
cisco Live!
Let's go

slido

ISE Deployments in the Cloud

Automate ISE Deployments in AWS

Join at

slido.com

#1675 736

Passcode: **q4owbb**

The bridge to possible

ISE Deployments in the Cloud

Automate ISE Deployments in AWS

Jesse Dubois, TAC Security Technical Leader
Patrick Lloyd, Senior Security Solutions Architect, CX Customer Delivery

cisco Live!

LTRSEC-2000

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

Senior Solutions Architect, Security Services

14 years @ Cisco, 10 in Security

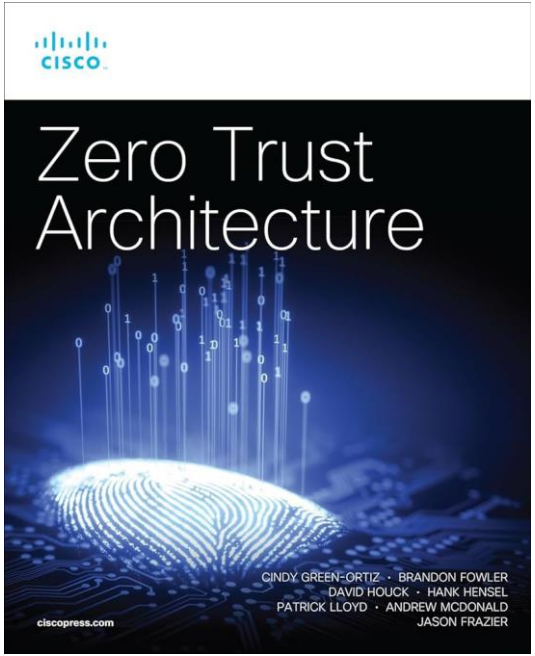
Previously DOD contractor, Higher Education

Private Pilot Working on Instrument

Ocala, FL

About Patrick Lloyd

Co-Author, Zero Trust Architectures



About Jesse Dubois

- name: Jesse Dubois

  Details.jessedubois:

  Location: Durham, North Carolina

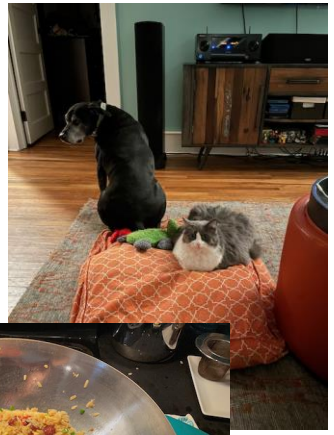
  Interests: Brewing, Golf, Cooking

  Pets: Dunkel, Apollo, Comet, Calypso

  Travel: Lots

  Fun Fact: Squirrels in your attic are not fun.





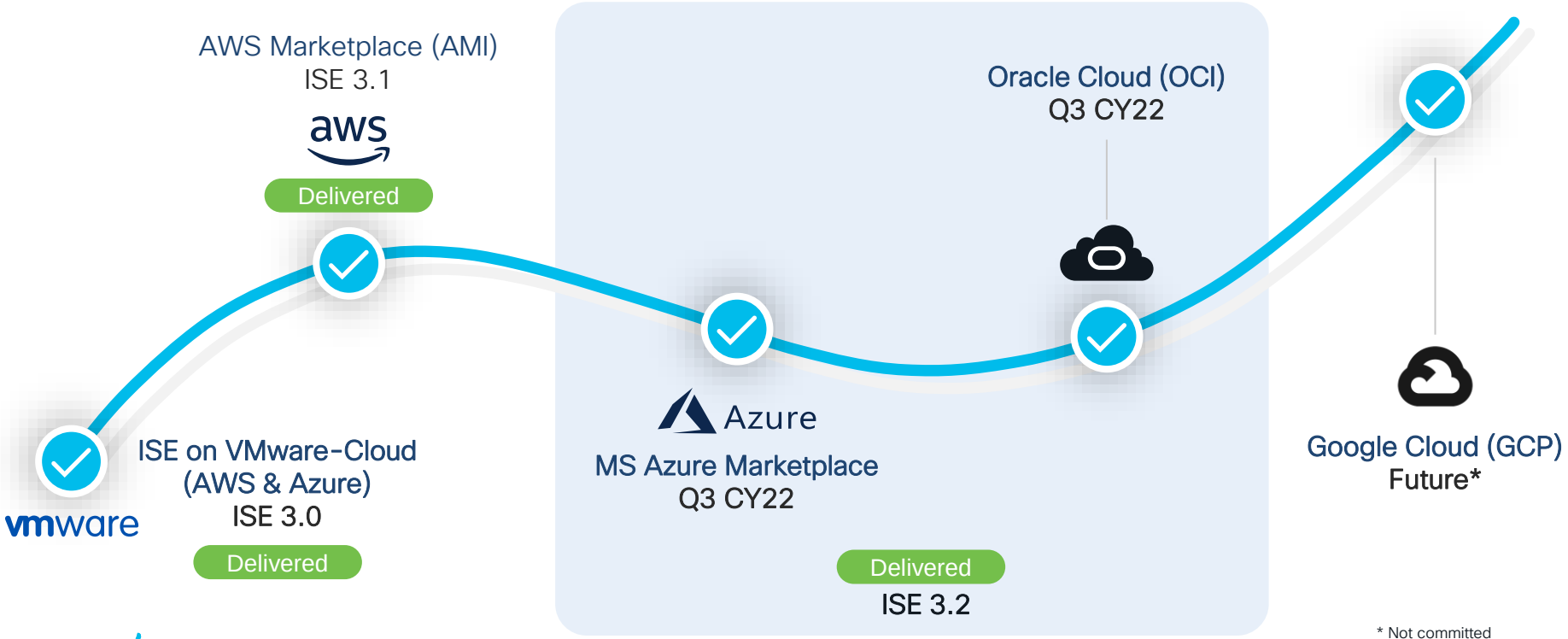




Agenda

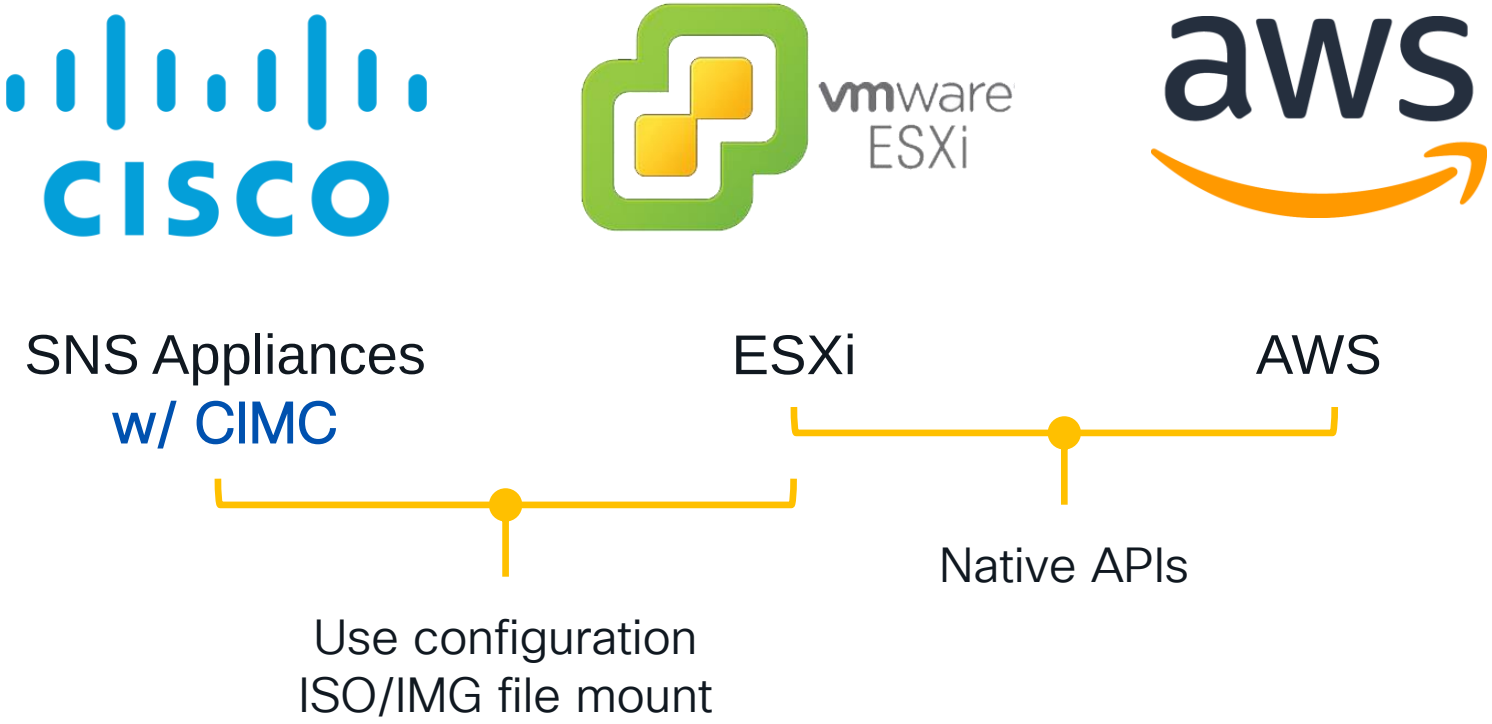
- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion

ISE journey on public cloud



* Not committed

Zero Touch Provisioning



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 25,000 concurrent endpoints	3600	Up to 2,000,000 concurrent endpoints
Up to 50,000 concurrent endpoints	3700	Up to 2,000,000 concurrent endpoints

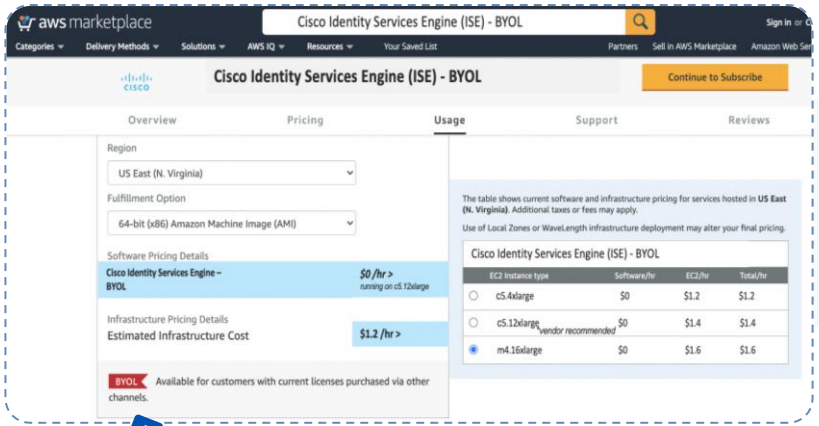
ISE 3.3 Supported AWS Platforms

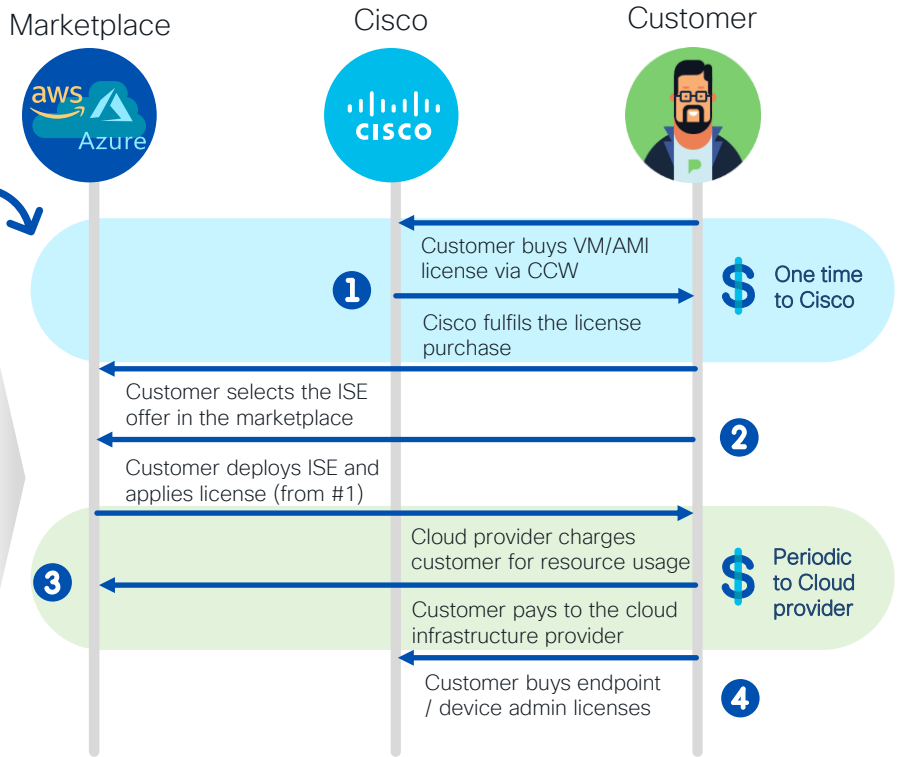
AWS Instance Type	Shared PSN Sessions	Dedicated PSN Sessions	Global Sessions	Cores	Memory	Disk
T3.xlarge	100	100	100	4	16 GB	300 – 600 GB
M5.2xlarge	N/A	12000	N/A	8	32 GB	300 – 600 GB
c5.4xlarge*	12,500	25,000	N/A	16	32 GB	300 GB – 600 GB
m5.4xlarge	20,000	40,000	500,000	16	64 GB	300 GB – 600 GB
c5.9xlarge* m5.8xlarge	25,000	50,000	500,000	36 32	72 GB 128 GB	300 GB – 2.4 TB
m5.16xlarge	50,000	100,000	2,000,000	64	256 GB	300 GB – 2.4 TB

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

ISE Cloud Instance Buying Experience

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





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

ISE Setup Options

AWS Marketplace

AWS CloudFormation Template

Amazon Elastic Compute Cloud AMI (Amazon Machine Image)

Infrastructure as Code (IoC) tools

Cisco MSX (Managed Services Accelerator)

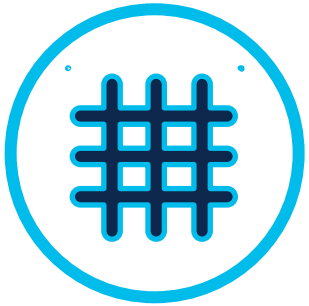
Bring up ISE node one at a time

Bring up multiple ISE nodes at the same time*

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

ISE APIs



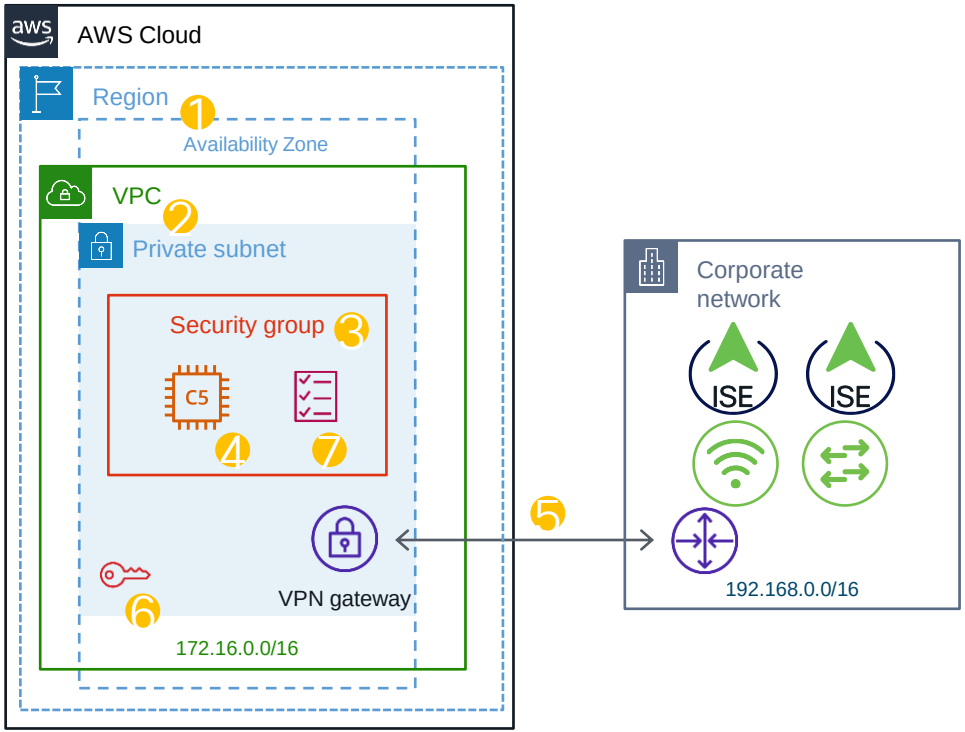



OpenAPIs	ERS	MNT	pxGrid
configuration	configuration	sessions	asynchronous endpoint context

cs.co/ise-api

github.com/cisco-pxgrid/pxgrid-rest-ws

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
  }
}
```

YAML

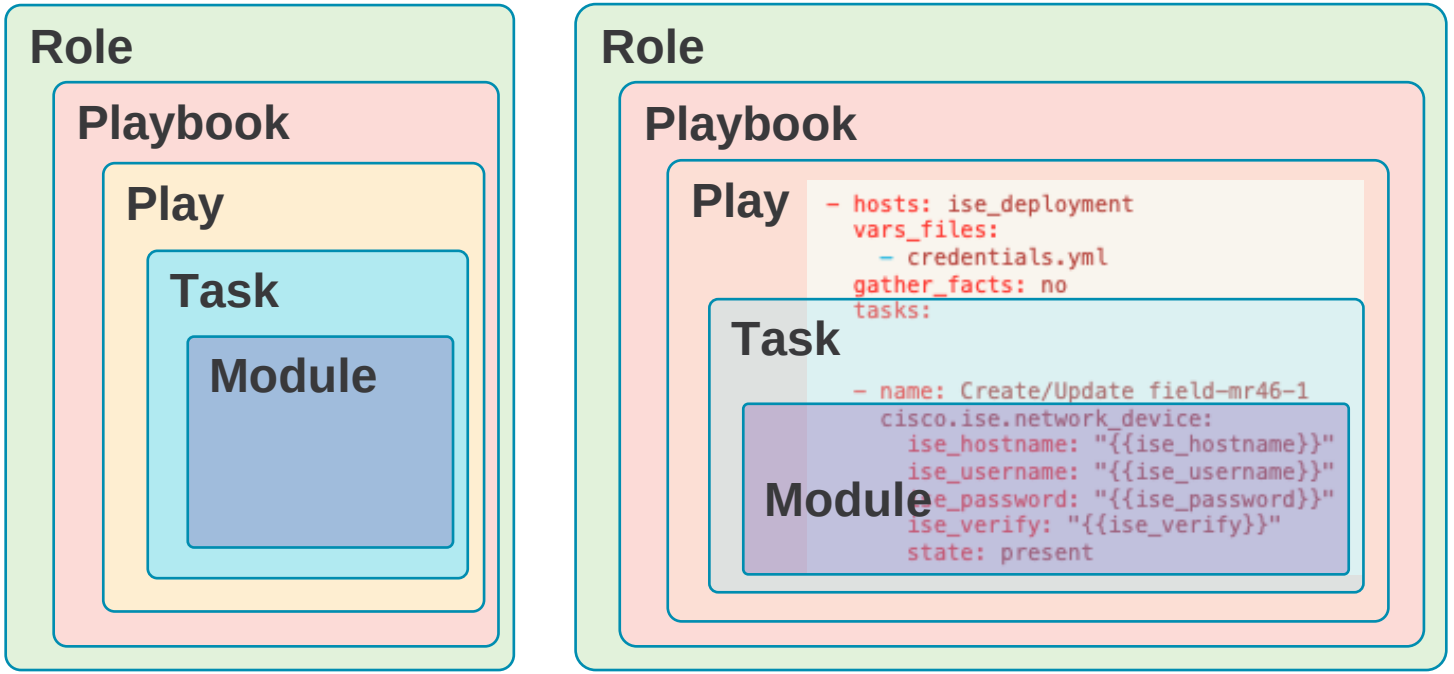
```
---
object:
  hostname: ise.securitydemo.net
  port: 443
  auth:
    username: admin
    password: C1sco12345
  verify: true

# YAML supports Comments!!!
```

ANSIBLE

Simple	Flexible	Agentless
• human-readable • declarative configs • ordered tasks • no coding required • start small and scale	• config management • workstations • servers / containers • applications • networks • security services • workflows	• SSH (Linux, macOS) • REST (ISE) • WinRM (Windows) • others as needed • efficient • secure

Ansible Taxonomy



Ansible Collections

amazon.aws	cisco.ise	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	dellemc.enterprise_sonic	junipernetworks.junos	ovirt.ovirt
arista.eos	cloudscale_ch.cloud	community.mysql	dellemc.openmanage	kubernetes.core	purestorage.flasharray
awx.awx	community.aws	community.network	dellemc.os10	mellanox.onyx	purestorage.flashblade
azure.azcollection	community.azure	community.okd	dellemc.os6	netapp.aws	sensu.sensu_go
check_point.mgmt	community.crypto	community.postgresql	dellemc.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	

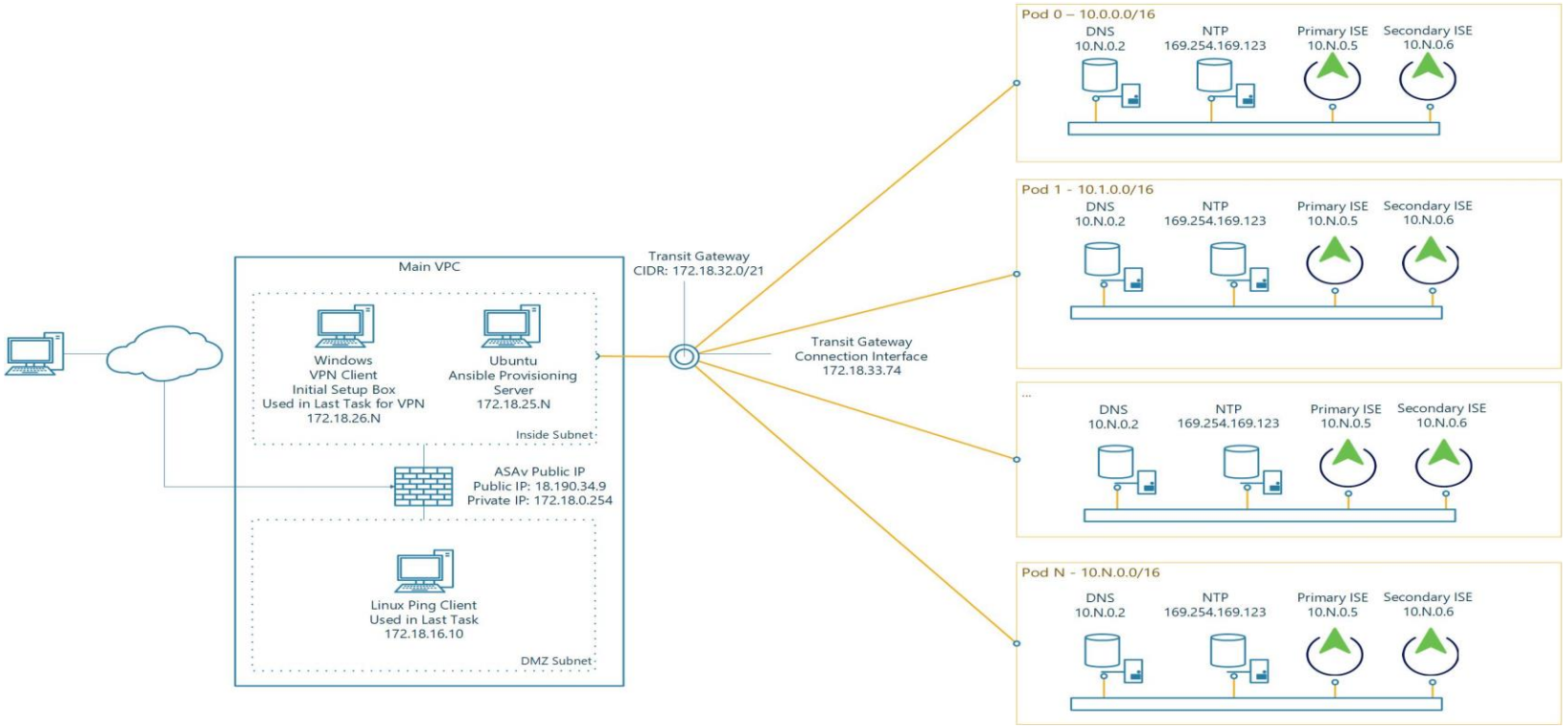
Agenda

- 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

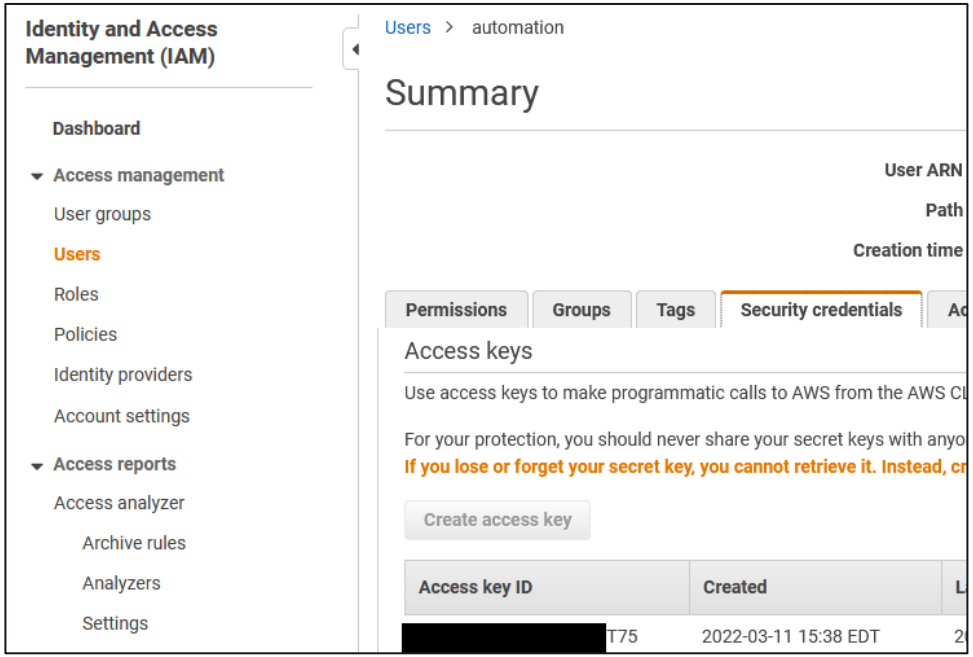


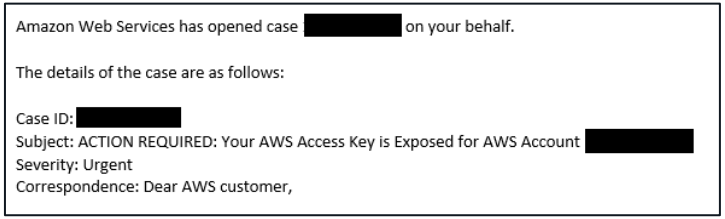
What You'll Need

- An AWS Account (and preferably budget to run that AWS instance!)
- An Ubuntu 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' {} \;






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

Agenda

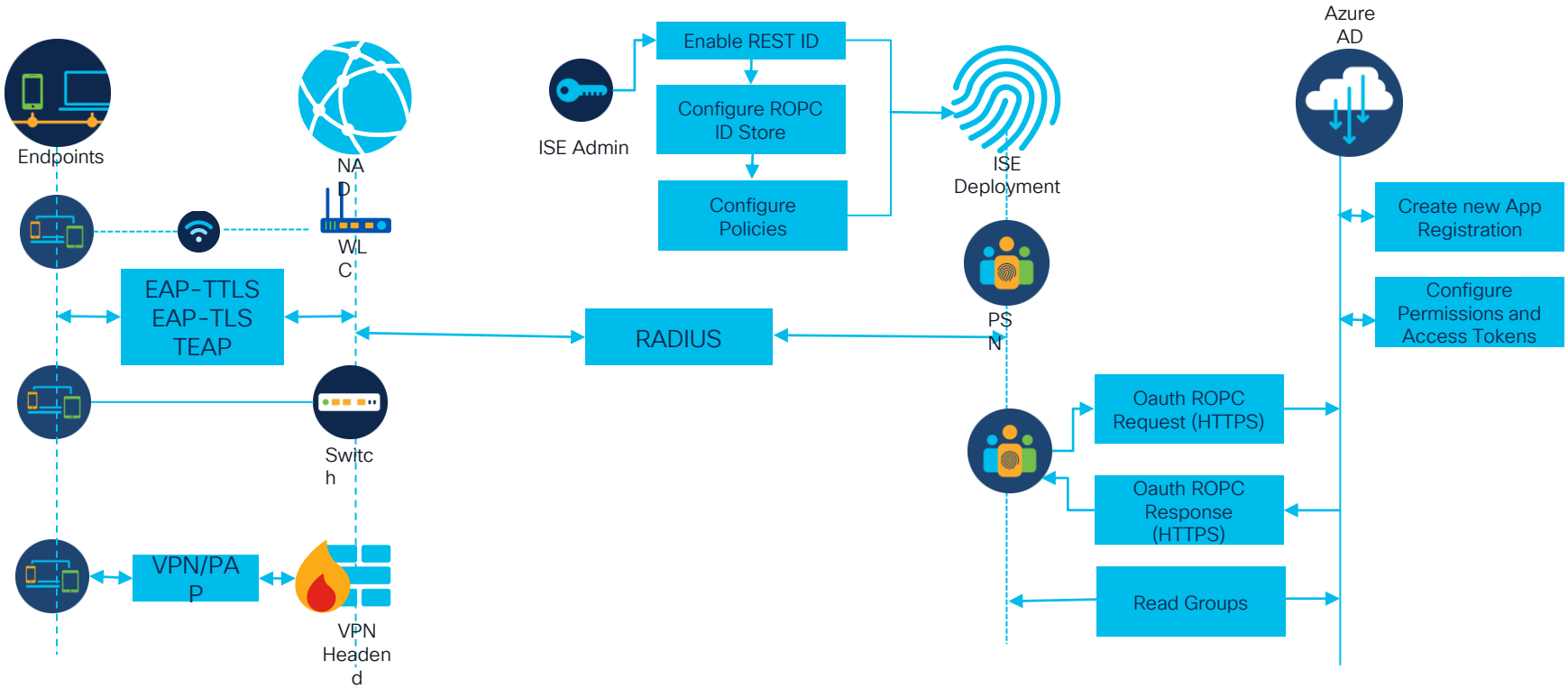
- Introduction
- Overview: ISE in AWS
- Overview: Ansible
- Deployment Caveats and Topology
- Integrations
- Conclusion

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+
- Introduced with new REST Auth Service

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	

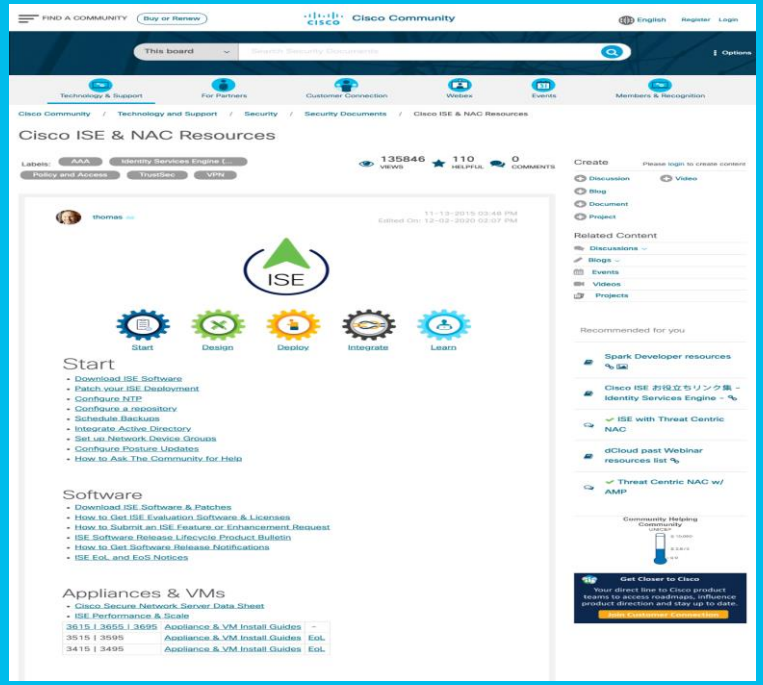
Azure AD Integration with ISE – High Level Flow Overview



Agenda

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

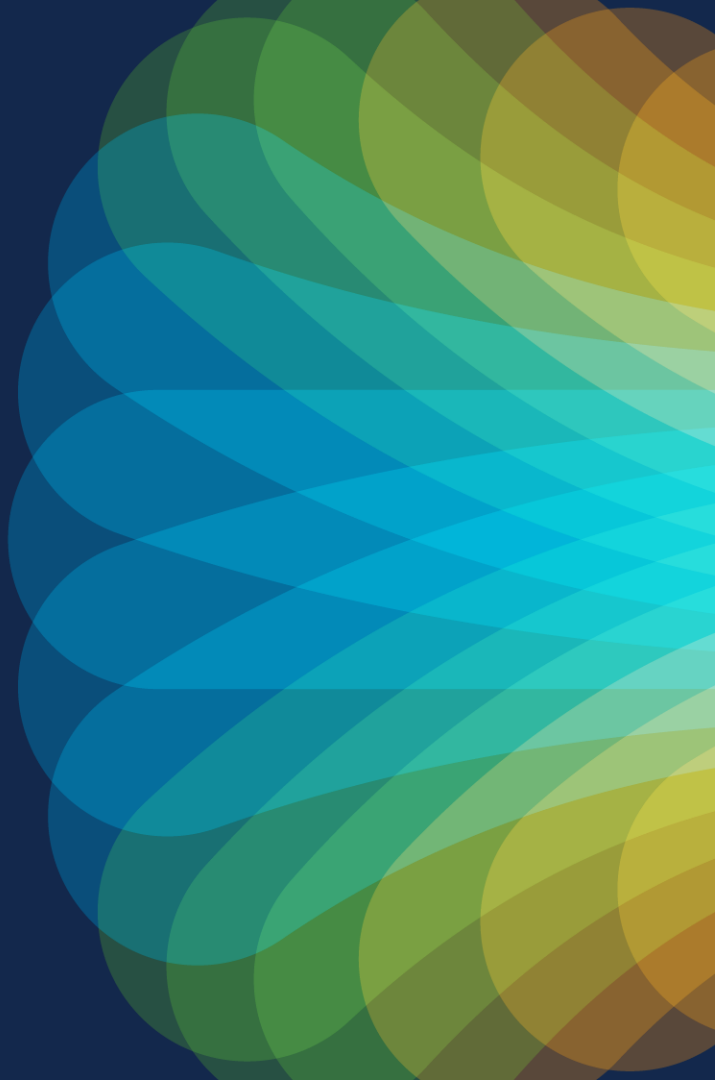
ISE Customer Resources



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

The bridge to possible

Thank you



cisco Live!


cisco Live!
Let's go