Workbook

SANS | GIAC CERTIFICATIONS

THE MOST TRUSTED SOURCE FOR INFORMATION SECURITY TRAINING, CERTIFICATION, AND RESEARCH | sans.org

All reference links are operational in the browser-based delivery of the electronic workbook.

Welcome to the SEC549 Electronic Workbook

E-Workbook Overview

This electronic workbook contains all lab materials for SANS SEC549, Enterprise Cloud Security Architecture. Each lab is designed to address a hands-on application of concepts covered in the corresponding courseware and help students achieve the learning objectives the course and lab authors have established.

Some of the key features of this electronic workbook include the following:

- Convenient copy-to-clipboard buttons at the right side of code blocks
- Inline drop-down solutions, command lines, and results for easy validation and reference
- Integrated keyword searching across the entire site at the top of each page
- Full-workbook navigation is displayed on the left and per-page navigation is on the right of each page
- Many images can be clicked to enlarge when necessary
- Repository for *draw.io* diagrams

Lab 1.1 - Threat Modeling S3

Summary

The Incite team has stood up an external S3 bucket as an easy mechanism for third-parties to ingest data points into their system. You've been brought in to consult on this ingestion pattern and address any immediate risks. As a first order of business, we'll stretch our threat modeling legs as we attempt to answer the question "What could go wrong?" Answering this question formally using the STRIDE methodology will help drive the implementation of mitigation's and controls.

Attack Surface

In this lab we are considering threats at different junction points in the data flow diagram.

1. Consider the trust boundary crossed as the Incite Teams on-premise application pulls files from the S3 bucket, ingesting the external data into its systems.
2. Consider the S3 bucket. The bucket has been made externally write-able to vendor partners in order to facilitate the ingestion of external data files. Consider the possible threats to the S3 bucket and the broader AWS account given the access provisioned to external parties.
3. Consider the trust boundary crossed as external vendor parties write objects to the S3 bucket. Additionally consider the credentials vendors are provisioned and the threats which target access keys.

Lab Preparation

1. Download the following diagram to your machine: Lab 1.1 Threat Modeling S3 - Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 1.1 Threat Modeling S3 - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 1.1 Threat Modeling S3 - Complete diagram and open it with draw.io.

Lab 1.1 Tasks

1. Review the data flow diagram. Access Keys are provisioned to external vendor parties allowing them to write objects to S3 a bucket. An on-premise application pulls the files, incorporating the data into downstream systems.
2. Review the description of the attack surface on the draw.io diagram. Enumerated are the points where threats could occur in the systems. Consider these trust boundaries when reviewing possible threats.
3. Refer the possible threats in your Toolbox. Consider each threat for plausibility given the system design and permissions granted to external parties.
4. Only six of the twelve threats will be applicable to the system. Drag and drop the threats that are applicable the attack surface. Place them into their corresponding STRIDE category.

5. Half of the threats in your toolbox will not apply to this system and will remain in place.

Lab 1.1 Summary Wrap Up

You've successfully threat modeled your first cloud architecture! Many traditional threats seen in on-premise architectures are not applicable, such as those relating to Denial of Service and those mitigated by encryption-in-transit. Some risks involving the access keys are mitigated given the limited (write-only) access provisioned to third-parties. However, there is still the possibility that threats could manifest in the AWS account the bucket is housed. An attacker (or someone by negligence) could escalate their permissions, gaining access to the bucket, which affects the logging of actions taken and/or affects the confidentiality of the objects stored in S3. We haven't been made aware of any input validation or data schema being enforced on ingestion, and as identified in the threat modeling exercise, there is the possibility for malicious or corrupted data to affect downstream, on-premise systems.

In this lab you....

- Reviewed the data flow diagram of an external ingestion pattern using S3.
- Evaluated the attack surface and the trust boundaries crossed when data is both written and read from S3.
- Considered possible threats to the system and identified which were plausible given the design.

Follow up questions....

What control is preventing an attacker from eavesdropping on network communication and reading S3 objects as they are either written or read?

https

Could isolating the S3 ingestion bucket in its own AWS Account help mitigate threats?

Yes, removing additional functionality from the Account naturally limits who has IAM access, thus reducing points of initial compromise

Are there concerns that the vendor-assigned credentials could be used to affect other resources in AWS?

No, given *write-only* access to an S3 bucket, we are considering the vendor access only presents risk around the possibility of malicious object uploads

Lab 1.2 - Centralizing User Account Provisioning

Summary

Presently, to fulfill new AWS access requests, end users are manually created in the built-in directory in AWS Identity Center (IdC). As a result, end users are forced to maintain separate sets of credentials and terminating their access to AWS becomes a separate, error prone process, one not tied to the user lifecycle. The solution is to configure AWS Identity Center to provision IdC users and groups from an upstream external Identity Provider (IdP) via SCIM.

In this lab, your task is to determine how to provision your `SEC549 Student` user and its groups from the Delos Azure Active Directory (AAD) so that it is mirrored into AWS Identity Center as a result of your users group membership.

Lab Preparation

1. Download the following diagram to your machine: Lab 1.2 Centralizing User Account Provisioning - Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 1.2 Centralizing User Account Provisioning - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 1.2 Centralizing User Account Provisioning – Complete diagram and open it with draw.io.

Lab 1.2 Tasks

1. Observe the the depiction of your `SEC549 Student` user on the diagram. Identify this user in AWS on the AWS Identity Center Console.
2. On the AWS Identity Center Console, discover which groups the `SEC549 Student` user is a member of. On the diagram, drag and drop the correlating AWS IdC Groups.
3. Drag and drop the AWSReadOnlyAccess Permission Set Icon into the yellow box - depicting `student` group being assigned the Permission Set.
4. Drag and drop the AAD Groups and Users into the Delos tenant which are needed to be automatically provisioned into AWS Identity Center via SCIM.
   NOTE: You will not use all the icons in your Toolbox.

Lab 1.2 Summary Wrap Up

The Delos AWS Admin changed the identity source in Identity Center to be 'External', enabling automatic provisioning via SCIM. This configuration change allowed for automatic user provisioning to be utilized to provision the `SEC549 Student` user and its group memberships.
Users, groups, and group memberships which originate in Azure Active Directory are sync'd over to the AWS Identity Center directory on a regular schedule. When users are added to the `aws-sync` group, their identities will automatically be provisioned into AWS Identity Center.

In this lab you....

- Logged into the AWS Console to discover the group membership of your `SEC549 Student` user.
- Depicted the creation of the `SEC549 Student` user and its group memberships into AWS Identity Center via Azure Active Directory (AAD) automatic SCIM provisioning.
- Represented the `AWSReadOnlyAccess` permission set in AWS Identity Center assigned to the `student` group.

Follow up questions....

Why is an Active Directory Group used to synchronize users into AWS Identity Center

Group membership is a mechanism to limit to scope of AAD users to be replicated in AWS

Can both AWS Identity Center manually created users and externally provisioned users co-exist?

No, only one directory source can be used at any given time

Lab 1.2 - See It In Action

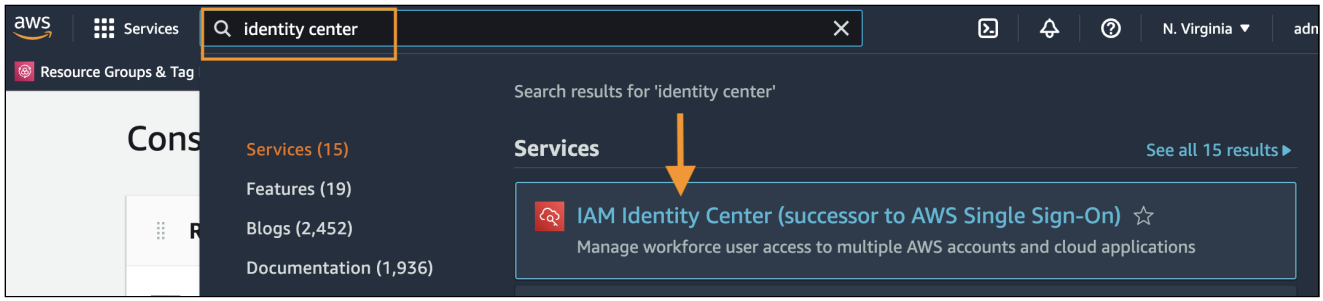
Log into the AWS access portal URL with your `SEC549 Student` user credentials.

Once authenticated to AWS, expand the **Delos International Management (SANS ORG10)** Account and select the **Management console** link.

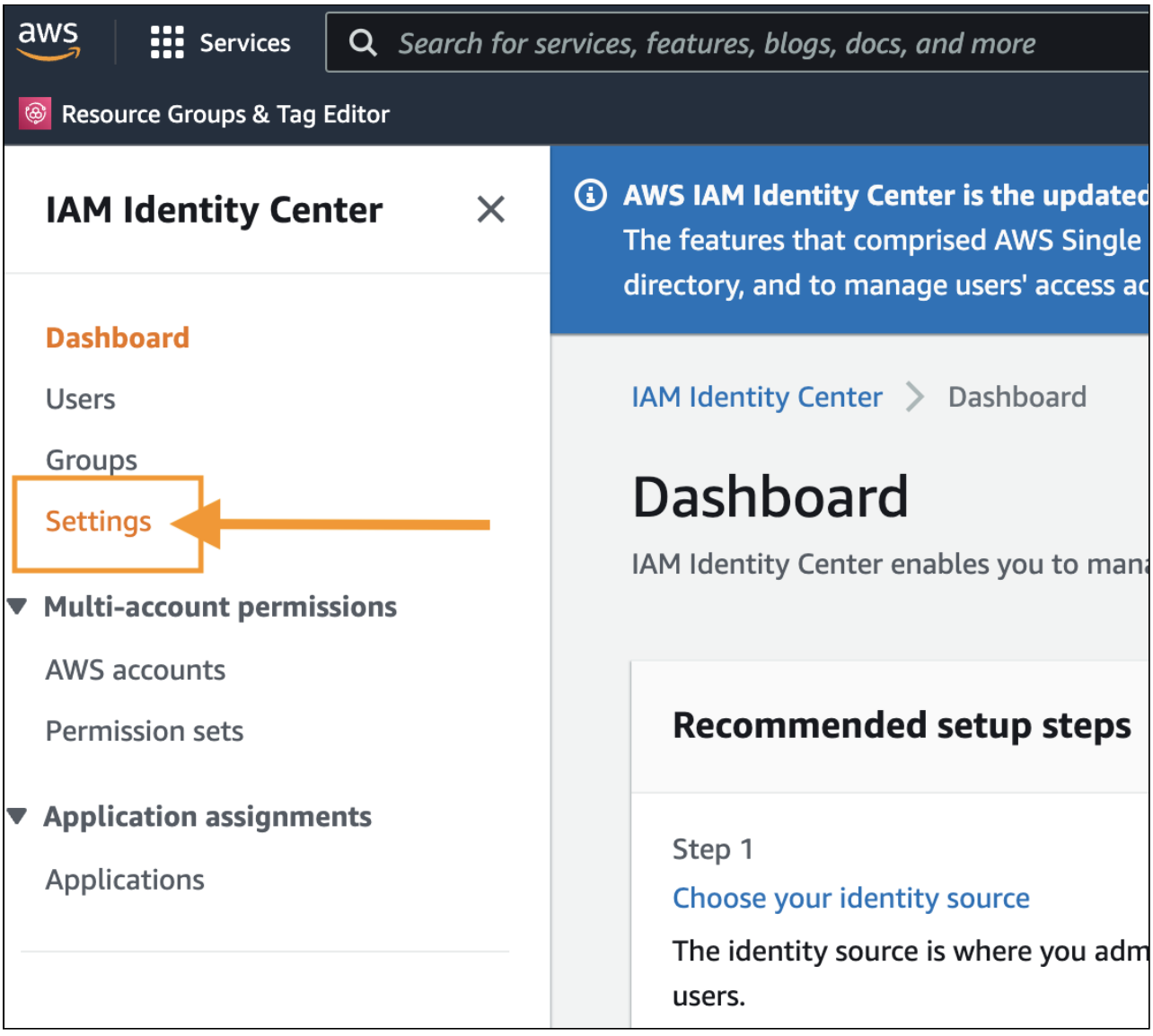
Answer the following questions about the automatic user provisioning

1. What is the provisioning method used in AWS Identity Center?

In the console, navigate to AWS Identity Center (successor to AWS Single Sign-On)

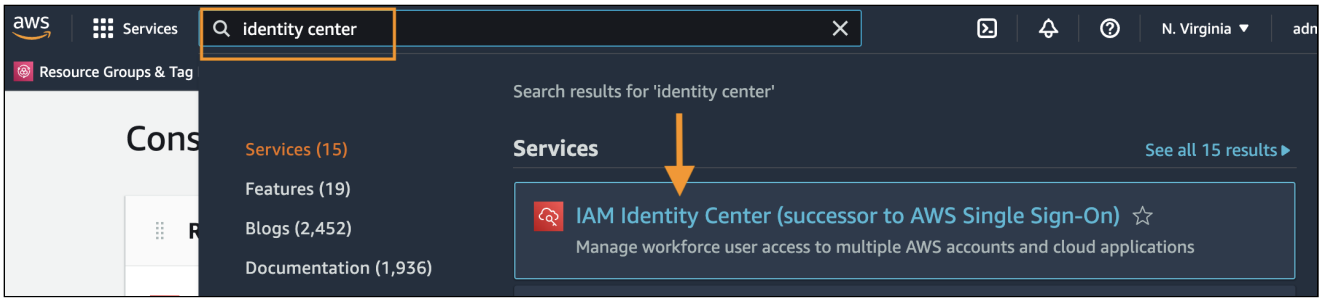


On the left, click on 'Settings'

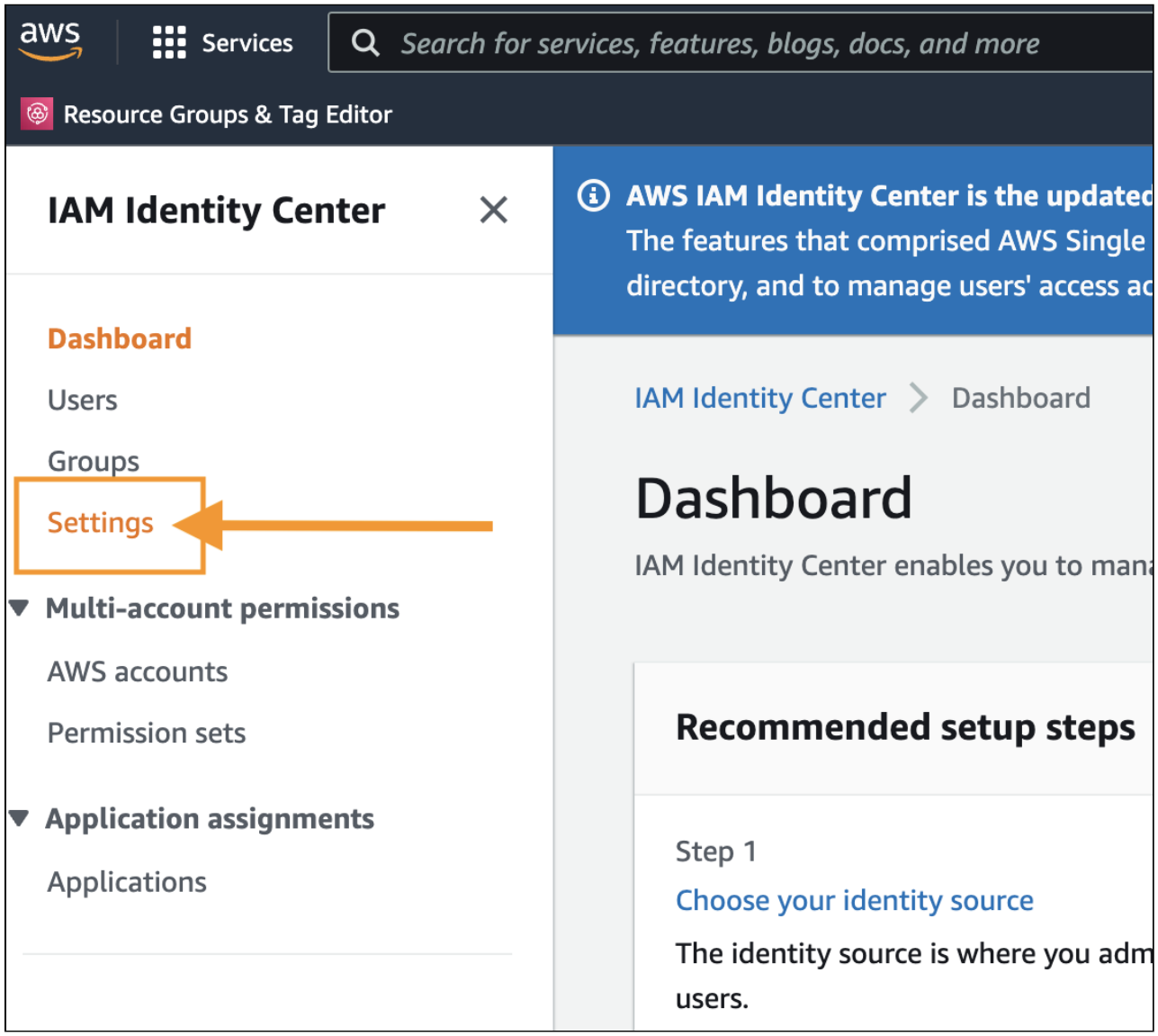


2. What URL does Azure call in order to replicate Users and Groups to AWS?

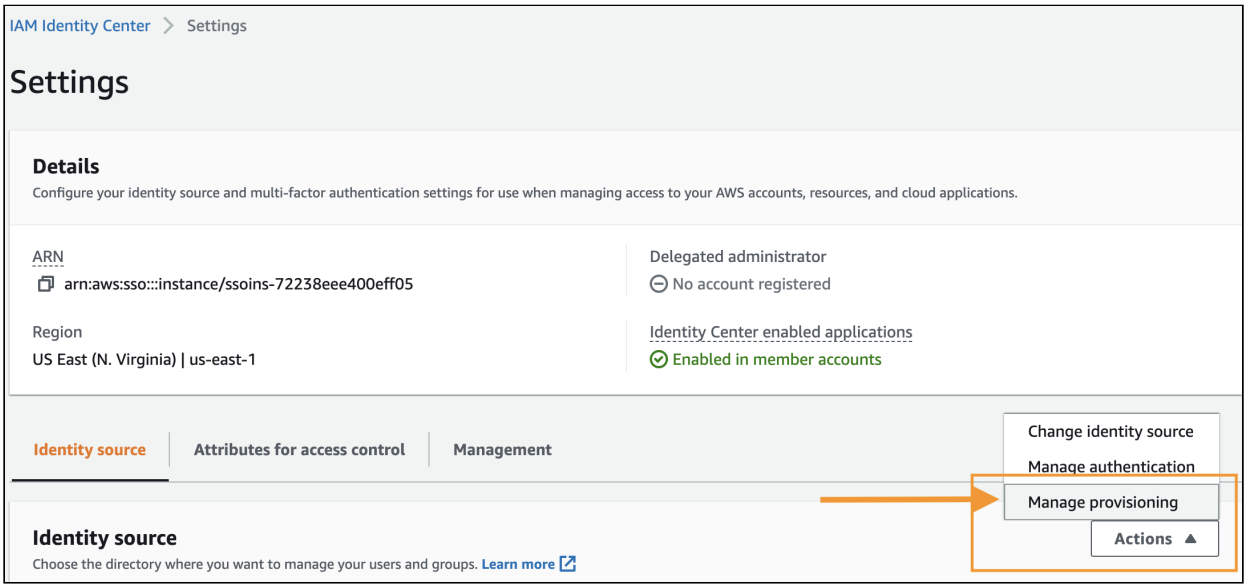
In the console, navigate to AWS Identity Center (successor to AWS Single Sign-On)



On the left, click on 'Settings'

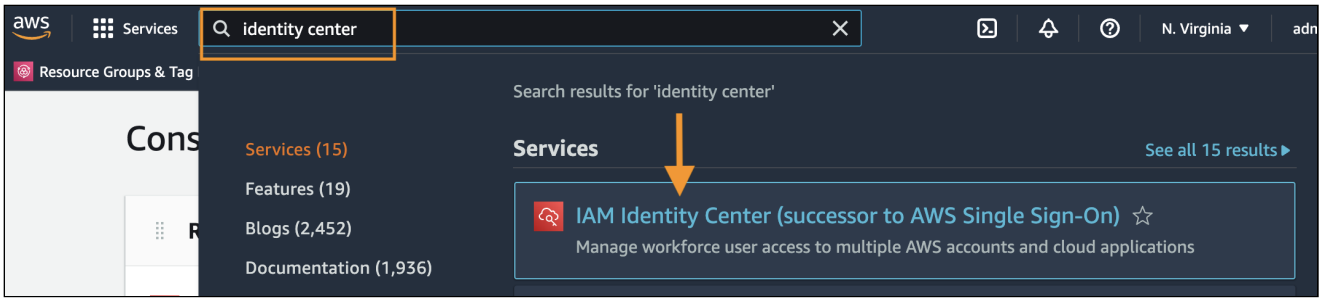


On the right, click on 'Actions' -> 'Manage Provisioning'

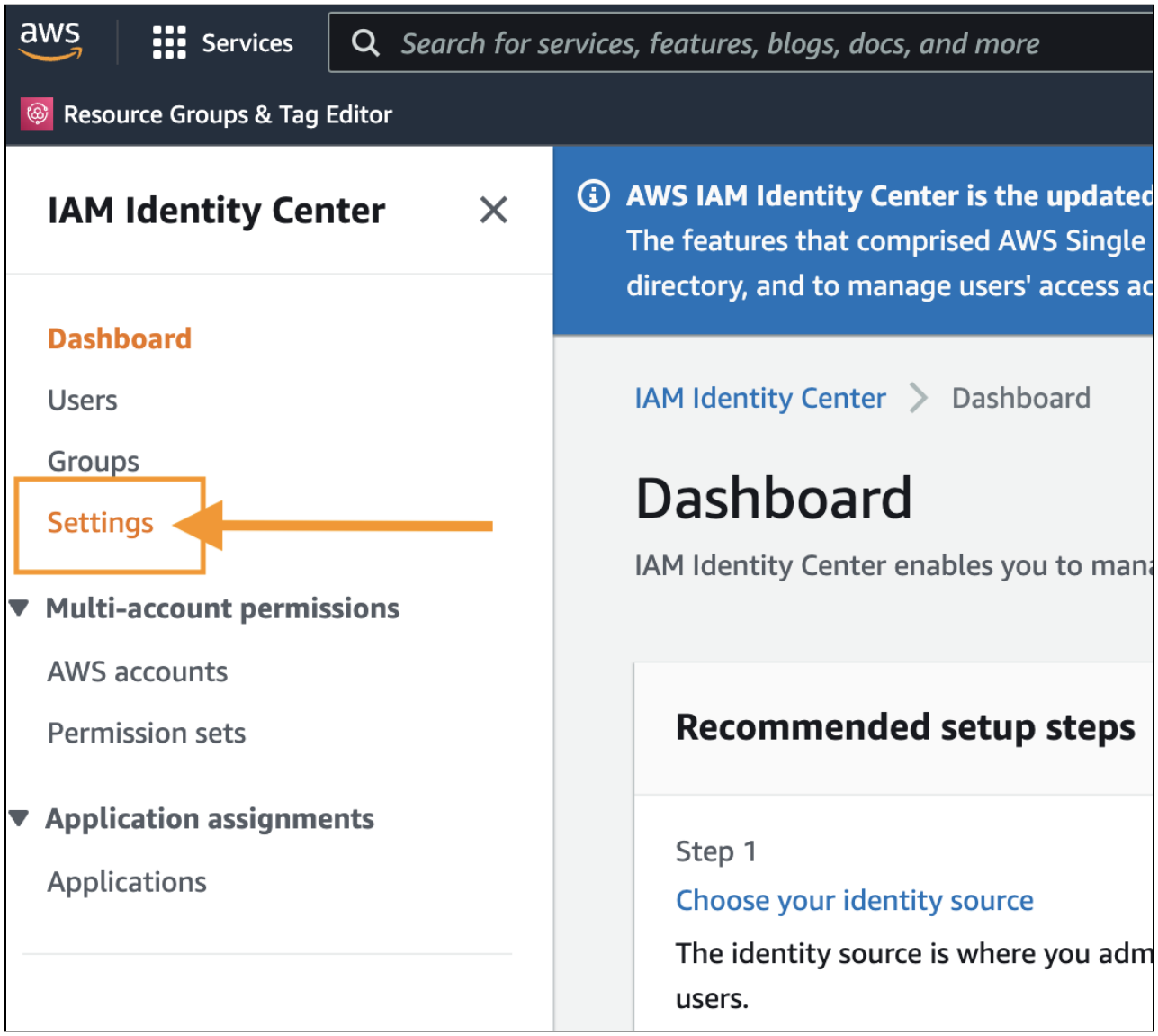


3. What type of credential is used to authenticate calls to the AWS SCIM endpoint?

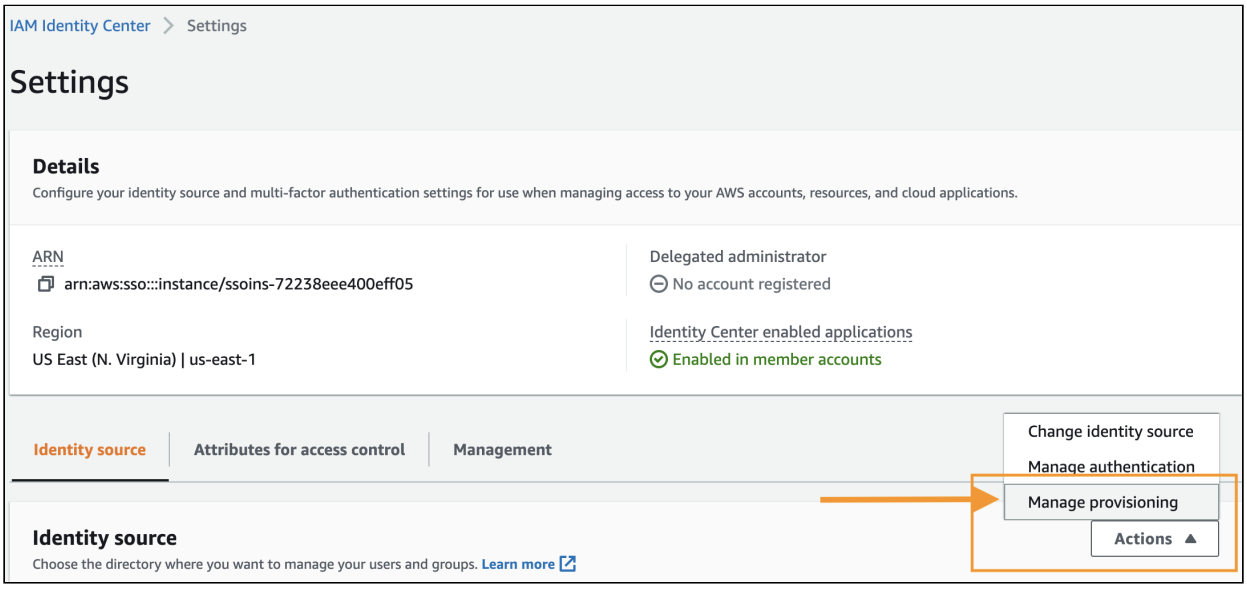
In the console, navigate to AWS Identity Center (successor to AWS Single Sign-On)



On the left, click on 'Settings'



On the right, click on 'Actions' -> 'Manage Provisioning'



See the debrief section below for answers

Lab 1.2 - Lab Debrief

What is the provisioning method used in AWS Identity Center

SCIM

What URL does Azure call in order to replicate Users and Groups to AWS?

https://scim.us-east-1.amazonaws.com/f3v03961bd7-692d-47b0-9f68-e576e291b85e/scim/v2/

What type of credential is used to authenticate calls to the AWS SCIM endpoint?

An OAuth bearer access token

Lab 1.3 - Structuring Accounts to Create Effective Hierarchies

Summary

In this exercise, your task is to help Delos, Inc create a solid identity foundation from which they will build their new cloud presence and design federation patterns.
Delos, Inc has created their first AWS Organization. After creating the Organization, IT invited the existing AWS Accounts to join and integrated them into the new Org.
With a phased cloud migration pending, the new Delos AWS Organization needs to be configured to support future requirements and use-cases including centralized networks, customer-facing workloads, and security services.

In the labs, you will arrange three different resources to help Delos transition their operations from a data center to a hybrid cloud architecture. Organizational Units (OUs) will be created to organize the initial set of AWS Accounts that Delos plans to launch in their new Organization. Security Control Policies (SCP) need to be applied in a judicious manner to ensure their migration can proceed with confidence and speed.

Lab Preparation

1. Download the following diagram to your machine: Lab 1.3: Structuring Accounts to Create Effective Hierarchies - Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 1.3: Structuring Accounts to Create Effective Hierarchies - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 1.3: Structuring Accounts to Create Effective Hierarchies – Complete diagram and open it with draw.io.

Lab 1.3 Tasks

1. Detailed in this Lab Work diagram is a collection of resources you will need to configure support Delos's expansion into the cloud.
2. Arrange the AWS Foundational OUs in a logical hierarchy that will support all activities, including security activities, any accounts needing exceptions, and workloads segregated by their SDLC or environment.
3. Place AWS Accounts supporting Delos below the appropriate OU.
4. Apply SCP from the available policies provided in your Toolbox.
5. Note that Service Control Policies (SCP) can be applied at various OU levels, at the Organizational Account (AWS root) or on individual AWS Accounts to enforce policy.
6. Challenge yourself to decide where on the hierarchy it would be best to apply SCP to support the accounts' wide-ranging needs.

Lab 1.3 Summary Wrap Up

Delos's AWS Organization is now scaffolded with several foundational Organization Units in place to help them scale during their transition to the cloud.
A set of starter policies have been applied to the new AWS Root, Organizational Units and in some cases, AWS Accounts to set guardrails. Implementing Guardrails ahead of a cloud migrations can help a business move with confidence and speed.

In this lab you....

- Arranged the AWS Foundational OUs in a logical hierarchy to support various workloads, including security activities, playgrounds, and workloads, segregated according to SDLC environment.
- Created a foundation that will help Delos scale up during their transition to the cloud.
- Applied Service Control Policies (SCP) at various OU Levels to enforce policy.
- Applied starter policies to the new AWS Root, Organizational Units, and in some cases, AWS Accounts, to set guardrails. You implemented Guardrails ahead of a cloud migration, which can help a business move forward with confidence and speed.

Lab follow up questions....

Are there any additional SCPs you can imagine being beneficial for the new Delos Organization?

There's no right or wrong answer, but here are some additional SCP that come to mind:

Additional Security Control Policies

```
- Prevent users from disabling Guardduty
- Require EC2 instance be of a specific type
- Require MFA to perform a particular API action
```

Are there any additional OUs that should have been created?

An OU can be created specifically for use testing SCP Policy. This type of OU is often called a PolicyStaging OU.

Lab 1.3 - See It In Action

The Organization Units (OUs) and Service Control Policies (SCP) have been created in the new Delos Organization.
Log into the AWS access portal URL with your `SEC549 Student` user credentials.

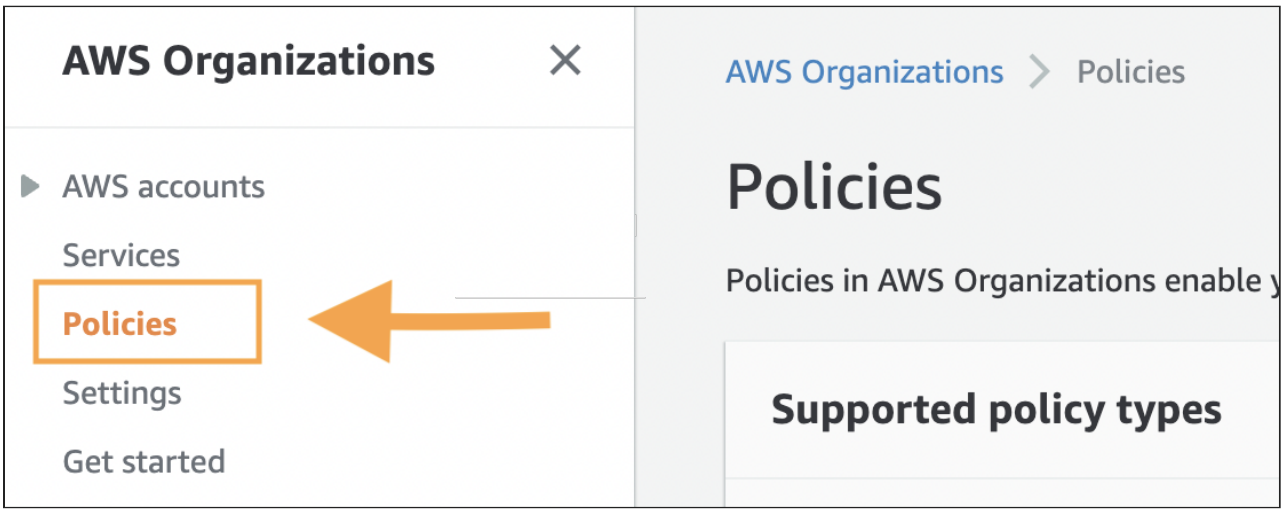
Once authenticated to AWS, expand the Delos International Management account and select the **Management console** link.

Answer the following questions about the new Delos Organization

1. Besides Service Control Policies (SCP), what other policies can be enabled from the AWS Organizations console?

Navigate the Console to find the 'Organizations' service

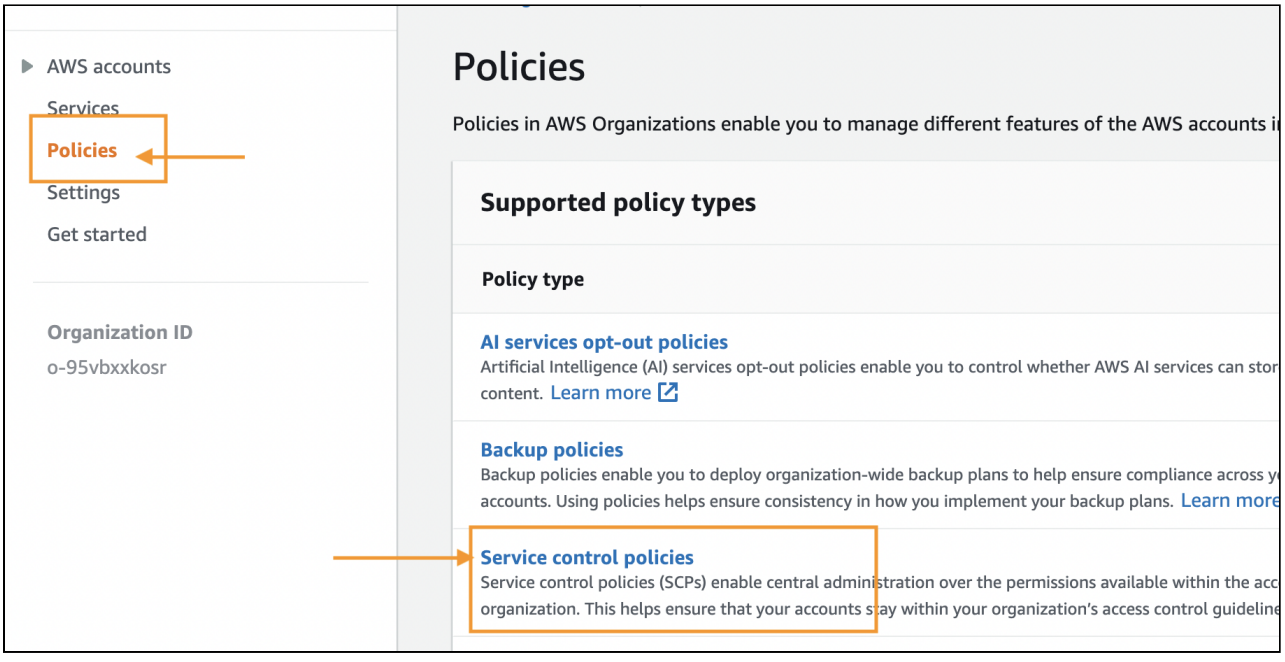
Click on 'Policies'



2. What services does the `basic-deny-without-conditions` SCP Policy restrict?

Navigate the Console to find the 'Organizations' service

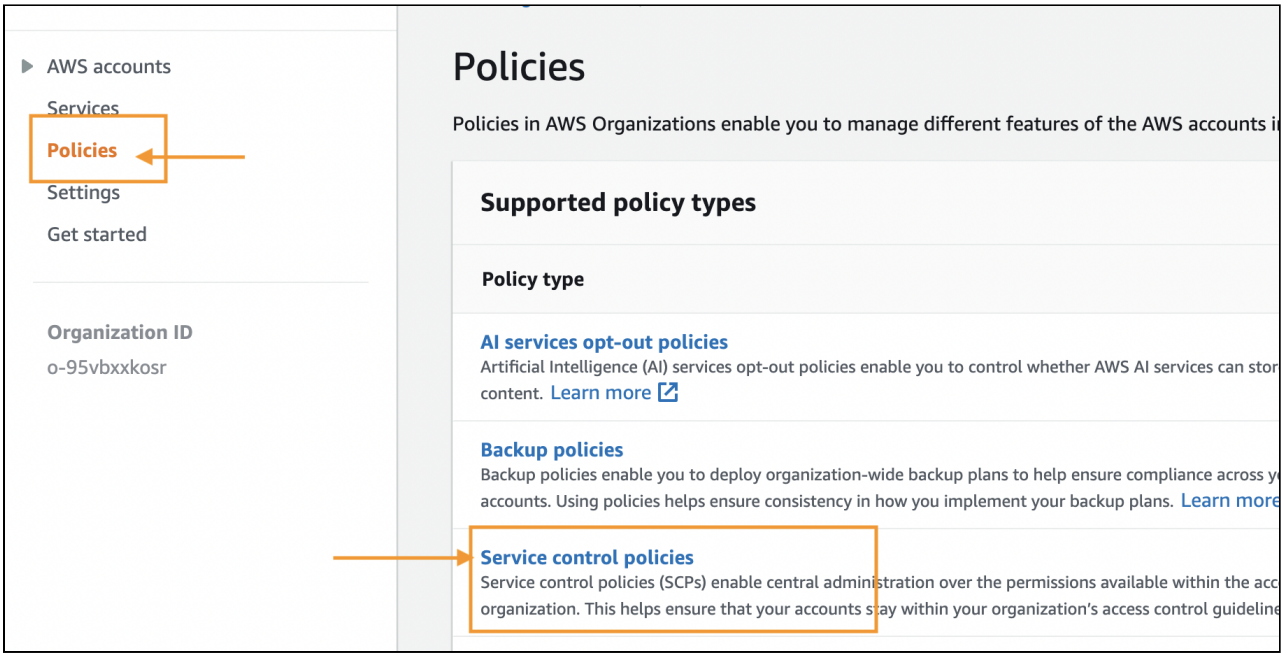
Click on 'Policies' and then 'Service Control Policies'



3. What are the names of the AWS Accounts that are allowed to create VPC Resource Shares?

Navigate the Console to find the 'Organizations' service

Click on 'Policies' and then 'Service Control Policies' to find the SCP controlling access to resource sharing



See the debrief section below for answers

Lab 1.3 - Lab Debrief

Besides Service Control Policies (SCP), what other Policies can be enabled from the AWS Organizations console?

AI services opt-out policies and Backup policies

What services does the 'Basic DENY SCP Policy without Conditions' SCP Policy restrict?

CloudTrail and Budgets

What are the AWS Accounts that are allowed to create VPC Resource Shares?

282048706357 (network-shared-services-prod), 012761524637(network-web-dev), 328860086869(network-web-prod)

Lab 1.4 - Transitioning Access from AWS IAM Users to Roles

Summary

In this lab, you are presented with two legacy AWS Accounts with siloed identity and access patterns. These accounts have operated as 'Shadow Accounts' by the research science team.

Because of the lack of oversight, these accounts each house native, duplicate AWS IAM users with somewhat chaotic access patterns. The lack of oversight has led to a tangled web of un-managed users and policies making it difficult to reason about who has access to what. Untangling this web will help to set the stage for centralized identity, while maintaining the users existing access levels.

Lab Preparation

1. Download the following diagram to your machine: Lab 1.4 Transitioning Users to Roles – Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 1.4 Transitioning Users to Roles - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 1.4 Transitioning Users to Roles – Complete diagram and open it with draw.io.

Lab 1.4 Tasks

1. Observe how each IAM user is granted access, whether they are allowed to assume a role directly or as a result of their group membership.
2. Take note where IAM users are duplicated between the two accounts. When building the new Identity Bastion Account there will be a single IAM user per individual needing access.
3. Arrange the IAM users in the Identity Bastion Account so that they are members of the appropriate groups.
4. Place IAM roles and policies as needed into the two legacy AI research Accounts to maintain the same level of access depicted in the current state architecture.
5. Indicate which IAM users should be members of which groups in the Identity Bastion Account.
6. Indicate which groups will be allowed to assume which IAM roles into the legacy AI research groups.
7. To get you started, the access patterns for the user 'Mark', has already been configured.

Lab 1.4 Summary Wrap Up

Access patterns have been streamlined so every individual on the AI Research Team only has a single IAM user to manage. From this single user housed in the Identity Bastion Account, users are arranged into AWS-native IAM groups from which they are allowed to assume roles into their operational accounts.

Previous access into their legacy accounts has been maintained but describing 'who has access to what' is easier to reason about, easier to audit and less prone to misconfigurations.

In this lab you....

- Traced the access granted to users through current access patterns.
- Recreated users in the new Identity Bastion Account, eliminating the need for individuals to have multiple, native IAM users created in every Account.
- Defined new groups in the Identity Bastion Account to facilitate each user's access to cross-account roles.
- Created new IAM roles in each of the legacy AI Research Accounts to be assumed by IAM users in the Identity Bastion Account.
- Indicated which users would assume which IAM roles to maintain their existing access.

Follow up questions....

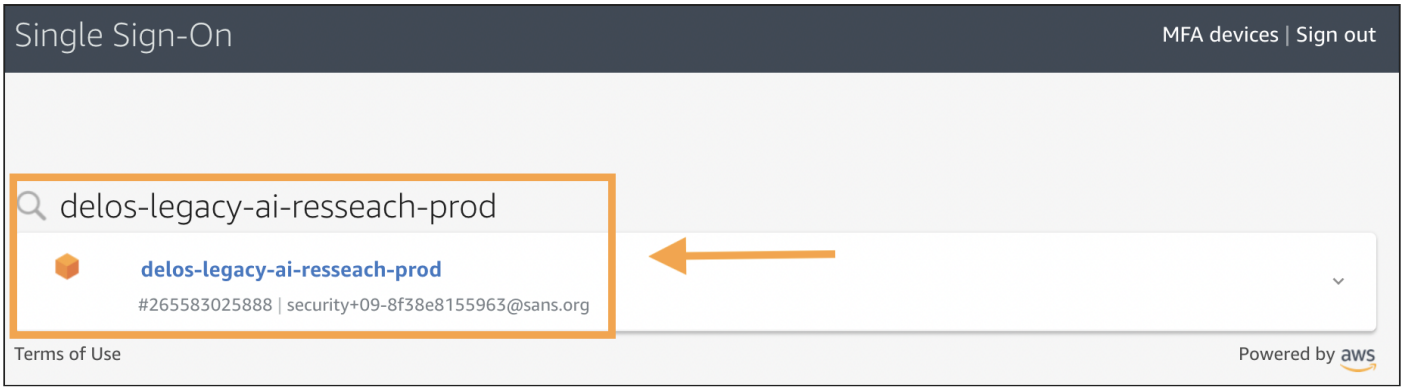
With this new access patterns, are there IAM resources that are being duplicated across accounts?

Roles and their attached policies are duplicated between accounts

Lab 1.4 - See It In Action

Log into the AWS access portal URL with your `SEC549 Student` user credentials.

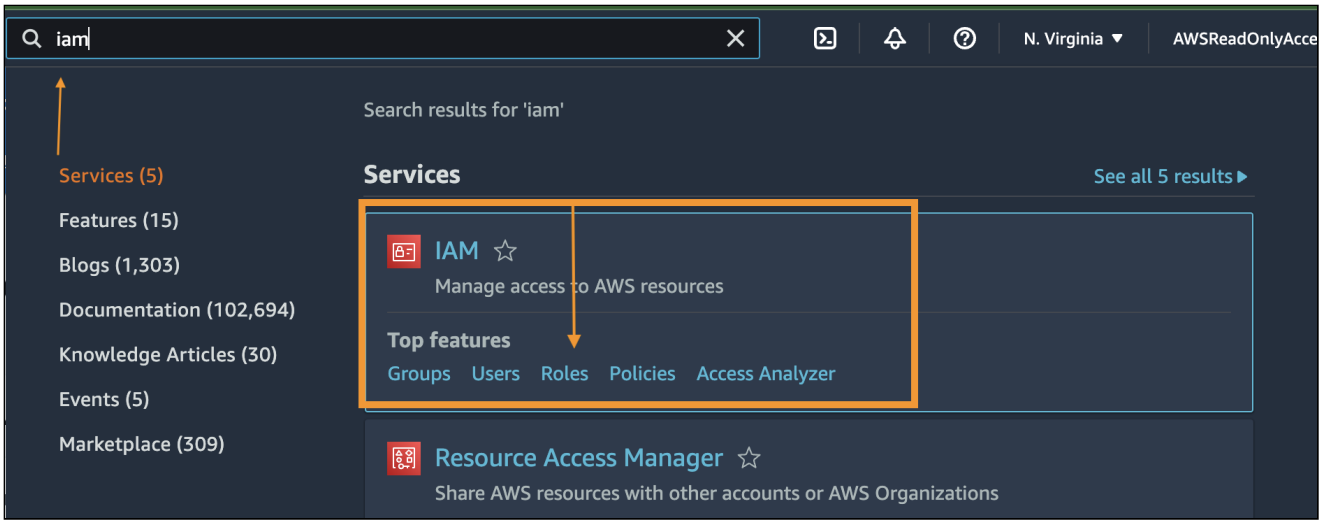
Once authenticated to AWS, expand the *delos-legacy-ai-research-prod* account and select the **Management console** link.



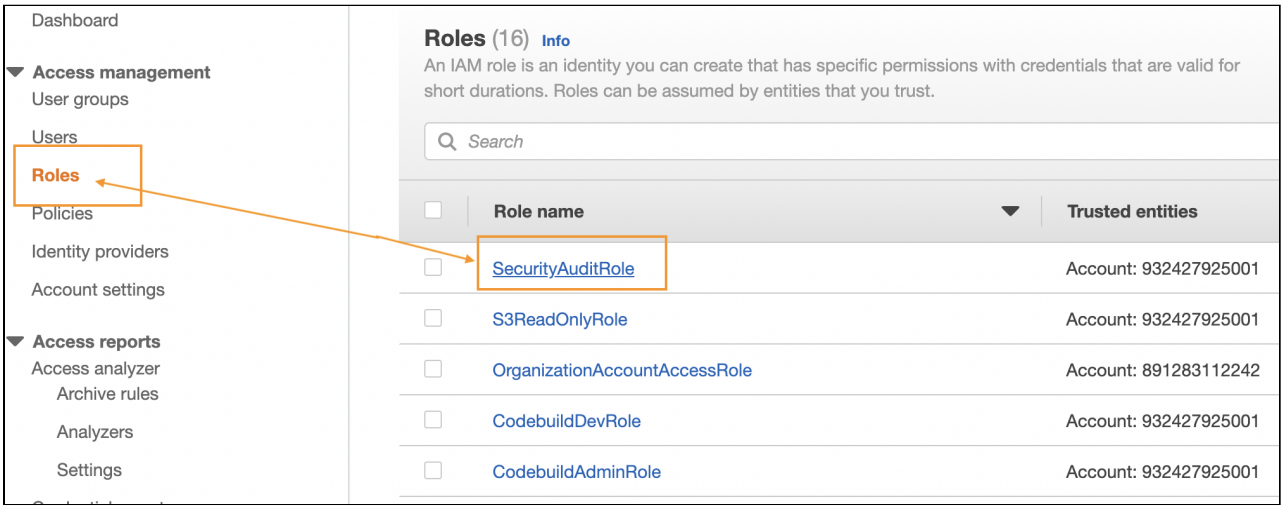
Answer the following questions about the new identity bastion pattern

1. What is the name of the resource-based policy type that allows users to assume roles in AWS Accounts *delos-legacy-ai-research-prod* or *delos-legacy-ai-research-dev*?

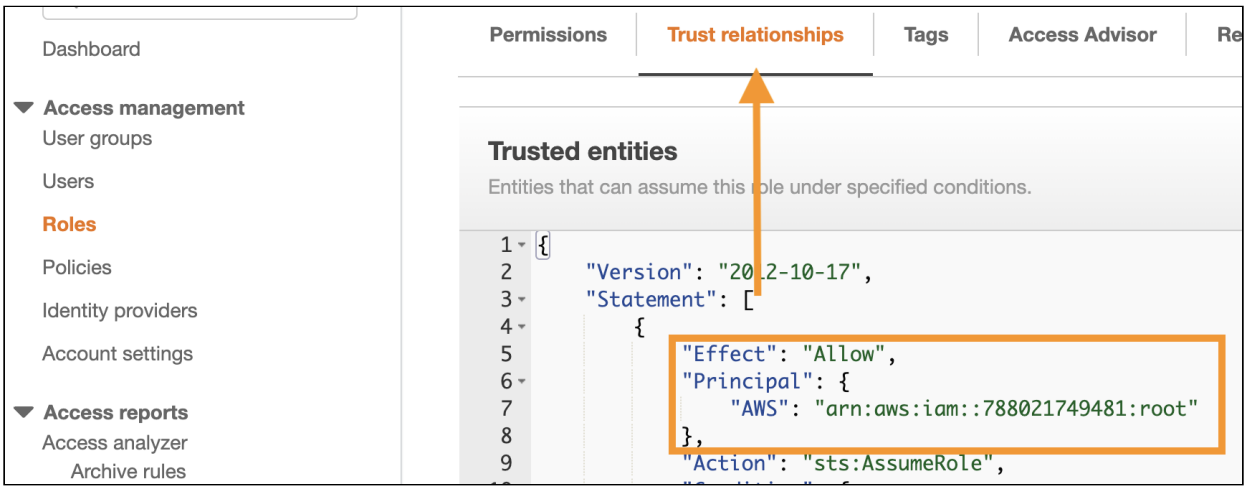
Navigate the Console to find 'IAM Roles'



Click on 'SecurityAuditRole'

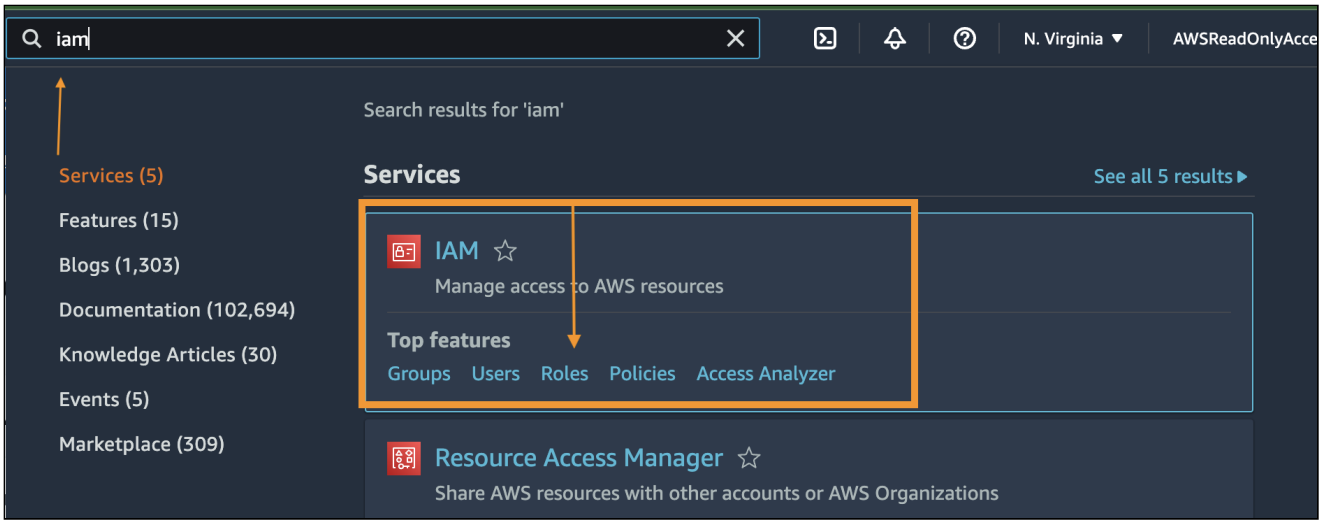


Click on 'Trust Relationships'. What type of policy is displayed?

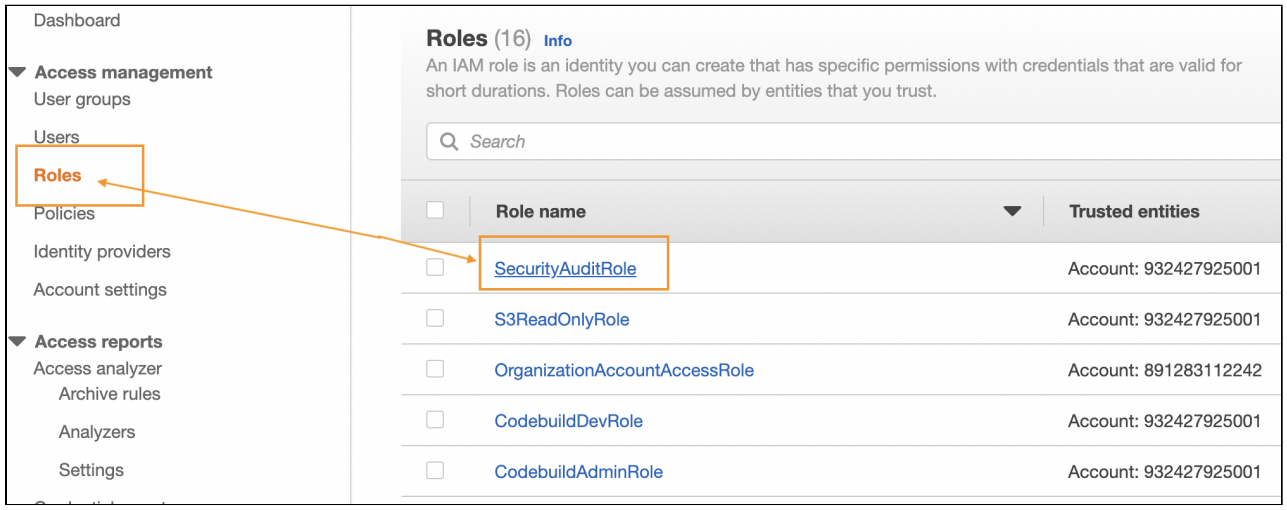


2. What condition must be met before AWS allows users to assume roles created during this lab?

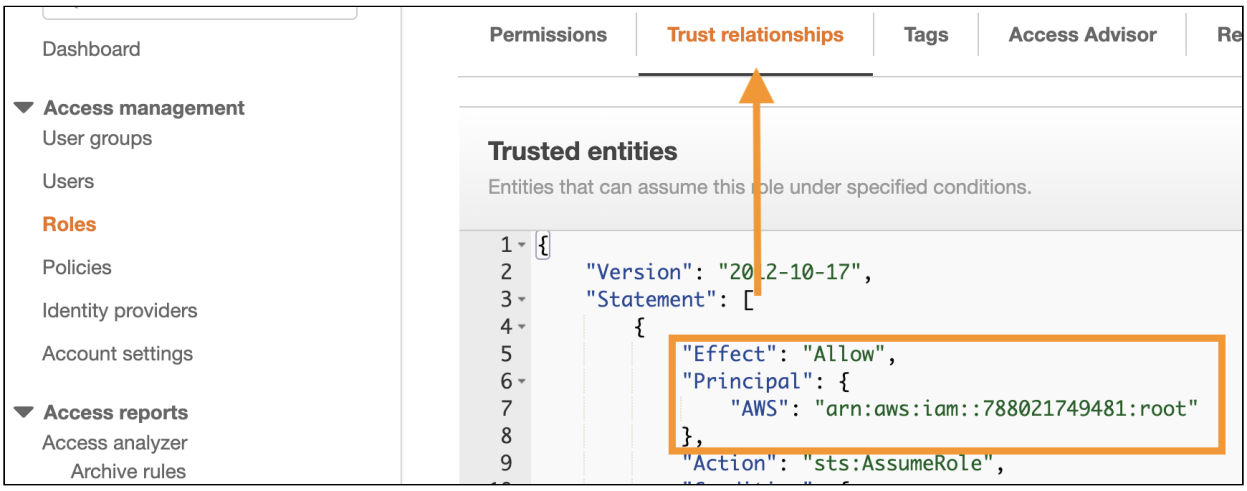
Navigate the Console to find 'IAM Roles'



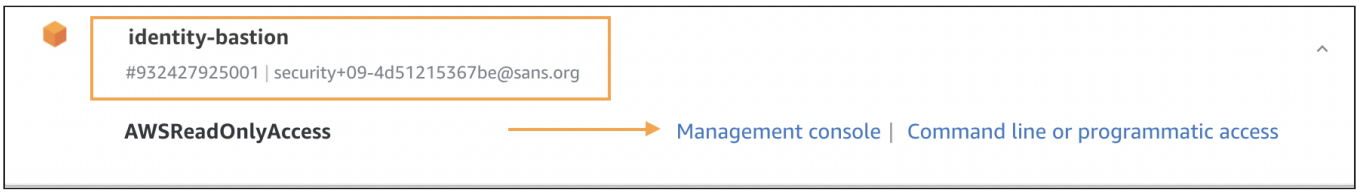
Click on 'SecurityAuditRole'



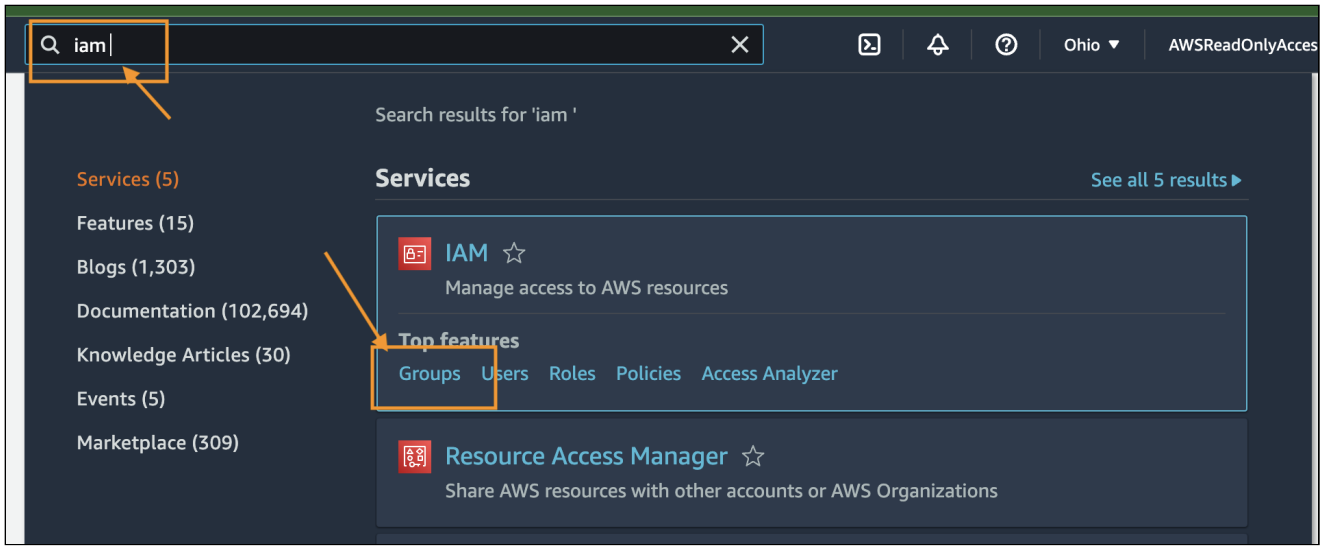
Click on 'Trust Relationships' to view the policy



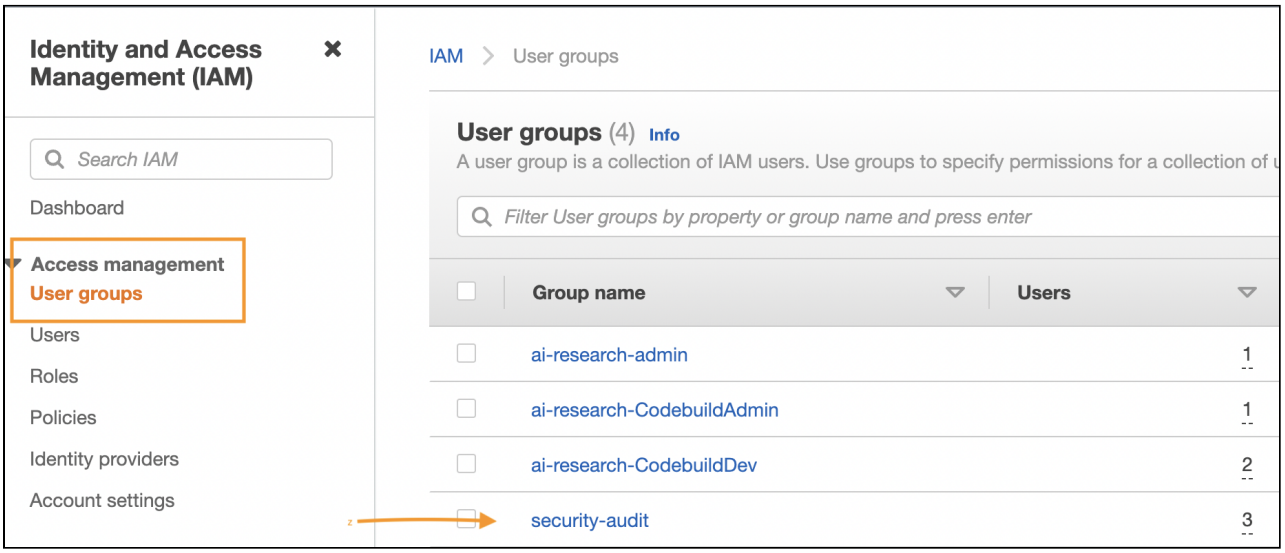
3. Next, head to the *identity-bastion* Account to answer the last question. What roles are members of the security-audit Group allowed to assume in the delos-legacy-ai-research-prod* Account?



Navigate the Console to find 'IAM Groups'



Click the 'security-audit' Group and read the policies attached to this Group



See the debrief section below for answers

Lab 1.4 - Lab Debrief

What is the name of the resource-based policy type that allows users to assume roles in AWS Accounts *delos-legacy-ai-research-prod* or *delos-legacy-ai-research-dev*?

Trust Policy

What condition must be met before AWS allows users to assume roles created during this lab?

```
"Condition": {
    "BoolIfExists": {
        "aws:MultiFactorAuthPresent": "true"
    }
}
```

What roles are members of the security-audit Group allowed to assume?

S3ReadOnly Role and SecurityAudit Role

Lab 2.1 - Integrating Modern Auth Into a Legacy Application

Summary

This lab depicts the Delos Destinations Park Tracker App after integration with AWS Cognito where authentication decisions have been delegated to Cognito as its third-party Identity Provider. In turn, administrators of the AWS Organization have configured the Cognito User Pools to integrate with Delos's central Identity Provider, Azure Active Directory. This configuration has allowed employees to use their corporate credentials to authenticate to the internally developed application hosted on AWS.
Your task is to document the login sequence end users experience with the new configuration and how each of the components issue and validate security assertions.

Lab Preparation

1. Download the following diagram to your machine: Lab 2.1 Integrating modern authentication into a Legacy Application - Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 2.1 Integrating modern authentication into a Legacy Application - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 2.1 Integrating modern authentication into a Legacy Application – Complete diagram and open it with draw.io.

Lab 2.1 Tasks

1. Review the sequence diagram. The Delos Destinations Park Tracker App has been configured to use AWS Cognito to authenticate employee users. In turn, AWS Cognito federates against the central Delos identity provider, Azure Active Directory.
2. Examine the actions listed in your tool box. Place the action on top of corresponding in arrow sequence in the diagram.
3. To get you started, the first and last action in the sequence diagram has been completed. After an employee tries to access the Park Tracker App, what is the next action in the integrated login process? Place that named action on top of the second arrow in the sequence.
4. Log into the Park Tracker App with your `SEC549 Student` user credentials to experience the new authentication flow.

Lab 2.1 Summary Wrap Up

Delos's AWS Organization is now scaffolded with several foundational Organization Units in place to help them scale during their transition to the cloud.
A set of starter policies have been applied to the new AWS Root, Organizational Units and in some cases, AWS Accounts to set guardrails. Implementing Guardrails ahead of a cloud migrations can help a business move with confidence and speed.

In this lab you....

- Depicted how the Delos Park employees are redirected to Azure Active Directory (AAD) to submit their corporate credentials
- Completed the sequence diagram to show AAD returning a SAML token to end users and AWS Cognito's role in validating the token.
- Showed how an identity token is obtained from AWS Cognito after it successfully validates the SAML token.
- Indicated the applications role in validating the integrity of the identity token.
- Experienced authenticating with AWS Cognito when configured with an external identity provider.

Lab follow up questions....

How does AWS Cognito validate the SAML token thats submitted to it?

When configuring the integration with Azure Active Directory, a certificate containing a public key is uploaded to Cognito. The signature on the SAML token is validated with public key of the identity provider configured during integration.

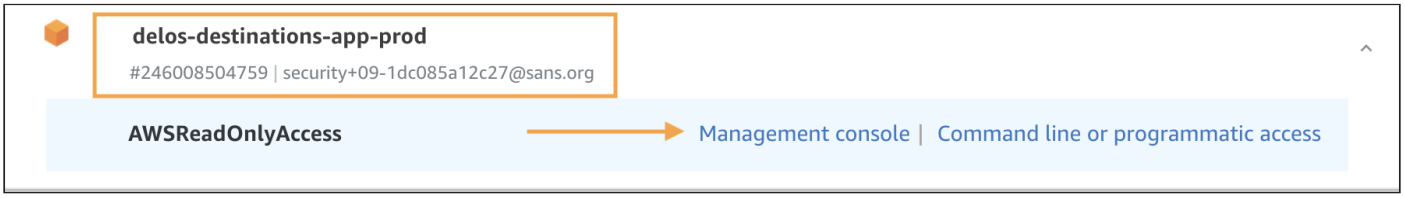
How does the application validate the Id Token submitted to it?

Similar to SAML tokens, id tokens are signed to ensure their integrity. Cognito publishes a public endpoint for each User Pool where the corresponding public key can be retrieved by the application and used to validate the token.

Lab 2.1 - See It In Action

Log into the AWS access portal URL with your `SEC549 Student` user credentials.

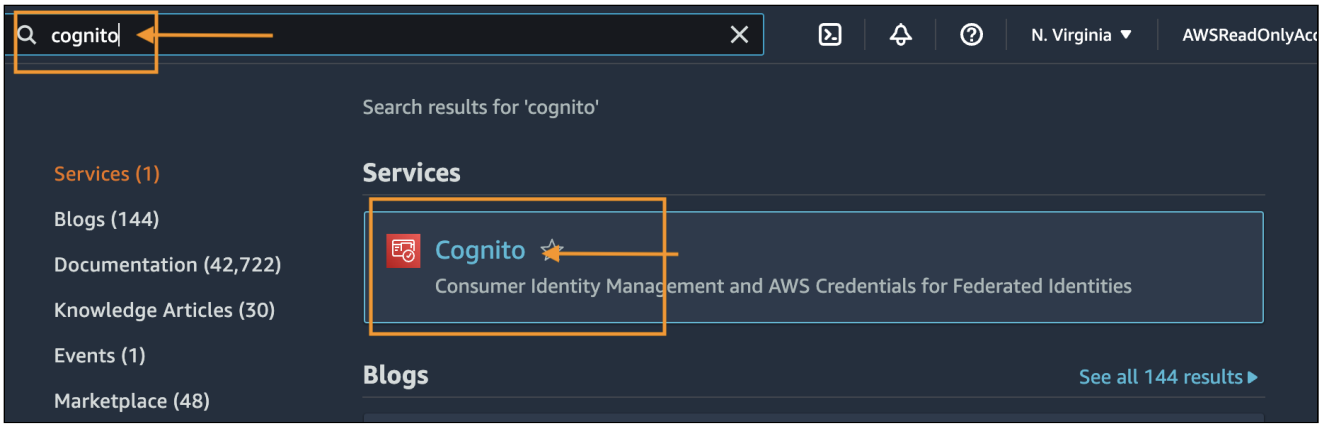
Once authenticated to AWS, click on the 'AWS Account' Icon -> *delos-destinations-app-prod*



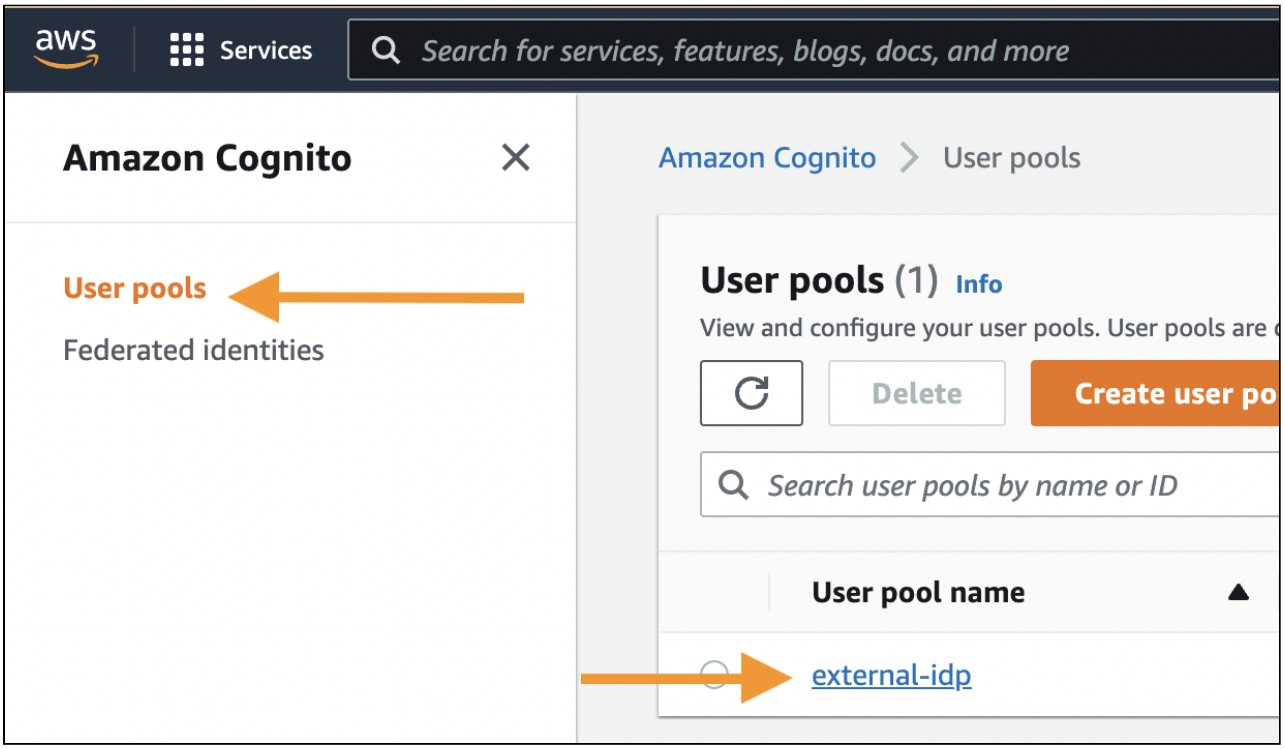
Answer the following questions about the User Pool configuration in Cognito

1. What is the name of the Active SAML Provider configured in the 'Identity Providers' section of the Cognito console?

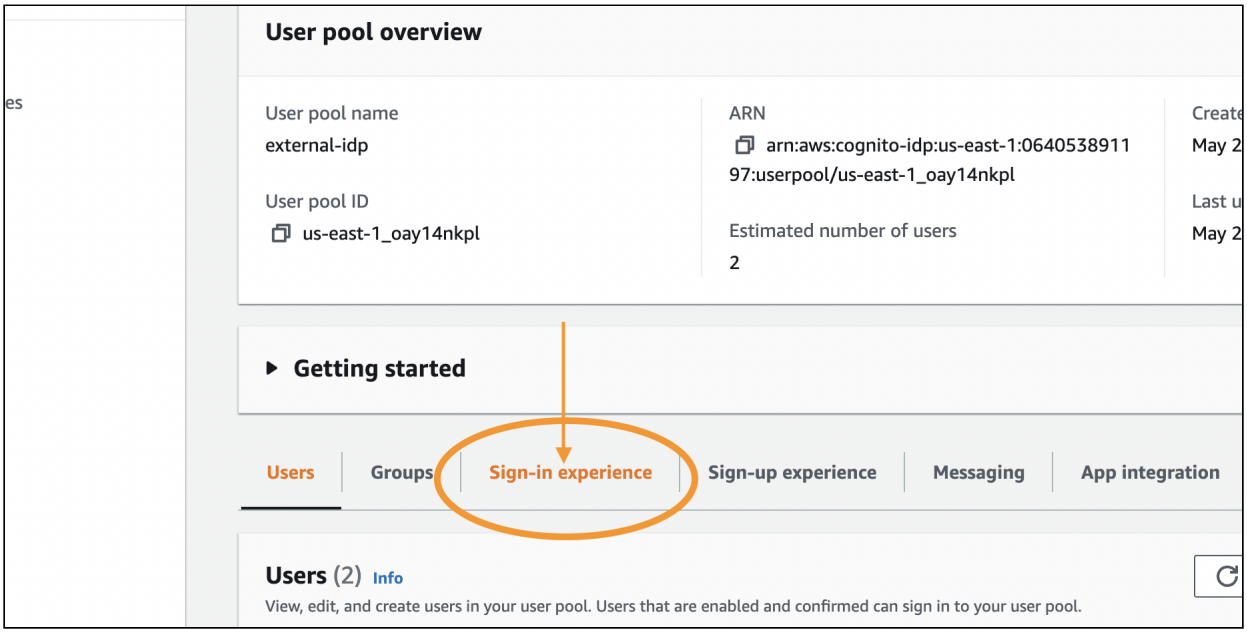
Navigate the Console to find 'Cognito'



Click on 'User Pools and then the user pool named 'external-idp'

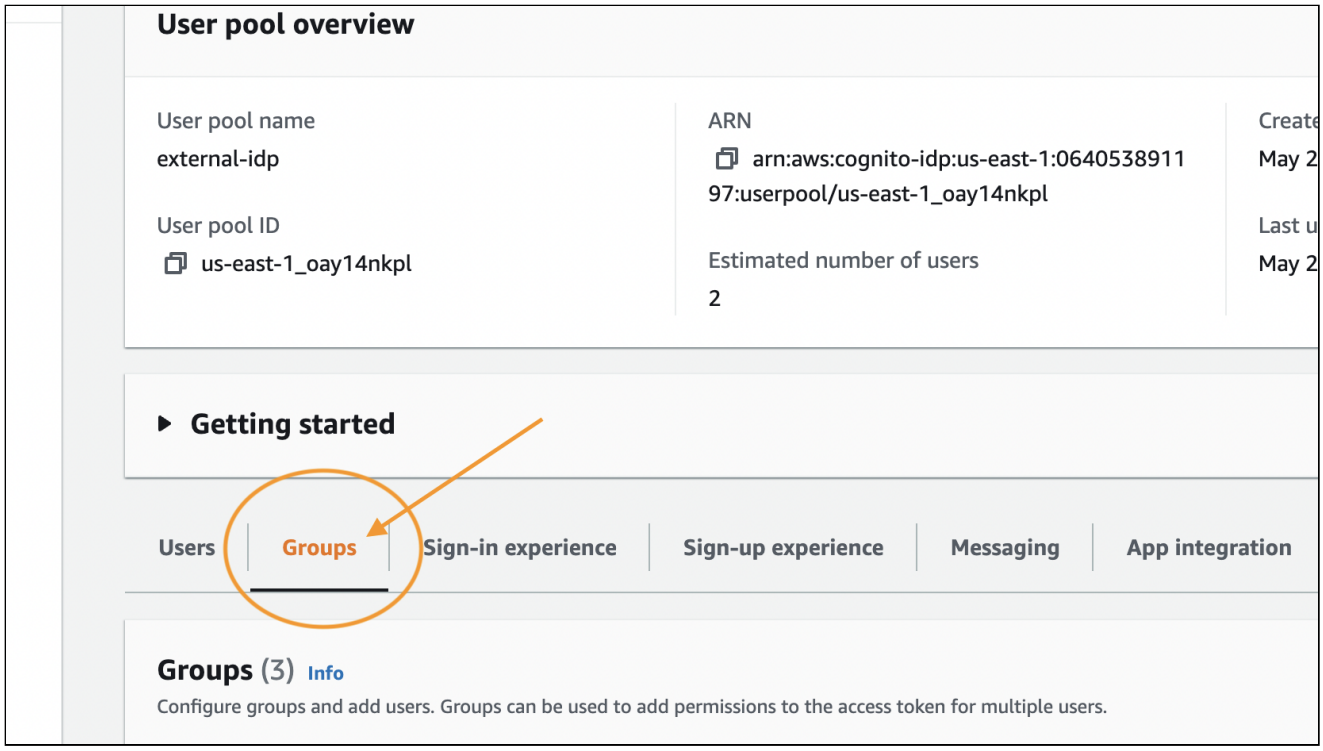


Click on 'Sign-in Experience'



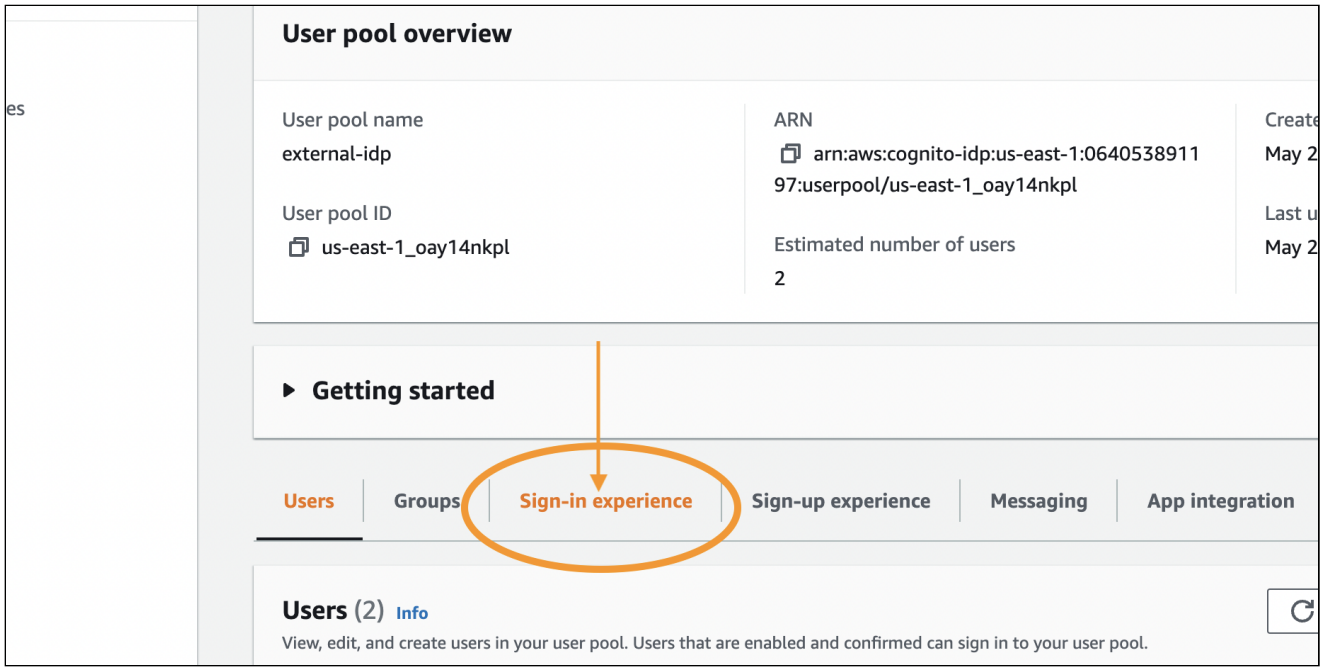
2. What is the name of the group autogenerated for users who sign in using AzureIDP?

Within the Cognito console, click on 'Groups' tab

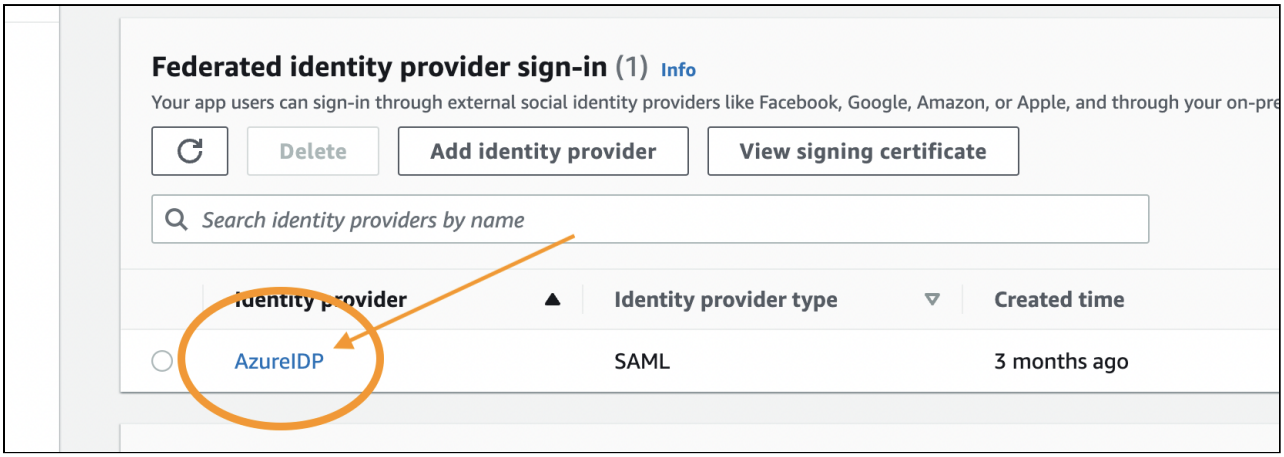


3. The SAML attribute 'groups' is mapped to what custom attribute?

Within the Cognito console, click on 'Sign-in Experience'



From the Sign-in Experience tab, click on 'AzureIDP' Identity Provider



See the debrief section below for answers

Lab 2.1 - Lab Debrief

What is the name of the Active SAML Provider configured in the 'Identity Providers' section of the Cognito console?

AzureIDP

What is the name of the group autogenerated for users who sign in using AzureIDP?

us-east-1_oay14nkpl_AzureIDP

The SAML attribute 'groups' is mapped to what custom attribute?

custom:groups

Lab 2.2 - Creating A Shared VPC Architecture

Summary

In this Lab, you are presented with the start of a shared VPC. The Networking Team is hosting a single VPC called 'prod-shared-vpc' and has created subnets for the delos-web-prod and delos-srv-prod AWS Accounts. Subnets for the *delos-srv-prod* AWS Account have already been shared, including a public subnet, private subnet and transit subnet. Your task is to provision subnets for the delos-web-prod Account, and indicate between which subnets network traffic should be explicitly blocked via NACL so that traffic between the delos-web-prod and delos-srv-prod Accounts and all egress traffic is forced through a SSL inspection appliance before being forwarded on.

Lab Preparation

1. Download the following diagram to your machine: Lab 2.2 Creating A Shared VPC Architecture - Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 2.2 Creating A Shared VPC Architecture - Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 2.2 Creating A Shared VPC Architecture - Complete diagram and open it with draw.io.

Lab 2.2 Tasks

1. Observe how subnets have been shared with the *delos-srv-prod* AWS Account and how NACLs have been used to explicitly allow traffic between the subnets.
2. Share the subnets to the *delos-web-prod* AWS Account, mimicking how they are deployed to the *delos-srv-prod* Account.
3. Using the green arrow, indicate how the subnets in the *delos-web-prod* AWS Account are allowed network connectivity between other subnets in the same account via NACLs.
4. Using the red arrow, show which subnets should be restricted from communicating between each other via NACLs.
5. Your final diagram should restrict east-west traffic between the subnets in the delos-web-prod and delos-srv-prod Accounts unless it passes through the inspection VPC managed by the Security team where traffic is inspected and forward by an appliance.

Lab 2.2 Summary Wrap Up

Several goals have been accomplished in this pattern. First and foremost, a single VPC is hosted in the infrastructure account. This allows the networking team to take ownership of the IP space, Network ACLs defining in broad-stokes the network traffic allowed inbound and outbound between VPC, Routes, Transit Gateway and Internet Gateways.

- The web and services Accounts are each provisioned with three subnets.
  - A public subnet for their publicly facing workloads
  - A private subnet for workloads and
  - A private transit subnet.
- Traffic has been allowed intra-account, between subnets and restricted directly between the *delos-web-prod* and the *delos-srv-prod* Account.
- The only traffic allowed between the *delos-web-prod* and the *delos-srv-prod* accounts is through their private transit subnet via the infrastructure account.
- This becomes an introspection point which can be leveraged by the security team to inspect traffic, either with cloud-native solutions or a 3rd-party offering from AWS marketplace.
- NACLs are used to enforce isolation between the subnets and are controlled by the infrastructure team who hosts the Shared VPC. More fine-grained access-controls via Security Groups are under the control of development team.

In this lab you....

- Shared the public, private and transit subnets to the *delos-web-prod* AWS Account.
- Denied all network traffic between the *delos-web-prod* and the *delos-srv-prod* subnets via NACLs.
- Allowed all network traffic between subnets in the same account via NACLs.
- Allowed traffic via NACLs between the team transit subnets and the infrastructure transit subnet.

Lab follow up questions....

NACLs are not restricting traffic between private or public subnets in the same AWS Account. What other controls might be in place, preventing a compromised EC2 instance in the public subnet from communicating with an instance in the private subnet?

Security Groups

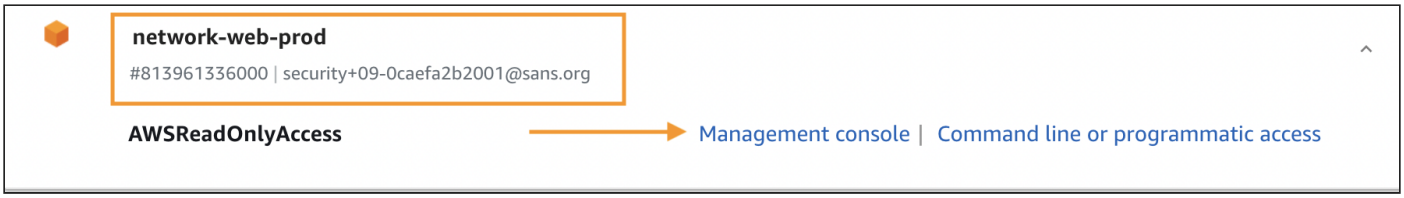
Why do NACLs need to be imposed restricting traffic between subnets in the same VPC?

There is a default NACL attached to every subnet allowing all inbound and outbound traffic

Lab 2.2 - See It In Action

Log into the AWS SSO Portal with your `SEC549 Student` user credentials.

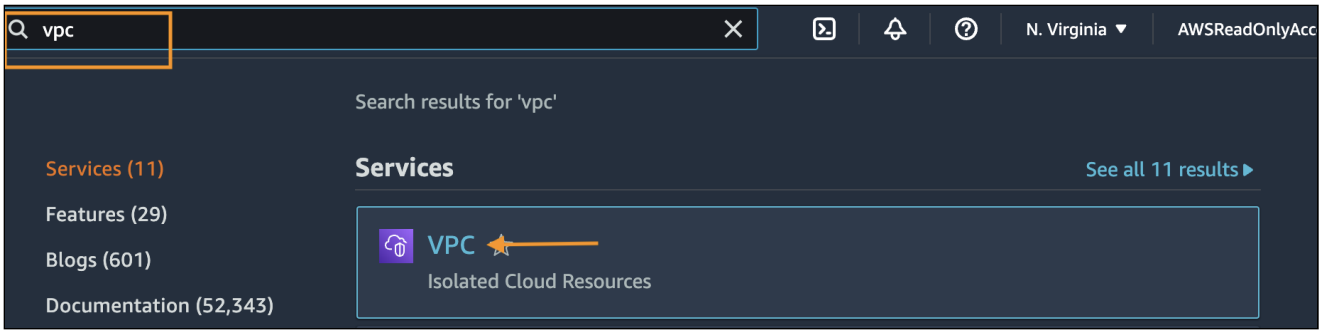
Once authenticated to AWS, click on the *network-web-prod* Account and navigate to view the VPCs in the console.



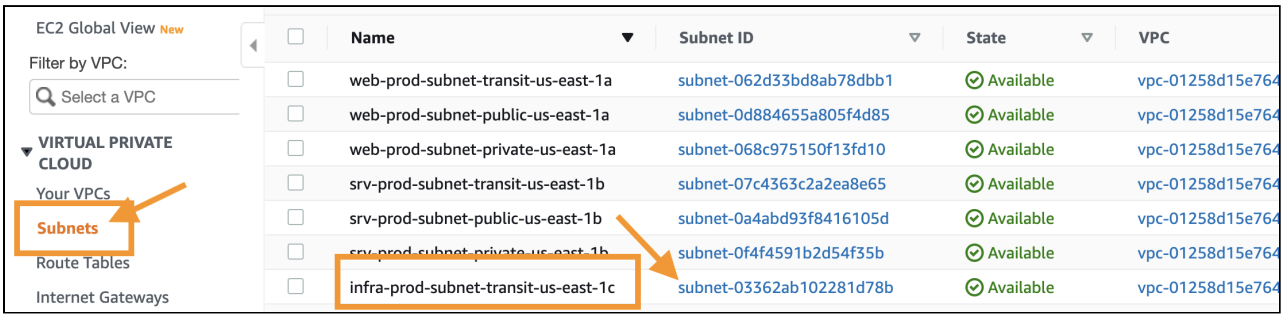
Answer the following questions about the Shared VPC

1. Which private IP ranges are allowed inbound and outbound of the *infra-prod-subnet-transit-us-east-1c* subnet via NACLs?

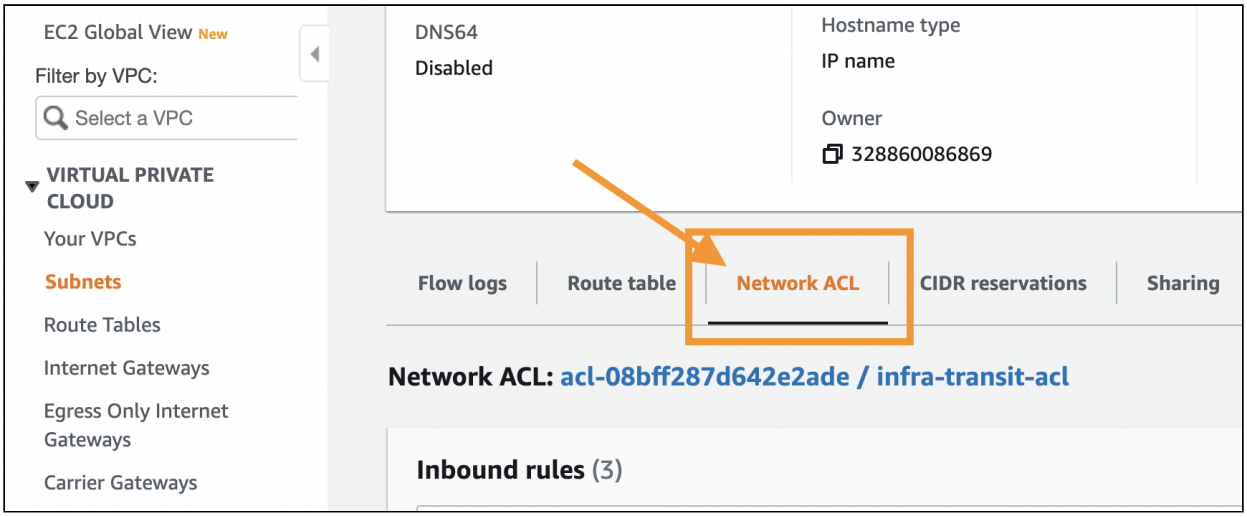
Navigate the Console to find 'VPC'



Click on 'Subnets' and then the *infra-prod-subnet-transit-us-east-1c* subnet

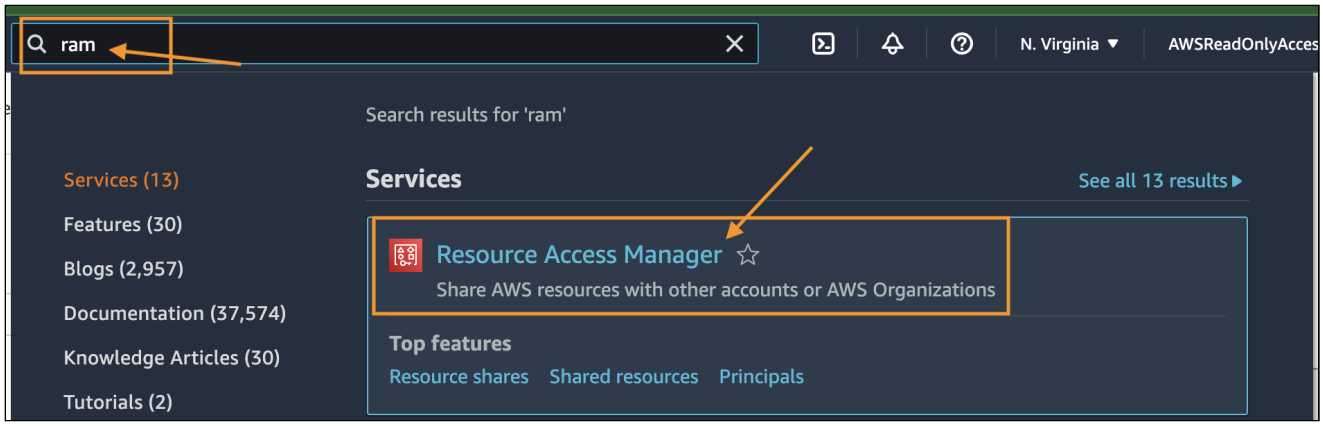


Click on the 'NACLs' tab to view the rules

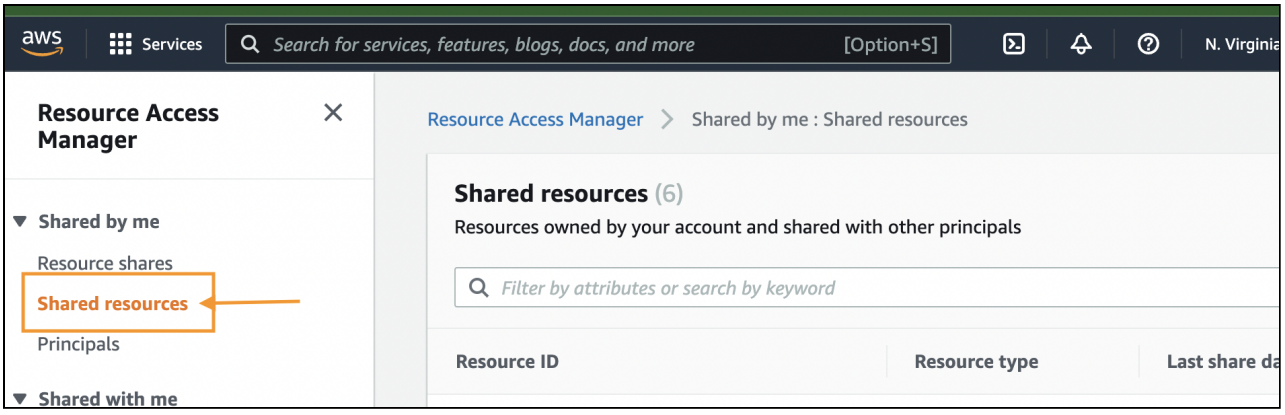


2. What resource types are being shared via Resource Access Manager (RAM)?

Navigate the Console to find 'RAM'



Click on 'Shared Resources'



See the debrief section below for answers

Lab 2.2 - Lab Debrief

Which private IP ranges are allowed inbound and outbound of the *infra-prod-subnet-transit-us-east-1c* subnet via NACLs?

10.0.0.16/28 and 10.0.0.64/28

What resource types are being shared via Resource Access Manager (RAM)?

ec2:Subnet

Lab 2.3 - Access Control for Shared Data Sets

Summary

In this Lab, you'll notice that the architecture has evolved from the 'current-state' to include 4 access points on top of the 'Rehoboam-sync' AWS S3 Bucket and a VPC Interface Endpoint in the *delos-web-prod* Account. In your toolbox you are presented with 6 different resource-level policies. Arrange each of the policy documents into the six slots provided so that consumers of data maintain their access while transitioning to consuming objects via access points. Where callers are expected to originate from a single VPC, provide policy allowing access points to be accessed via a VPC Interface Endpoint.

Lab Preparation

1. Download the following diagram to your machine: Lab 2.3 Configuring Access Controls for Data-Lakes – Lab Work.
2. Navigate to draw.io.
3. Use the *File > Open from > Device* menu option to load the draw.io file named *Lab 2.3 Configuring Access Controls for Data-Lakes – Lab Work* to get started.
4. To see what a 'finished' solution might look like, download the Lab 2.3 Configuring Access Controls for Data-Lakes - Complete diagram and open it with draw.io.

Lab 2.3 Tasks

1. Observe the shift in architecture from the previous 'current-state' diagram. Notice the 4 Access Points that have been created to represent each of the 4 data consumers.
2. Of the 6 policies, identify one which delegates the s3:getObject permission to all Access Points originating from a particular account. Place this policy next to the S3 Bucket.
3. Of the remaining 5 policies, identify one which grants the s3:getObject permission to the EC2-Maze Rendering Role. Place this policy next to the VPC Endpoint.
4. Of the remaining 4 policies, take note which policies grant permissions to which prefixes.
5. Place the policies next to the appropriate Access Point ensuring the data consumer maintains the same access level they had when access was dictated with a single bucket policy.

Lab 2.3 Summary Wrap Up

Access Points have been created for each data consumer, the Monitoring Account, Data Science Team, Park Admins and the Maze Rendering App.
Each newly created Access Point has resource-based policies attached granting access to only specific, corresponding prefixes.
The 'Maze Rendering' Access Point is consumed privately from a VPC Interface Endpoint. Its resource-based policy allows actions only when the caller originates from the *delos-web-prod* VPC.
VPC Endpoint in the *delos-web-prod* Account is provisioned in its private subnet allowing backend components of the application to

privately access the '/maze-plots' prefix. Policy attached to the VPC Endpoint scopes permissions to the 'Maze Rendering' Access Point with the resource field.

This pattern successfully breaks up the clunky bucket-level policy into smaller, more manageable Access Point policies and allows for the prefix requiring private access to be consumed via a VPC Interface Endpoint.

In this lab you....

- Identified the 4 data consumers and which prefixes they should be granted access.
- Configured bucket-level policy delegating access control to the access points.
- Configured access point-level policy for all 4 access points, ensuring parody with older bucket-level access model
- Configured VPC endpoint policy, allowing the Maze Rendering application to access the '/maze-plot' prefix

Lab follow up questions....

If a Principal was granted S3 permissions via an identity-based policy, does this bucket policy prevent them accessing objects?

No

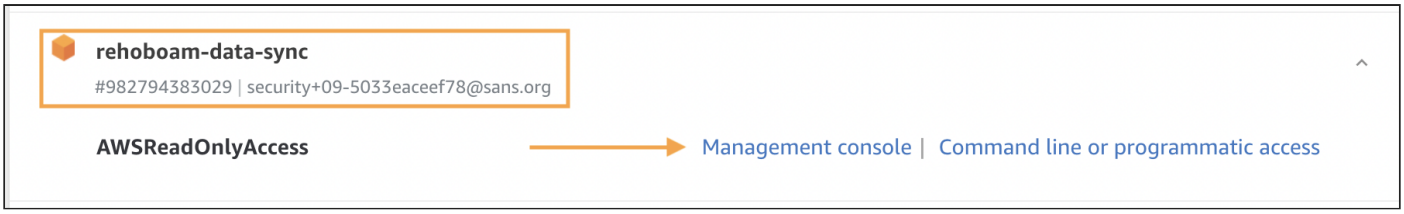
What conditional key could have been used in the VPC endpoint policy to scope access in lieu of leveraging the resource field.

S3:DataAccessPointARN

Lab 2.3 - See It In Action

Log into the AWS SSO Portal with your `SEC549 Student` user credentials.

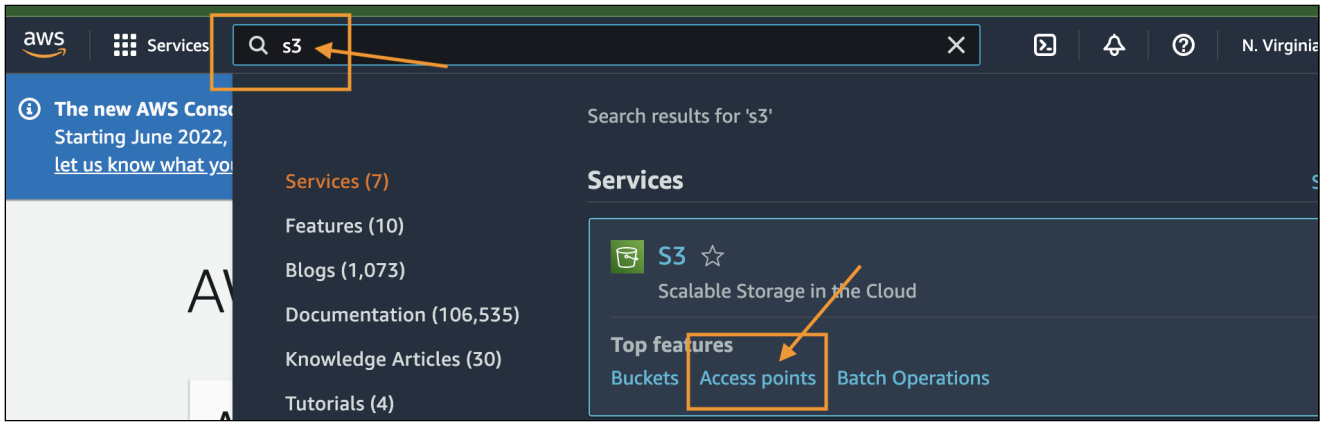
Once authenticated to AWS, click on the *Rehoboam-Data-Sync* Account.



Answer the following questions about the Bucket, Access Point and VPC Endpoint Policies

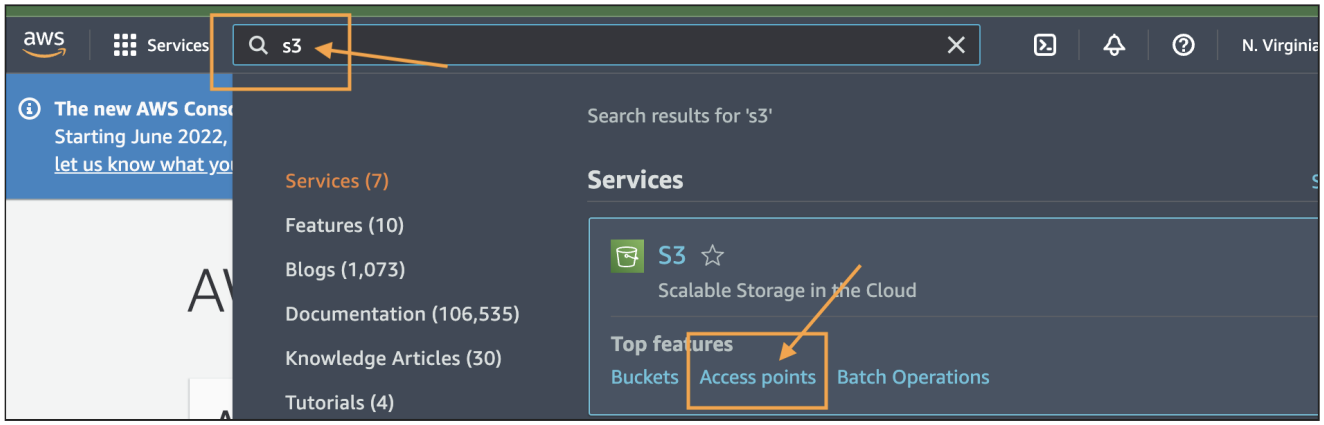
1. Which is the only Access Point listed to have its Network Origin type equal to Virtual Private Cloud (VPC)?

Navigate the Console to find 'S3' and click on 'Access Points'



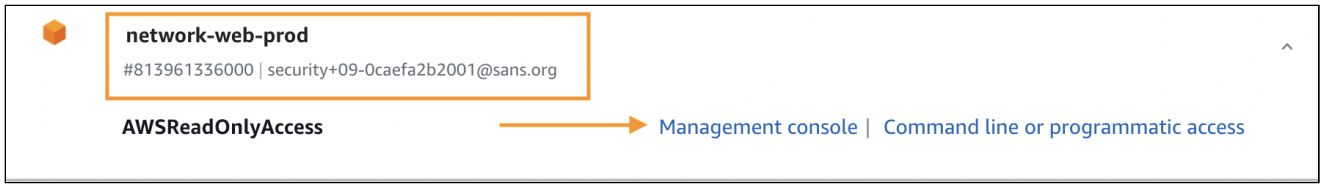
2. What is the Access Point alias for the 'monitoring' Access Point?

Navigate the Console to find 'S3' and click on 'Access Points'

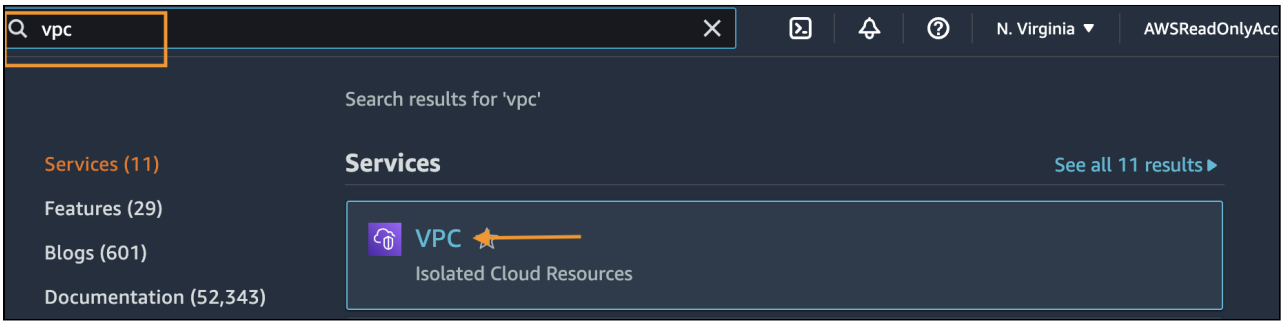


3. What is the name of the Security Group the VPC Interface Endpoint is associated with?

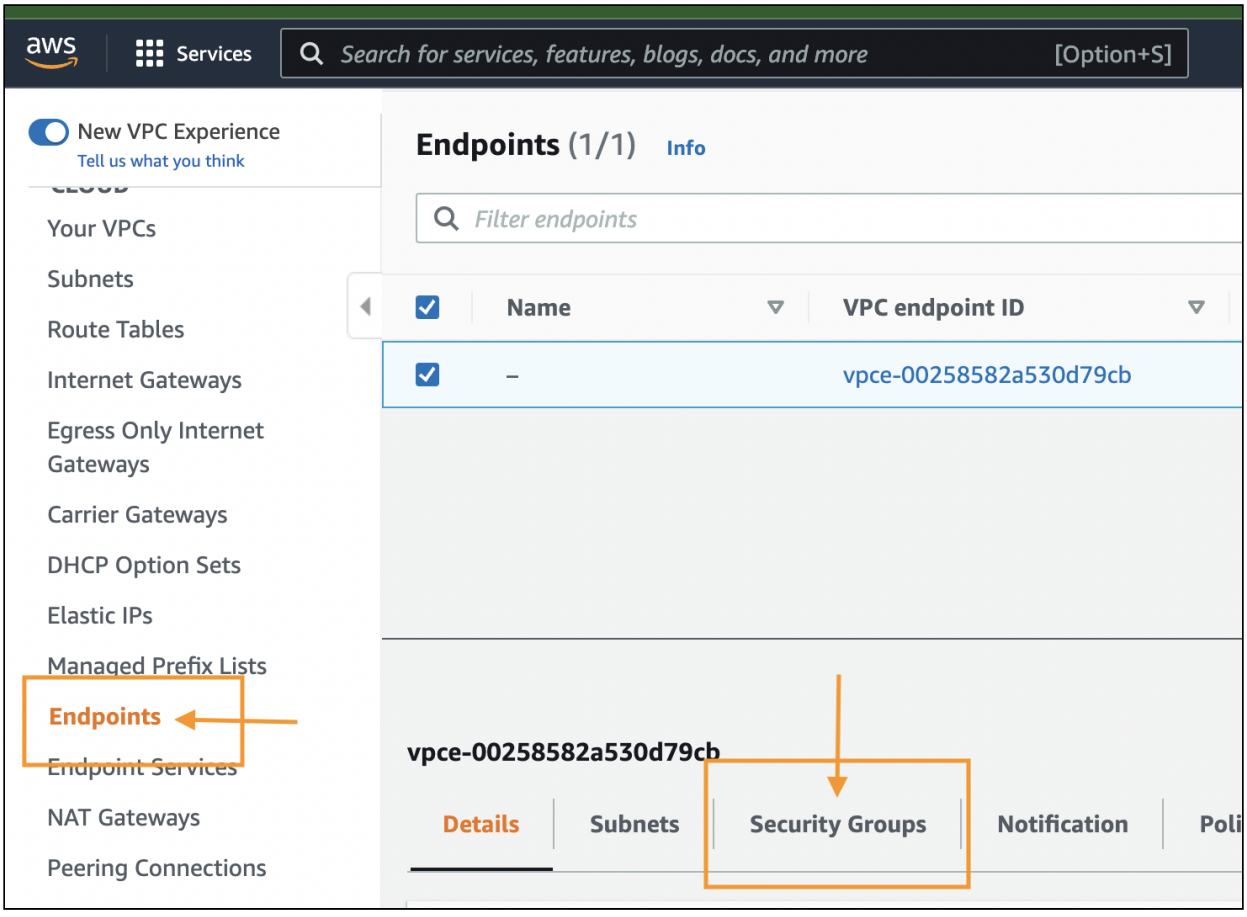
Navigate to the *network-web-prod* Account



Navigate the Console to find 'VPC'



Click on the 'Endpoints' and then the 'Security Groups' tab



See the debrief section below for answers

Lab 2.3 - Lab Debrief

Which is the only Access Point listed to have its Network Origin type equal to Virtual Private Cloud (VPC)?

maze-rendering

What is the Access Point alias for the 'monitoring' Access Point?

monitoring-wq53jizx3otzf3w4ap9agihknqwfguse1a-s3alias

What is the name of the Security Group the VPC Interface Endpoint is associated with?

default

How to Approach the Labs

The SEC549 Enterprise Cloud Security Architecture Workbook is full of critical information that will help you visualize complex cloud architectures and see those architectures in action.

Every lab consists of two parts, diagraming in draw.io and the "See It In Action" portion which has you logging into the AWS console to look at the finished solution.

Part 1 - Diagraming with Draw.io

Diagraming

Draw.io is the tool of choice for this course. You'll be using it to load three types of diagrams for every lab.

1. **Current State Diagrams**: Each lab has a 'Current State' Diagram. This is a representation of the legacy or bad condition which you will be uplifting during the lab.
2. **Lab Work Diagrams**: Each lab has a 'Lab Work' Diagram. This is where you will do your lab work by altering the diagram. Follow the instructions for each lab to arrive at new architecture which meets the stated needs of the business.
3. **Complete Diagrams**: Each lab has a 'Complete' Diagram. Load this diagram in draw.io to see what a finished state might look like.

Follow-up Questions

The first half of every lab will conclude with follow-up questions. These are questions designed to spark conversation and thought about the tasks you just performed in draw.io.

Often, there are no right or wrong answers rather they are meant to pique curiosity about the completed architectural pattern and thoughts about other ways to achieve the same goals.

Part 2 - See It In Action

Logging into AWS

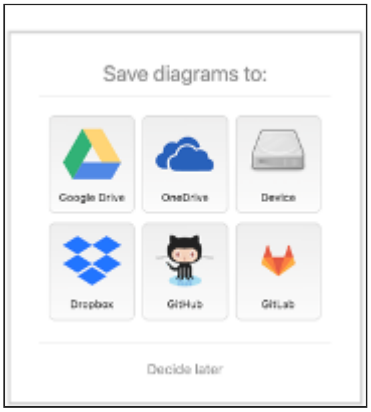
After creating new architectural patterns in draw.io, you'll want to head over to the AWS Console to see the live infrastructure running. During the course, you'll be using the `SEC549 Student` user credentials to authenticate to the AWS console via an integration with Microsoft AAD.

Questions

The "See It In Action" portion of every lab will always include a set of questions to answer as you navigate through the AWS console. For the second half of every lab, you will both observe the configurations of the uplifted cloud infrastructure and answer questions that can only be found on the AWS Console.

Getting Familiar with Draw.io

When you first navigate to draw.io, the application will ask you where you want to save diagrams. Several options are available to you including storing copies on Google Drive, OneDrive, Dropbox or on your local device. You can configure this now, or decide later.



Draw.io Tutorial

1. If you've never visited draw.io before, You will be asked where you want to store your diagrams and then if you want to begin a new diagram or continue a preexisting one.
2. To create a new diagram, click 'File' -> 'New...'. Your page will pop up. Name the document.
3. Use the icons available on the lefthand side of the screen to select the icon you wish. Drag, drop, and resize it if needed. Move by clicking it and dragging it.
4. To ensure you have access to all cloud relevant shapes, click on 'More Shapes' and add in elements from the cloud providers.
5. If a connector is desired, select from the connector list at the top. You can drag and drop an arrow, for example, to the edges of the two icons you want to connect. That connection will remain, even if you move one of the icons.
6. You can select a grouping by drawing a box around the items you wish to group. Right-click on the selected grouping and click 'Group'. They will move together unless you ungroup the selection.
7. You can copy any icon you wish and can use the text section on the right. Images and boxes around them can be filled with any color.
8. All your changes are saved automatically to the storage site you chose. You can also export your diagram in other formats, including png, html, jpg, and pdf. You can turn off the grid to make a professional-looking diagram.

Diagrams

The following links reflect a consolidated list of all Draw.io diagrams used in the course.

Set-Up - Lab 0

Getting Familiar with Draw.io

- Lab 0 Diagram

Lab 1.1

Threat Modeling S3

- Lab Work
- Complete

Lab 1.2

Centralizing User Account Provisioning

- Lab Work
- Complete

Lab 1.3

Structuring Accounts to Create Effective Hierarchies

- Current State
- Lab Work
- Complete

Lab 1.4

Structuring Accounts to Create Effective Hierarchies

- Current State
- Lab Work
- Complete

Lab 2.1

Integrating Modern Auth Into a Legacy Application

- Current State
- Lab Work
- Complete

Lab 2.2

Creating A Shared VPC Architecture

- Current State
- Lab Work
- Complete

Lab 2.3

Configuring Access Controls for Data-Lakes

- Current State
- Lab Work
- Complete

Cheat Sheets

- Multicloud Cheat Sheet
- Fix Security Issues Left of Prod
- Secure Service Configuration in AWS, Azure, & GCP

SANS Courseware License Agreement

PLEASE READ THE TERMS AND CONDITIONS OF THIS COURSEWARE LICENSE AGREEMENT ("CLA") CAREFULLY BEFORE USING ANY OF THE COURSEWARE ASSOCIATED WITH THE SANS COURSE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU (THE "USER") AND SANS INSTITUTE FOR THE COURSEWARE. YOU AGREE THAT THIS AGREEMENT IS ENFORCEABLE LIKE ANY WRITTEN NEGOTIATED AGREEMENT SIGNED BY YOU.

With this CLA, SANS Institute hereby grants User a personal, non-exclusive license to use the Courseware subject to the terms of this agreement. Courseware includes all printed materials, including course books and lab workbooks, as well as any digital or other media, virtual machines, and/or data sets distributed by SANS Institute to User for use in the SANS class associated with the Courseware. User agrees that the CLA is the complete and exclusive statement of agreement between SANS Institute and you and that this CLA supersedes any oral or written proposal, agreement or other communication relating to the subject matter of this CLA.

BY ACCEPTING THIS COURSEWARE, USER AGREES TO BE BOUND BY THE TERMS OF THIS CLA. BY ACCEPTING THIS SOFTWARE, USER AGREES THAT ANY BREACH OF THE TERMS OF THIS CLA MAY CAUSE IRREPARABLE HARM AND SIGNIFICANT INJURY TO SANS INSTITUTE, AND THAT SANS INSTITUTE MAY ENFORCE THESE PROVISIONS BY INJUNCTION (WITHOUT THE NECESSITY OF POSTING BOND) SPECIFIC PERFORMANCE, OR OTHER EQUITABLE RELIEF.

If User does not agree, User may return the Courseware to SANS Institute for a full refund, if applicable.

User may not copy, reproduce, re-publish, distribute, display, modify or create derivative works based upon all or any portion of the Courseware, in any medium whether printed, electronic or otherwise, for any purpose, without the express prior written consent of SANS Institute. Additionally, User may not sell, rent, lease, trade, or otherwise transfer the Courseware in any way, shape, or form without the express written consent of SANS Institute.

If any provision of this CLA is declared unenforceable in any jurisdiction, then such provision shall be deemed to be severable from this CLA and shall not affect the remainder thereof. An amendment or addendum to this CLA may accompany this Courseware.

SANS acknowledges that any and all software and/or tools, graphics, images, tables, charts or graphs presented in this Courseware are the sole property of their respective trademark/registered/copyright owners, including:

AirDrop, AirPort, AirPort Time Capsule, Apple, Apple Remote Desktop, Apple TV, App Nap, Back to My Mac, Boot Camp, Cocoa, FaceTime, FileVault, Finder, FireWire, FireWire logo, iCal, iChat, iLife, iMac, iMessage, iPad, iPad Air, iPad Mini, iPhone, iPhoto, iPod, iPod classic, iPod shuffle, iPod nano, iPod touch, iTunes, iTunes logo, iWork, Keychain, Keynote, Mac, Mac Logo, MacBook, MacBook Air, MacBook Pro, Macintosh, Mac OS, Mac Pro, Numbers, OS X, Pages, Passbook, Retina, Safari, Siri, Spaces, Spotlight, There's an app for that, Time Capsule, Time Machine, Touch ID, Xcode, Xserve, App Store, and iCloud are registered trademarks of Apple Inc.

PMP® and PMBOK® are registered trademarks of PMI.

SOF-ELK® is a registered trademark of Lewes Technology Consulting, LLC. Used with permission.

SIFT® is a registered trademark of Harbingers, LLC. Used with permission.

Governing Law: This Agreement shall be governed by the laws of the State of Maryland, USA.

All reference links are operational in the browser-based delivery of the electronic workbook.