

CISCO *Live!*

PALESTINE

#CiscoLive



# ISE Deployments in the Cloud

Automate ISE Deployments in AWS

Jesse Dubois

Patrick Lloyd, Senior Security Solutions Architect, CX Customer  
Delivery  
LTRSEC-2000



#CiscoLive

# 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

Webex spaces will be moderated by the speaker until June 17, 2022.



#CiscoLive LTRSEC-2000

The screenshot shows a mobile application interface for a session titled "Catalyst 9000 Series Switching Family". The screen includes the following information:

- Speaker(s): Kenny Lei, Cisco Systems, Inc. | Technical Market...
- Categories: Intermediate (596)
- Tracks: Networking (220)
- Session Type: Breakout (453)
- Show 2 more
- Webex
- Join the Discussion (highlighted with a blue oval)
- Notes: Enter your personal notes here

A blue horizontal line with a dot at its midpoint connects the "Join the Discussion" button to the "How" section above it. A blue circle is positioned near the bottom center of the phone icon.

<https://cislive.ciscoevents.com/cislivebot/#LTRSEC-2000>

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public



# Agenda

- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion

# Agenda

- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion



# About Patrick Lloyd

- name: Patrick Lloyd

Details.patricklloyd:

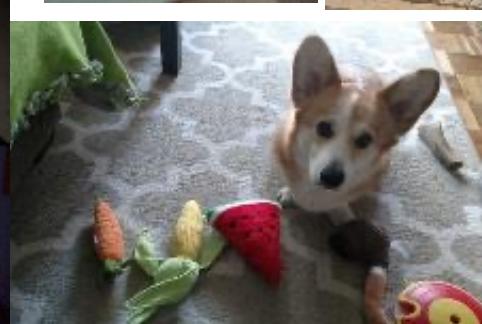
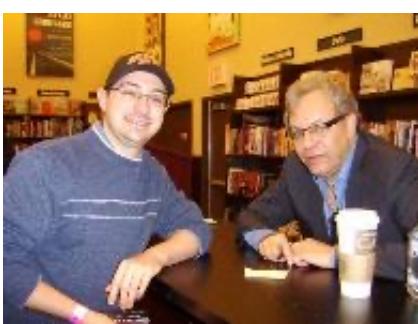
Location: Raleigh, NC

Interests: Technology, Brewing

Pets: Luna the Corgi

Travel: All over the world

Fun Fact: New home owner



# About Jesse Dubois

- name: Jesse Dubois

Details.jessedubois:

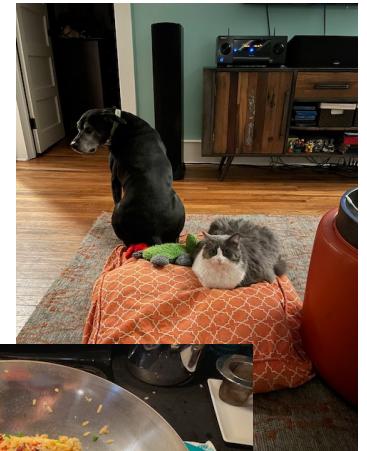
Location: Durham, North Carolina

Interests: Brewing, Golf, Cooking

Pets: Dunkel, Apollo, Comet, Calypso

Travel: Lots

Fun Fact: Squirrels in your attic are not fun.



# Agenda

- Introduction
- **Overview: ISE in AWS**
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion



# ISE 3.1 Release Highlights

SAML SSO for admin login

ISE deployment on AWS

APIs for system and policy management

Random & Changing MAC address

Zero-touch provisioning

Streamlined upgrade experience

Enhanced audit logs

Endpoint Remediation Scripts

Linux posture

Posture bi-directional trigger

Enhanced posture discovery

Authentication Dashboard Alarms

Active Directory DC failover enhancement

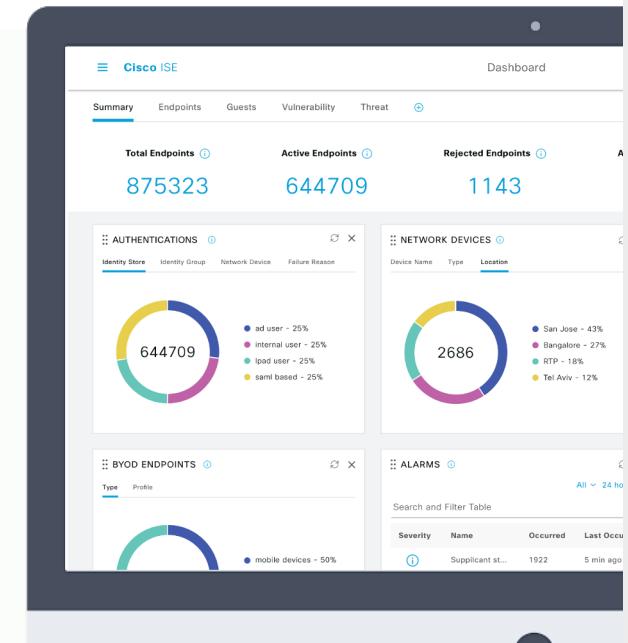
Context visibility import/export

Prevent AD account lockout

RADIUS CoA Proxy

Seamless EA integration

Logical profile dashlet



cisco *Live!*

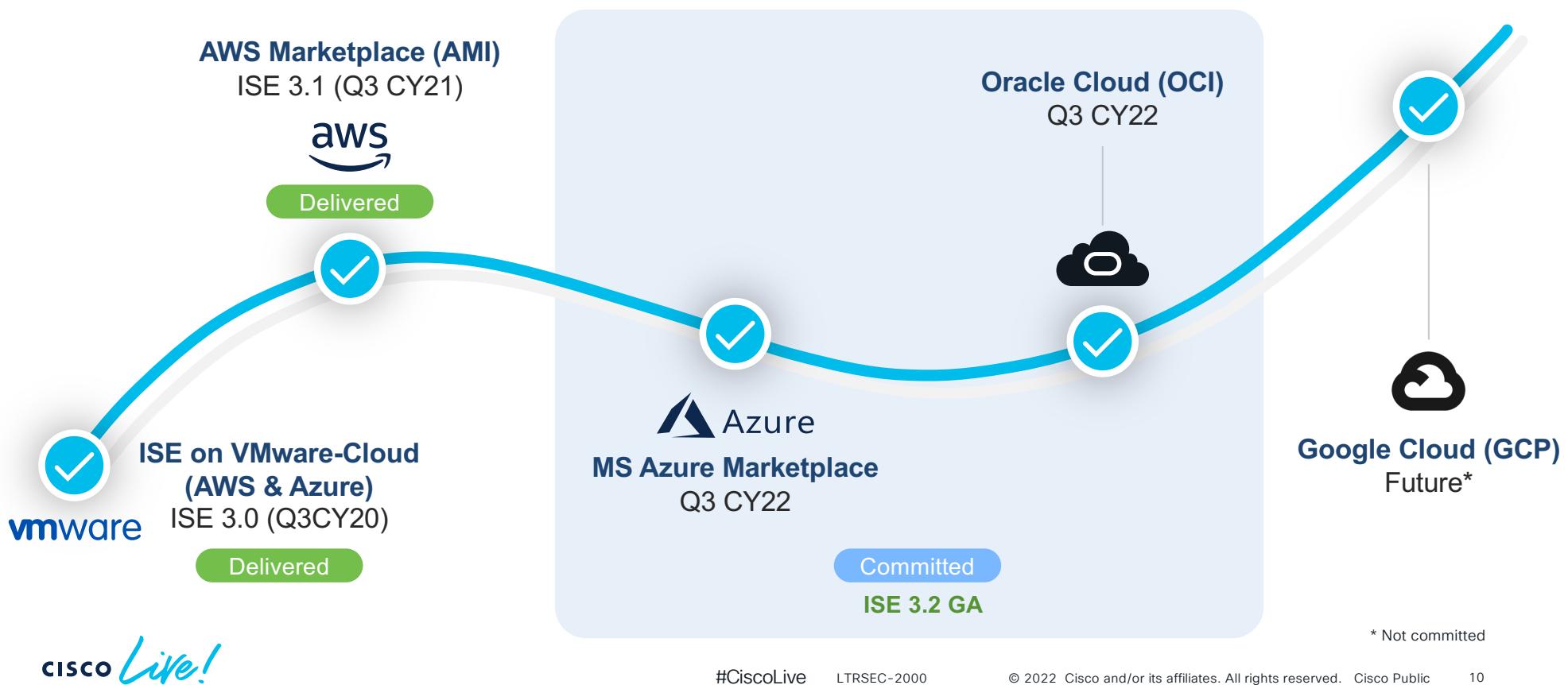
[cs.co/ise-webinars](https://cs.co/ise-webinars)

#CiscoLive

LTRSEC-2000

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

# ISE journey on public cloud



cisco *Live!*

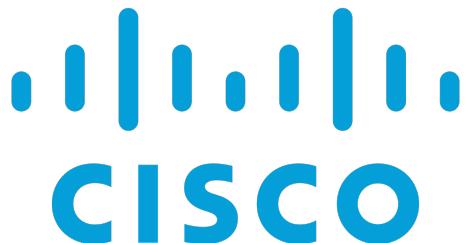
#CiscoLive

LTRSEC-2000

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

10

# Zero Touch Provisioning



SNS Appliances  
w/ CIMC

ESXi

AWS

Use configuration  
ISO/IMG file mount

Native APIs

CIMC – Cisco Integrated Management Controller

# ISE Architecture

## Standalone ISE



### Policy Administration Node (PAN)

- Single plane of glass for ISE admin
- Replication hub for all config changes



### Monitoring & Troubleshooting Node (MnT)

- Reporting and logging node
- Syslog collector from ISE Nodes



### Policy Services Node (PSN)

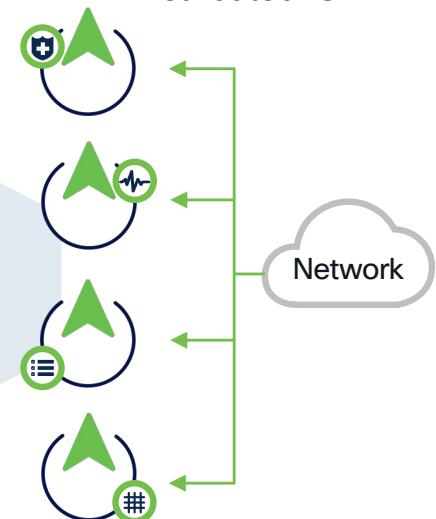
- Makes policy decisions
- RADIUS / TACACS+ Servers



### pxGrid Controller

- Facilitates sharing of context

## Distributed ISE



Single Node (Virtual/Appliance)



Multiple Nodes (Virtual/Appliance)

Up to **20,000** concurrent endpoints

**3500**

Up to **500,000** concurrent endpoints

Up to **50,000** concurrent endpoints

**3600**

Up to **2,000,000** concurrent endpoints

# ISE 3.1 Supported AWS Platforms



AWS Instance Type	Standalone Sessions	PSN Sessions	PAN/MNT Total Sessions	Cores	Memory	Disk
c5.4xlarge	10,000	40,000	-	16	32 GB	300 GB – 2.4 TB
c5.9xlarge	25,000	100,000	-	36	72 GB	300 GB – 2.4 TB
m5.4xlarge	-	-	500,000	16	64 GB	300 GB – 2.4 TB

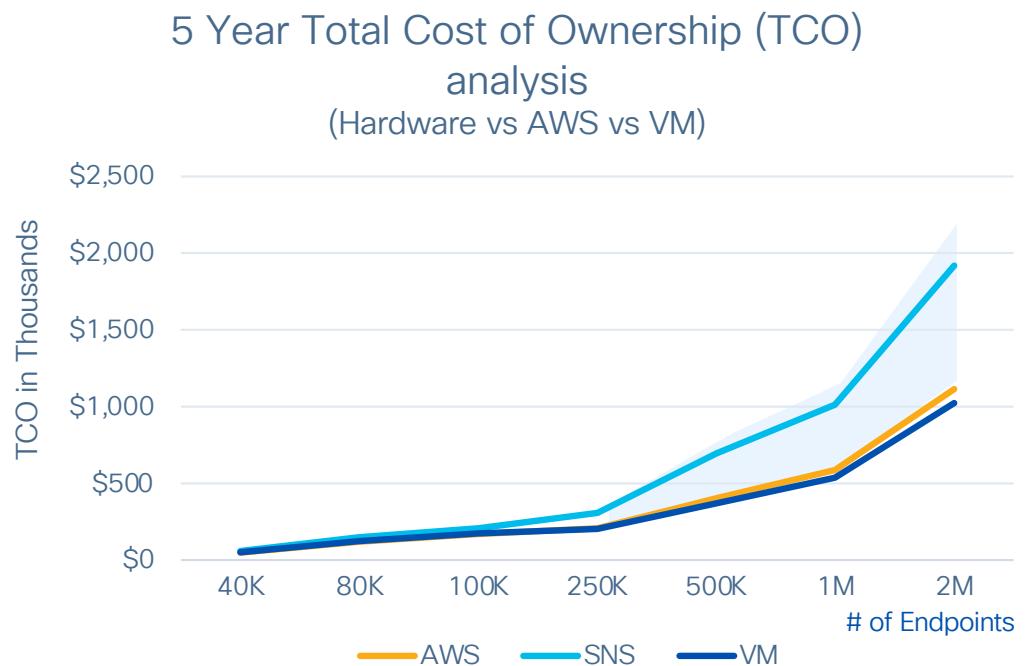
# ISE on AWS TCO

## Discount Assumptions

- Hardware and VM appliance/solution support with 65% discount.
- AWS costing is calculated for 3 years reserved EC2 and all upfront pay.

## Conclusion

- AWS is significantly cheaper than hardware for S/M/L deployments.
- AWS marginally costlier than VM deployments for larger deployments.



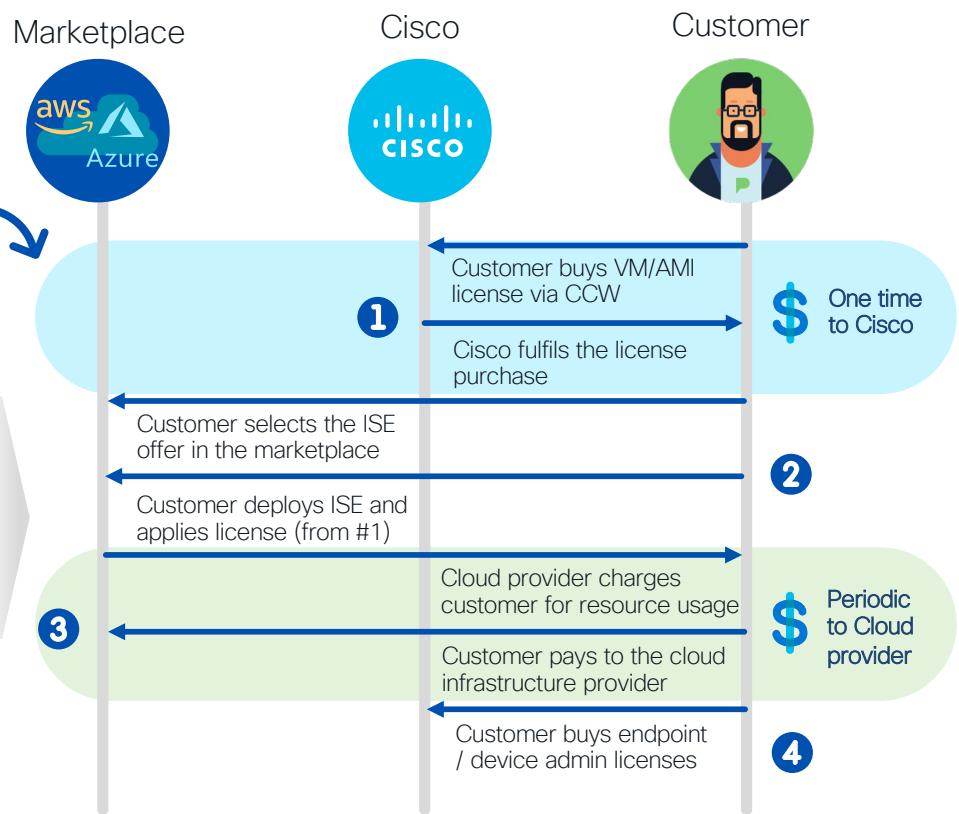
# ISE Cloud Instance Buying Experience

Flexibility to move from virtual appliances to AWS/Azure without license transaction.

The screenshot shows the AWS Marketplace interface for the Cisco Identity Services Engine (ISE) - BYOL. It includes sections for Overview, Pricing, Usage, Support, and Reviews. The Usage section provides a breakdown of costs for different EC2 instance types and software usage. A note at the bottom states: "BYOL Available for customers with current licenses purchased via other channels."

BYOL – Bring Your Own License  
Customer will purchase VM license from Cisco and use it in either in VM or Cloud IaaS.

**CISCO Live!**



# ISE Setup Options



AWS Marketplace



AWS CloudFormation  
Template



Amazon Elastic Compute  
Cloud AMI (Amazon  
Machine Image)



ANSIBLE  
Infrastructure as Code  
(IoC) tools



TERRAFORM



Cisco MSX (Managed  
Services Accelerator)

Bring up ISE node  
one at a time

Bring up multiple ISE  
nodes at the same  
time\*

\* Initial release of ISE + MSX will be single node only

## ISE APIs



New in  
ISE 3.1

OpenAPIs

configuration



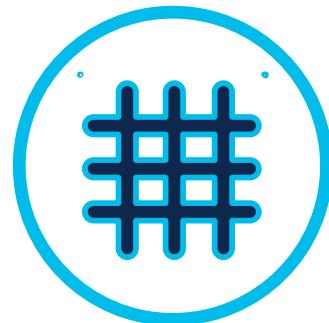
ERS

configuration



MNT

sessions



pxGrid

asynchronous  
endpoint  
context

cisco *Live!*



[cs.co/ise-api](https://cs.co/ise-api)

#CiscoLive

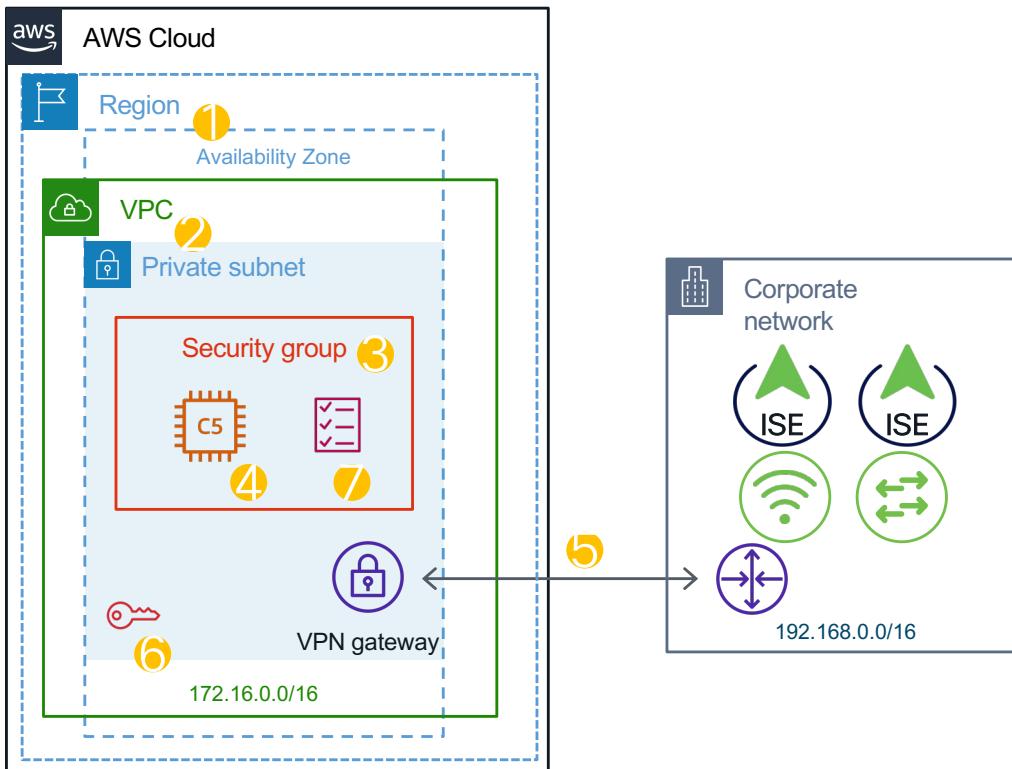
LTRSEC-2000



[github.com/  
cisco-pxgrid/pxgrid-rest-  
ws](https://github.com/cisco-pxgrid/pxgrid-rest-ws)

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

# ISE Installation Prerequisites



1. Decide on Region and Availability zones
2. Create VPC & Subnet
3. Create Security Group
4. Decide on Instance Type
5. Setup VPN between AWS and on-prem network
6. Create Key pair for SSH
7. Collect ISE setup information: hostname, domain, DNS, NTP, Timezone, Admin credentials

# Agenda

- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion



## {JSON}

```
{  
  "object": {  
    "hostname": "ise.securitydemo.net",  
    "port": 443,  
    "auth": {  
      "username": "admin",  
      "password": "C1sco12345"  
    },  
    "verify": true  
  }  
}
```

cisco *Live!*

## YAML

```
---  
object:  
  hostname: ise.securitydemo.net  
  port: 443  
  auth:  
    username: admin  
    password: C1sco12345  
  verify: true  
  
# YAML supports Comments!!!
```



# ANSIBLE

Simple	Flexible	Agentless
<ul style="list-style-type: none"><li>• human-readable</li><li>• declarative configs</li><li>• ordered tasks</li><li>• no coding required</li><li>• start small and scale</li></ul>	<ul style="list-style-type: none"><li>• config management</li><li>• workstations</li><li>• servers / containers</li><li>• applications</li><li>• networks</li><li>• security services</li><li>• workflows</li></ul>	<ul style="list-style-type: none"><li>• SSH (Linux, macOS)</li><li>• REST (ISE)</li><li>• WinRM (Windows)</li><li>• others as needed</li><li>• efficient</li><li>• secure</li></ul>



# Terminology



galaxy.ansible.com

## Collections



cisco.ios.\*

...



cisco.ise.\*



endpoint

## Modules



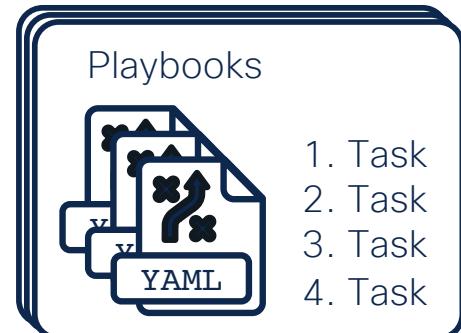
network\_device



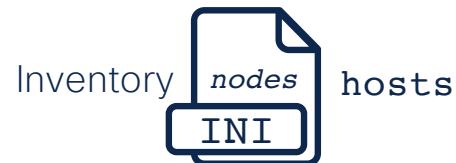
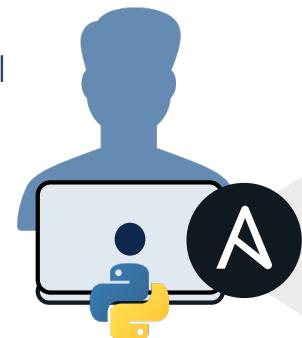
...

**cisco** *Live!*

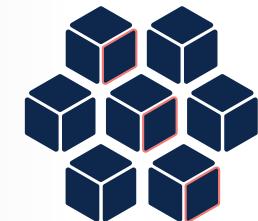
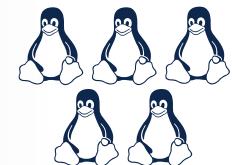
## Roles



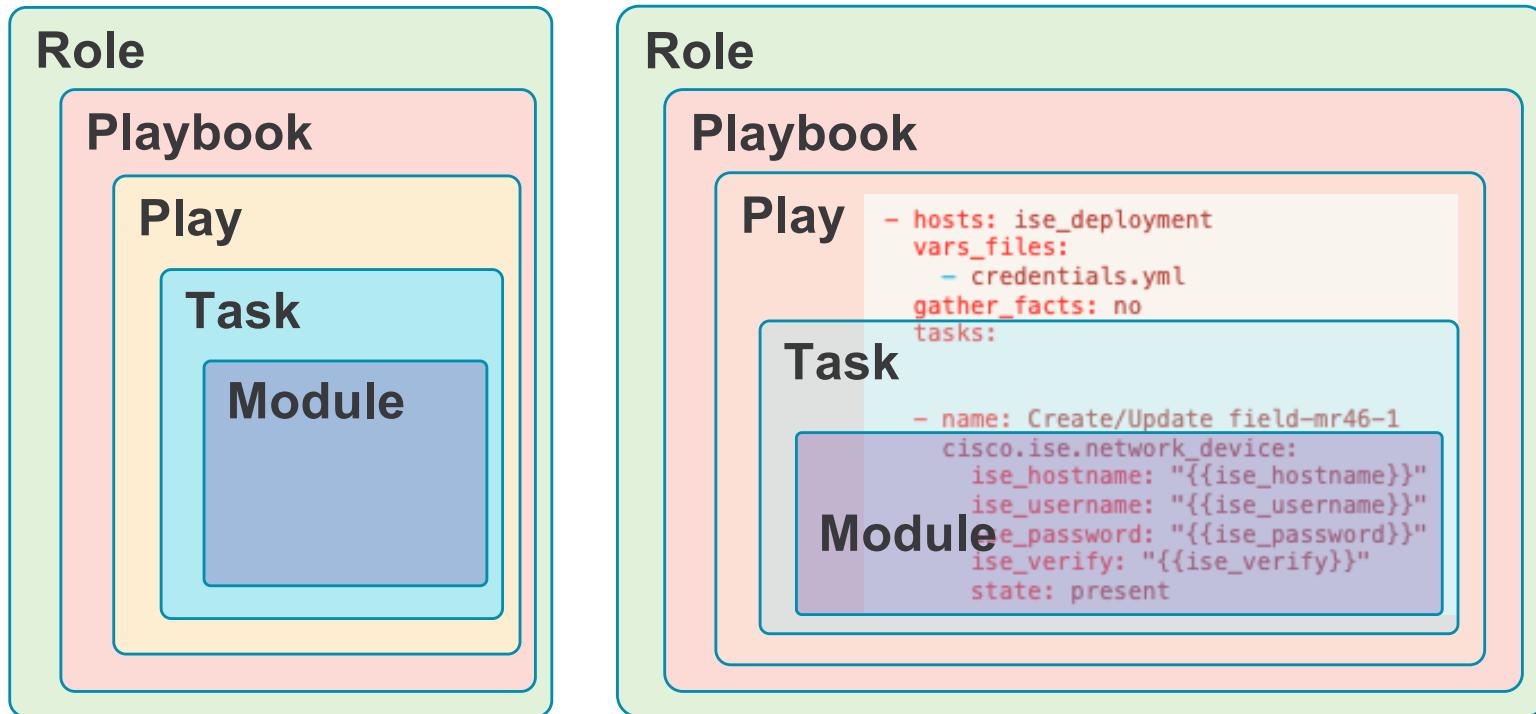
## Control Node



## Managed Nodes



# Ansible Taxonomy





```
pip3 install --upgrade pip
pip3 install pipenv
pipenv install --python 3.9
pipenv install ciscoisesdk
pipenv install ansible
pipenv install jmespath
pipenv shell
```

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

ansible-galaxy collection install community.general
```

# Ansible Collections

<b>amazon.aws</b>	<b>cisco.ise</b>	community.hashi_vault	community.windows	hetzner.hcloud	ngine_io.cloudstack
ansible.builtin	cisco.meraki	community.hrobot	community.zabbix	hpe.nimble	ngine_io.exoscale
ansible.netcommon	cisco.mso	community.kubernetes	containers.podman	ibm.qradar	ngine_io.vultr
ansible.posix	cisco.nso	community.kubevirt	cyberark.conjur	infinidat.infinibox	openstack.cloud
ansible.utils	cisco(nxos)	community.libvirt	cyberark.pas	inspur.sm	openvswitch.openvswitch
ansible.windows	cisco.ucs	community.mongodb	dell EMC.enterprise_sonic	junipernetworks.junos	ovirt.ovirt
arista.eos	cloudscale_ch.cloud	community.mysql	dell EMC.openmanage	kubernetes.core	purestorage.flasharray
awx.awx	<b>community.aws</b>	community.network	dell EMC.os10	mellanox.onyx	purestorage.flashblade
azure.azcollection	community.azure	community.okd	dell EMC.os6	netapp.aws	sensu.sensu_go
check_point.mgmt	community.crypto	community.postgresql	dell EMC.os9	netapp.azure	servicenow.servicenow
chocolatey.chocolatey	community.digitalocean	community.proxysql	f5networks.f5_modules	netapp.cloudmanager	splunk.es
cisco.aci	community.docker	community.rabbitmq	fortinet.fortimanager	netapp.elementsw	t_systems_mms.icinga_director
cisco.asa	community.fortios	community.routeros	fortinet.fortios	netapp.ontap	theforeman.foreman
cisco.intersight	community.general	community.skydive	frr.frr	netapp.um_info	vyos.vyos
cisco.ios	community.google	community.sops	gluster.gluster	netapp_eseries.santricity	wti.remote
cisco.iosxr	community.grafana	community.vmware	google.cloud	netbox.netbox	

# Agenda

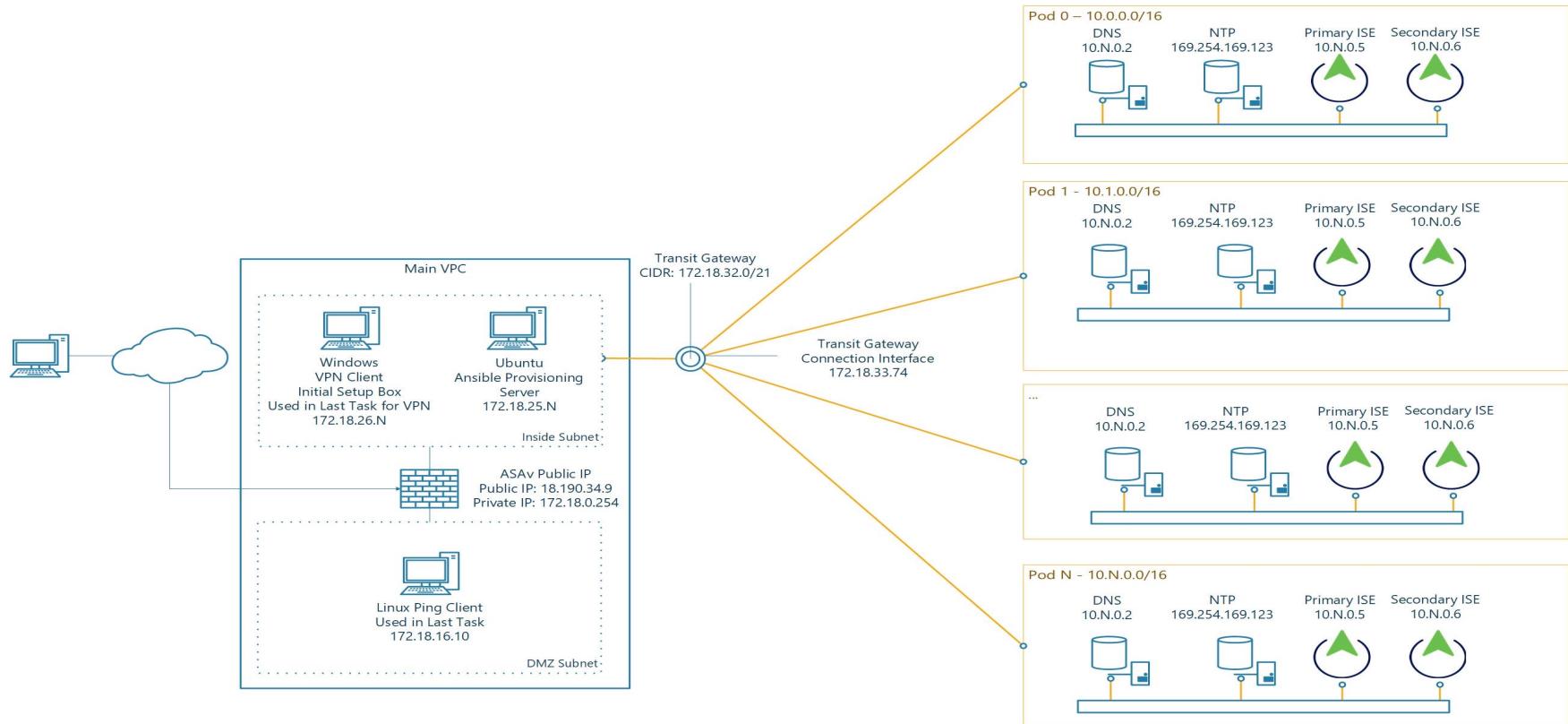
- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion



# What Are We Doing?

- If you were to deploy this manually, the following tasks would be accomplished:
  - Create an SSH Key Pair
  - Create AWS VPC
  - Create Subnets
  - Create Route Tables
  - Edit Route Tables
  - Create a Linux Test Instance for Pinging

# Topology



# What You'll Need

- An AWS Account (and preferably budget to run that AWS instance!)
- A Linux Deployment Machine
  - Access to Git
  - Ansible Installed
- Knowledge of your Deployment
  - AWS Region
  - AWS Access Key
  - AWS Secret Key
  - Expected ISE Credentials

# What You'll Need

- An AWS Account with Programmatic Access
- Don't be like Patrick!
  - Save files and hidden files
  - Search for secrets with Linux Utilities
    - `find . -type f -exec grep -H 'YOUR_SECRET_KEY' {} \;`

The screenshot shows the AWS Identity and Access Management (IAM) console. The left sidebar has a tree view with 'Identity and Access Management (IAM)' selected. Under 'Access management', 'Users' is selected. The main area is titled 'Summary'. At the top right, there are filters for 'User ARN', 'Path', and 'Creation time'. Below these are tabs for 'Permissions', 'Groups', 'Tags', and 'Security credentials' (which is highlighted in orange). A section titled 'Access keys' contains a note about protecting secret keys. A button labeled 'Create access key' is visible. A table below lists an access key entry:

Access key ID	Created
[REDACTED]	T75 2022-03-11 15:38 EDT

Amazon Web Services has opened case [REDACTED] on your behalf.

The details of the case are as follows:

Case ID: [REDACTED]

Subject: ACTION REQUIRED: Your AWS Access Key is Exposed for AWS Account [REDACTED]

Severity: Urgent

Correspondence: Dear AWS customer,

```
ubuntu@ip-10-0-1-217:~/CiscoLive_ISE_in_AWS/ISE_with_Meraki_in_Aws$ find . -type f -exec grep -H 'YOUR_SECRET_KEY' {} \;
./vars/main.yaml.save:AWS_ACCESS_KEY: [REDACTED] T75
./vars/main.yaml.save:export AWS_ACCESS_KEY=[REDACTED] T75
```

# What You'll Need

- An Ubuntu Deployment Machine
- Routing tables must be present for addressing!
- Separate Region Model (Public address)
- Same Region Model (Private address)

```
---  
#  
# Tasks to enable and confirm ISE APIs  
#  
  
- name: Enable ISE OpenAPIs (ISE 3.1+)  
  delegate_to: Localhost  
  ansible.builtin.uri:  
    # note that the following all references the private IP address  
    # if this script sits outside of the region or subnet, use public  
    # url: "https://{{ item.private_ip }}/admin/API/apiservice/update"  
    # url: "https://{{ item.public_ip }}/admin/API/apiservice/update"  
    method: POST ... ...
```

# What You'll Need

- Knowledge of your Deployment
  - AWS Region
  - AWS Access Key
  - AWS Secret Key
  - Expected ISE Credentials

```
pod_id: pod4
#set this to your ip used to access ise, or a hostname if DNS configured
#called in tasks/radius_probes.create.yaml
inventory_hostname: 18.218.29.225
ise_hostname: test-hostname.palloyd.xyz
ise_username: admin
ise_password: Cis12345!
AWS_REGION: us-east-2
ise_verify: false
```



# Agenda

- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- **Integrations**
- Conclusion

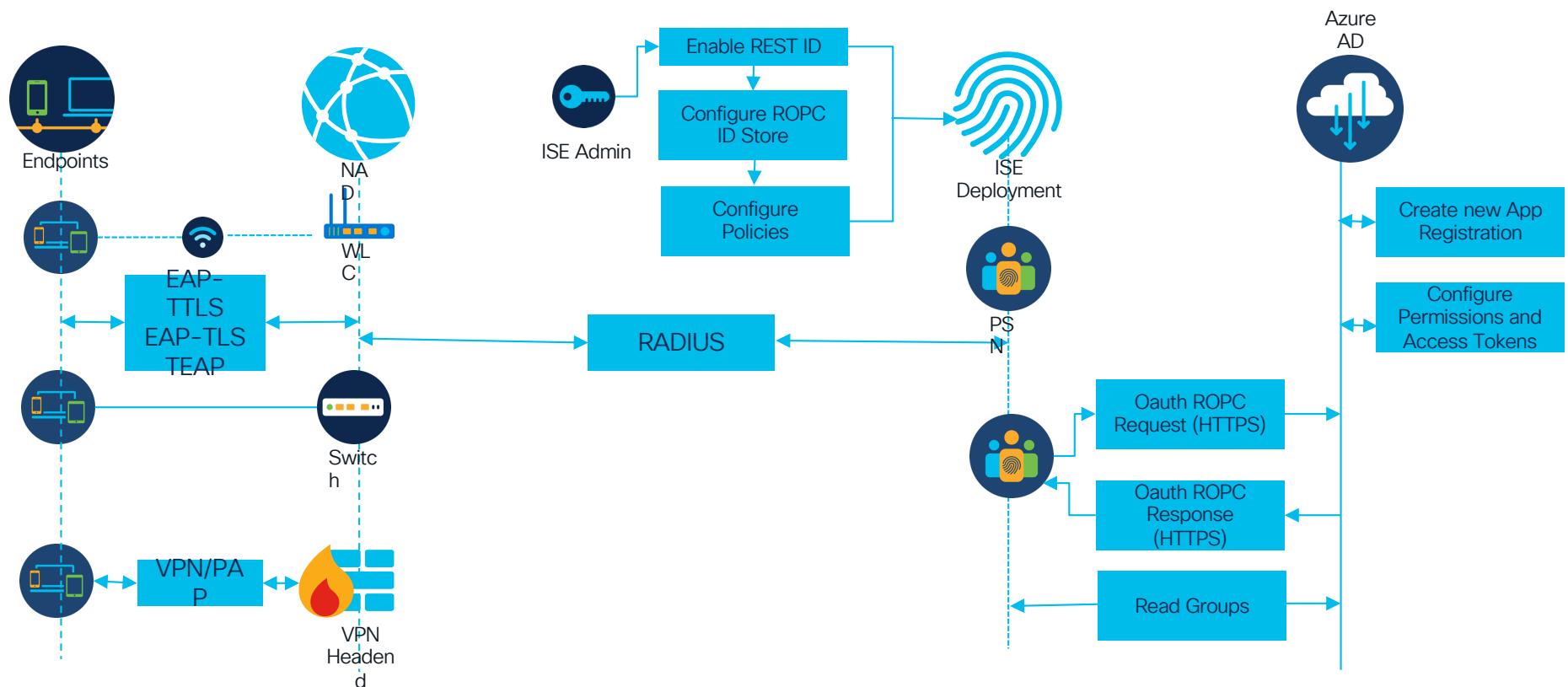
# Azure AD / ROPC

- Resource Owner Password Credentials (ROPC) is an OAuth 2.0 grant type that allows Cisco ISE to carry out authorization and authentication in a network with cloud-based identity providers.
- Controlled Access Introduction Feature
- Supports EAP-TTLS and PAP authentications with ISE 3.0+
- Supports EAP-TLS and TEAP with ISE 3.2+

cisco *live!*

ISE PROCESS NAME	STATE	PROCESS ID
Database Listener	running	8864
Database Server	running	115 PROCESSES
Application Server	running	26777
Profiler Database	running	17001
ISE Indexing Engine	running	28790
AD Connector	running	30324
M&T Session Database	running	23085
M&T Log Processor	running	27013
Certificate Authority Service	running	30113
EST Service	running	74954
SXP Engine Service	running	3497002
TC-NAC MongoDB Container	running	3508280
TC-NAC Core Engine Container	running	3509361
VA Database	running	3511016
VA Service	running	3511272
PassiveID WMI Service	running	3486473
PassiveID Syslog Service	running	3487203
PassiveID API Service	running	3488149
PassiveID Agent Service	running	3489868
PassiveID Endpoint Service	running	3493221
PassiveID SPAN Service	running	3495802
DHCP Server (dhcpd)	disabled	
DNS Server (named)	disabled	
ISE Messaging Service	running	12100
ISE API Gateway Database Service	running	15723
ISE API Gateway Service	running	21553
ISE EDDA Service	running	51664
REST Auth Service	running	1486625
Hermes (pxGrid Cloud Agent)	disabled	
ISE Node Exporter	running	40606
ISE Prometheus Service	running	43036
ISE Grafana Service	running	49934
ISE MNT LogAnalytics Elasticsearch	disabled	
ISE Logstash Service	disabled	
ISE Kibana Service	disabled	

# Azure AD Integration with ISE - High Level Flow Overview





# Agenda

- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion

# Continue Your Learning

 [devnetsandbox.cisco.com](https://devnetsandbox.cisco.com)

SANDBOX LABS RESERVATIONS THOMAS ▾ DEVNET ▾ HELP ▾

Search Sandbox Labs SECURITY (10) Reset filters

VIEW ▾

Sandbox Labs Reservations 0 New, 0 Total

FILTER BY:

Sandbox Lab Status

Available

Unavailable

View only

Back to Sandbox Lab Catalog

TYPE All ▾

Security (10)

ISE with Ansible Automation with Radius Simulator (Version 3.1) Cisco Application-First Security (Version 1.0) Cisco FMC & Splunk (Version 1.0) Cisco Secure Workload (Tetration) (Version 7.1.1) Cisco Stealthwatch (Version 7.1.1)

Automate ISE with... Sandbox with ISE 3.1 showing all of the ways to Cisco Application-... Explore how to bring security closer to your Cisco FMC and Sp... FMC eStreamer API and Splunk Cisco Secure Work... Explore how to bring security closer to your Cisco Stealthwatch Stealthwatch v7.1.1 with Traffic, REST API samples

RESERVE RESERVE RESERVE RESERVE RESERVE

Security ALL CATEGORIES

Networking Collaboration IoT



#CiscoLive

LTRSEC-2000

© 2022 Cisco and/or its affiliates. All rights reserved. Cisco Public

# ISE Customer Resources

The screenshot shows a community post titled "Cisco ISE & NAC Resources". The post has 135846 views, 110 helpful votes, and 0 comments. It was created on 11-13-2015 at 03:48 PM by thomas. The post includes a summary of ISE features like Start, Design, Deploy, Integrate, and Learn, followed by sections for Software, Appliances & VMs, and a list of related resources.

cisco *Live!*

- Resources  
[cs.co/ise-resources](https://cs.co/ise-resources)
- Community  
[cs.co/ise-community](https://cs.co/ise-community)
- YouTube Channel  
[cs.co/ise-videos](https://cs.co/ise-videos)
- Licensing Guide  
[cs.co/ise-licensing](https://cs.co/ise-licensing)
- API SDK [cs.co/ise-api](https://cs.co/ise-api)
- Future webinars! [cs.co/ise-webinars](https://cs.co/ise-webinars)
- Devnet <https://cs.co/ise-devnet>
- ISE Github <https://github.com/CiscoISE>
- Patrick Lloyd's GitHub  
<https://github.com/plloyd44>

# Technical Session Surveys

- Attendees who fill out a minimum of four session surveys and the overall event survey will get Cisco Live branded socks!
- Attendees will also earn 100 points in the Cisco Live Game for every survey completed.
- These points help you get on the leaderboard and increase your chances of winning daily and grand prizes.





# Continue your education

cisco *Live!*

- Visit the Cisco Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at [www.CiscoLive.com/on-demand](http://www.CiscoLive.com/on-demand)



The bridge to possible

# Thank you

cisco *Live!*

#CiscoLive

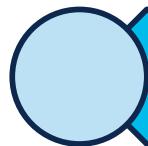


CISCO *Live!*

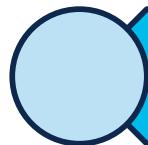
PALESTINE

#CiscoLive

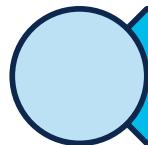
# Launch ISE using AWS Market Place



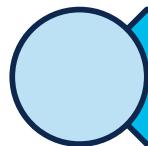
Complete prerequisites



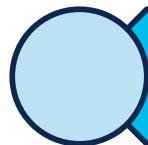
Search ISE in the AWS market place



Clone the Git Repository



Populate the Ansible Scripts



Launch!

# Prerequisites: Critical Information

- Does your organization have a centralized SSH key for AWS?
- What region are you deploying ISE to?
- Do you know your access key?
- Do you know your secret key?
- How will you extend your domain into the cloud?
- What IP's will you be using for ISE?

# Prerequisites: Regions and Availability Zones

The screenshot shows the AWS Management Console interface for the EC2 Instances service. At the top, there's a navigation bar with icons for Home, Help, and Account information (admin/palloyd@cisco.com @ palloyd-aws). Below the navigation bar is a toolbar with buttons for Create (C), Connect, Instance state, Actions, and Launch instances. The Actions button has a dropdown arrow. To the right of the toolbar, there are navigation controls (< 1 >) and a settings gear icon.

The main content area displays a table header with columns: Availability Zone, Public IPv4 DNS, Public IPv4 ..., Elastic IP, IPv6 IPs, Monitoring, Security group name, and Key name. Below the header, a message states: "You do not have any instances in this region".

Two specific elements are highlighted with red boxes: the "Ohio" region dropdown menu in the toolbar and the message in the main content area.

# Prerequisites: Regions and Availability Zones

< Product Detail    Subscribe    [Configure](#)

## Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option

Amazon Machine Image

Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2

64-bit (x86) Amazon Machine Image (AMI)

Software version

3.1 Patch1 (Dec 09, 2021)

Region

US East (N. Virginia)

Use of Local Zones or WaveLength infrastructure deployment may alter your final pricing.

Ami Id: ami-0bb0a9d243824a077

Product Code: basttrzv6xwc4yn2uup6bh730

Release notes (updated December 9, 2021)

< Product Detail    Subscribe    [Configure](#)

## Configure this software

Choose a fulfillment option and software version to launch this software.

Fulfillment option

Amazon Machine Image

Deploy a vendor-provided Amazon Machine Image (AMI) on Amazon EC2

64-bit (x86) Amazon Machine Image (AMI)

Software version

3.1 Patch1 (Dec 09, 2021)

Region

US West (N. California)

Ami Id: ami-0965fef2e601ad4d0

Product Code: basttrzv6xwc4yn2uup6bh730

Release notes (updated December 9, 2021)

# Prerequisites: Regions and Availability Zones

- \$ env
  - AWS\_REGION: us-east-2
- \$ more main.yaml
  - aws\_region: "{{ lookup('env','AWS\_REGION') | default('us-east-2') }}"

# Prerequisites: Regions and Availability Zones

- \$ export AWS\_REGION=us-west-1
- \$ ansible-playbook ise\_in\_aws.vpc.yaml
- fatal: [localhost]: FAILED! => changed=false
  - msg: The amazon.aws.ec2\_vpc\_net module requires a region and none was found in configuration, environment variables or module parameters <===**Missing Env**
- OR
- msg: 'Failed to create new EC2 instance: An error occurred (InvalidAMIID.NotFound) when calling the RunInstances operation: The image id "[ami-0bb0a9d243824a077]" does not exist' <===**Wrong AMI for the Region**

# Prerequisites: Access Keys

- To manage access keys when signed in as the root user
  - Sign in to the AWS Management Console as a user with programmatic access.
  - Search for “IAM” in the top search bar. Click “Users” on the left
  - Expand the Access keys (access key ID and secret access key) section. Create as needed

# Search for ISE In AWS Marketplace

The screenshot shows the AWS Marketplace search results for 'identity services engine'. The search bar at the top contains the query 'identity services engine'. Below the search bar, there are filters on the left: Services (84), Features (68), Blogs (9,109), Documentation (1,457), Knowledge Articles (30), Tutorials (35), Events (206), and Marketplace (37). The main area is titled 'Marketplace' and displays four results:

- Cisco Identity Services Engine (ISE)** (Version: 3.1 Patch1) | Sold by: Cisco Systems, Inc. [Bring Your Own License](#)
- Cisco Identity Services Engine (ISE) Jump Start by Aqueduct Technologies** | Sold by: Aqueduct Technologies
- Ping Identity Consultancy** | Sold by: e92plus
- Okta Implementation and Consultancy Services** | Sold by: Squareball

# Search for ISE In AWS Marketplace: Subscribe

## Cisco Identity Services Engine (ISE)

By: Cisco Systems, Inc.  Latest Version: 3.1 Patch1

Cisco ISE on AWS provides secure network access control for IoT, BYOD, and corporate owned endpoints. Cisco ISE enables you to easily segment network access for employees, contractors, [Show more](#)

Linux/Unix  [0 AWS reviews | 10 external reviews](#) 

**BYOL**

**Continue to Subscribe**

**Save to List**

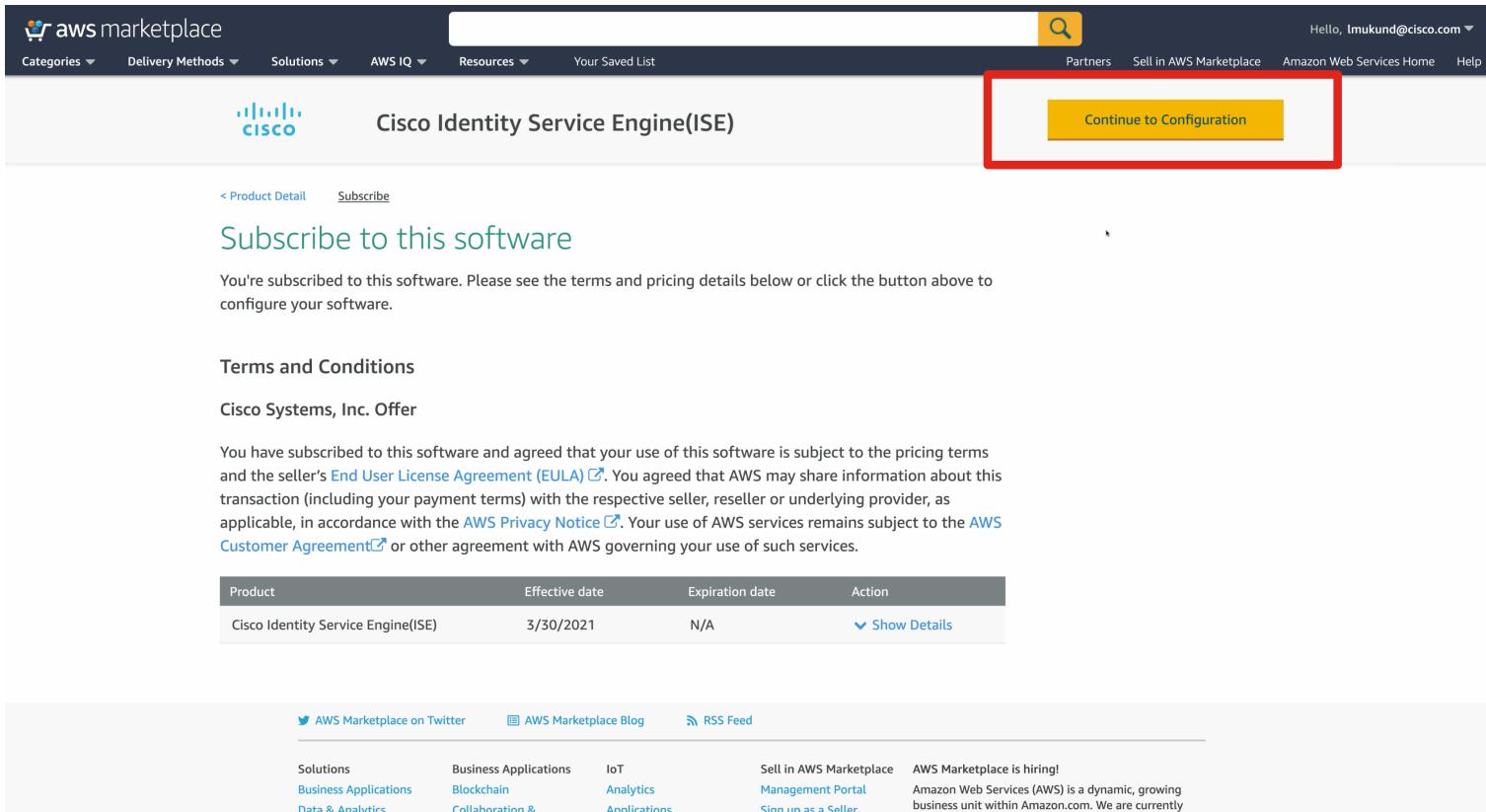
Typical Total Price  
**\$0.68/hr**

Total pricing per instance for services hosted on c5.4xlarge in US East (N. Virginia). [View Details](#)

---

Pricing      Usage      Support      Reviews

# Search for ISE in AWS Marketplace: Configure



The screenshot shows the AWS Marketplace product page for Cisco Identity Service Engine (ISE). At the top, there's a navigation bar with links for Categories, Delivery Methods, Solutions, AWS IQ, Resources, Your Saved List, Partners, Sell in AWS Marketplace, Amazon Web Services Home, and Help. A search bar is also present. The main content area features the Cisco logo and the product name "Cisco Identity Service Engine(ISE)". Below this, there's a yellow "Continue to Configuration" button, which is highlighted with a red box. Underneath the button, there are links for < Product Detail and Subscribe. A section titled "Subscribe to this software" contains text about subscription terms and a link to the End User License Agreement (EULA). Another section titled "Terms and Conditions" discusses the Cisco Systems, Inc. Offer. It states that users have agreed to the EULA and AWS Customer Agreement, and that AWS may share information about the transaction with the seller or reseller. A table provides details about the subscription, showing the product name, effective date (3/30/2021), expiration date (N/A), and an "Action" column with a "Show Details" link. At the bottom of the page, there are links for AWS Marketplace on Twitter, AWS Marketplace Blog, and RSS Feed. There are also links for Solutions, Business Applications, IoT, Analytics, and Applications, as well as links for Sell in AWS Marketplace, Management Portal, and Sign up as a Seller. A note mentions that AWS Marketplace is hiring and describes it as a dynamic, growing business unit within Amazon.com.

# Search for ISE in AWS Marketplace: AMI ID

The screenshot shows the AWS Marketplace product page for Cisco Identity Services Engine (ISE). At the top, there's a Cisco logo and the product name "Cisco Identity Services Engine (ISE)". A prominent yellow button on the right says "Continue to Launch". Below the title, there are links for "[Product Detail](#)", "[Subscribe](#)", and "[Configure](#)".

The main section is titled "Configure this software" and contains instructions: "Choose a fulfillment option and software version to launch this software." It includes dropdown menus for "Fulfillment option" (set to "Amazon Machine Image"), "Software version" (set to "3.1 Patch1 (Dec 09, 2021)"), and "Region" (set to "US East (Ohio)").

A red box highlights the "Ami Id: ami-0262130ee7b27f122" field, which is located below the fulfillment options. Other visible fields include "Product Code: basstrzv6xwc4yn2uup6bh730" and "Release notes (updated December 9, 2021)".

To the right, a "Pricing information" sidebar provides details about the estimated costs for running the software on Amazon EC2. It lists the "Cisco Identity Services Engine (ISE)" as running on a "c5.4xlarge" instance at \$0/hr, with a monthly estimate of \$490.00/month.

# Clone the GIT Repository

- [https://github.com/plloyd44/CiscoLive\\_ISE\\_in\\_AWS](https://github.com/plloyd44/CiscoLive_ISE_in_AWS)

# Populate the Ansible Scripts: Env Variables

```
(ubuntu) ubuntu@ip-10-0-1-217:~/ISE_with_Meraki_in_AWS$ env  
  
# AWS IAM API Keys  
  
AWS_ACCESS_KEY=ABCXYZ  
  
AWS_SECRET_KEY=ZYXCBA  
  
AWS_REGION=us-east-2  
  
  
# ISE Options  
  
ise_password=Cis12345!  
  
ise_username=admin
```

# Populate the Ansible Scripts

## Variables, Variables Everywhere

```
pod_id: pod4

#set this to your ip used to access ise, or a
hostname if DNS configured

#called in tasks/radius_probes.create.yaml

inventory_hostname: 18.218.29.225

ise_hostname: test-hostname.palloyd.xyz

ise_username: admin

ise_password: Cis12345!

AWS_REGION: us-east-2

ise_verify: false
```

```
project_name: ISEinAWS-{{ pod_id }}          # use
for tagging VMs and resources

aws_vpc_cidr: 10.192.0.0/16

aws_public_subnet_cidr: 10.192.169.0/24

aws_private_subnet_cidr: 10.192.168.0/24

aws_public_access_cidr: 0.0.0.0/0

ise_dns_server: 169.254.169.253
```

# Running Scripts Individually

- Ansible-playbook ssh\_key\_pair.yaml
- Ansible-playbook ise\_in\_aws.vpc.yaml
- Ansible-playbook ise\_in\_aws.ise.yaml
- ssh -i ~/.ssh/ISEinAWS-pod#.pem admin@<ip>
- Ansible-playbook ise.configuration.yaml

# Launch: Result

```
ise/admin# show run

hostname ise

ip domain-name zer0k.org

interface GigabitEthernet 0

    ip address 10.192.168.44 255.255.255.0

    ipv6 address dhcp

    ipv6 address autoconfig

    ipv6 enable

ip name-server 208.67.222.222

ip default-gateway 10.192.168.1

clock timezone EST5EDT

ntp server time.nist.gov

username admin password hash
$6$bLgPMB97IZT3lJF$4313EFueywsy16ZG5iAV94R5RA3FgW4s0YLuuVru7XJFtLVimgWf8HaXYkPDZkejxw2FfbArz2X20jYOGuEX.
1 role admin
```



# Clean Up – Start with Subnets

### Delete subnets

The following subnets will be deleted permanently and cannot be recovered later.

Name	▲	Subnet ID	▼	State	▼	VPC ID	▼
Private_Subnet		subnet-042d7d750042bc64c		<input checked="" type="checkbox"/> Available		vpc-0011b10530185e905	

To confirm deletion, type *delete* in the field

[Cancel](#) [Delete](#)

# Clean Up - Route Tables

### Delete route tables

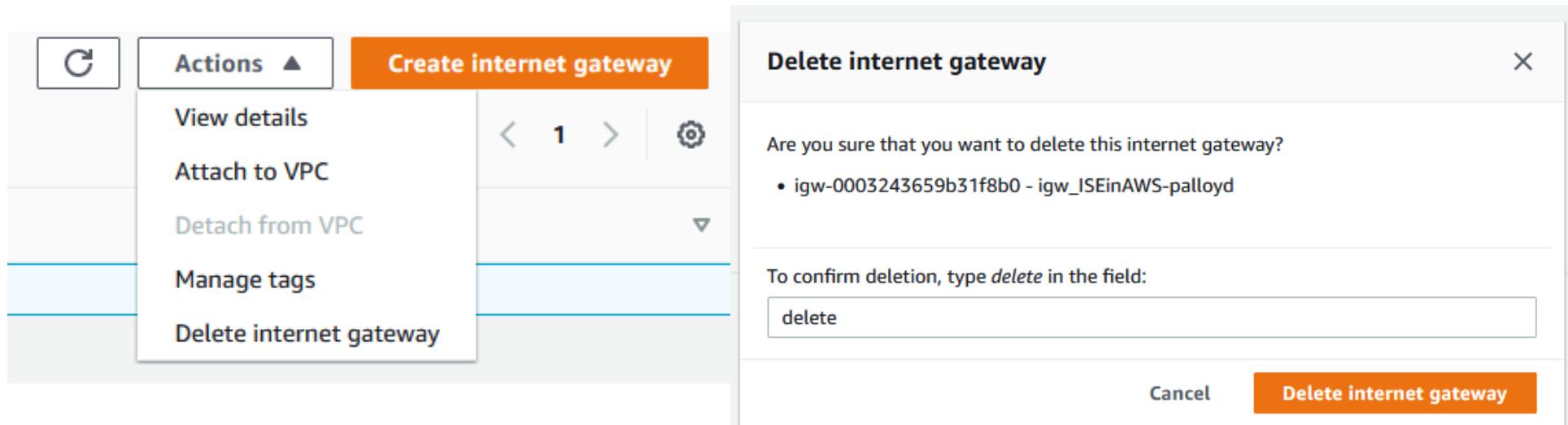
The following route tables will be deleted permanently and can't be recovered later.

Name	Route table ID	VPC ID
RT_Private	rtb-0997d5455756a32bf	vpc-0011b10530185e905

To confirm deletion, type *delete* in the field:

**Cancel** **Delete**

# Clean Up - Detach and Delete Internet Gateway from VPC



# Clean Up - Or Just Delete VPC

**Delete VPC**

**⌚ Will be deleted**  
This VPC will be deleted permanently and cannot be recovered later:

Name <a href="#">ISEinAWS-"pod4"</a>	VPC ID <a href="#">vpc-0d4c507841ccbe9ad</a>	State <span style="color: green;">⌚ Available</span>
---	---	---

**⌚ Will also be deleted**  
The following 5 resources will also be deleted permanently and cannot be recovered later:

Name	Resource ID	State
Private_Subnet	<a href="#">subnet-0c1775c1c2235f919</a>	<span style="color: green;">⌚ Available</span>
Public_Subnet	<a href="#">subnet-034e0c3ca355a34b2</a>	<span style="color: green;">⌚ Available</span>
RT_Private	<a href="#">rtb-01f5e6722ce73a08c</a>	-
RT_Public	<a href="#">rtb-0a6469a619042e2da</a>	-
igw_ISEinAWS-"pod4"	<a href="#">igw-0efb2d87627906b6b</a>	<span style="color: green;">⌚ Available</span>

To confirm deletion, type *delete* in the field:

[Cancel](#) [Delete](#)

# Clean Up – Or Do It Programmatically

- Ansible-playbook ise\_in\_aws.terminate.yaml