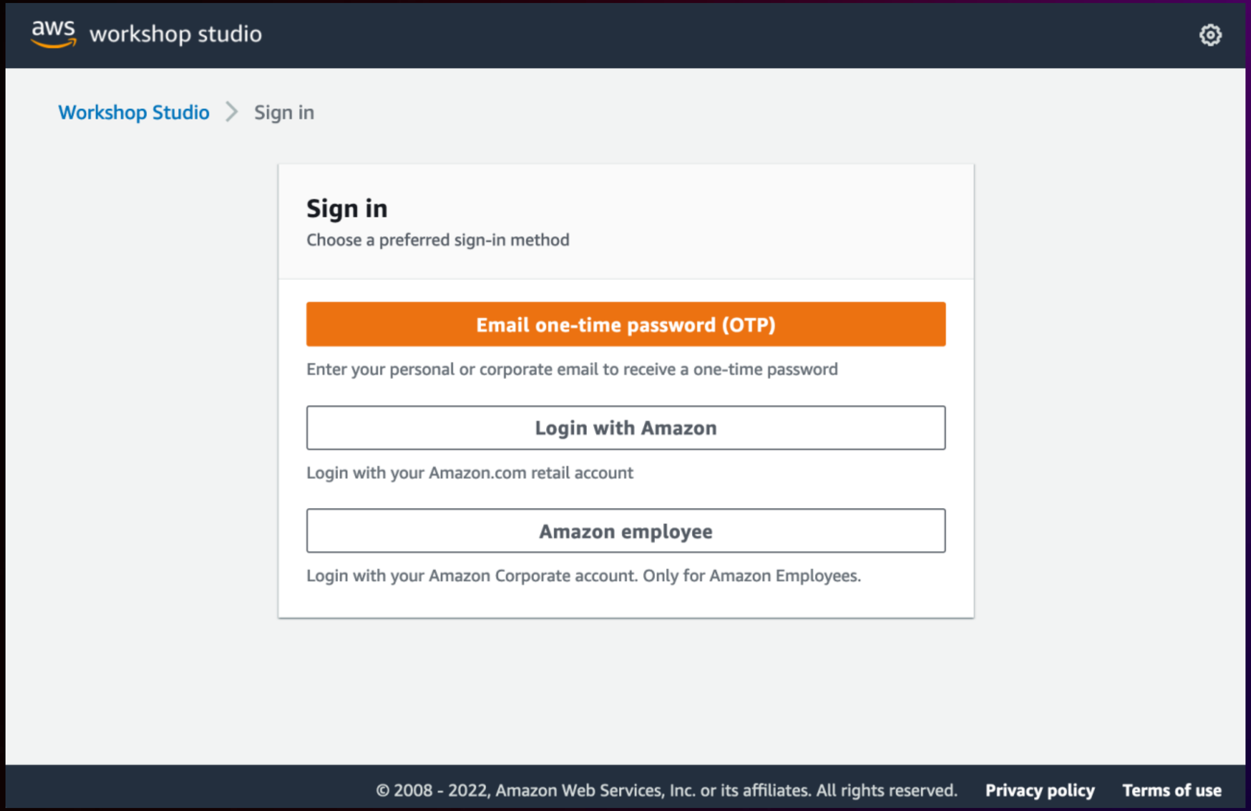
eni-0a507230d5542c4a3

Attached To
tgw-attach-03b7e62a8aec51b61 (Spoke A VPC TGW Attachment)

Amazon VPC Network Access Analyzer workshop

Access workshop

Workshop link: https://s12d.com/nXnAA34a



Workshop Studio > Sign in

Sign in

Choose a preferred sign-in method

Email one-time password (OTP)

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

Login with Amazon

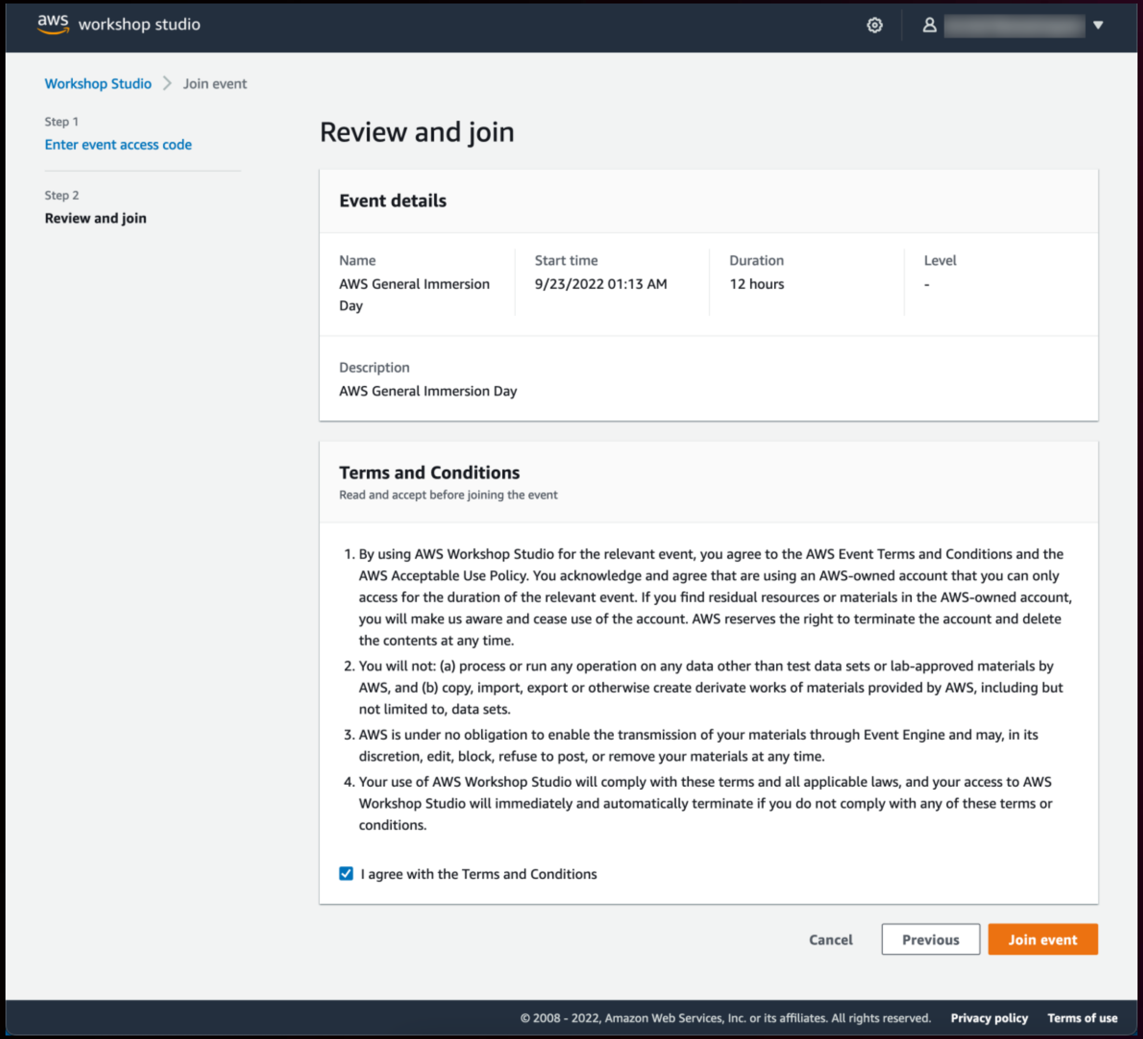
Login with your Amazon.com retail account

Amazon employee

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

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

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

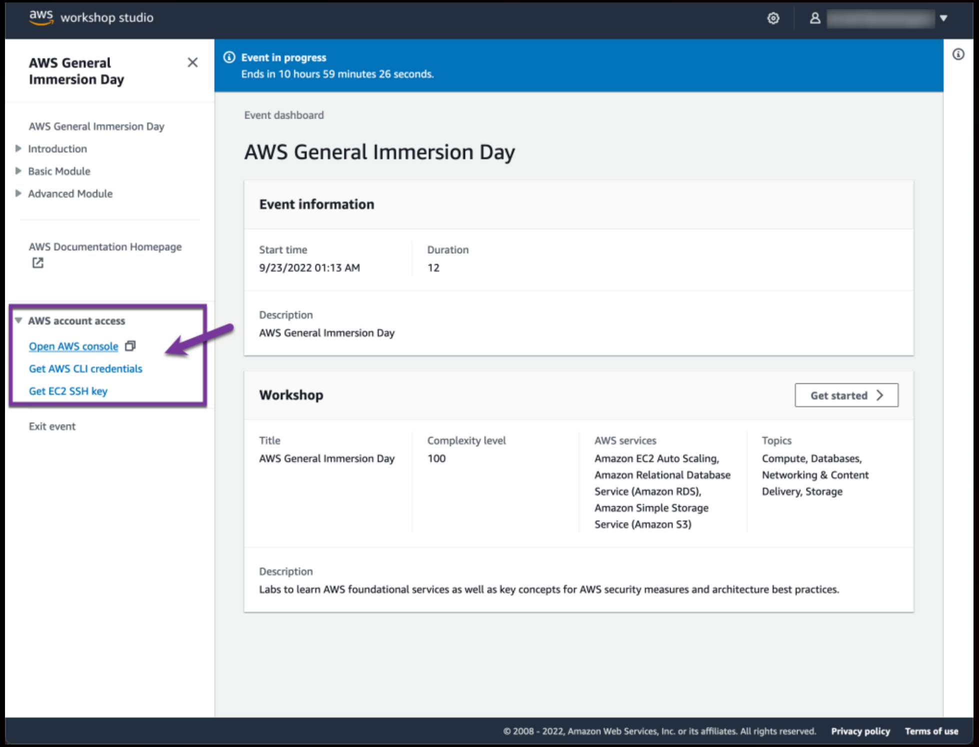
Read and accept before joining the event

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

Access AWS account

Access the AWS Console or generate AWS CLI credentials as needed



[redacted]

AWS General Immersion Day

- AWS General Immersion Day
- Introduction
- Basic Module
- Advanced Module

AWS Documentation Homepage

AWS account access

- Open AWS console
- Get AWS CLI credentials
- Get EC2 SSH key

Exit event

Event in progress
Ends in 10 hours 59 minutes 26 seconds.

Event dashboard

AWS General Immersion Day

Event information

Start time	Duration
9/23/2022 01:13 AM	12

Description
AWS General Immersion Day

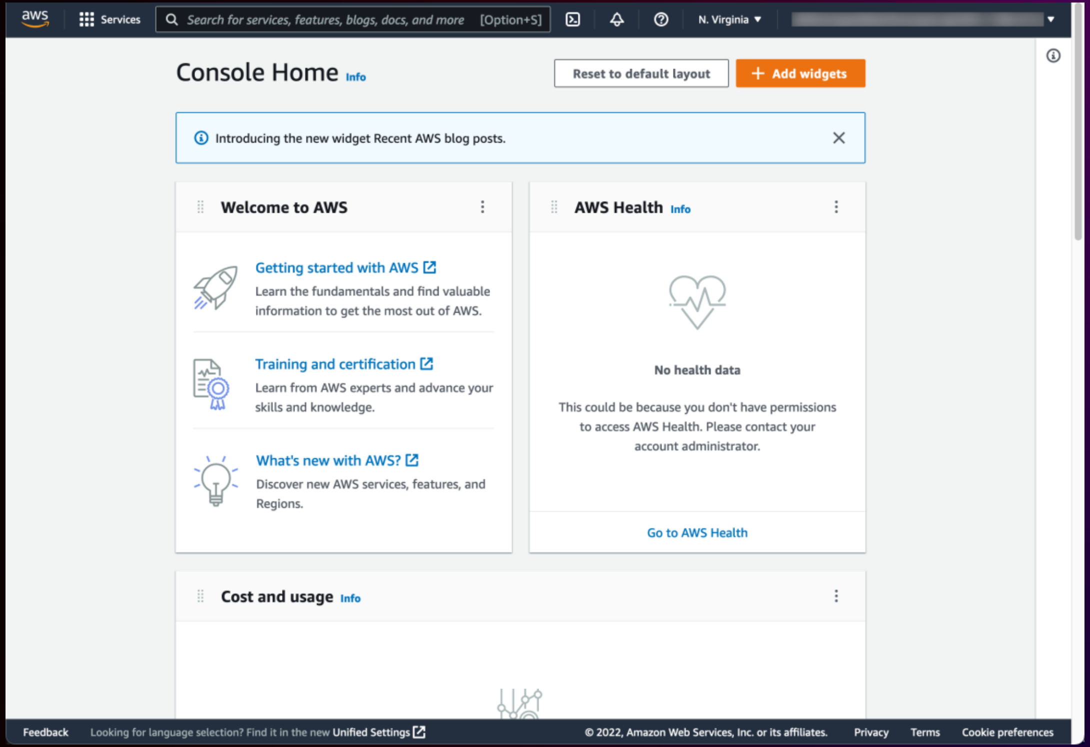
Workshop

Get started

Title	Complexity level	AWS services	Topics
AWS General Immersion Day	100	Amazon EC2 Auto Scaling, Amazon Relational Database Service (Amazon RDS), Amazon Simple Storage Service (Amazon S3)	Compute, Databases, Networking & Content Delivery, Storage

Description
Labs to learn AWS foundational services as well as key concepts for AWS security measures and architecture best practices.

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



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

Call to action

Learn more about Network Access Analyzer

Thank you!

Suresh Patnam
surpatna@amazon.com

Tom Santuccio
tomsant@amazon.com

Akshay Karanth
akaranth@amazon.com

Ruchi Mishra
rucmish@amazon.com

Ramesh Adabala
adabalar@amazon.com

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