

ISE Deployments in the Cloud - Automate ISE Deployments in AWS and Integrate Them with Azure Active Directory

LTRSEC-2000

Speakers:

Jesse Dubois

Patrick Lloyd



Table of Contents

Learning Objectives or Table of Contents	4
Scenario	4
Recommended Equipment	4
Network Diagram.....	5
Task 1: Initial Connectivity	6
Step 1: Connect to the Lab VPN.....	6
Step 2: Establish RDP Session to Windows Provisioning Host	6
Step 3: Connect to AWS.....	6
Step 4: EC2	7
Step 5: Change AWS Regions	7
Step 6: Generate your AWS Access and Secret Key	7
Task 2: Deploy Ubuntu Provisioning Machine / Building Blocks	8
Step 1: Create Security Group	8
Step 2: Create a Key Pair.....	10
Step 3: Convert PEM to PPK format for dual use.....	11
Step 4: Create Network Interface	13
Step 5: Deploy Ubuntu Provisioning Machine.....	14
Step 6: Prepare Private Key on Local Machine	17
Step 7: Verify Connectivity.....	18
Task 3: Configure DNS in Route 53	19
Task 4: VPC Automation	20
Step 1: Deploy Ansible.....	20
Step 2: Clone the GIT Repository for Script Execution	21
Step 3: Configure the Environmental Variables to be Used	22
Step 4: Deploy the AWS Network Environment and Primary ISE Node	23
Step 5: Visit the AWS Environment to Ensure the Network Environment Was Provisioned	25
Step 6: Add Transit Gateway Attachment and Route	26
Step 7: Establish an SSH session with ISE	27
Step 8: Verify the running configuration of ISE to align with your Pod.....	28
Step 9: Launch ISE from a Web Browser	29
Step 10: Configure ISE Programmatically	30
Step 11: Verify what the Script Configured	31

Task 5: Azure AD integration via ROPC for Remote Access VPN	31
Step 1: Log into Azure and Configure Users/Groups.....	33
Step 2: Configure application integration in Azure.....	35
Step 3: Enable the ROPC feature in ISE	37
Step 4: Register ISE with Azure	38
Step 5: Configure ISE Policy for VPN Authentication	39
Task 6: Test VPN Authentication	41
Step 1: Test VPN Authentication	41
Task 7: (Bonus) Deploy Secondary ISE through AWS Marketplace from CloudFormation	
Template.....	42
Step 1: Subscribe to ISE in AWS Marketplace.....	42
Step 2: CloudFormation Stack Creation	42

Learning Objectives or Table of Contents

Upon completion of this lab, you will be able to:

- Provision an Ubuntu Linux machine with Ansible to automate configurations.
- Automatically provision AWS VPC's, Subnets, Routes, and Transit Gateway Attachment via Ansible.
- Provision ISE using a CloudFormation template.
- Provision ISE programmatically into the AWS cloud with your own credentials.
- Configure network device groups, network access devices, users and roles via Ansible configuration scripts.
- Create the ODBC object for provision of Azure Active Directory.

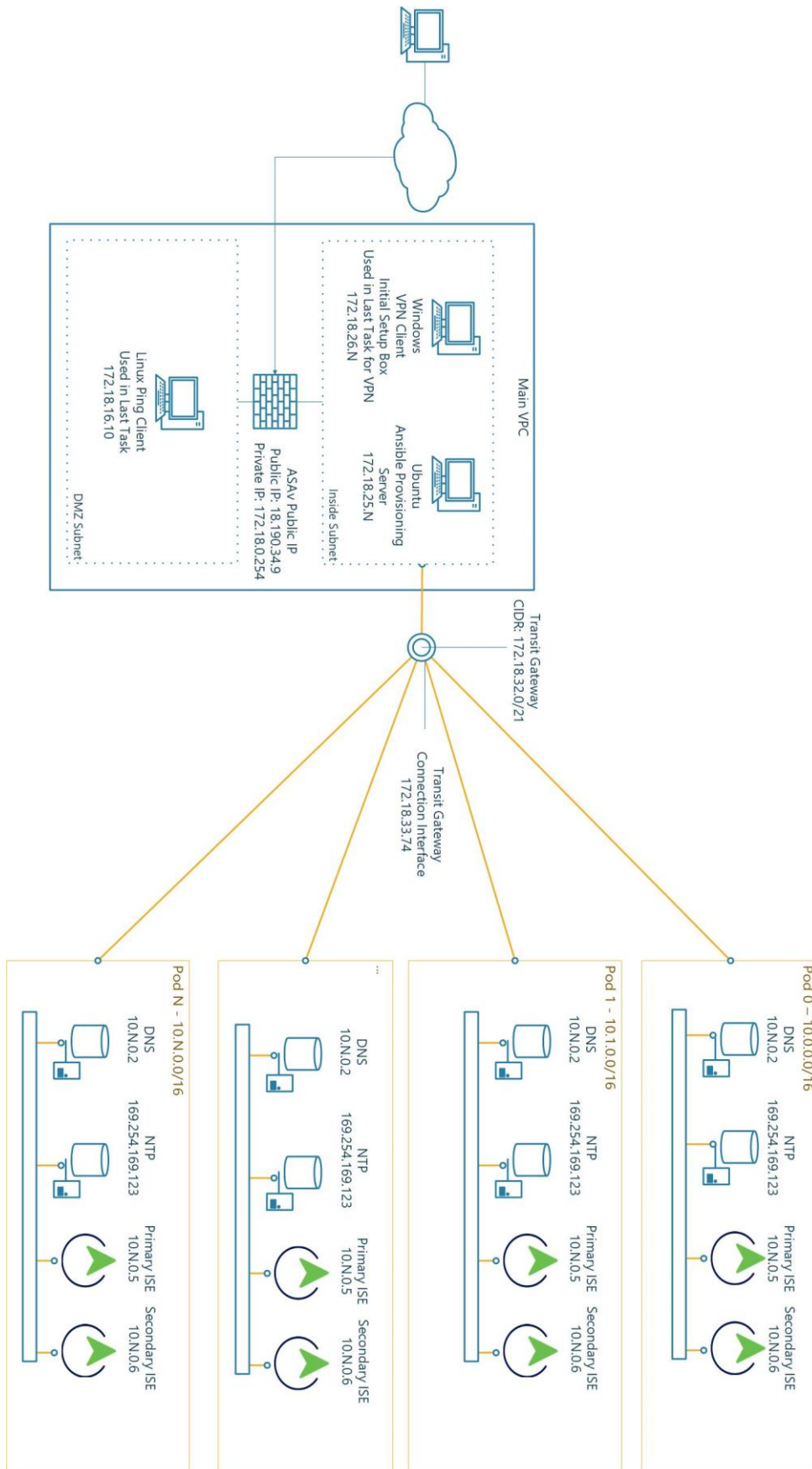
Scenario

In this lab activity, you will learn how to utilize an Ubuntu Linux machine to deploy ISE into an AWS environment, which is dynamically allocated via Ansible. The ansible script, found on github.com for later consumption, will be used to provision the VPC, subnet, routing table, and internet gateway into an AWS tenant already created. It will then deploy ISE within the VPC with a specified private IP address which will then be used to provision network device groups, network access devices, user roles, and users. You will then provision the Azure Active Directory connector, which requires manual intervention to join to Azure Active Directory.

Recommended Equipment

1. A laptop with VMWare workstation installed.
2. A virtual image you are familiar with.
3. AnyConnect on the virtual image. If you do not have AnyConnect, reach out to your lab proctor.
4. Internet Connectivity.

Network Diagram



Task 1: Initial Connectivity

Each pod is accessible via VPN with a provisioning machine on the required subnet. From this provisioning machine, you'll execute tasks allowing you to deploy AWS and ISE components and configurations. Access your pod based on the pod number assigned to you by the instructors:

Table 1-1

Pod Number	Windows Provisioning Host	Windows and VPN Password	Ubuntu Ansible Host	AWS Username	VPN Username
1	172.18.26.1		172.18.25.1	pod1-awsadmin	pod1-ravpn
2	172.18.26.2		172.18.25.2	pod2-awsadmin	pod2-ravpn
3	172.18.26.3		172.18.25.3	pod3-awsadmin	pod3-ravpn
4	172.18.26.4		172.18.25.4	pod4-awsadmin	pod4-ravpn
5	172.18.26.5		172.18.25.5	pod5-awsadmin	pod5-ravpn
6	172.18.26.6		172.18.25.6	pod6-awsadmin	pod6-ravpn
7	172.18.26.7		172.18.25.7	pod7-awsadmin	pod7-ravpn
8	172.18.26.8		172.18.25.8	pod8-awsadmin	pod8-ravpn
9	172.18.26.9		172.18.25.9	pod9-awsadmin	pod9-ravpn
10	172.18.26.10		172.18.25.10	pod10-awsadmin	pod10-ravpn

Step 1: Connect to the Lab VPN

Using AnyConnect VPN, connect to the ASA to gain access to the inside network. Connect to IP **18.190.34.9**. Choose the group "RA_VPN" and login with the username (**podX-ravpn**) assigned to your pod in table 1-1 above. The password for the account is provided by your proctor. Ignore any certificate warnings presented on connection. There is no public IP access to any of the machines in the pods. When trying to connect to any of the lab machines, ensure VPN is active.

If you do not have the AnyConnect client, browse to <https://18.190.34.9/> and authenticate with the information above. The AnyConnect client will be provisioned during the initial connection process.

Step 2: Establish RDP Session to Windows Provisioning Host

Establish a remote desktop connection to the Windows provisioning host associated with your pod. User credentials for this machine are username **Administrator**, password is **provided by your proctor**. This will be the host which provisions Ubuntu and provides the SSH key to be used for connectivity. Verify two files exist on the desktop:

- A shortcut to putty for connectivity: Putty will be used to establish an SSH session to Ubuntu where ansible and other tasks will be performed.
- A Pod Important Information Document: The Important information document contains the environmental variables for Ansible. These will be used in future steps.

Step 3: Connect to AWS

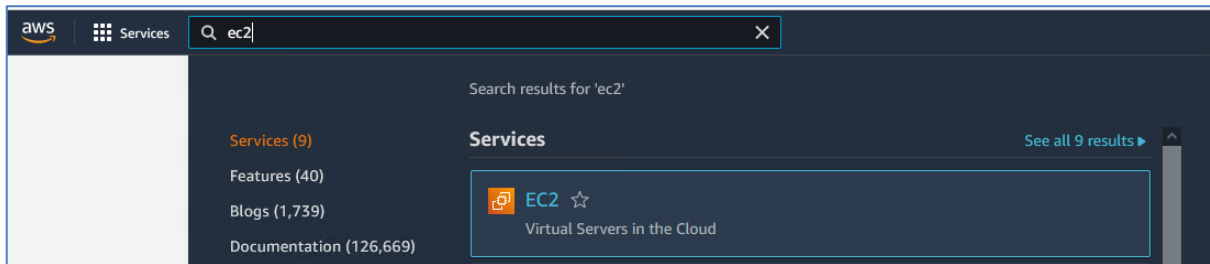
Open the Firefox web browser on the desktop of the windows provisioning machine and utilize the link **AWS Sign In** on the bookmarks toolbar to connect to the AWS cloud under the zer0k account. If this is not shown or is unavailable, navigate to <https://zer0k.signin.aws.amazon.com/console>. Use

Account ID zer0k if not already populated. Login with the username assigned to your pod in table 1-1 above (**podX-awsadmin**). The password for the

account is **is provided by your proctor** You may be prompted to switch to the new AWS home experience, select “Switch to the new Console Home”. Anytime you are prompted to use the new AWS experience select to do so as the lab guide is written based on this.

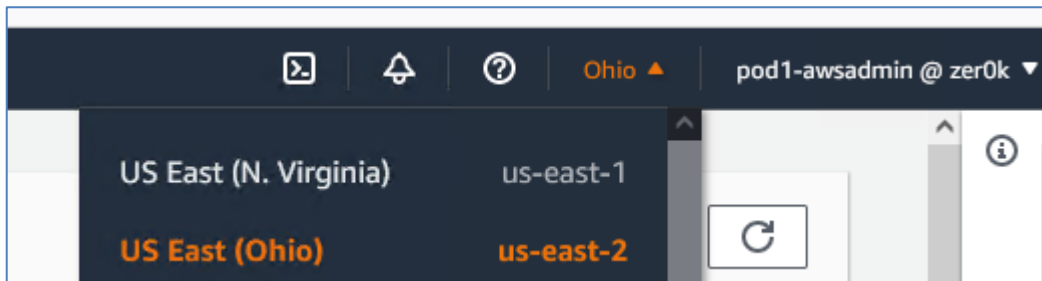
Step 4: EC2

Navigate to the EC2 area of AWS to access available virtual machines and virtual machine settings. In the search box at the top of the screen, type “EC2” and use the EC2 service link. Please do not access any virtual resources not associated with your pod number. Consult a lab proctor for assistance if you are unsure if a resource is one assigned to you or is one that you created.



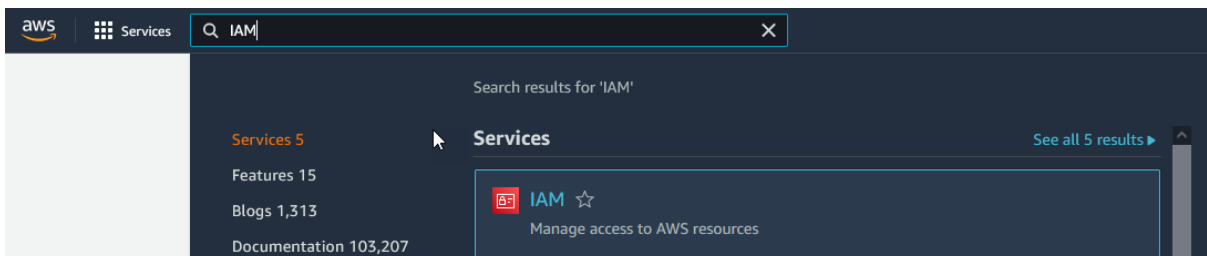
Step 5: Change AWS Regions

The Ansible lab is built within the EAST-2 Ohio region, which is required for connectivity to work between machines. In the EC2 dashboard, ensure that the region, located on the top right of the page, is EAST-2, or “Ohio”.



Step 6: Generate your AWS Access and Secret Key

From the top search bar in AWS, type IAM to navigate to Identity and Access Management. Click IAM.



From the left bar, click “Users” and select your pod username.

- ▼ Access management
 - User groups
 - Users**
 - Roles
 - Policies
 - Identity providers
 - Account settings
- ▼ Access reports
 - Access analyzer

An IAM user is an identity with long-term credentials that is used to interact with AWS in an account.

Find users by username or access key

<input type="checkbox"/>	User name	Groups
<input type="checkbox"/>	automation	None
<input type="checkbox"/>	pod0-awsadmin	LabAdmin
<input type="checkbox"/>	pod1-awsadmin	LabAdmin

Warning: Common mistake area!

Select “Security Credentials” and “Create Access Key”. You will use this access key for your environmental variables used in future steps. Click “Show” to show this secret key. **Ensure you copy the secret key, as it will not be available again. We recommend placing this in your “Pod<#> - Important Information” file.**

Access keys

Create access key

Warning: Never post your secret access key on public platforms, such as GitHub. This can compromise your account security.

Success: This is the **only** time that the secret access keys can be viewed or downloaded. You cannot recover them later. However, you can create new access keys at any time.

Access key ID	Secret access key
AKIAWFIN7EPKAQ5BZDPW	qxP6D0clwFLPY+znJwpQNh0Y+ONuIBpbXLV2RzW4 Hide

Task 2: Deploy Ubuntu Provisioning Machine / Building Blocks

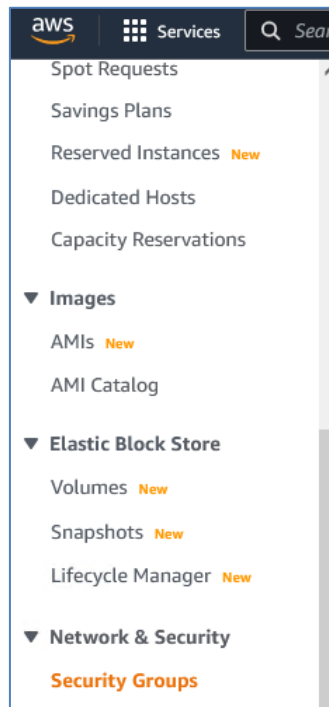
There are many ways to create an instance in AWS without creating each object ahead of time but it is helpful to understand each object when CloudFormation templates and scripts are used later in the lab. It is also helpful to know where each of these objects resides when troubleshooting connectivity problems.

Step 1: Create Security Group

Security Groups are AWS ACLs that control network traffic, by default all outbound network traffic from a security group is permitted as well as the return traffic from that outbound connection (stateful).

1. Navigate back to EC2 using the search bar at the top of the page.
2. Ensure you are using the “New EC2 Experience” indicated at the top left of the screen.

3. In the left navigation panel within the EC2 dashboard, Browse to Network & Security -> Security Groups.



4. Select “Create Security Group” from the upper right-hand side of the page.
5. Name the security group podX-management where X is your assigned pod number, add a required description, we recommend “Management security group for pod <3>”
6. Make sure the VPC is set to vpc-0a61b7f1d92102ad6 (zer0k-main-vpc) since this is where the provisioning of additional VPCs will be done from.

Note: You should be able to delete the current VPC name and begin typing “zer0k” to show available VPC’s.

A screenshot of the AWS 'Create security group' page. The 'Basic details' section shows the security group name 'pod1-management', description 'Management security group for Pod 1', and VPC 'vpc-0a61b7f1d92102ad6 (zer0k-main-vpc)'. The page includes a breadcrumb trail 'EC2 > Security Groups > Create security group' and a title 'Create security group'. A note states: 'A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.'

7. Add an inbound rule allowing ICMPv4 traffic from all IPs.

Inbound rules [Info](#)

Type Info	Protocol Info	Port range Info	Source Info	Description - optional Info
All ICMP - IPv4 ▼	ICMP	All	Anywhere... <input type="text" value="0.0.0.0/0"/>	ICMP from Anywhere

8. Ensure you click “Add Rule” under the inbound rules header.
9. Do not add any other rules at this time.
10. Under Tags, add a new tag. Enter “Name” under Key and podX-management under value where X is your pod number.
11. Under Tags, add a second tag. Enter “event” under Key and “CLUS2022” under value.

Tip – AWS does not name anything by default, always add a “Name” tag to easily find the object later.

Tags - optional
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

Key	Value - optional	
<input type="text" value="Name"/>	<input type="text" value="pod10-management"/>	<input type="button" value="Remove"/>

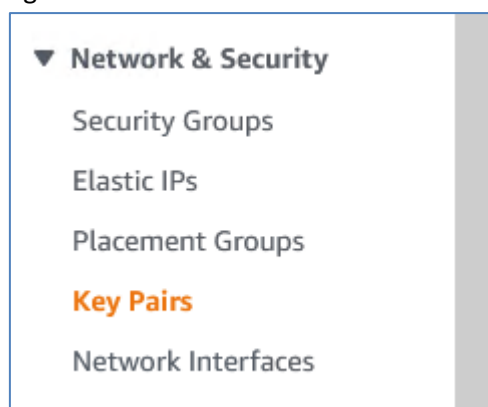
12. Create the security group.

Step 2: Create a Key Pair

Key pairs are used to connect to instances after creation and can be used for other tasks in AWS such as decrypting Windows passwords.

Note: For the following step, the private key created is NEVER available for download again, if it is lost a new key pair must be created.

1. In the EC2 service, navigate in the left bar to Network & Security -> Key Pairs.



2. Select “Create Key Pair”.
3. Name your keypair podX-keypair where X is your pod number. Leave RSA and .pem as default. In this case the AWS UI populates the Name tag as an option, so no tags are required.

aws Services Search for services, features, blogs, docs, and more [Alt+S]

EC2 > Key pairs > Create key pair

Create key pair [Info](#)

Key pair
A key pair, consisting of a private key and a public key, is a set of security credentials that you use to prove your identity when connecting to an instance.

Name
pod1-keypair
The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type [Info](#)
☒ RSA
☐ ED25519

Private key file format
☒ .pem
For use with OpenSSH
☐ .ppk
For use with PuTTY

Tags (Optional)
No tags associated with the resource.

[Add tag](#)
You can add up to 50 more tags.

[Cancel](#) [Create key pair](#)

4. Select “Create key pair” and save the .pem file to your Windows Provisioning Machine. Downloading the file as .pem will allow it to be used from a Linux or Mac host and can be converted later for use in Putty.

This private key is never available for download again, if it is lost a new key pair must be created.

Step 3: Convert PEM to PPK format for dual use

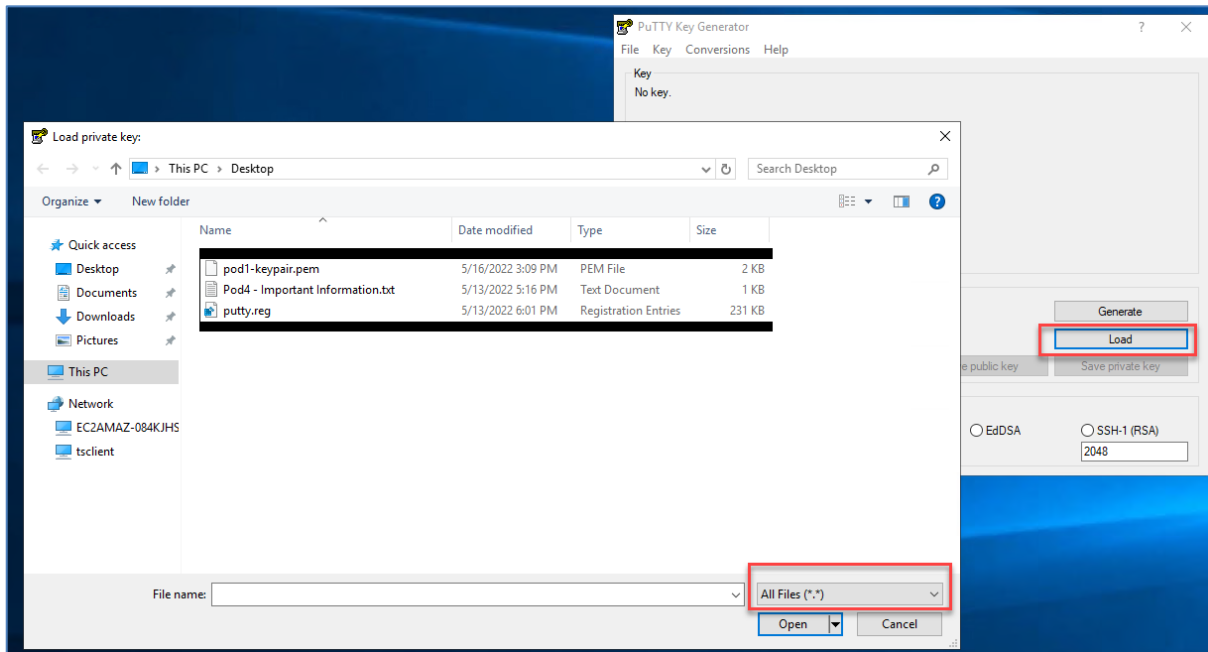
The PEM file downloaded for use as a keypair within AWS will both serve as the keypair within AWS, as well as the connectivity file used for Putty. To use this file within Putty, it must be in PPK format. Locate the PEM file on the Windows Provisioning Machine, it is recommended you move it to the desktop for easy retrieval. By default, Firefox will put it in the Downloads folder.

Putty on Windows:

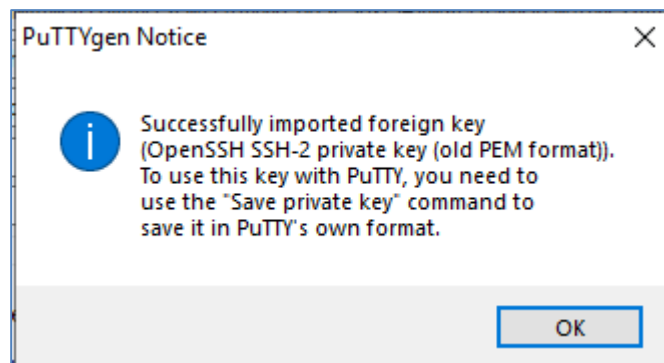
PuTTY is installed on the Windows Provisioning Host and is recommended to be used, however it can be downloaded if doing this on an alternative machine. If you don't already have PuTTY and PuTTYgen, download them from here: <https://www.chiark.greenend.org.uk/~sgtatham/putty/>

1. In the start menu of the Windows Provisioning Machine, navigate to PuTTY -> PuTTYgen and open PuTTYgen.

- Click “Load” and change the file type to “All Files (*.*)” to select the PEM keypair you created in the last task, it should have been named podX-keypair.pem where X is your assigned pod number.



- The selection of the keypair should result in a successful imported foreign key dialog.



- Leave RSA chosen as the default key type under parameters. Save the **private key** without passphrase to the same location as the PEM file. Name this keypair “podX-keypair.ppk” where X is your assigned pod number.

PuTTY Key Generator

File Key Conversions Help

Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAQCTNP56bI68qlpyYxMIARFRGxw3acYJ6Brf84P/4DIRWZWdaZb2N
+q6zw9bjjA/IC7NVnbPKkdu2K0XVSCCxBvR1FRWVOfB4KMcxkJcHS7I0Us7cyw1Qdkzpbj4PTPkz4p2A5QRD
DaYxtD6kOZyQXqkc8MFeE7FnH0EH7ZkMjgQSEqKy9OUxnnndhOnlYCrS6qIf5jgVLiDMCGlhyXxiB5jlz5F1gqWX
5sUxmi40p/Y81VsxRMAAdQ7khLntS/F6fRT/O3H8KGzn7zMhkYCvAGW33yx51zXc8VJPFRqQHpnj7xSo361zqq
```

Key fingerprint: ssh-rsa 2048 SHA256:He4q4RiFge8+LtYa4oMSRD8lqKpYl0vztwyQH0TbSEo

Key comment: imported-openssh-key

Key passphrase:

Confirm passphrase:

Actions

Generate a public/private key pair Generate

Load an existing private key file Load

Save the generated key Save public key **Save private key**

Parameters

Type of key to generate:

☒ RSA ☐ DSA ☐ ECDSA ☐ EdDSA ☐ SSH-1 (RSA)

Number of bits in a generated key:

5. Close PuTTYgen.
6. This converted key will be used later in this task.

Step 4: Create Network Interface

Double check that the Ohio region is chosen in the top right of the AWS console.

1. In the EC2 service, browse to Network & Security -> Network Interfaces.



2. Select "Create network interface".
3. Enter a description of "podX-Ubuntu-Ansible" with X being your pod number
4. Under subnet, choose subnet-0cf86b138b53ba3c9 (zer0k-inside-subnet).

Note: You should be able to delete the current VPC name and begin typing “zer0k” to show available Subnets.

Details [Info](#)

Description - *optional*
A descriptive name for the network interface.

Subnet
The subnet in which to create the network interface.

✕
↻

Use: ins

subnet-0cf86b138b53ba3c9	us-east-2a
zer0k-inside-subnet	Owner: 423620453332

- Under Private IPv4 address, choose custom and enter the IP address of the Ubuntu Ansible Host from table 1-1 above from your assigned pod. It will be 172.18.25.X where X is your assigned pod number.
- Under Security Groups choose the security group created in step 1 of this task above, it should be podX-management where X is your pod number. The filter box can be used to find security groups with your pod number in the name.

Security groups (1/13) [Info](#)

✕
1 match
< 1 >
⚙

<input checked="" type="checkbox"/>	Group ID	Group name	Description
<input checked="" type="checkbox"/>	sg-0cd7f88ae208a10ae	pod10-management	Management security group f...

Note: There are multiple pages in the security groups table. Navigate through them using the arrows next to the search bar, or search for the proper security group.

- Under Tags, add a new tag with a key of “Name” and a value of “podX-Ubuntu-Ansible” where X is the number of your assigned pod.
- Under Tags, add a new tag with a key of “Event” and a value of “CLUS2022” where X is the number of your assigned pod.
- Select “Create network interface” to finish the configuration.

Step 5: Deploy Ubuntu Provisioning Machine

All of the building blocks are in place from a networking standpoint to create an Ubuntu linux instance. The only piece not pre-created is an EBS volume which will be created as part of the current step.

- In the EC2 service, browse to Instances -> Instances.
- Select “Launch instances” from the upper right corner.

- Under Name enter “podX-Ubuntu-Ansible” where X is the number of your assigned pod.
- Under Application and OS Images, choose Ubuntu under quick start and leave the rest default. There should be a Free Tier Eligible Ubuntu instance chosen.

pod1-Ubuntu-Ansible

Add additional tags

▼ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Recents

Quick Start

Amazon Linux

aws

Ubuntu

ubuntu®

Windows

Microsoft

Red Hat

Red Hat

SUSE Linux

SUSE

Browse more AMIs

Including AMIs from AWS, Marketplace and the Community

Amazon Machine Image (AMI)

Ubuntu Server 22.04 LTS (HVM), SSD Volume Type

Free tier eligible

ami-0aeb7c931a5a61206 (64-bit (x86)) / ami-0717cbd2f49a61ed0 (64-bit (Arm))

Virtualization: hvm ENA enabled: true Root device type: ebs

Description

Canonical, Ubuntu, 22.04 LTS, amd64 jammy image build on 2022-04-20

Architecture

AMI ID

64-bit (x86)

ami-0aeb7c931a5a61206

- Under Instance Type leave it as default t2.micro.
- Under Key pair, choose the key pair you created under Step 2 of this task. This is the key pair you have downloaded to your local machine. It should have been named “podX-keypair” where X is your assigned pod number.

CISCO *Live!*

15 | Page

▼ Key pair (login) Info
 You can use a key pair to securely connect to your instance. Ensure that you have access to the selected key pair before you launch the instance.

Key pair name - *required*

▲

×

Proceed without a key pair (Not recommended) Default value

Pod10_Windows_Keypair
Type: rsa

pod10-keypair
Type: rsa

[Create new key pair](#)

[Edit](#)

- Under Network Settings click "Edit".
- Set the VPC to vpc-0a61b7f1d92102ad6 (zer0k-main-vpc).
- Set the Subnet to subnet-0cf86b138b53ba3c9 (zer0k-inside-subnet).
- Leave Auto Assign Public IP disabled as there is no direct internet access from this subnet.

▼ Network settings

VPC - *required* [Info](#)

▼

172.18.0.0/16

Subnet [Info](#)

▼

zer0k-inside-subnet

VPC: vpc-0a61b7f1d92102ad6 Owner: 423620453332
 Availability Zone: us-east-2a IP addresses available: 2030

Auto-assign public IP [Info](#)

▼

[Create new subnet](#)

Warning: Common mistake area!

- Choose Select existing security group but do not select a security group. This was already set under the interface in step 3! This is a quirk of AWS since normally it would just be created or selected here instead of the previously created interface.

Firewall (security groups) Info
 A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

☐ Create security group
 ☒ Select existing security group

Common security groups [Info](#)

▼

[Compare security group rules](#)

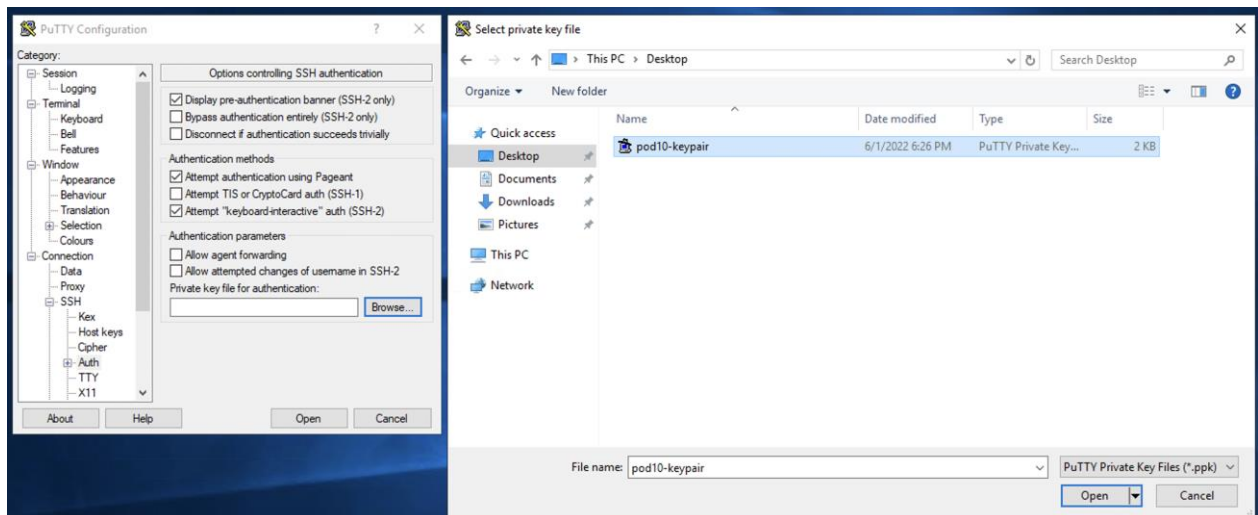
Security groups that you add or remove here will be added to or removed from all your network interfaces.

- You can filter for the appropriate interface by typing podX- in the box and select the interface accordingly.

14. Leave the options under Configure storage and Advanced details as defaults.
15. Select “Launch instance” on the bottom right of the page.
16. If the creation of the instance is successful, click on “View all instances” to go back to the instance list.

In this section the SSH client is just being setup, SSH will not work until Step 6 is completed.

- CISCO** *Live!*



4. Optional: Navigate to Session -> Logging, select "All Session Output", browse, and place the log file in the desktop. This is strictly for future troubleshooting if desired.
5. Do not change any additional settings.
6. Go back to Session and save again.

If using Linux/Mac Command Line

The permissions of the key file must be changed to 400 for the command line ssh client to use the key:

```
> chmod 400 <keyfile>
```

To use the private key file use ssh -i

```
> ssh -i <keyfile> <username>@<host>
```

Step 7: Verify Connectivity

1. In the EC2 service, browse to Instances -> Instances.
2. Verify that the status check for your podX-Ubuntu-Ansible machine is showing **2/2 checks passed**. If it isn't, refresh the page until the status is **2/2 checks passed** or you see a red status. It will have to be troubleshoot if red, move on once it is **2/2 checks passed**.

pod10-Ubuntu-Ansible	i-0f701170fbbe76fa1	Running	t2.micro	2/2 checks passed
----------------------	---------------------	---------	----------	-------------------

3. From your Windows provisioning machine, ping your podX-Ubuntu-Ansible server, remember the IP is 172.18.25.X. This should be successful. If it isn't, recheck your security group. The following steps will also help to troubleshoot.
4. Attempt to SSH to your podX-Ubuntu-Ansible machine from your Windows host using the previously set up profile. It timed out!
5. On the AWS EC2 console, select your podX-Ubuntu-Ansible machine and click on the networking tab below. There should be a message to run the Reachability Analyzer, select this. If you don't see the option, use the search feature to search for VPC Reachability Analyzer, click Create and analyze path.
6. Name it "VPNtoPodX-Ubuntu" where X is the pod number you were assigned.
7. Set the source type to "Instances" and locate the instance named "PodX_Windows_Provisioning", enter the IP address as 172.18.26.X which is your Windows Provisioning host.
8. Set the destination type to "Network Interfaces" and locate the network interface named "podX-Ubuntu-Ansible" where X is your pod number. Also leave the IP blank.

- Set the destination port to “22” for SSH and the protocol as TCP.

Path configuration

Name tag - *optional*
Creates a tag with a key of 'Name' and a value that you specify.

VPNtoPod10-Ubuntu

Source type: Instances
Source: i-0ef82f123d2bdb649
Source IP address - *optional*: 172.18.26.10

Destination type: Network Interfaces
Destination: eni-018749fae055d3c69
Destination IP address - *optional*: 192.0.2.1

Destination port - *optional*: 22
Number must be between 0 and 65535

Protocol: TCP
Use the appropriate protocol

- Select Create and analyze path in the bottom right.
- You will see the Analyses as pending, refresh the page until you see success. The reachability status should be **Not Reachable**.

Analysis ID	Analysis run date	Reachability status	Intermediate comp...	State
nia-0d15960615ec989b0	Sun May 08 2022 20:5...	Not reachable	-	Succeeded

- Check under Explanations to see why AWS thinks your instance isn't reachable on port 22. It should be because of a missing security group rule.

Explanations

None of the ingress rules in the following security groups apply: [sg-0a35a35a7327b7fb6](#).

- Click on the link to the security group and add another inbound entry for SSH from anywhere, all hosts are behind the ASA firewall already so allowing from anywhere is fine for this lab.

SSH TCP 22 Anywh... SSH from Anywhere

0.0.0.0/0

- Go back to the VPC Reachability Analyzer and select the radio button for your path analysis. From the Actions menu select Analyze Path, click confirm.
- There will be a new entry pending under Analysis, click refresh until it succeeds. The Reachability status should now be reachable. If it is not, view the Explanations.
- From your Windows machine, attempt to SSH to your provisioning machine, it should succeed this time and you should be at an ubuntu command prompt.

Task 3: Configure DNS in Route 53

ISE requires DNS for many operations including initial database priming and any internode operations.

Figure 4-1

Pod	Primary Hostname	Primary IP Address	Secondary Hostname	Secondary IP Address
-----	------------------	--------------------	--------------------	----------------------

Pod 1	pod1-ise1	10.1.0.5	pod1-ise2	10.1.0.6
Pod 2	pod2-ise1	10.2.0.5	pod2-ise2	10.2.0.6
Pod 3	pod3-ise1	10.3.0.5	pod3-ise2	10.3.0.6
Pod 4	pod4-ise1	10.4.0.5	pod4-ise2	10.4.0.6
Pod 5	pod5-ise1	10.5.0.5	pod5-ise2	10.5.0.6
Pod 6	pod6-ise1	10.6.0.5	pod6-ise2	10.6.0.6
Pod 7	pod7-ise1	10.7.0.5	pod7-ise2	10.7.0.6
Pod 8	pod8-ise1	10.8.0.5	pod8-ise2	10.8.0.6
Pod 9	pod9-ise1	10.9.0.5	pod9-ise2	10.9.0.6
Pod 10	pod10-ise1	10.10.0.5	pod10-ise2	10.10.0.6

1. Search for "Route 53" in the AWS Console.
2. Under DNS Management, choose "Hosted zones"
3. Zer0k has already been registered so click on zer0k.org.
4. As part of the ISE provisioning, the Primary ISE node in your pod (10.x.0.5) will be provisioned into Route53. To help understand the task done via script, you will register the second node manually.
5. Click "Create record" and enter the following information (replace X with your pod number):
 - a. Record name – podX-ise2
 - b. Value – 10.X.0.6
6. Leave the rest of the values as default then click "Create records".

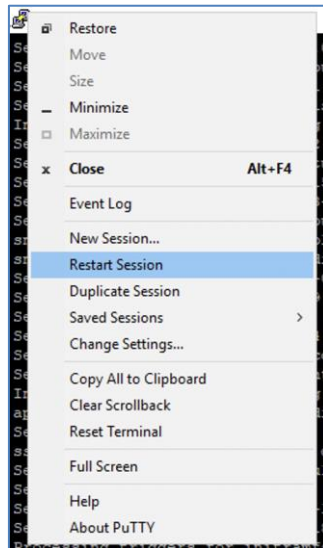
<input type="checkbox"/>	pod0-ise1.zer0k.org	A	Simple	-	10.0.0.5
<input type="checkbox"/>	pod0-ise2.zer0k.org	A	Simple	-	10.0.0.6

Task 4: VPC Automation

Step 1: Deploy Ansible

First the ansible/python environment needs to be set up on the Ubuntu server. If you are not connected to your pod's Ubuntu server, do that now. The private key currently only exists on the Windows Provisioning machine so use the previously setup putty profile to connect.

1. Open PuTTY and load the saved session created previously.
2. Ubuntu uses apt for its package manager, first apt needs to be updated to get the most current package and version list from the default package repository: ***sudo apt-get update***.
3. Upgrade the packages on the system to the most current versions: ***sudo apt-get upgrade***. Answer "Y" when shown how much space the upgrades will take.
4. You will be prompted to restart services that are using some of the packages that were updated. Leave the defaults selected and select (tab, enter) OK.
5. There are some services that cannot be restarted individually so restart the system to get those services using the latest package versions: ***sudo shutdown -r now***. This will prevent further restart messages in the future.
6. Restart the putty session by right clicking the putty icon on the window and selecting Restart Session. If it times out, try again until it connects, it could take a couple of minutes.



7. This lab will use a python virtual environment. Venv is not installed by default so install it: **`sudo apt install python3.10-venv`**. A virtual python environment allows for different projects on the same machine to use different versions of shared python libraries.
8. Create a venv for this lab, this will create a new folder in the /home/ubuntu directory: **`python3 -m venv ISEonAWS`**.
9. Activate the newly created ISEonAWS virtual environment by running the activation script: **`source ISEonAWS/bin/activate`**. This script sets up environment variables on the system to use the activated virtual environment. You should see the linux prompt prepended with (ISEonAWS) at this time.
10. Install the python packages required to run ansible for ISE: **`python -m pip install ansible boto boto3 botocore ciscoisesdk jmespath`**. This step will take a few minutes.
11. Add the ISE collection to ansible: **`ansible-galaxy collection install cisco.ise`**.

Step 2: Clone the GIT Repository for Script Execution

Clone the scripts to be used for execution from GIT into the production provisioning machine. These will be used to execute all tasks for the remainder of the lab. There isn't enough time in the lab for you to write the scripts but as you go through and execute them, take some time to read over the scripts first.

1. Download (Clone) the GIT repository to the local machine. Execute the command:

```
git clone https://github.com/plloyd44/CiscoLive_ISE_in_AWS.git
```

```
Cloning into 'CiscoLive_ISE_in_AWS'...
```

```
...
```

```
Receiving objects: 100% (228/228), 190.28 KiB | 17.30 MiB/s, done.
```

```
Resolving deltas: 100% (125/125), done.
```

2. There should be 2 directories in your home directory at this point, run **`ls -l`** to verify.

```
(ISEonAWS) ubuntu@ip-172-18-25-10:~$ ls -l
total 8
drwxrwxr-x 7 ubuntu ubuntu 4096 Jun  1 20:33 CiscoLive_ISE_in_AWS
drwxrwxr-x 5 ubuntu ubuntu 4096 Jun  1 20:27 ISEonAWS
(ISEonAWS) ubuntu@ip-172-18-25-10:~$
```

Step 3: Configure the Environmental Variables to be Used

As part of the deployment process, multiple variables are used to ensure configurations are populated and access keys are available to the Python virtual environment running Ansible. There are two areas where variables are stored for the script to work, the first is locally in the vars/main.yaml file, the second is as deployed into the environment via export statements.

The following is to be done within the SSH session to Ubuntu:

1. Edit the vars/main.yaml file to update your pod number, which will be utilized throughout the lab. Execute the commands:

```
cd CiscoLive_ISE_in_AWS
```

```
cd vars
```

```
nano main.yaml
```

2. Edit the line in main.yaml **pod_id**: to match your pod number. Exit and save from nano utilizing the key sequence "Ctrl-X, Y, <enter>"
3. Once back at the Ubuntu command line, execute the export commands found in the file "PodX Important Information.txt" on the Windows desktop. It should look like the following:

```
export ise_username=admin
```

```
export ise_password=ABCXYZ
```

```
export AWS_REGION=us-east-2
```

```
export AWS_ACCESS_KEY= XXXXXXXXXXXXXXXXXXXXXXXX
```

```
export AWS_SECRET_KEY= YYYYYYYYYYYYYYYYYYYYYYYYYYYY
```

```
export ise_verify=false
```

4. Replace the access key and secret key with the one you created in Task 1, Step 6.
5. Paste this block of text into the Ubuntu CLI.

Note: Right click in PuTTY will paste commands, do not use ctrl+v

6. Verify by running the **env** command:

```
(ubuntu) root@ip-10-0-1-217:/home/ubuntu# env
...
ise_password=ABCXYZ
AWS_ACCESS_KEY=XXXXXXXXXXXXXXXXXXXXX
AWS_SECRET_KEY=YYYYYYYYYYYYYYYYYYYYYYY
```

```
ise_username=admin
...
AWS_REGION=us-east-2
...
ise_verify=false
```

Step 4: Deploy the AWS Network Environment and Primary ISE Node

Configure the AWS environment to create a network into which ISE will get deployed.

1. View the playbook that will create the ssh key pair ansible will use to install and connect to ISE. This task will generate a new key and save it for use later locally.

```
cd /home/ubuntu/CiscoLive_ISE_in_AWS/  
cat ssh_key_pair.yaml
```

2. Generate the SSH Key to be used from the provisioning machine to access all nodes within the AWS environment. Execute the following command:

```
ansible-playbook ssh_key_pair.yaml
```

Expected Output:

```
PLAY [AWS VPC with Cisco ISE and Meraki vMX]  
***
```

```
TASK [Gathering Facts]  
***
```

```
ok: [localhost]
```

```
TASK [Check for existing keypair]  
***
```

```
ok: [localhost]
```

```
TASK [Create EC2 SSH Key Pair]  
***
```

```
changed: [localhost]
```

```
TASK [Show key_pair]  
***
```

```
msg: key pair created
```

```
TASK [Save Private Key Locally]  
***
```

```
changed: [localhost]
```

```
PLAY RECAP  
***
```

```
localhost      : ok=5  changed=2  unreachable=0  failed=0  skipped=0  rescued=0  
ignored=0
```

3. Verify that there are no skipped or failed steps in the play recap. If so, determine which step needs to be followed to remediate.

Note: If the private key is not displayed, or the task is marked as “skipped”, contact a lab proctor.

4. Deploy the VPC, Subnet, Routing Table, and Internet gateway for the ISE environment. This will deploy your pod VPC as shown in the initial network diagram. Execute the command:

ansible-playbook ise_in_aws.vpc.yaml

Expected Output:

PLAY [AWS VPC with Cisco ISE and Meraki vMX]

TASK [Gathering Facts]

ok: [localhost]

TASK [Create VPC]

changed: [localhost]

TASK [Create an Internet Gateway to connect VPC to Internet]

changed: [localhost]

TASK [Create Public_Subnet]

changed: [localhost]

TASK [Create Private_Subnet]

changed: [localhost]

TASK [Create Public Route Table; Add Route from VPC to Internet Gateway]

changed: [localhost]

TASK [Create Private Route Table]

changed: [localhost]

TASK [Show VPC(s)]

ok: [localhost]

TASK [Create SG-ISE Security Group]

7. Deploy the ISE primary node into the ISE environment. Execute the command:

```
ansible-playbook ise_in_aws.ise.yaml
```

Expected Output:

```
PLAY [AWS VPC with Cisco ISE and Meraki vMX]
```

```
TASK [Create ISE 3.1 Instance in AWS]
```

```
***
```

```
changed: [localhost] => (item={'name': 'ise', 'instance_type': 'c5.4xlarge', 'public_dns_name': 'ise.zer0k.org', 'private_dns_name': 'ise.zer0k.org', 'dns_alias': 'ise.zer0k.org', 'private_ip': '10.0.0.5', 'role': 'Primary', 'personas': ['Standalone']})
```

```
TASK [Show SSH Commands for ISE Instances]
```

```
***
```

```
ok: [localhost] => (item={'name': 'ise', 'instance_type': 'c5.4xlarge', 'public_dns_name': 'ise.zer0k.org', 'private_dns_name': 'ise.zer0k.org', 'dns_alias': 'ise.zer0k.org', 'private_ip': '10.0.0.5', 'role': 'Primary', 'personas': ['Standalone']}) =>
```

```
msg:
```

```
- ping 10.192.168.44
- ssh -i ~/.ssh/ISEinAWS-palloyd.pem admin@10.0.0.5
- ping ise.zer0k.org
- ssh -i ~/.ssh/ISEinAWS-palloyd.pem admin@ise.zer0k.org
```

```
PLAY RECAP
```

```
***
```

```
localhost: ok=11 changed=8 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
```

Step 5: Visit the AWS Environment to Ensure the Network Environment Was Provisioned

With the scripts being successfully run it is time to verify that they created and configured the environment as expected.

1. Verify the VPC was deployed. Navigate to the search bar in AWS, type VPC. Click VPC in the results, the VPC should be named ISEinAWS-podX where X is your assigned pod number.

<input type="checkbox"/>	zer0k-pod0	vpc-0105fb3ba3f6cbec3	✔ Available	10.0.0.0/16
<input type="checkbox"/>	ISEinAWS-pod9	vpc-0dbba522e2e80f740	✔ Available	10.9.0.0/16
<input checked="" type="checkbox"/>	ISEinAWS-pod10	vpc-06c27a7f1c1c05e39	✔ Available	10.10.0.0/16
<input type="checkbox"/>	zer0k-main-vpc	vpc-0a61b7f1d92102ad6	✔ Available	172.18.0.0/16

2. Navigate to Subnets in the left menu. Verify the Private subnet is deployed in accordance with your pod. It should be named zer0k_podX_Private_Subnet where X is your assigned pod number.

<input type="checkbox"/>	zer0k-public-subnet	subnet-0653589a8ba2fa824	Available	vpc-0a61b7f1d92102ad6 zer...	172.18.0.0/21
<input type="checkbox"/>	zer0k-private-subnet	subnet-059dc621173c4d170	Available	vpc-0a61b7f1d92102ad6 zer...	172.18.16.0/21
<input type="checkbox"/>	zer0k-inside-subnet	subnet-0cf86b138b53ba3c9	Available	vpc-0a61b7f1d92102ad6 zer...	172.18.24.0/21
<input checked="" type="checkbox"/>	zer0k_pod10_Private_Su...	subnet-029c6bc2fea840f4c	Available	vpc-06c27a7f1c1c05e39 ISEi...	10.10.0.0/24

3. Navigate to Route Tables in the left menu. Verify a routing table was provisioned for your pod. It should be named zer0k_podX_Private_Subnet where X is your assigned pod number.

<input type="checkbox"/>	zer0k-pod0-routes	rtb-0a3688c11d7f9d1e5	-	-	Yes
<input type="checkbox"/>	-	rtb-087124f0d6b64d4e9	-	-	Yes
<input checked="" type="checkbox"/>	zer0k_pod10_RT_Private	rtb-0c9efdacacd157476	subnet-029c6bc2fea840...	-	No

Step 6: Add Transit Gateway Attachment and Route

The lab is routing all traffic through the main VPC through the ASA. To get traffic to the main VPC from the Pod VPC a transit gateway is needed. As of the writing of this lab the ansible collection does not include the ability to attach to a transit gateway so that will be done in this step manually. The Transit gateway has already been created so all that is left is to attach to the transit gateway then update the routing in the Pod VPC to route traffic to the transit gateway.

1. In the AWS console go to the VPC service -> Transit Gateways -> Transit Gateway Attachments
2. Click Create transit gateway attachment on the top right of the page.
3. Name it podX-transit-attach where X is your assigned pod number.
4. Choose the "zer0k-transit-gateway" under the Transit gateway ID, it should be the only entry.
5. Leave the Attachment type as VPC since you are attaching to another VPC.

Details

Name tag - optional
Creates a tag with the key set to Name and the value set to the specified string.

pod10-transit-attach

Transit gateway ID [Info](#)

tgw-00ecf6a9a26ff37cf (zer0k-transit-gateway)

Attachment type [Info](#)

VPC

6. Under VPC attachment, leave DNS support enabled and select your VPC from the list of VPC IDs. It will be named ISEinAWS-podX where X is your assigned pod.
7. A list of subnets will be shown, select the zer0k_podX_Private_Subnet. It should be the only entry available as the VPC setup script only created a single subnet.

VPC attachment
Select and configure your VPC attachment.

☒ DNS support [Info](#)

☐ IPv6 support [Info](#)

VPC ID
Select the VPC to attach to the transit gateway.

vpc-06c27a7f1c1c05e39 (ISEinAWS-pod10) ▼

Subnet IDs [Info](#)
Select the subnets in which to create the transit gateway VPC attachment.

☐ us-east-2a

☐ us-east-2b

☒ us-east-2c

subnet-029c6bc2fea840f4c (zerOk_pod10_Private_Subnet)

subnet-029c6bc2fea840f4c (zerOk_pod10_Privat... ▲

subnet-029c6bc2fea840f4c X

8. The Name tag should already be filled out from above, select Create transit gateway attachment.
9. Next browse to Virtual Private Cloud -> Route Tables and find your pod VPC routing table. It is named zerOk_podX_RT_Private where X is your assigned pod number. Check the box next to the name of the Route Table.
10. The bottom half of the screen will load the Route table details, select the Routes tab and then select Edit routes.

rtb-0c9efdacacd157476 / zerOk_pod10_RT_Private

Details **Routes** Subnet associations Edge associations Route propagation Tags

Routes (1) Edit routes

Q Filter routes Both ▼

11. Add a default route pointing to the transit gateway by selecting 0.0.0.0/0 under the Destination and by selecting Transit Gateway -> podX-transit-attach under Target where X is your assigned pod number.

Destination	Target	Status
10.10.0.0/16	Q local X	Active
Q 0.0.0.0/0 X	Q tgw-00ecf6a9a26ff37cf X	-

12. Save the changes.

Step 7: Establish an SSH session with ISE

Note: ISE will need to initialize and can take up to 15 minutes to fully deploy. You can verify the status of your ISE instance in EC2 -> Instances. In the Status check header in the EC2 dashboard, the status for ISE must have all checks passed, as opposed to "initializing"

1. Establish an SSH session with ISE to verify services transition through a Not Running -> Initializing -> Running cycle. This should be done from the Ubuntu machine.

NOTE: SSH will fail until ISE is fully provisioned and running. This can take up to 15 minutes. Progress can be monitored in the AWS console within the EC2 Instances area. This will manifest itself as:

```
“(ISEonAWS) ubuntu@ip-172-18-25-4:~/.ssh$ ssh -i ISEinAWS-pod4.pem admin@10.4.0.5
admin@10.4.0.5: Permission denied (publickey).”
```

2. Execute the following command:

`ssh -i ~/.ssh/ISEinAWS-pod<#>.pem admin@10.X.0.5` where X is your pod number.

3. You will be prompted to accept the ssh fingerprint of the ISE server. Enter yes.

Run the following command:

ise/admin# **`show application status ise`**

ISE PROCESS NAME	STATE	PROCESS ID

Database Listener	running	32895
Database Server	running	85 PROCESSES
Application Server	not running	
...		
Application Server	initializing	49728
...		
Application Server	running	

4. Once the Application Server shows as “running” move on to the next step.

Step 8: Verify the running configuration of ISE to align with your Pod

Verify the running configuration, including IP address for the private facing interface, aligns with expected IP’s for your pod. Also verify DNS is provisioned to the correct server.

Execute the command: ise/admin# **`show run`**

Expected Output:

Generating configuration...

!

```

ip domain-name zer0k.org

interface GigabitEthernet 0

    ip address 10.X.0.5 255.255.255.0

    !

ip name-server 169.254.169.253

ip default-gateway 10.X.0.1

clock timezone EST5EDT









    !

```

Step 9: Launch ISE from a Web Browser

Launch a web browser to ISE from your Windows Provisioning machine, ignoring any certificate errors. Ensure login to the GUI is successful, and that no configurations are currently present in the Users, Roles, Network Devices or Network Device Groups areas.

1. Log into ISE using the administrative username **admin** password **is provided by your proctor**
2. Using the hamburger menu on the top left of the screen, navigate to Administration -> Identity Management -> Groups -> User Identity Groups
3. Verify only default ISE groups are populated, including OWN_ACCOUNTS, ALL_ACCOUNTS

<input type="checkbox"/>	 ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>	 Employee	Default Employee User Group
<input type="checkbox"/>	 GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/>	 GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group

4. Navigate to Administration -> Identity -> Identities
5. Verify there are no users present in the identity store
6. Navigate to Administration -> Network Device Groups
7. Verify only default ISE NDG's are present.

<input type="checkbox"/>	All Device Types	All Device Types
<input type="checkbox"/>	All Locations	All Locations
<input type="checkbox"/>	> Is IPSEC Device	Is this a RADIUS over IPSEC Device

8. Navigate to Administration -> Network Devices
9. Verify no Network Devices are currently present.

Step 10: Configure ISE Programmatically

Note: Should the following steps be performed outside of the lab or across regions, ensure that the correct IP is used for the `ise.configuration.yaml` script. If not, the script will perform 1000 pings before timing out.

If this happens it can be interrupted with `ctrl+c`.

1. Exit from the ISE SSH session using the “exit” command.
2. Configure ISE from the Ansible virtual environment, to populate the Network Device Groups, Network Devices, User Roles, and Users. Run these commands from the Ubuntu-Ansible machine.

Execute the command: **`ansible-playbook ise.configuration.yaml`**

Expected Output:

PLAY [ISE Configuration Playbook]

TASK [Query for ISE instances in project "ISEinAWS-palloyd"] ...

TASK [Show instances] ...

TASK [Test for ISE Application Server Initialization] ...

TASK [Ping 10.X.0.5] ...

TASK [Wait for <private_IP> App Server (GUI)] ...

TASK [Show <private_IP> Initialized] ...

TASK [Enable ISE ERS & OpenAPIs] ...

TASK [Enable ISE OpenAPIs (ISE 3.1+)] ...

TASK [Show ISE OpenAPIs Enabled Status] ...

TASK [Show ISE OpenAPIs Disabled Status] ...

TASK [Get ISE ERS APIs Status] ...

TASK [Enable ise.zer0k.org ERS APIs] ...

TASK [Show ise.zer0k.org ERS Enabled Status] ...

TASK [Show ise.zer0k.org ERS Disabled Status] ...

TASK [Create RADIUS Probes - identity_group and internal_users] ...

TASK [Create `RADIUS_Probes` identity group] ...

TASK [Create Internal Users] ...

TASK [Create Internal User Accounts] ...

TASK [Create Network Device Groups] ...

TASK [Create demo network_devices] ...

TASK [Include Endpoints] ...

TASK [Create Endpoints] ...















PLAY RECAP

localhost : ok=39 changed=6 unreachable=0 failed=0 skipped=4 rescued=0 ignored=0

Step 11: Verify Newly Configured Users, Groups, and Network Access Devices

1. On your Ubuntu provisioning machine, navigate to ~/CiscoLive_ISE_in_AWS/vars.
2. Execute a more on each file to explore what is expected to be configured, including users, groups, network device groups, and network devices.
3. Using the hamburger menu on the top left of the screen, navigate to Administration -> Identity Management -> Groups -> User Identity Groups
4. Verify the RADIUS_Probes group has been created as a group to assign users to.

User Identity Groups

 Edit  Add  Delete  Import  Export		
	Name	Description
<input type="checkbox"/>	 ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/>	 Employee	Default Employee User Group
<input type="checkbox"/>	 GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/>	 GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_SocialLogin (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/>	 OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/>	 RADIUS_Probes	Group for RADIUS probe internal users

5. Navigate to Administration -> Identity -> Identities

6. Verify the users found in the “internal_users.thomas.yaml” are configured as expected.

Identities Groups External Identity Sources Identity Source Sequences Setting

Users

Latest Manual Network Scan Res...

Network Access Users

[Edit](#) [+ Add](#) [Change Status](#) [Import](#) [Export](#)

	Status	Username	Description
<input type="checkbox"/>	✓ Enabled	chmula	
<input type="checkbox"/>	✓ Enabled	cocarson	
<input type="checkbox"/>	✓ Enabled	elparis	
<input type="checkbox"/>	✓ Enabled	jedubois	
<input type="checkbox"/>	✓ Enabled	meraki_8021x_test	
<input type="checkbox"/>	✓ Enabled	palloyd	
<input type="checkbox"/>	✓ Enabled	radius-probe	
<input type="checkbox"/>	✓ Enabled	thomas	
<input type="checkbox"/>	✓ Enabled	vibobrov	

7. Navigate to Administration -> Network Device Groups
8. Verify the network device groups found in “network_device_groups.yaml” are configured as expected.

Network Device Groups

All Groups

Choose group

Refresh

+

Add

Duplicate

Edit

Trash

Show group members

Import

Export

Flat Table

Expand All

Collapse All

<input type="checkbox"/>	Name	Description
<input type="checkbox"/>	> All Device Types	All Device Types
<input type="checkbox"/>	> All Locations	All Locations
<input type="checkbox"/>	▼ Enforcement	All Enforcement Options
<input type="checkbox"/>	Closed	Closed
<input type="checkbox"/>	LowImpact	LowImpact
<input type="checkbox"/>	Monitor	Monitor
<input type="checkbox"/>	> Is IPSEC Device	Is this a RADIUS over IPSEC Device
<input type="checkbox"/>	▼ PIN	Place in the Network (PIN)
<input type="checkbox"/>	Branch	Branch
<input type="checkbox"/>	Campus	Campus
<input type="checkbox"/>	Cloud	Cloud
<input type="checkbox"/>	InternetEdge	InternetEdge

9. Navigate to Administration -> Network Devices

10. Verify only one network device, the ASA Headend, was configured.

Network Devices

Edit

+

Add

Duplicate

Import

Export

Generate PAC

Delete

<input type="checkbox"/>	Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/>	ASA_Headend	172.18.24.254/32	Cisco	AMER	VPN_Headend#ASA	ASA_Headend

Task 5: Azure AD integration via ROPC for Remote Access VPN

This task will have you create the basics needed for ISE integration with Azure and

Step 1: Log into Azure and Configure Users/Groups

1. Log into <https://portal.azure.com> with the pod administrator: **podX-admin@zer0k.onmicrosoft.com** where X is the number of your pod and the password is **provided by your proctor**
2. Using the search bar, search for “groups” and add a new group of type Security.
3. Name the group **podX-vpn-users** where X is your pod number, and give it a description for users who will be allowed to log into VPN later.

Group type * ⓘ
 Security

Group name * ⓘ
 pod10-vpn-users

Group description ⓘ
 Pod 10's VPN Users

Membership type ⓘ
 Assigned

Note: It may take a minute before the group shows up in the All Groups area of Azure Active Directory. Please be patient and hit refresh.

- Using the search bar at the top of the page, search for “users” and add a new user. Name it **podX-vpn-user** where X is your pod number and give it a name.
- Under “Groups and roles, click the “0 groups selected” link to select the group you created in the prior step.

Groups

Select groups in which this user is to be a member


Search

PO pod4-vpn-users
Selected

PO pod7-vpn

- You can use an auto-generated password or create a password, make sure you note the password before submitting the user.

Identity

User name * ⓘ @ 
The domain name I need isn't shown here


Name * ⓘ

First name

Last name

Password

☒ Auto-generate password
☐ Let me create the password

Initial password 

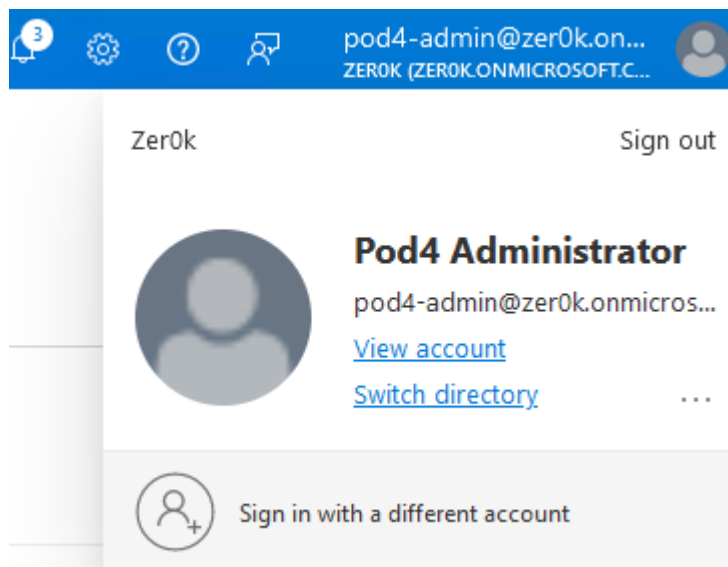
☒ Show Password

Groups and roles

Groups [1 groups selected](#)

Roles [User](#)

7. Azure requires the password to be reset before authentication can be done to that user. This cannot be done through the VPN auth so click your username at the top right of the screen and “sign in with a different account”



8. Sign in with the user you just created (the @zer0k.onmicrosoft.com suffix is required). You will be prompted to reset your password. Once you successfully log in, note the new password you just created and switch back to the pod admin user.

Step 2: Configure application integration in Azure

1. Search for App Registrations and choose “New registration”, name the app **podX-ise-integration** where X is your assigned pod number, and leave

the Support account types as “Accounts in this organizational directory only”. This application will not need a redirect URI.

*** Name**
The user-facing display name for this application (this can be changed later).

pod10-ise-integration ✓

Supported account types
Who can use this application or access this API?

☒ Accounts in this organizational directory only (Zero only - Single tenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform ▼ e.g. https://example.com/auth

2. Click Register.
3. On the left menu bar, select “Certificates & secrets”. This is the OAuth secret key that will be used to integrate ISE with Azure. Click “New Client Secret” and enter a description of “podX-ISE” where X is your pod number. Click Add at the bottom of the dialog box.
4. Copy the secret key value to a notepad before leaving the page

Warning: This value cannot be viewed again after leaving the page. If you forget this step, delete the client secret and create a new one.

Certificates (0) Client secrets (1) Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

Description	Expires	Value ⓘ	Copy to clipboard	Set ID
Secret for ISE Integration	12/3/2022	Stm8Q~b8ft_lul29HAdBEVZbtnJXrLDRo4 ...		a4911819-5d55-4bad-9812-1d537f2d19de

5. Configure the application for ROPC by going to the Authentication tab on the left menu. ISE does not use a URI based redirect flow so under Advanced Settings set the “Allow public client flows” setting to Yes. Click Save.

Advanced settings

Allow public client flows ⓘ

Enable the following mobile and desktop flows:

Yes

No

- App collects plaintext password (Resource Owner Password Credential Flow) [Learn more](#)
- No keyboard (Device Code Flow) [Learn more](#)
- SSO for domain-joined Windows (Windows Integrated Auth Flow) [Learn more](#)

6. Under Token Configuration in the left menu, add a groups claim so that you can later create ISE policies that refer to groups in Azure. The groups claim should allow access to the following group types:

- Security Groups
- Directory Roles
- All Groups

Click Add.

Select group types to include in Access, ID, and SAML tokens.

☒ Security groups

☒ Directory roles

☒ All groups (includes distribution lists but not groups assigned to the application)

☐ Groups assigned to the application

7. Add API permission for the groups graph API. In the left menu select API permissions then click Add a permission. In the window that pops up choose Microsoft Graph then Application Permissions.
8. Search for group then under the group drawer, select Group.Read.All, notice that Admin consent required is shown as Yes. Select Add Permissions at the bottom of the screen.

Select permissions

group

Permission	Admin consent required
> Calls	
<div> <div>Group (1)</div> <div> <div><input type="checkbox"/> Group.Create ⓘ Create groups</div> <div><input checked="" type="checkbox"/> Group.Read.All ⓘ Read all groups</div> <div><input type="checkbox"/> Group.ReadWrite.All ⓘ Read and write all groups</div> </div> </div>	<div>Yes</div> <div>Yes</div> <div>Yes</div>

9. Before moving on ask your lab proctor to provide consent for your new API Permission.
10. Open the overview page for the application, that information will be needed in the next steps.

Step 3: Enable the ROPC feature in ISE

1. Go to Administration -> Identity Management -> Settings -> REST ID Store Settings and enable the feature. This is required as of ISE 3.1 since the feature is currently a beta feature.

Step 4: Register ISE with Azure

1. In ISE, browse to Administration -> Identity Management -> External Identity Sources from the hamburger menu icon at the top left of the ISE UI.
2. From the REST (ROPC) option, add a new entry.
3. Name it **zer0k_azure** and fill in the information obtained from the overview page under the application created in Step 2 from Azure. The client secret should have been saved to a notepad. The username suffix for this lab is **@zer0k.onmicrosoft.com**.

^ Essentials

Display name	: pod10-ise-integration
Application (client) ID	: 6846a86b-36b5-4e7c-bc96-7e98b5dda0a8
Object ID	: 89de3286-75f2-46f9-9d3c-318164d42ad0
Directory (tenant) ID	: 6d92df37-cb73-4152-bfd5-54c7828c09c4
Supported account types	: My organization only

Note: In the Azure overview, the Client ID is the “Application (client) ID” and the tenant ID is the “Directory (tenant) ID”.

General Groups

Name *
zer0k_azure

Description

REST Identity Provider *
Azure Identity Store

Client ID *
6846a86b-36b5-4e7c-bc96-7e98b5dc

Client Secret *
●●●●●

Tenant ID *
6d92df37-cb73-4152-bfd5-54c7828c

Test connection

Username Suffix
@zer0k.onmicrosoft.com

4. Test the connection, if it is successful go to the groups tab and select the **podX-vpn-users** group you created earlier.
5. In order to use groups in policy they need to be selected here in the ROPC connection. Click in the drop down to select the group you created in earlier steps. You only have to hit the Load Button once to get groups to populate into the dropdown.

REST (ROPC) > zer0k_azure

REST ID Store

General **Groups**

Groups
pod10-vpn-users

Load Groups

Cancel Save

6. Save the connection.

Step 5: Configure ISE Policy for VPN Authentication

1. Go to the ISE menu -> Policy -> Policy Sets and select the "+" in the top left to add a new policy set.

2. Give the policy set a name of “PodX-VPN-Policy” where X is your pod number, and select “Default Network Access” under Allowed Protocols / Server Sequence.

Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence
	✓	Pod4-VPN-Policy		+	Default Network Access +

3. Click the “+” under conditions which will launch the conditions studio.
4. The network device and network device group were created by the initial configuration ansible scripts. They will be used here to match authentication from the VPN headend.
 - “click to add an attribute” and use the “network device” filter icon:

Conditions Studio

Library

Search by Name

- Catalyst_Switch_Local_Web_Authentication
- Switch_Local_Web_Authentication
- Switch_Web_Authentication

Editor

Click to add an attribute

Select attribute for condition

Click to add an attribute

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
DEVICE	Device Type		


- Choose Device: Device Type and choose the “All Device Types#VPN Headends#ASA” device type with the equals operator. The save button will allow you to save the condition for later, in this case choose “Use” at the bottom of the page to use it now.

✓	Remote Access VPN	DEVICE-Device Type EQUALS All Device Types#VPN Headends	Default Network Access + 0
---	-------------------	---	-----------------------------

5. Save the policy sets.
6. Click the “View” arrow on the right side of the policy set line to enter the policy set configuration.
7. Expand “Authentication Policy” and set the default entry to what you named your ROPC connection.

✓	Default	zerOk_azure
		> Options

8. Expand “Authorization Policy” and click the “+” on the top of the authorization policy list to add a new entry, this entry will be used to match the group created on Azure and permit access to the VPN.

- “click to add an attribute and select the groups icon to filter the attributes: 
- Choose your ROPC connection name: External Groups and then select the group you have added your user to in Azure.

Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow

Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID
All Dictionaries	Attribute	ID
CWA	CWA_ExternalGroups	
IdentityGroup	Description	
IdentityGroup	Name	
InternalUser	IdentityGroup	
PassiveID	PassiveID_Groups	
zer0k_azure	ExternalGroups	

- Leave the default as equals and choose use at the bottom of the screen to use the newly created condition.

9. Back on the Policy Set page set the Result to “Permit Access” then save.


VPN Users
zer0k_azure-ExternalGroups EQUALS pod0_users
PermitAccess x
+
Select from list

Task 6: Test VPN Authentication

Step 1: Test VPN Authentication

- On your Windows Provisioning Machine, browse to <https://172.18.24.254>, accept any certificate errors that are presented.
 - Choose your pod number from the drop down (If authentication fails the dropdown is reset every time).
 - Log in using the Azure user previously created. The username should be **podX-VPN-user** where X is your assigned pod number.

If you did not populate the user suffix in previous steps, you may need to add @zer0k.onmicrosoft.com

2. You will be prompted to install AnyConnect, complete the installation. When the install completes, launch AnyConnect from the Windows start menu and connect to 172.18.24.254. You will be prompted for the pod number and the same username/password.
3. You will get a Certificate warning - Click change settings -> De-Select Block connections to untrusted servers, Connect again -> Connect anyway.
4. After successfully connecting you should be able to ping the super secret linux server at 172.18.16.10.
5. On ISE, browse to the ISE Menu -> Operations -> Radius -> Live Logs. Here you can see the authentication attempts and successful authentications to the VPN.
6. Click the details icon  on one of the successful authentications where you can see the attributes available on the authentication and the steps ISE took to authenticate the user.

Task 7: (Bonus) Deploy Secondary ISE through AWS Marketplace from CloudFormation Template

Step 1: Subscribe to ISE in AWS Marketplace

1. In the AWS console search for AWS Marketplace Subscriptions.
2. Got to Discover Products on the left menu.
3. Search for ISE and click on Cisco Identity Services Engine (ISE).
4. Click on "Continue to Subscribe" on the top right after reading through some of the options on the subscription if you like.
5. Click on Continue to Configuration.
6. Under fulfilment option, select "CloudFormation Template".
7. A new drop down will be displayed, select Cisco Identity Services Engine (ISE).
8. 2 new drop downs will be presented, select 3.1 Patch1 (or whatever is latest) and select the Region as US East (Ohio).
9. Click Continue to Launch on the top right.
10. Under Choose Action, select "Launch CloudFormation", then select the Launch button.

Step 2: CloudFormation Stack Creation

Market place has launched into CloudFormation with a link to the publicly available CloudFormation Template uploaded to S3.

1. Copy the Amazon S3 URL and open it in a new tab/browser and save it to your local machine. This can be used later directly in CloudFormation rather than going through the subscription as another option. This lab will not this method unless initial Cloud Formation fails.
2. With the "Template is ready" option selected, and the Amazon S3 URL still populated, click Next.
3. The template includes all the provisioning information needed to launch an ISE instance. Fill out all the fields:
 - a. Stack Name – Since this is a single instance set this to the hostname podX-ise2 where X is your pod number.
 - b. Hostname – podX-ise2 where X is your pod number.
 - c. Instance Key Pair – Select the key pair you created in Task 1 and have already saved to your local machine.

- d. Management Security Group – ISEinAWS-podX where X is your assigned pod number. This was created in the Ansible ISE deployment steps.
 - e. Management Network – Select the subnet in the new VPC created in Task 3, it should be zer0k_podX_Private_Subnet where X is your assigned pod number.
 - f. Management Private IP – Given in the Table above as configured in Route53. It will be 10.X.0.6 where X is your assigned pod number.
 - g. Time Zone – Etc/UTC
 - h. Instance Type – C5.4xlarge
 - i. EBS Encryption – false
 - j. Volume Size – 600
 - k. DNS Domain – zer0k.org
 - l. Name Server – 10.X.0.2 where X is the number of your assigned pod.
 - m. NTP Server - 169.254.169.123
 - n. ERS – yes
 - o. OpenAPI – yes
 - p. pxGrid – no
 - q. pxGrid Cloud – no
 - r. Password – **Provided by your proctor**
4. Click Next.
 5. Under Tags add a Key “Name” with value “podX-ise2” where X is the number of your pod. CloudFormation is going to add an instance, EBS volume, and network interface that will all get named via this tag.
 6. Leave the rest of the options default though you are welcome to browse through them to see the options AWS provides. Click Next when you are done.
 7. Review the information to make sure you entered everything correctly, then click “Create stack” at the bottom of the page.
 8. Under events you should see “CREATE_IN_PROGRESS”, refresh the table until you see podX-ise2 with “CREATE_COMPLETE”.

Timestamp	Logical ID	Status	Status reason
2022-05-09 16:44:06 UTC-0400	pod0-ise	✔ CREATE_COMPLETE	-
2022-05-09 16:44:04 UTC-0400	IseEc2Instance	✔ CREATE_COMPLETE	-
2022-05-09 16:43:57 UTC-0400	IseEc2Instance	ⓘ CREATE_IN_PROGRESS	Resource creation Initiated
2022-05-09 16:43:55 UTC-0400	IseEc2Instance	ⓘ CREATE_IN_PROGRESS	-
2022-05-09 16:43:49 UTC-0400	pod0-ise	ⓘ CREATE_IN_PROGRESS	User Initiated