The bridge to possible

Secure Access with ISE in the Cloud

Eugene Korneychuk, Technical Leader

About Eugene Korneychuk

- Security TAC Technical Leadership Team
- 15+ years of security and networking experience
- 20+ published documents
- On personal note:
  - Family time
  - Travel
  - Football
- Lives in Cary, North Carolina, US

Session Objective

The Goal of this session is to:

- Make you familiar with ISE Cloud deployments and designs
- Cover ISE automation techniques
- Explain the SAML Authentication functionality and its implementation on ISE
- Walk you through ROPC authentication with ISE and Azure Active Directory

Agenda

- ISE Architecture Concepts
- ISE in the Cloud
- ISE in AWS and Azure
- AWS Partner Solution
- ISE SAML SSO
- ISE Azure Active Directory Authentication
- Conclusion

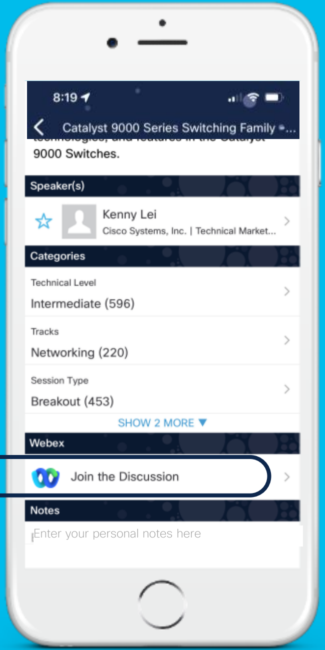
Cisco Webex App

Questions?

Use Cisco Webex App to chat
with the speaker after the session

How

1. Find this session in the Cisco Live Mobile App
2. Click “Join the Discussion”
3. Install the Webex App or go directly to the Webex space
4. Enter messages/questions in the Webex space



8:19

Catalyst 9000 Series Switching Family ▪...

9000 Switches.

Speaker(s)

☆ Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

Webex spaces will be moderated until February 24, 2023.

ISE Architecture Concepts

ISE Design Concepts

Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Owns ISE database and replicates it to other nodes

Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Collects health and log information from other nodes

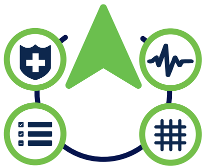
Policy Services Node (PSN)

- Makes policy decisions
- RADIUS / TACACS+ Servers

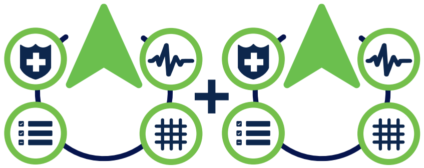
pxGrid Controller

- Facilitates sharing of context

ISE Scaling

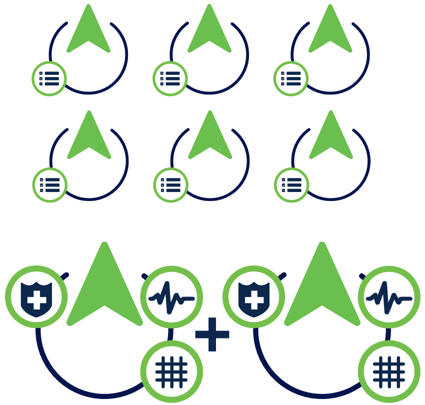


Lab and Evaluation



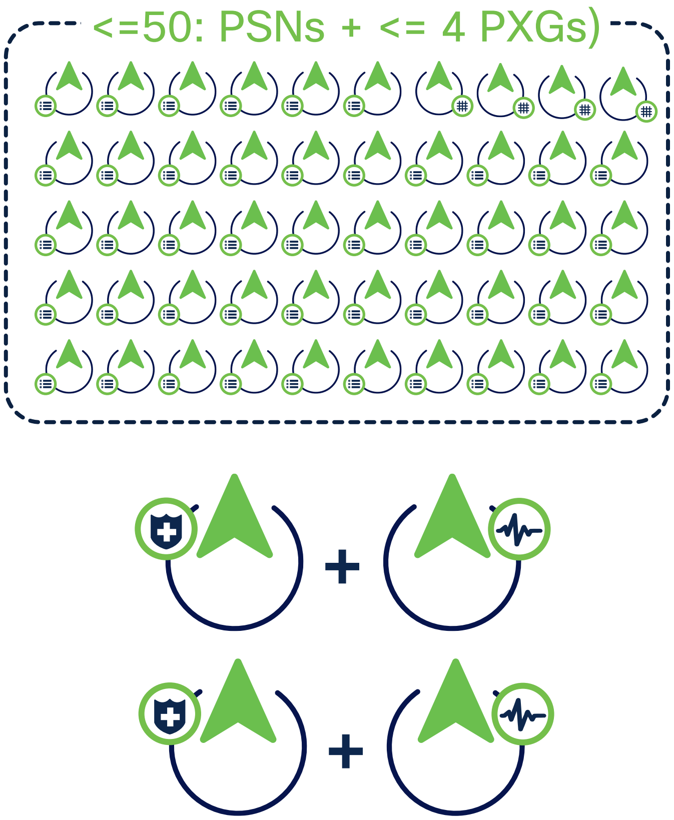
Small HA Deployment

2 x (PAN+MNT+PSN)



Medium Multi-node Deployment

2 x (PAN+MNT+PXG), <= 6 PSN



Large Deployment

2 PAN, 2 MNT, <=50: PSNs + <= 4 PXGs

PSN Sizing Across Platforms

Cisco ISE

PSN Profile	Extra Small	Small	Medium	Large
Physical Appliance	-	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655 Cisco SNS 3695
VM Appliance	Extra Small VM (8vCPU, 32 GB)	VM Equivalent of SNS 3615 (16vCPU, 32 GB)	VM Equivalent of SNS 3595 (16vCPU, 32 GB)	VM Equivalent of SNS 3655 (24vCPU, 96 GB) VM Equivalent of SNS 3695 (24vCPU, 256 GB)
AWS	m5.2xlarge	c5.4xlarge* m5.4xlarge	-	c5.9xlarge
Azure	Standard_D8s_v4	Standard_F16s_v2* Standard_D16s_v4	-	Standard_F32s_v2
OCI	Standard3.Flex (4 OCPU and 32 GB)	Optimized3.Flex* (8 OCPU and 32 GB) Standard3.Flex (8 OCPU and 64 GB)	-	Optimized3.Flex (16 OCPU and 64GB)

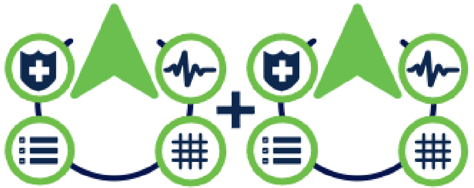
* This instance is compute-optimized and provides better performance compared to the general purpose instances

PSN Maximum Concurrent Active Sessions

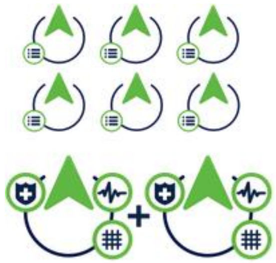
Cisco ISE

PSN Profile	Extra Small	Small	Medium	Large
Concurrent active endpoints supported by a dedicated PSN (Cisco ISE node has only PSN persona)	12,000	25,000	40,000	50,000
Concurrent active endpoints supported by a shared PSN (Cisco ISE node has multiple personas)	Unsupported	12,500	20,000	25,000

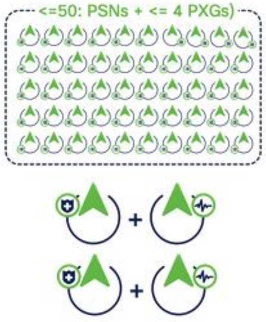
Small Deployment



Medium Deployment



Large Deployment



PAN/MNT Sizing Across Platforms

Cisco ISE

PAN/MNT Profile	Small	Medium	Large	Extra Large
Physical Appliance	Cisco SNS 3615	Cisco SNS 3595	Cisco SNS 3655	Cisco SNS 3695
VM Appliance	VM 16vCPU, 32 GB	VM 16 vCPU, 64 GB	VM 24vCPU, 96 GB	VM 24vCPU, 256 GB
AWS	c5.4xlarge	m5.4xlarge c5.9xlarge*	m5.8xlarge	m5.16xlarge
Azure	Standard_F16s_v2	Standard_D16s_v4 Standard_F32s_v2*	Standard_D32s_v4	Standard_D64s_v4
OCI	Optimized3.Flex (8 OCPU and 32 GB)	Standard3.Flex (8 OCPU and 64 GB) Optimized3.Flex* (16 OCPU and 64 GB)	Standard3.Flex (16 OCPU and 128 GB)	Standard3.Flex (32 OCPU and 256 GB)

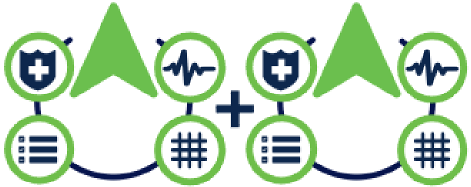
* This instance is compute-optimized and provides better performance compared to the general purpose instances

Total Maximum Concurrent Active Sessions

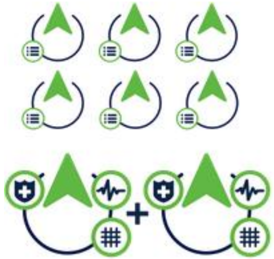
Cisco ISE

PAN, MNT or both PAN and MNT Profiles	Small	Medium	Large	Extra Large
Large deployment	Unsupported	500,000	500,000	2,000,000
Medium deployment	10,000	20,000	25,000	50,000
Small deployment	10,000	20,000	25,000	50,000

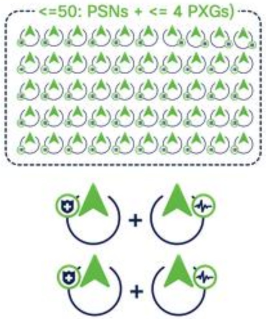
Small Deployment



Medium Deployment

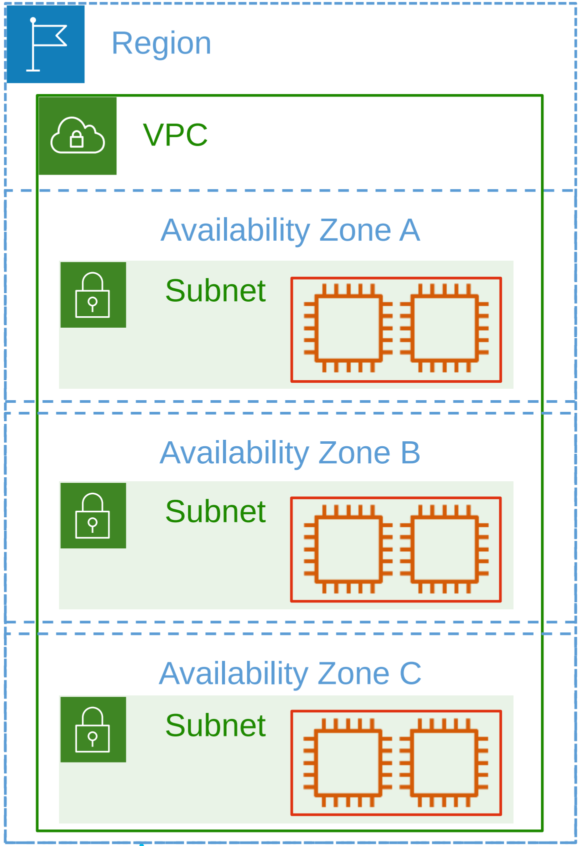


Large Deployment



ISE in the Cloud

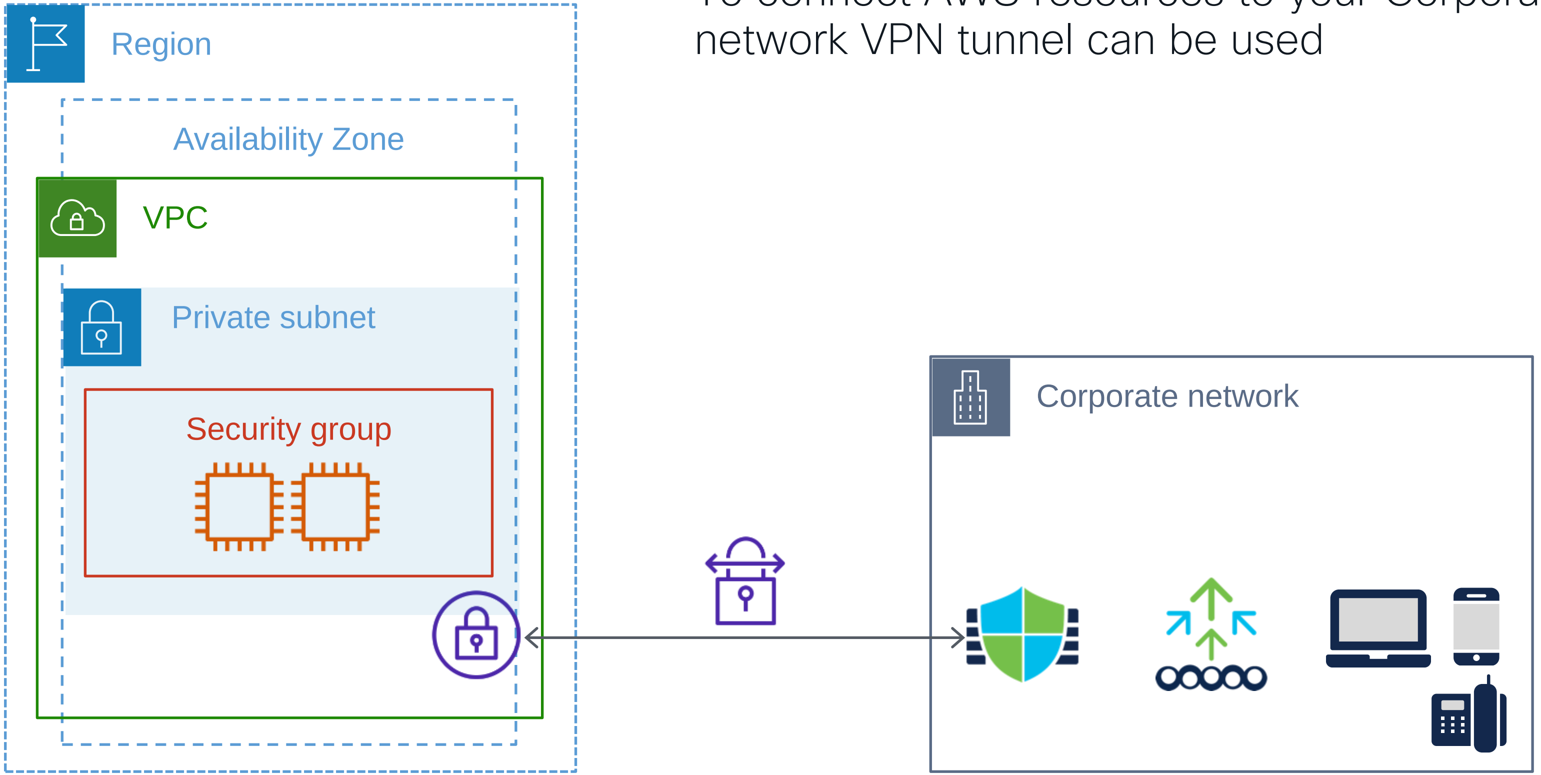
AWS basics



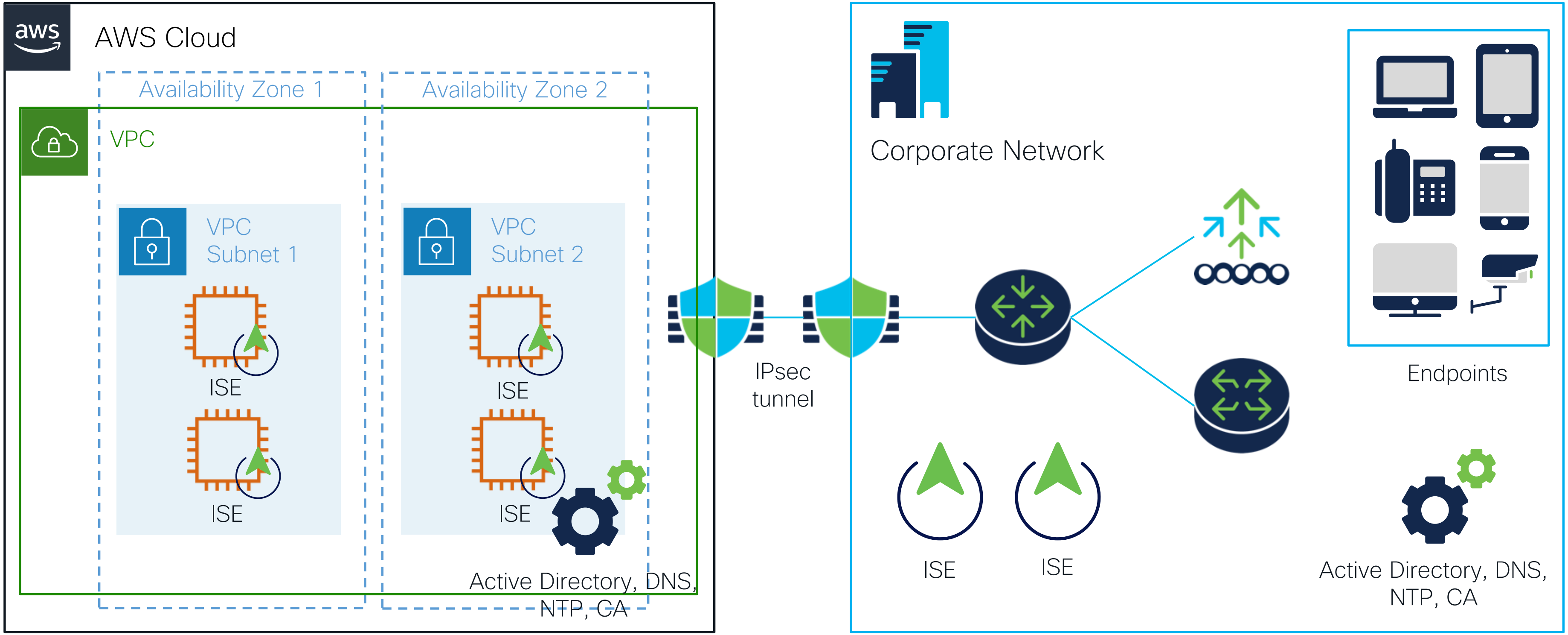
- Each Region is fully isolated from another region to achieve fault tolerance.
  - us-east-2 (Ohio)
  - eu-central-1 (Frankfurt)
  - ap-south-1 (Mumbai)
- Each Region has multiple isolated locations known as Availability Zones. The code for Availability Zone is its Region code followed by a letter identifier.
  - us-east-1a
  - us-east-1b
- VPC is a Virtual Network which spans all of the Availability Zones in the Region.
  - After creating a VPC you can add one or more subnets in each Availability Zone
- Security Group acts like virtual firewall, controlling the traffic which is allowed to reach and leave the resources associated with it.

AWS basics

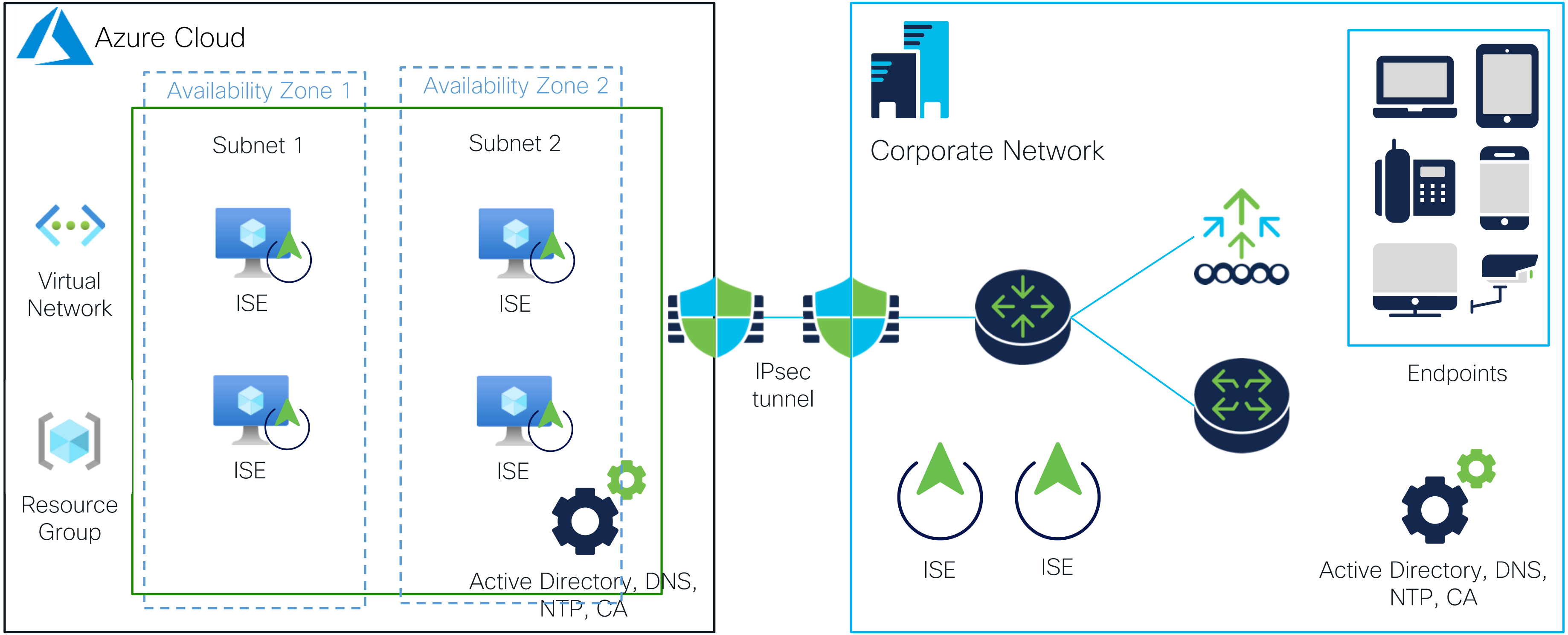
- To connect AWS resources to your Corporate network VPN tunnel can be used



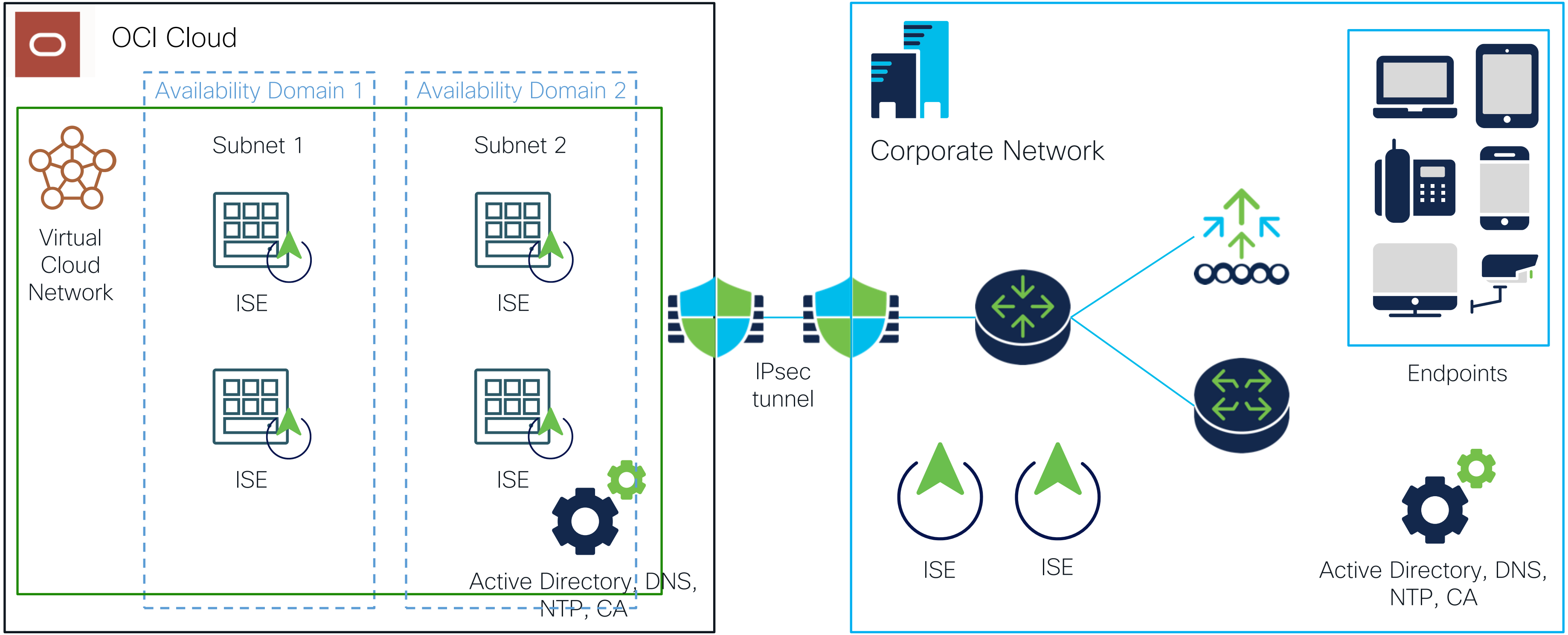
Design Scenarios - AWS



Design Scenarios - Azure



Design Scenarios - OCI



ISE in AWS

ISE Setup Options

AWS Marketplace

Amazon Elastic Compute Cloud (Amazon EC2)

AWS CloudFormation

Setup ISE Manually

ANSIBLE

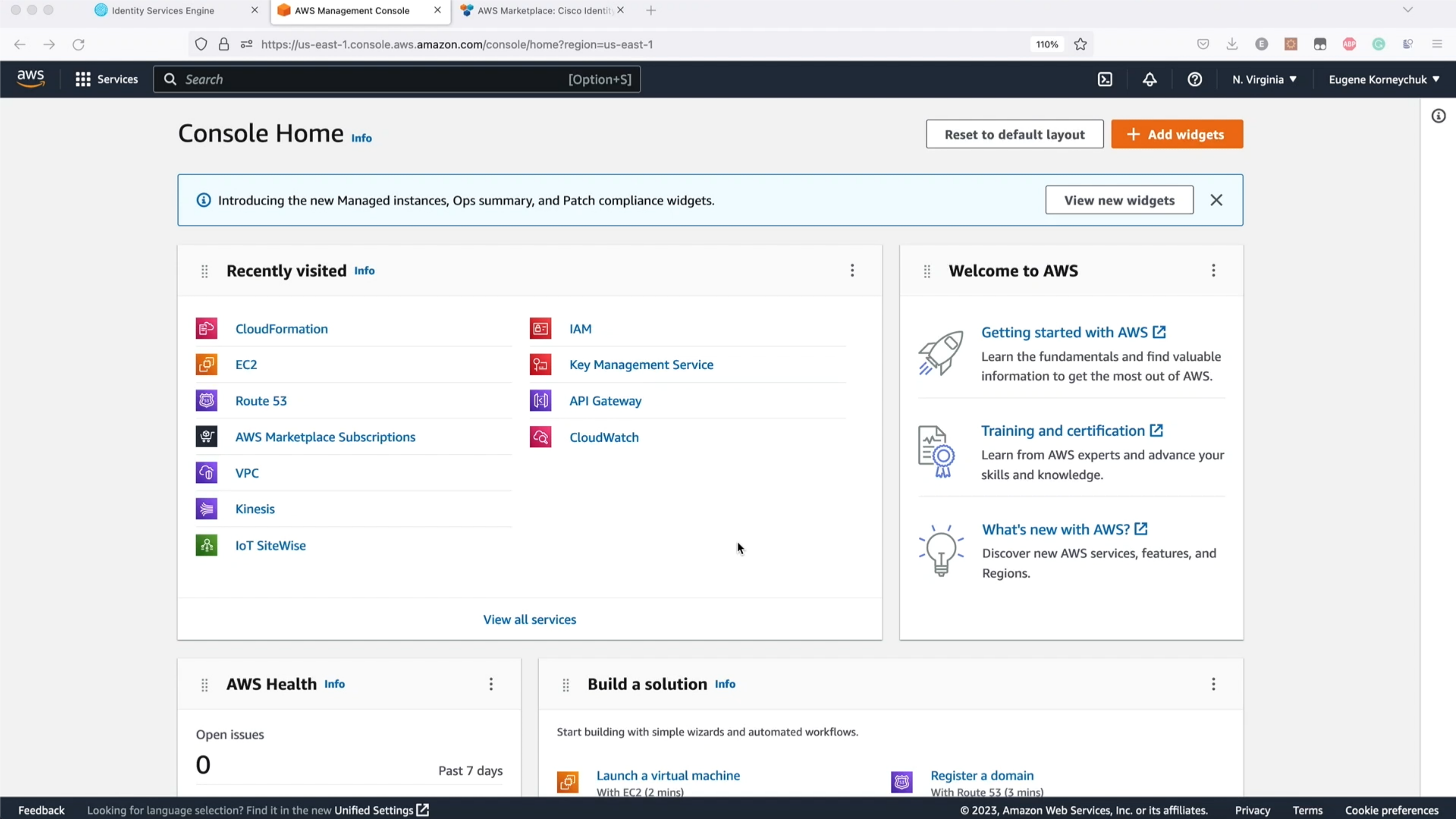
TERRAFORM

Automate ISE deployment

Checklist for ISE setup on AWS

1. Decide on Region and Availability Zone
2. Create a VPC and Subnet
3. Create a Security Group
4. Setup VPN between AWS and On-Prem Network
5. Create a Key Pair for SSH
6. Keep ISE setup information handy (hostname, DNS, Domain, NTP, Timezone, credentials)

Demo. ISE installation on AWS using CloudFormation



Console Home Info

Introducing the new Managed instances, Ops summary, and Patch compliance widgets.

Recently visited Info

- CloudFormation
- EC2
- Route 53
- AWS Marketplace Subscriptions
- VPC
- Kinesis
- IoT SiteWise
- IAM
- Key Management Service
- API Gateway
- CloudWatch

View all services

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

Open issues
0
Past 7 days

Build a solution Info

Start building with simple wizards and automated workflows.

Launch a virtual machine
With EC2 (2 mins)

Register a domain
With Route 53 (3 mins)

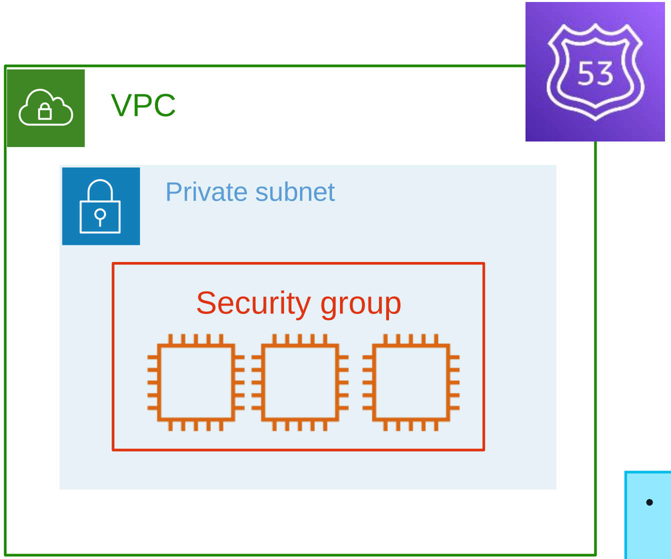
Feedback Looking for language selection? Find it in the new Unified Settings

© 2023, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

What if you would like to install whole infrastructure?

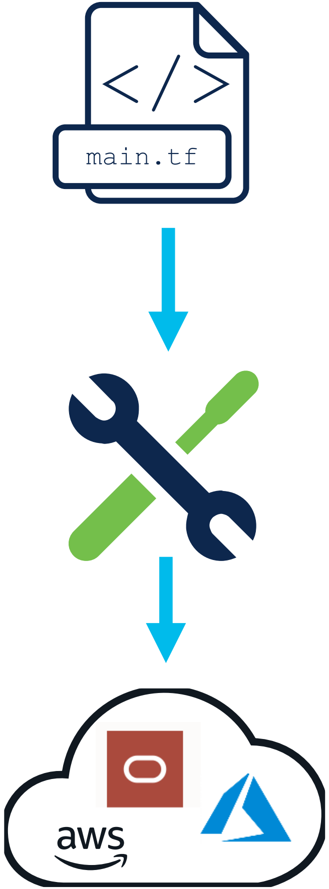
Terraform

- Infrastructure as a Code to automate the provisioning of your infrastructure resources



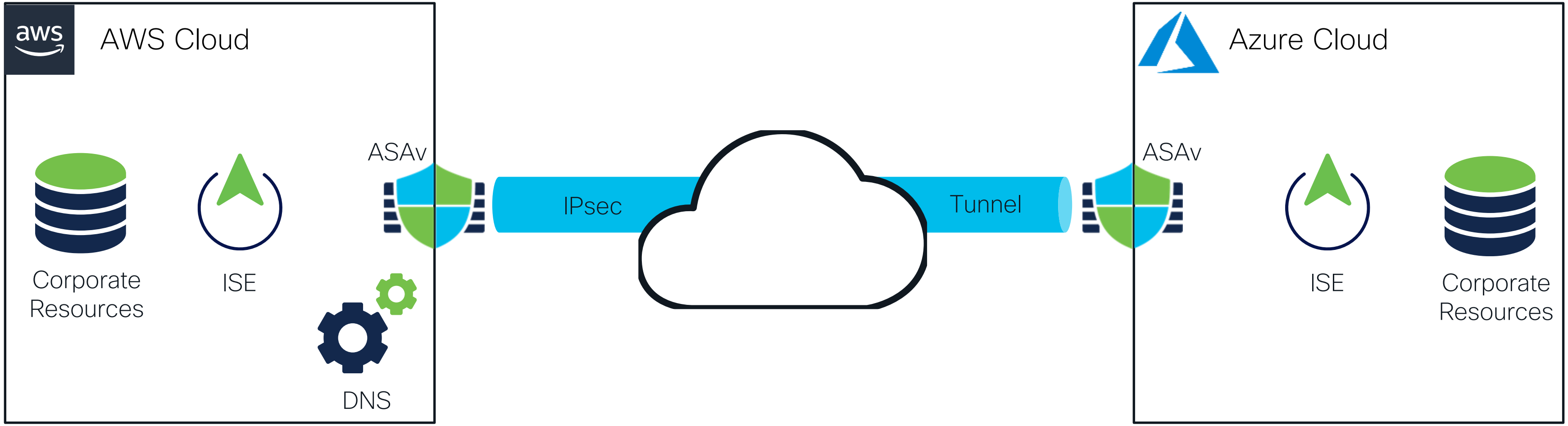
- Create VPC
- Create a Subnet
- Create Security Group
- Create EC2 Instances
- Create DNS records

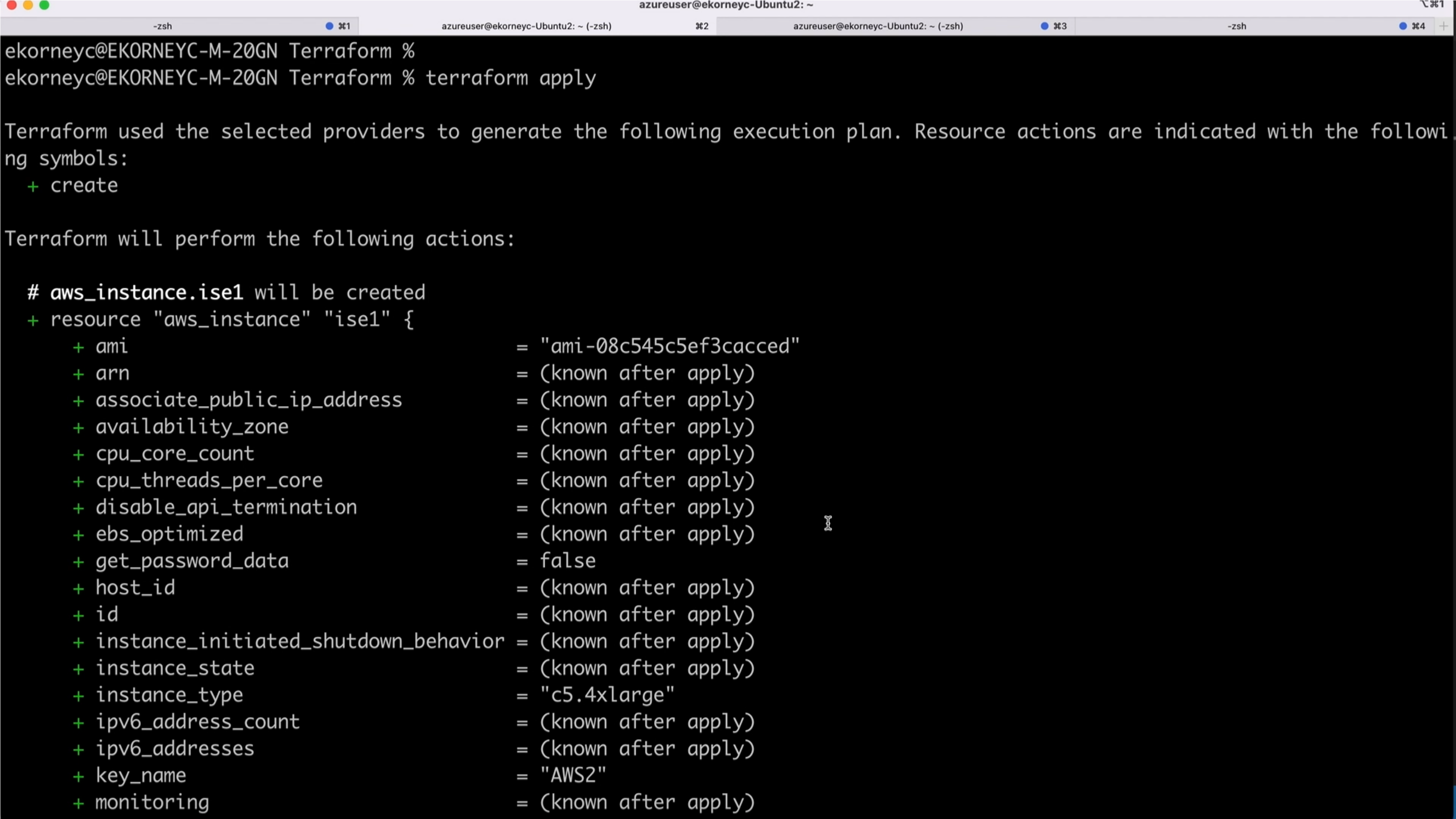
- Relies on the main.tf (terraform config) file to provision resources
- Terraform keeps the state of the infrastructure, compare the end result to what the current state is and provisions resources accordingly



Demo. ISE installation on AWS and Azure using Terraform

Deployment Topology




azureuser@ekorneyc-Ubuntu2: ~
⌥⌘1
-zsh ⌘1
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘2
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘3
-zsh ⌘4

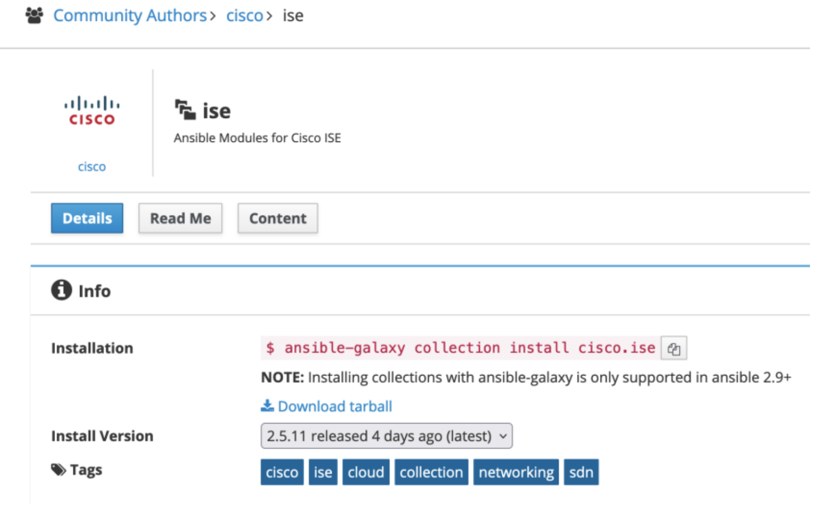
```
ekorneyc@EKORNEYC-M-20GN Terraform %
ekorneyc@EKORNEYC-M-20GN Terraform % terraform apply

Terraform used the selected providers to generate the following execution plan. Resource actions are indicated with the followi
ng symbols:
  + create

Terraform will perform the following actions:

  # aws_instance.ise1 will be created
  + resource "aws_instance" "ise1" {
      + ami                                  = "ami-08c545c5ef3cacced"
      + arn                                  = (known after apply)
      + associate_public_ip_address          = (known after apply)
      + availability_zone                    = (known after apply)
      + cpu_core_count                       = (known after apply)
      + cpu_threads_per_core                 = (known after apply)
      + disable_api_termination              = (known after apply)
      + ebs_optimized                        = (known after apply)
      + get_password_data                    = false
      + host_id                              = (known after apply)
      + id                                   = (known after apply)
      + instance_initiated_shutdown_behavior = (known after apply)
      + instance_state                       = (known after apply)
      + instance_type                        = "c5.4xlarge"
      + ipv6_address_count                   = (known after apply)
      + ipv6_addresses                       = (known after apply)
      + key_name                             = "AWS2"
      + monitoring                           = (known after apply)
```

That’s not it, you need to configure things…

Ansible

- Ansible playbooks are written in YAML
- Ansible playbooks consist of plays, which are sets of Tasks

galaxy.ansible.com



Community Authors > cisco > ise

cisco

ise

Ansible Modules for Cisco ISE

Info

Installation

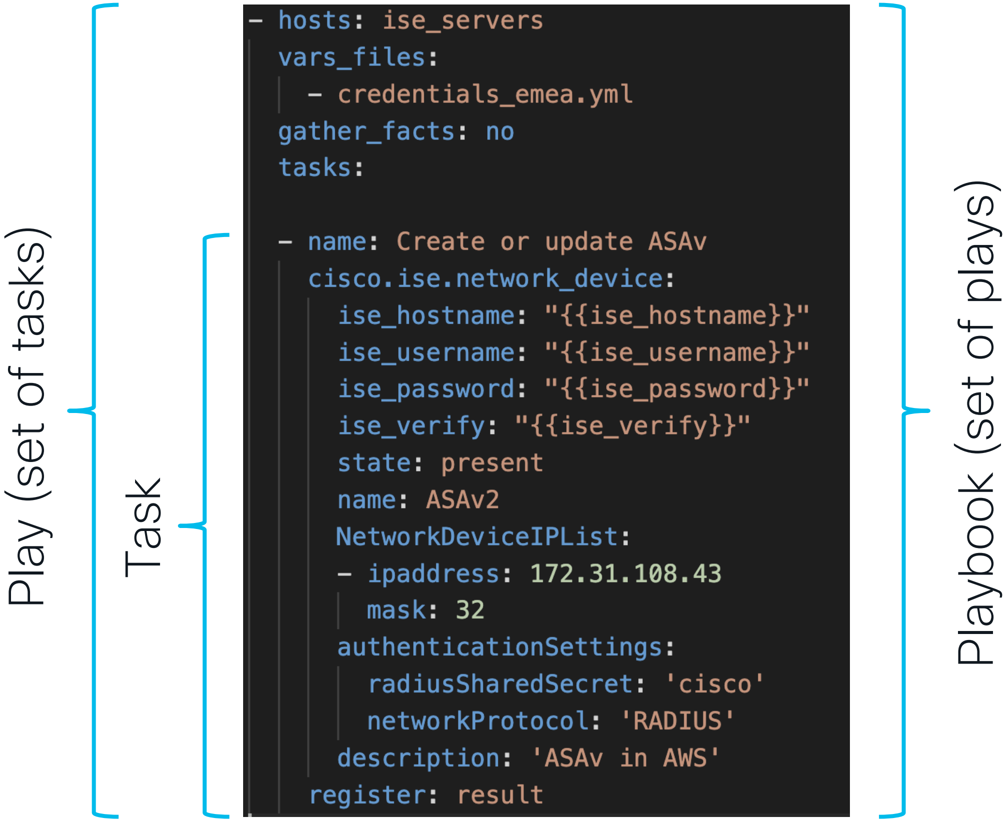
```
$ ansible-galaxy collection install cisco.ise
```

NOTE: Installing collections with ansible-galaxy is only supported in ansible 2.9+

Download tarball

Install Version: 2.5.11 released 4 days ago (latest)

Tags: cisco, ise, cloud, collection, networking, sdn



Play (set of tasks)

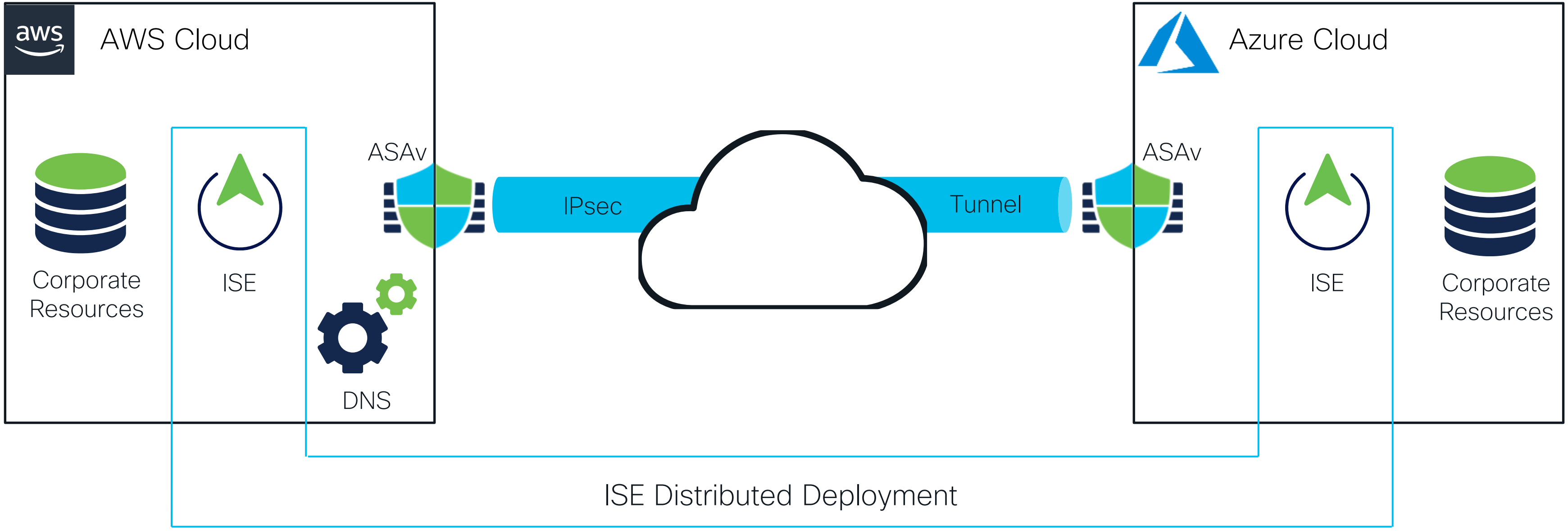
Task

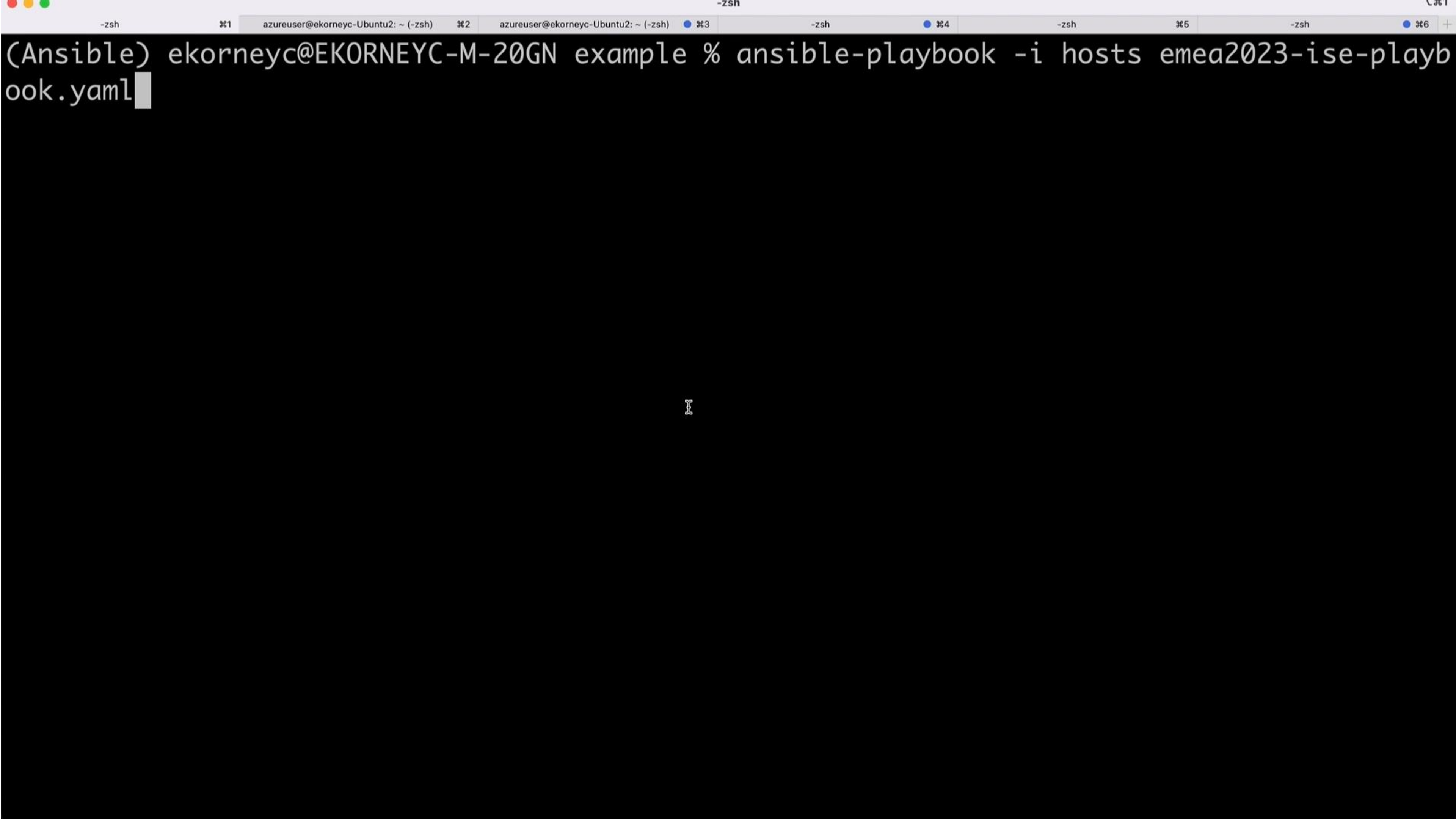
Playbook (set of plays)

```
- hosts: ise_servers
  vars_files:
    - credentials_emea.yml
  gather_facts: no
  tasks:

  - name: Create or update ASAv
    cisco.ise.network_device:
      ise_hostname: "{{ise_hostname}}"
      ise_username: "{{ise_username}}"
      ise_password: "{{ise_password}}"
      ise_verify: "{{ise_verify}}"
      state: present
      name: ASAv2
      NetworkDeviceIPList:
      - ipaddress: 172.31.108.43
        mask: 32
      authenticationSettings:
        radiusSharedSecret: 'cisco'
        networkProtocol: 'RADIUS'
      description: 'ASAv in AWS'
    register: result
```

Demo. ISE configuration using Ansible

Deployment Topology




-zsh
-zsh ⌘1
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘2
azureuser@ekorneyc-Ubuntu2: ~ (-zsh) ⌘3
-zsh ⌘4
-zsh ⌘5
-zsh ⌘6

```
(Ansible) ekorneyc@EKORNEYC-M-20GN example % ansible-playbook -i hosts emea2023-ise-playb
ook.yaml
```

AWS Partner Solution – Cisco ISE

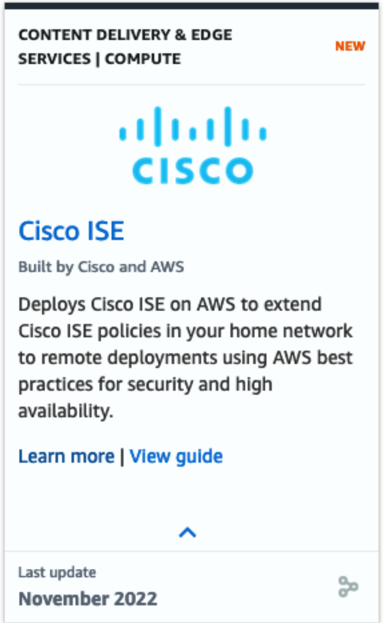
Partner Solutions Overview (formerly Quick Starts)

Automated Deployments built by Amazon Web Services solutions Architects and AWS Partners

Helps customers deploy popular technologies on AWS according to AWS Best Practices

Reduces hundreds of manual procedures into just few steps, so AWS customers can build production environments quickly

Automate deployments to the AWS Cloud



CONTENT DELIVERY & EDGE SERVICES | COMPUTE

NEW

CISCO

Cisco ISE

Built by Cisco and AWS

Deploys Cisco ISE on AWS to extend Cisco ISE policies in your home network to remote deployments using AWS best practices for security and high availability.

Learn more | View guide

Last update

November 2022

https://aws.amazon.com/quickstart/

Even more terminology

Route 53

DNS Web Service

EventBridge

Serverless Service which can receive events from applications and invoke AWS Lambda Function based on Rules

Systems Manager

Parameter Store provides a storage for configuration data

Amazon SNS

Managed Messaging Service

AWS Lambda

Runs code in response to events

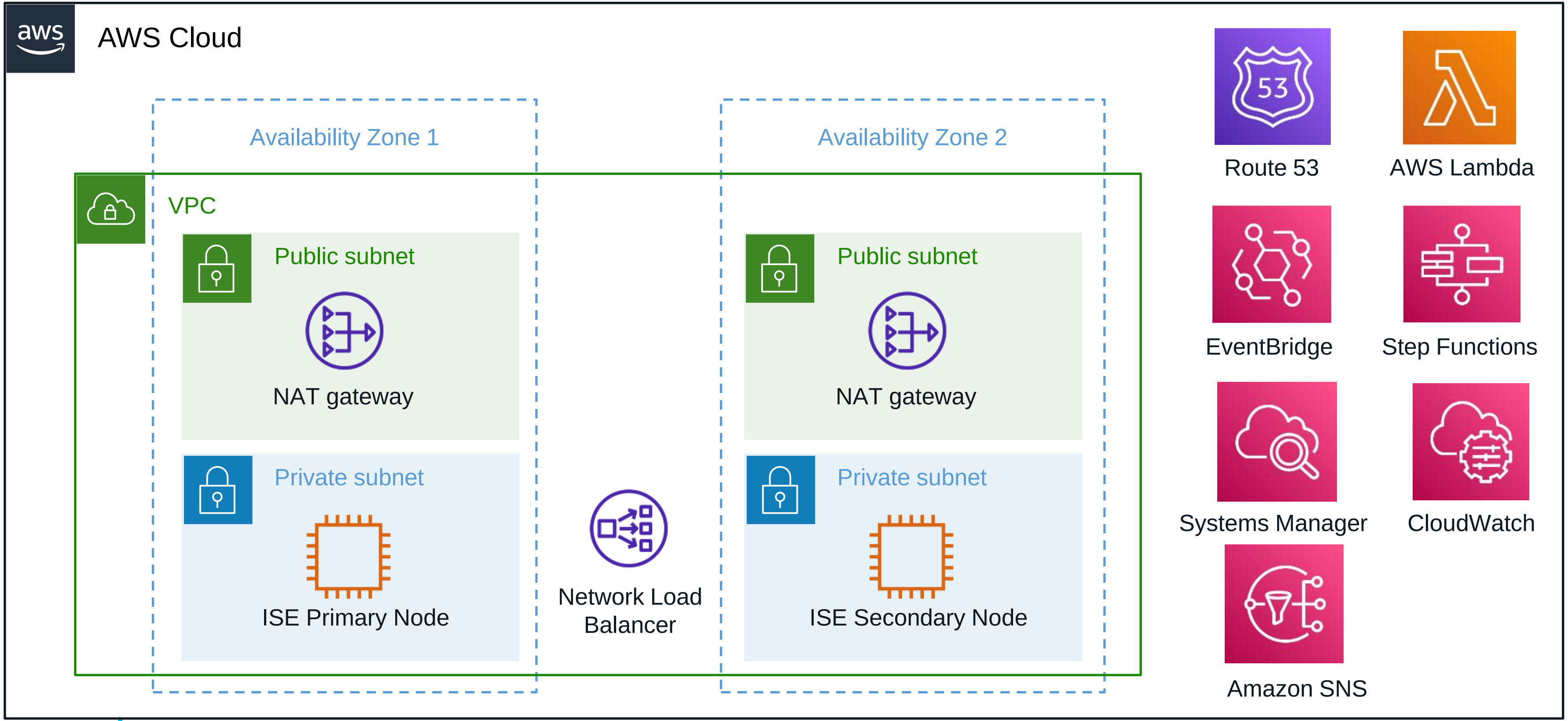
Step Functions

Orchestration for AWS services based on workflows

CloudWatch

Monitors application and takes automated actions

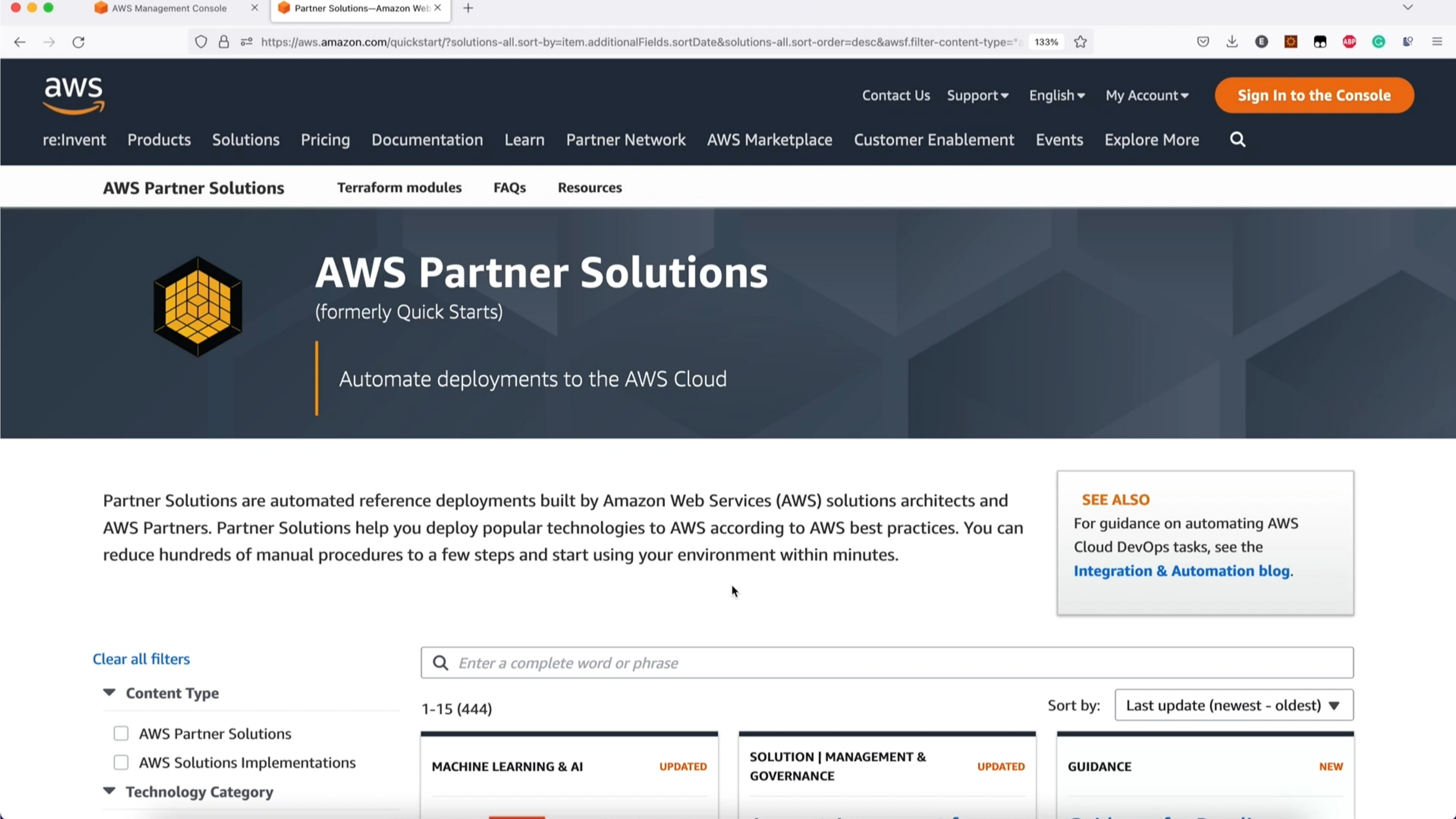
AWS Partner Solution – Cisco ISE Architecture



Implementation

Functionality	Amazon	Cisco
Create or leverage underlying network resources (VPC + Subnets + Routing)	✓	
Bring up ISE Instances (EC2)	✓	
Load Balancer (AWS ELB)	✓	
DNS (Route 53)	✓	
Form 2-node ISE deployment (Lambda + Step Functions + SSM Parameter store + SNS)		✓
Automatic PAN failover (CloudWatch + Lambda + Step Functions + SSM Parameter store + SNS)		✓
Health check Service (Event Bridge + Lambda + SNS)		✓

Demo. AWS Partner Solution – Cisco ISE



AWS Partner Solutions

(formerly Quick Starts)

Automate deployments to the AWS Cloud

Partner Solutions are automated reference deployments built by Amazon Web Services (AWS) solutions architects and AWS Partners. Partner Solutions help you deploy popular technologies to AWS according to AWS best practices. You can reduce hundreds of manual procedures to a few steps and start using your environment within minutes.

SEE ALSO

For guidance on automating AWS Cloud DevOps tasks, see the **Integration & Automation blog**.

1-15 (444)

Sort by: Last update (newest - oldest)

ISE in the Cloud. Design Considerations

- Upgrade workflow is not supported. Only fresh installs are supported. However, you can carry out backup and restore of configuration data

- SSH access to Cisco ISE CLI using password-based authentication is not supported. You can only access the Cisco ISE CLI through a key pair

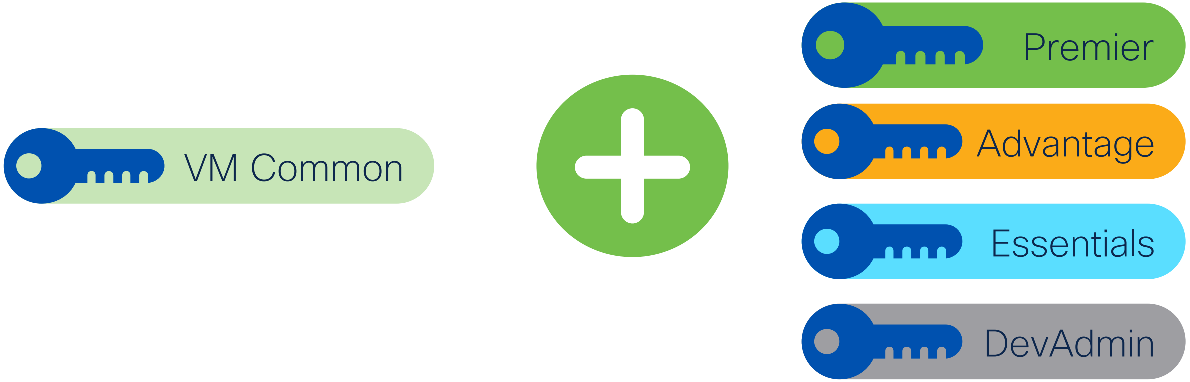
- Latency should be below 300 msec

- Starting ISE 3.2 default GUI username is “iseadmin”

ISE in the Cloud. Licensing

Cisco ISE leverages the Bring Your Own License (BYOL)

- ISE Comes with 90-days Evaluation License
- Use the Common VM License to enable Cisco ISE on cloud platforms, in addition to the other Cisco ISE licenses that you need for the Cisco ISE features you want to use.



VM Common

Premier

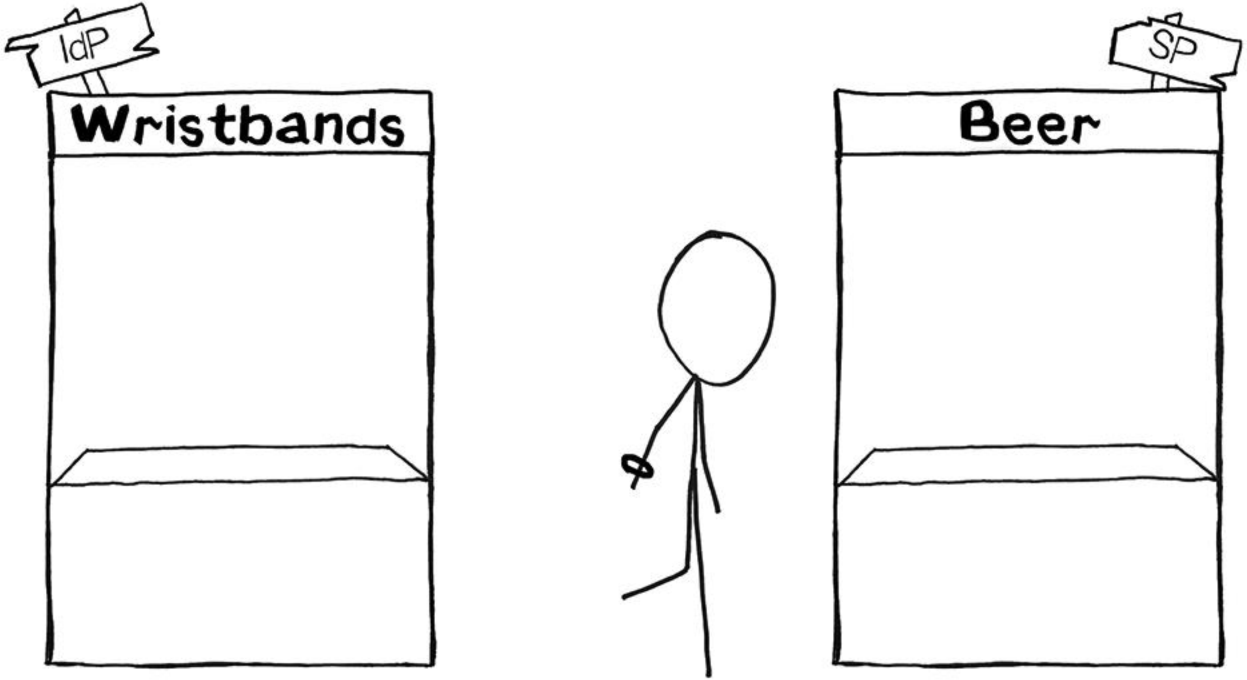
Advantage

Essentials

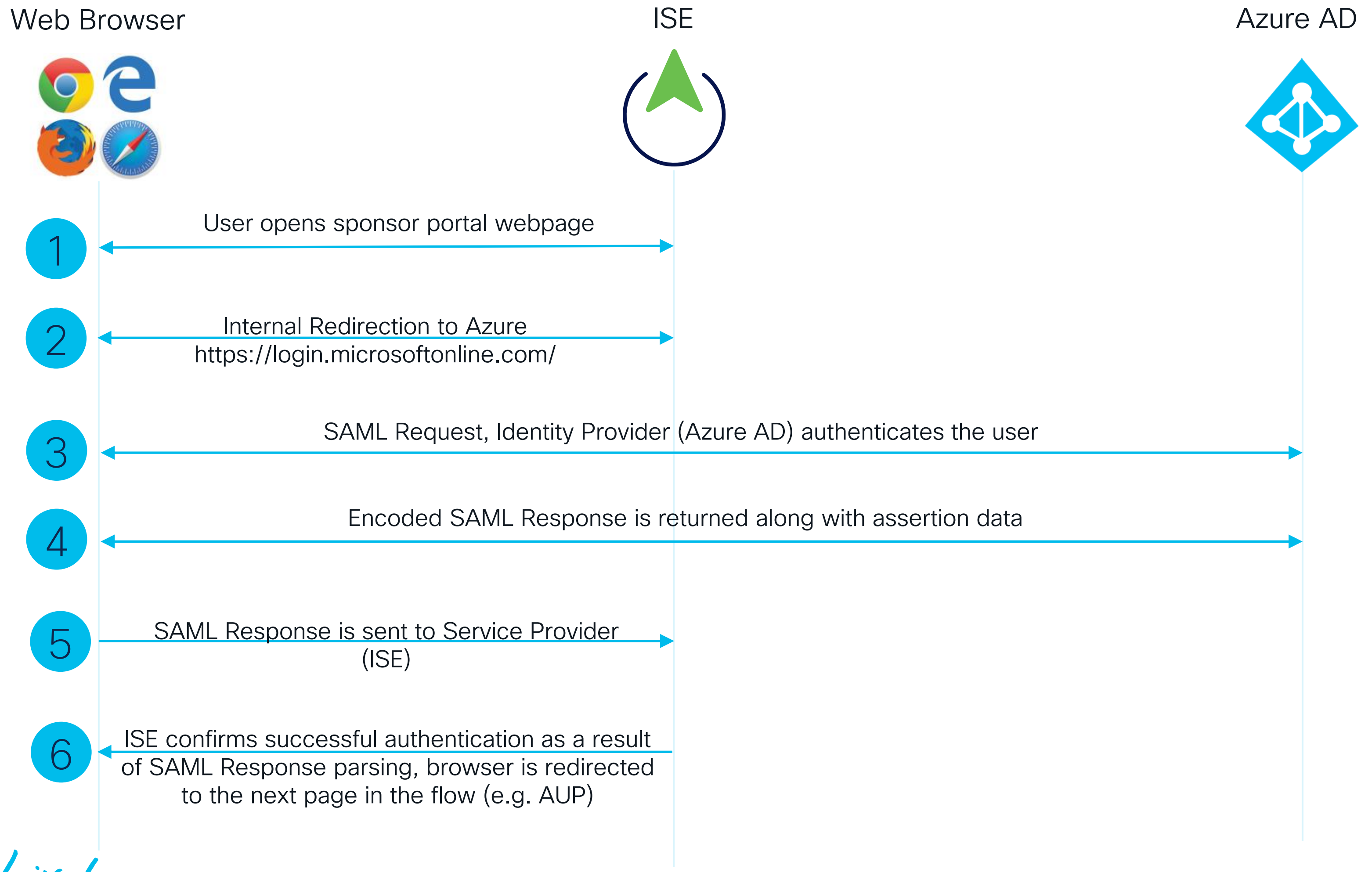
DevAdmin

ISE SAML SSO

What is SAML?



The Beer Drinker's Guide to SAML



1 User opens sponsor portal webpage

2 Internal Redirection to Azure https://login.microsoftonline.com/

3 SAML Request, Identity Provider (Azure AD) authenticates the user

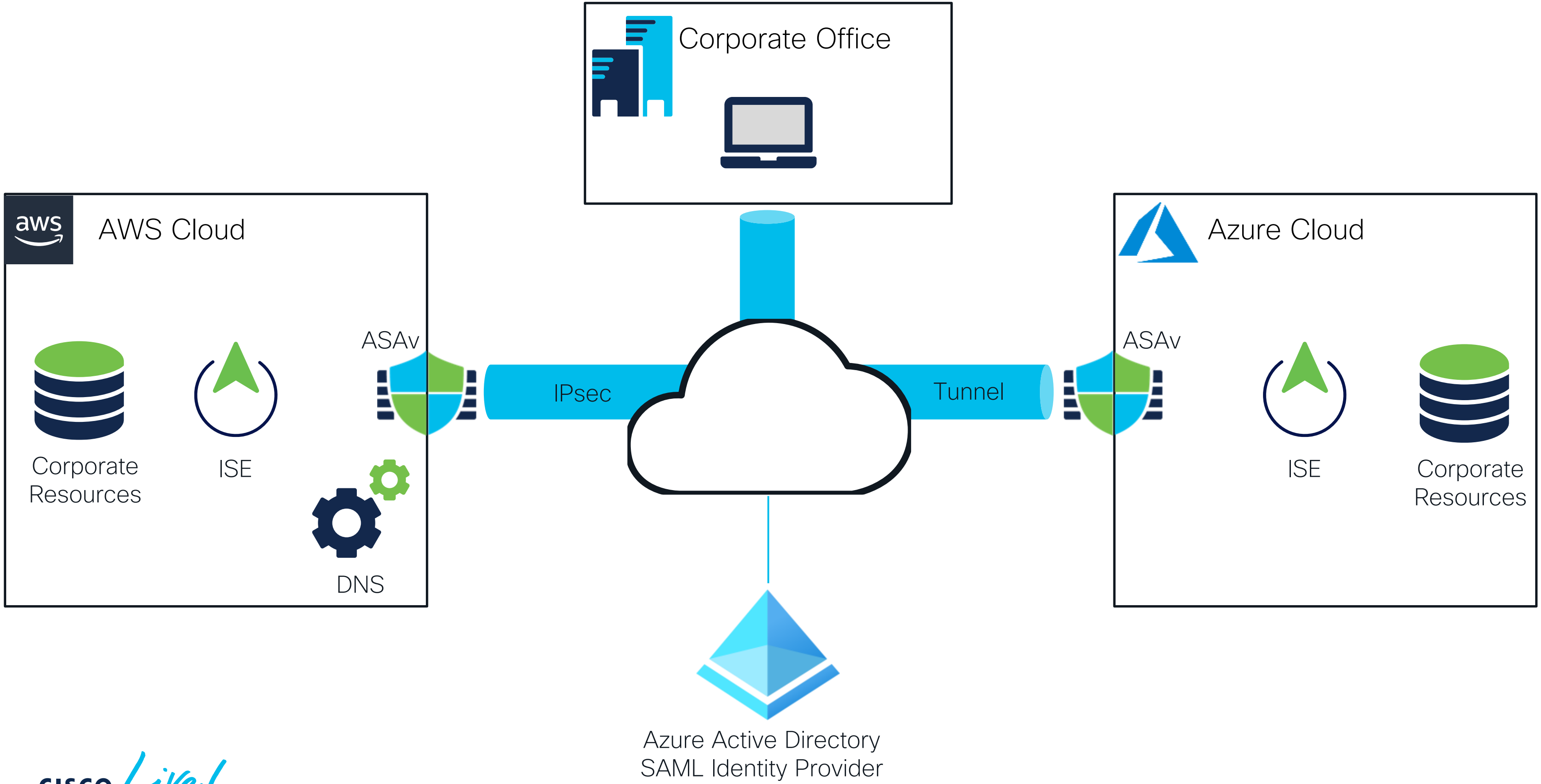
4 Encoded SAML Response is returned along with assertion data

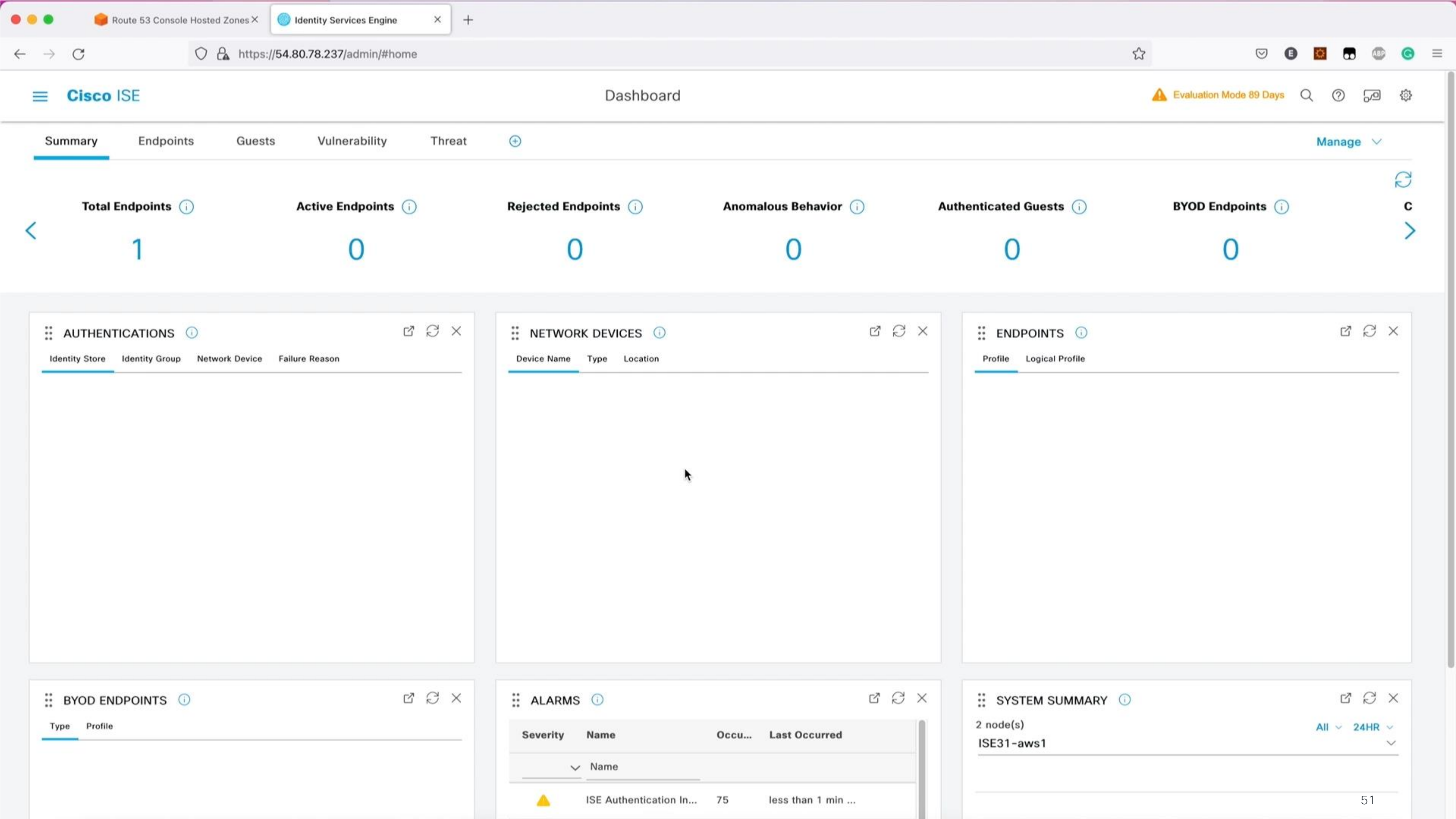
5 SAML Response is sent to Service Provider (ISE)

6 ISE confirms successful authentication as a result of SAML Response parsing, browser is redirected to the next page in the flow (e.g. AUP)

Demo. ISE Sponsor Portal Authentication with SAML

Deployment Topology





Dashboard

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests	BYOD Endpoints
1	0	0	0	0	0

AUTHENTICATIONS

Identity Store | Identity Group | Network Device | Failure Reason

NETWORK DEVICES

Device Name | Type | Location

ENDPOINTS

Profile | Logical Profile

BYOD ENDPOINTS

Type | Profile

ALARMS

Severity	Name	Occu...	Last Occurred
	Name		
⚠	ISE Authentication In...	75	less than 1 min ...

SYSTEM SUMMARY

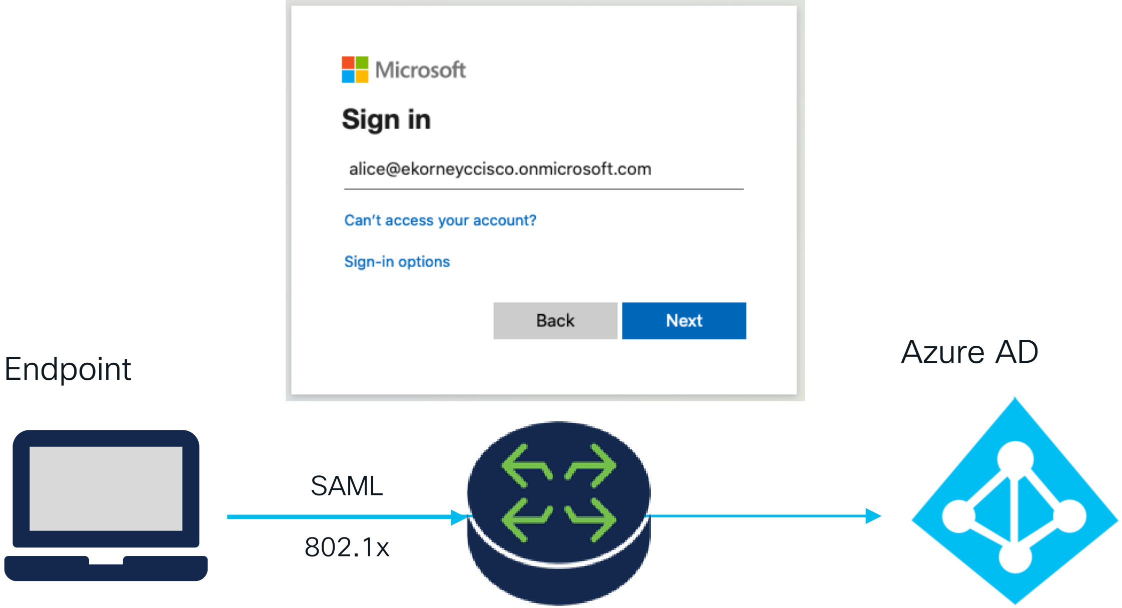
2 node(s)

All 24HR

ISE31-aws1

ISE Azure Active Directory Authentication

802.1x Authentication Problem with SAML



Microsoft

Sign in

alice@ekorneyccisco.onmicrosoft.com

Can't access your account?

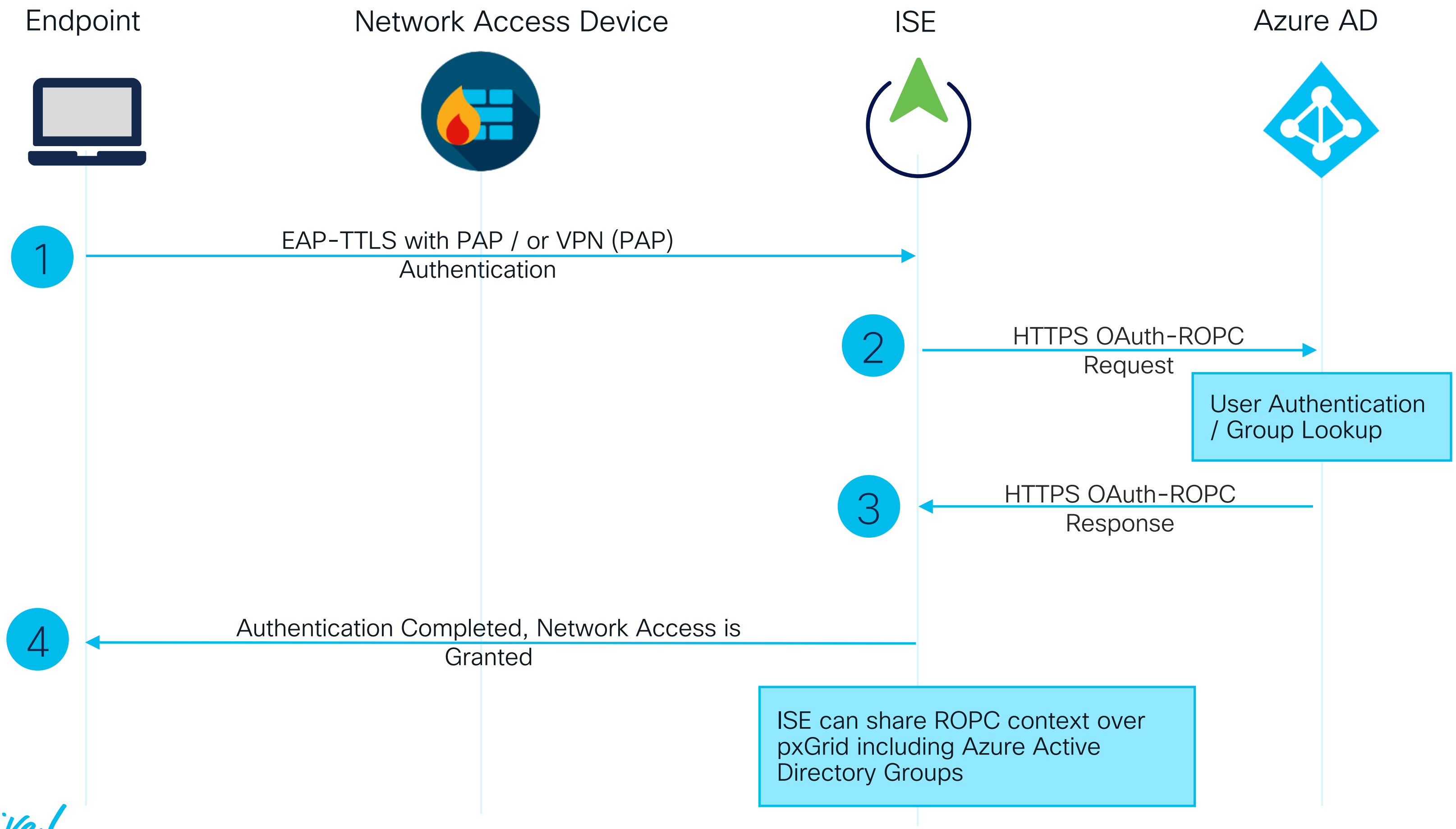
Sign-in options

SAML assumes network connectivity, so the Endpoint can reach Identity Provider

802.1x being a Layer 2 authentication protocol, will grants Network Access after Authentication is completed

No Access Before Authentication ✗

ROPC Flow Diagram



Endpoint

Network Access Device

ISE

Azure AD

1 EAP-TTLS with PAP / or VPN (PAP) Authentication

2 HTTPS OAuth-ROPC Request

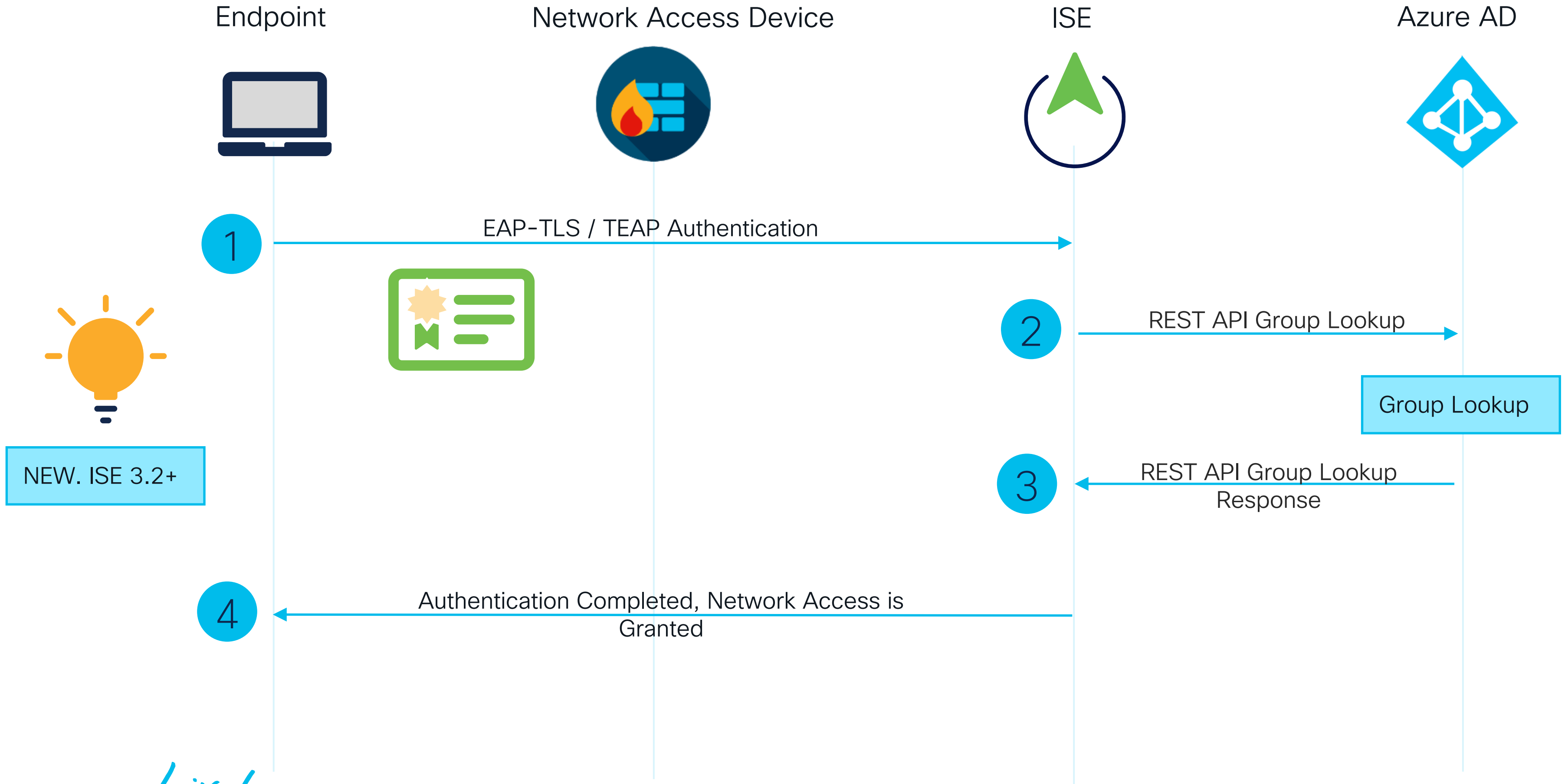
User Authentication / Group Lookup

3 HTTPS OAuth-ROPC Response

4 Authentication Completed, Network Access is Granted

ISE can share ROPC context over pxGrid including Azure Active Directory Groups

EAP-TLS Authorization with Azure Active Directory



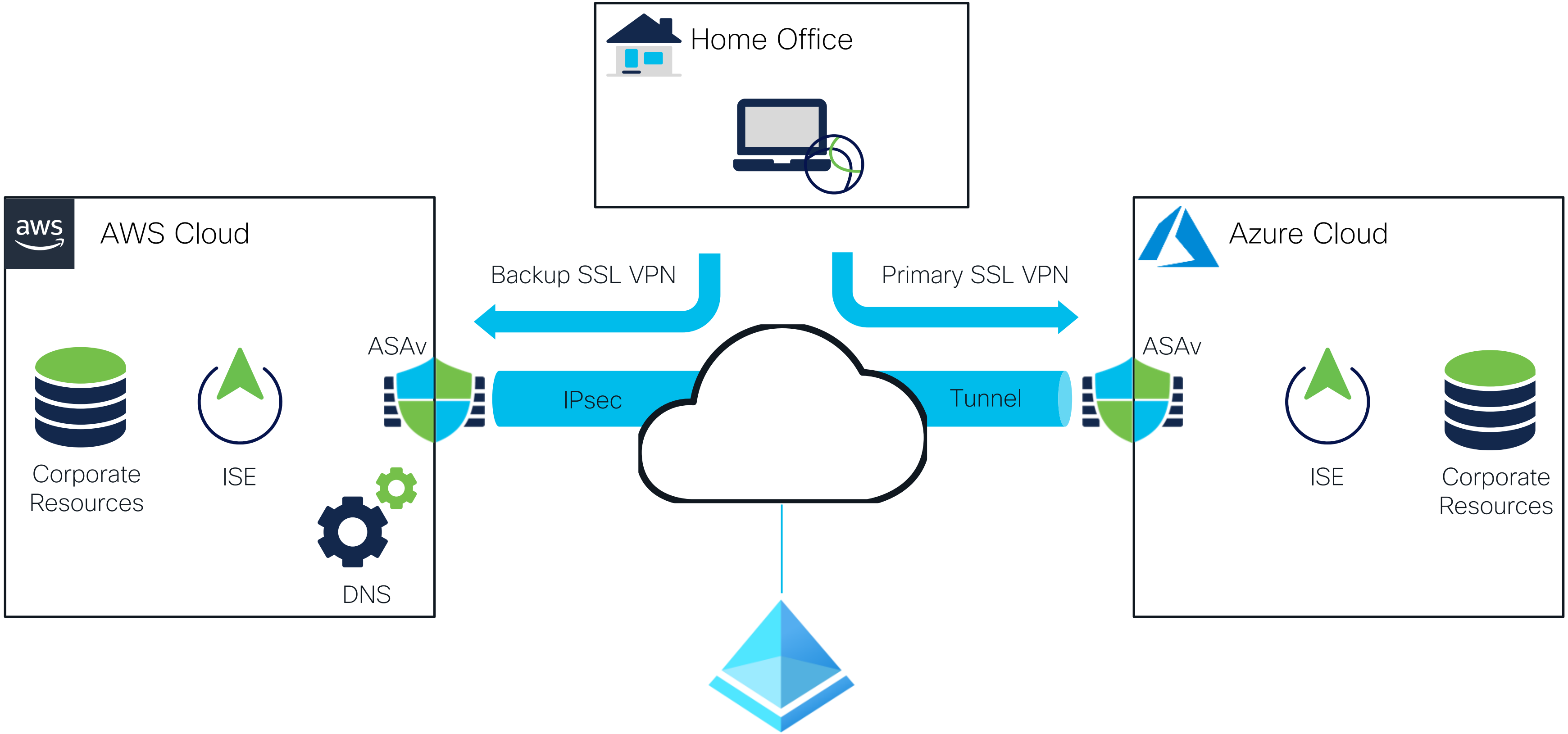
Endpoint
Network Access Device
ISE
Azure AD
1
EAP-TLS / TEAP Authentication
2
REST API Group Lookup
Group Lookup
3
REST API Group Lookup Response
NEW. ISE 3.2+
4
Authentication Completed, Network Access is Granted

ROPC Limitations

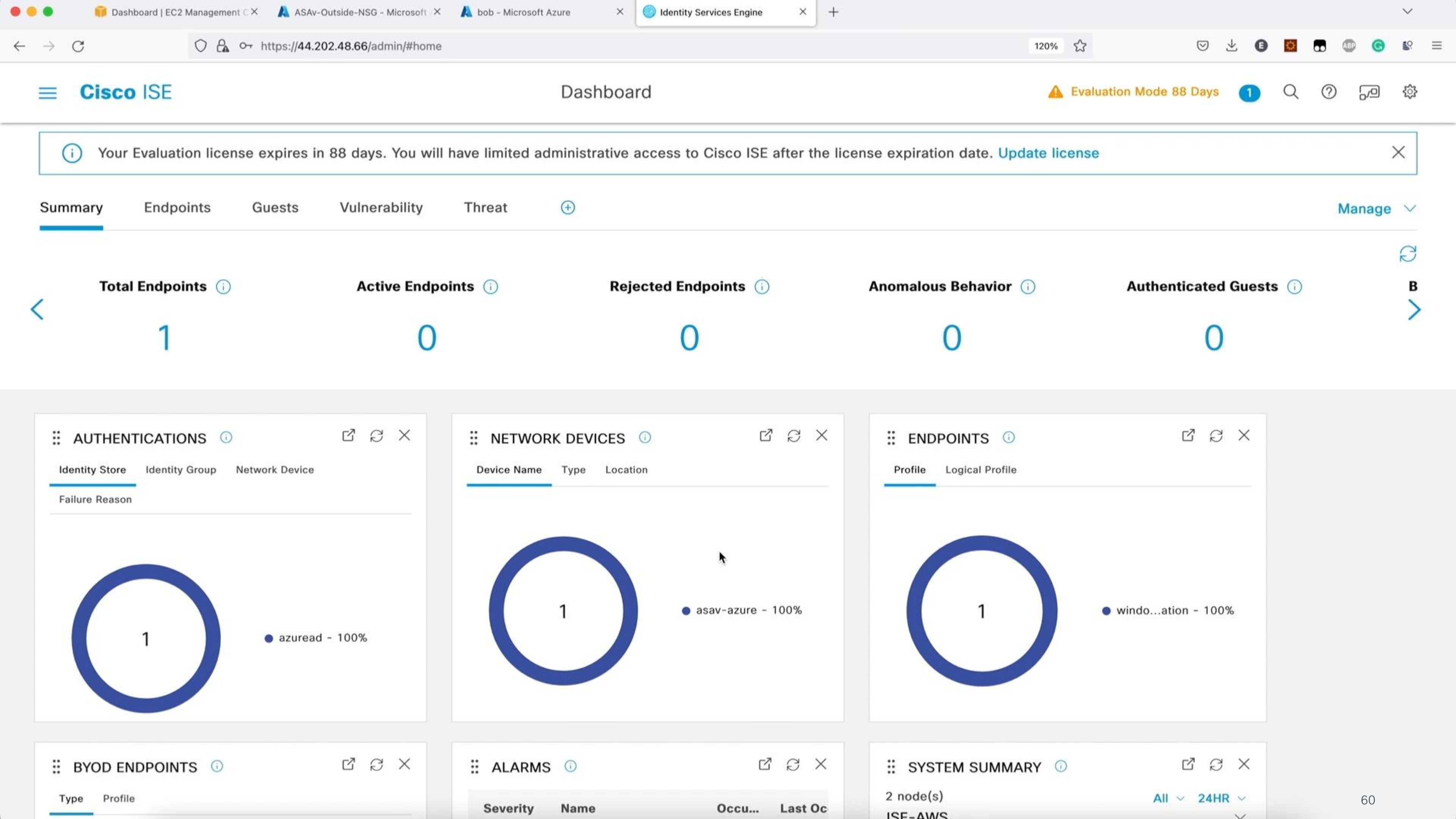
- No user interactions allowed for password changes, MFA, or AUPs
- No new accounts that have not yet changed the default password
- Azure AD tenants and accounts only. No invited personal accounts or federated IdPs like Microsoft, Google+, Twitter, AD-FS, Facebook
- Only user authentication is supported

Demo. Remote Access VPN Authentication with Azure Active Directory

Deployment Topology



Azure Active Directory External Identity Provider



https://44.202.48.66/admin/#home

Your Evaluation license expires in 88 days. You will have limited administrative access to Cisco ISE after the license expiration date. Update license

Total Endpoints	Active Endpoints	Rejected Endpoints	Anomalous Behavior	Authenticated Guests
1	0	0	0	0

AUTHENTICATIONS

1

● azuread - 100%

NETWORK DEVICES

1

● asav-azure - 100%

ENDPOINTS

1

● windo...ation - 100%

BYOD ENDPOINTS

ALARMS

SYSTEM SUMMARY

2 node(s)

Conclusion

Key Takeaways

- ISE can be deployed natively on AWS, Azure, OCI
- SAML SSO is available on ISE for Portals (Admin, Guest, Sponsor, etc.)
- 802.1X authentications, RA VPN authentications are possible with Azure Active Directory as an External Identity Store

Complete your Session Survey

- Please complete your session survey after each session. Your feedback is very important.
- Complete a minimum of 4 session surveys and the Overall Conference survey (open from Thursday) to receive your Cisco Live t-shirt.
- All surveys can be taken in the Cisco Events Mobile App or by logging in to the Session Catalog and clicking the "Attendee Dashboard" at https://www.ciscolive.com/emea/learn/sessions/session-catalog.html

Continue Your Education

- Visit the Cisco Showcase for related demos.
- Book your one-on-one Meet the Engineer meeting.
- Attend any of the related sessions at the DevNet, Capture the Flag, and Walk-in Labs zones.
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand.

Security Technologies

General Security Technologies

Learn about the different shades of cyber security in our daily lives and join us for a journey through various topics, from the depths of the darknet to the peak of crypto-analysis.

START

Feb 7 | 08:30
BRKSEC-2487
Cat and Mouse - Defender's need better Mousetraps!

Feb 7 | 10:00
BRKSEC-2727
6 Years of Supply Chain Attacks

Feb 7 | 11:30
BRKSEC-1240
If you don't have a Security Reference Architecture, you must get one!

Feb 7 | 11:30
BRKSEC-2037
Securing Starlink Internet Services

Feb 7 | 12:20
PSOSEC-1213
The Evolution of Ransomware

Feb 7 | 13:30
BRKSEC-2354
Automating Security: Just Because You Can, Doesn't Mean You Should

Feb 7 | 14:00
IBOSEC-3000
Critical Requirements for Securing Government Networks

Feb 7 | 15:00
BRKSEC-2051
The Evolution of DNS Security

Feb 7 | 17:15
IBOSEC-2012
Ransomware Role-Playing: A Guided Tabletop Exercise with Talos Incident Response

Feb 8 | 08:45
BRKSEC-2227
Evaluating and Improving Defenses With MITRE ATT&CK

Feb 8 | 10:45
BRKSEC-2172
Peeling an Onion: A Short Travel into the Darknet

If you are unable to attend a live session, you can watch it On Demand after the event

Security Technologies

Zero Trust

Learn how Cisco will help you deploy a broad range of technologies in order to deploy your end to end Zero Trust strategy.

START

Feb 5 | 16:00
LABSEC-2089
Multi-factor Authentication: Integration of DUO with ISE for MFA

Feb 6 | 08:45
TECSEC-2007
Find Your Zen with Cisco Secure Workload for Zero Trust Segmentation

Feb 6 | 08:45
TECSEC-2781
Zero Trust: From understanding the risks to architecting a practical solution

Feb 6 | 15:20
PSOSEC-1210
A global view on Zero-Trust - mapping your business resilience requirements

Feb 7 | 08:45
BRKSEC-2445
The Art of ISE Posture, Configuration and Troubleshooting

Feb 7 | 16:45
BRKSEC-2053
Zero Trust: Securing the Evolving Workplace

Feb 7 | 17:00
BRKSEC-1139
Application Security - The Final Frontier

Feb 8 | 10:45
BRKSEC-2096
Securing Industrial Networks: Where do I start?

Feb 8 | 13:30
BRKSEC-2748
Taking Authentication to the Next Level with Cisco Secure Access by Duo

Feb 8 | 17:00
BRKSEC-2123
Solving the Segmentation Puzzle! Secure Workload and Secure Firewall Integration

If you are unable to attend a live session, you can watch it On Demand after the event

CISCO Live!

The bridge to possible

Thank you

cisco Live!

ALL IN