1. **How do you connect from Azure to AWS**

[**https://youtu.be/r2YO6QSqJog?si=YT2or\_ZL2KYth-qV**](https://youtu.be/r2YO6QSqJog?si=YT2or_ZL2KYth-qV)

<https://youtu.be/qGpMQIzGw_w?si=QABJMLSCCSsEgJlm>

**Configure Azure**

1) Create the resource group

2) create virtual network  [172.10.0.0/16](http://172.10.0.0/16), subnet [172.10.0.0/24](http://172.10.0.0/24), resource group required to create the virtual network

3) create the VPN gateway, gate way types, VPN, express Route ,VPN type :  route based , policy based (legacy application)

  Resource and virtunal network required to creat the VPN gateway

  Subnet can create VPN gateway itself

**Configure AWS**

1) create VPC(virtual private cloud)

2) creat subnet [10.10.0.0/16](http://10.10.0.0/16), subnet ip address  [10.10.0.0/24](http://10.10.0.0/24)

3)  Virtual private network under that 4,5 and 6 available

4) custmer gateways , you need to give public IP address of Azure which is created under point 3 in azure

5) virtual private gateways , attach to VPC

6) site to site VPN , need to provide the subnet Azure IP address, we will get two tunals

7) download the configuration file

          get the shared key, outside IP address (Cutomer gateway IP and Virtual private dateway IP) , inside of IP address

**Connecting to Azure and AWS**

**These steps in azure**

1) Local network gateways , provide the AWS outside Virtual IP address, which present in the config file

     and address range : 10,10.0.0.6

 2)  Under VPC, go to connections, click add connections, aws SHARED KEY need to provided and local network gateway

In Azure create internet gateway and attach to VPC

Rote table add the azure IP address [172.10.0.0/24](http://172.10.0.0/24), [0.0.0.0/0](http://0.0.0.0/0) for internet , allow the other networks

Security group, add the azure IP address [172.10.0.0/24](http://172.10.0.0/24) , SSH

ICMP or SSH can be added

**2)How do you find data source in cloud ? how do you confirm where the data are coming from**

ANS) When working with data in the cloud, there are a few methods you can use to find the data source and confirm its origin:

**Data Catalogs and Metadata:** Cloud platforms often provide data cataloging and metadata management services. These services help organize and document information about your data sources. By accessing the data catalog, you can obtain details about the data source, such as its location, format, and origin.

**Data Logging and Monitoring:** Cloud services typically offer logging and monitoring capabilities that track data movement and activities. By examining the logs and monitoring data, you can identify the sources of incoming data and track their flow through various services.

**3)how aws connect to on premise with examples**

AWS Direct Connect establishes a dedicated network connection between your on-premises data center and AWS.

You can provision a physical connection by partnering with an AWS Direct Connect location or use a hosted connection via an AWS Direct Connect partner.

This provides a private and dedicated network link with high bandwidth and low latency between your on-premises environment and AWS services.

VPN (Virtual Private Network):

AWS supports VPN connections, allowing you to create a secure connection between your on-premises network and AWS.

You can use a hardware VPN appliance or software-based VPN client to establish an encrypted connection over the public internet.

AWS provides a Virtual Private Gateway that acts as the VPN endpoint on the AWS side, and you would configure the corresponding VPN device or software on your on-premises network.

AWS Transit Gateway:

AWS Transit Gateway simplifies network connectivity between multiple VPCs, on-premises networks, and remote networks.

It acts as a hub that allows you to consolidate your network connectivity and control traffic flow between various environments.

By establishing a VPN connection or using AWS Direct Connect with AWS Transit Gateway, you can connect your on-premises environment to AWS and route traffic efficiently.

AWS Storage Gateway:

AWS Storage Gateway enables you to integrate on-premises applications with AWS storage services like Amazon S3, Amazon EBS, or Amazon Glacier.

It provides a virtual appliance that you can deploy on-premises, acting as a bridge between your local applications and AWS storage.

You can use different modes of the Storage Gateway, such as File Gateway, Volume Gateway, or Tape Gateway, based on your specific storage requirements.

Hybrid DNS Resolution:

**4)To establish an AWS Direct Connect connection between your on-premises environment and AWS, you need to follow these steps:**

Prerequisites:

Have an AWS account with appropriate permissions to create and manage Direct Connect resources.

Identify the AWS Direct Connect location that is geographically closest to your on-premises environment.

Ensure you have a compatible network device (router) that supports Direct Connect.

Set up the Direct Connect connection in the AWS Management Console:

Log in to the AWS Management Console.

Open the Direct Connect console.

Click on "Create Direct Connect Connection" and provide the necessary information:

Connection name: A unique name for the connection.

Location: Choose the AWS Direct Connect location closest to your on-premises environment.

Bandwidth: Select the desired bandwidth for the connection.

VLAN: Specify the VLAN ID for the connection.

Review and confirm the connection details.

Create a virtual interface:

After creating the Direct Connect connection, you need to create a virtual interface to connect the on-premises network to AWS.

Specify the connection ID of the Direct Connect connection you created.

Provide the BGP (Border Gateway Protocol) information for routing between your on-premises network and AWS.

Configure your network device (router) for Direct Connect:

6) How AWS identity and access management, integration with

active directory

System manager

1) Create self signed certificate

2) Instal and configure ADFS

3) Download federation metadata XML file

AWS

4) Create identity provider and IAM roles in AWS console

 -ARN of SAML provider , ARN of role to assume

5) Configure AWS as trusted replying party

ADFS

6) configure claim rules for the AWS relaying party

addubg name id

 adding a role session name

 adding role attributes (AD groups  & role)

7) Testing the configuration

<https://youtu.be/fyF0cPP0xfo>

1) Configure the active directory service

2) active directory federation services - identity  provider

2) Finally config AWS to trust ADFS

user login using his browser login the active directory web page

it is validate the user credential with local database and senout the same back to the user browser

post the saml assetion request to AWS, which rerun the tmp credential to the browser

 then user able to login the AWS services

SetSPM -a host/localhost adfsrv

self sign cretificate

user access the ADFS site, which run on Https ://

user id autnticate with active directory . user receive teh authentication response

browser post the sample package to end points to AWS

user is redirect to AWS console

**6) how do you achieve anonymization of data especially if the data are personal and are sensitive information in AWS cloud**

Encryption:

Utilize encryption techniques to protect the data at rest and in transit.

AWS provides services like AWS Key Management Service (KMS) to manage encryption keys and AWS Certificate Manager (ACM) for managing SSL/TLS certificates.

Data Masking:

Apply data masking techniques to replace sensitive information with fictional or altered data.

AWS services such as Amazon RDS for Oracle or Amazon Redshift support built-in data masking capabilities to help protect sensitive data.

Tokenization:

Tokenization involves replacing sensitive data with unique tokens while maintaining referential integrity.

AWS services like Amazon S3 and Amazon DynamoDB can be used with tokenization techniques to preserve data privacy.

Data Lifecycle Management:

Implement data lifecycle management policies to control data retention, archival, and disposal.

AWS services like Amazon S3 and Amazon Glacier offer lifecycle management features to automate data retention and archival processes.

Identity and Access Management (IAM):

Implement proper IAM policies and roles to control access to sensitive data.

Use AWS IAM features like fine-grained permissions, multi-factor authentication (MFA), and temporary security credentials to limit access to sensitive data.

Data Minimization:

Reduce the amount of personal and sensitive data stored or processed in the cloud.

Implement data minimization practices by only collecting and retaining the necessary data for business purposes.

Compliance and Governance:

Leverage AWS services and features that assist with compliance and governance requirements.

AWS provides services like AWS CloudTrail for audit logging, AWS Config for configuration management, and AWS CloudWatch for monitoring and alerting.

Privacy by Design:

Adopt privacy by design principles to ensure that privacy considerations are incorporated into the design and implementation of your AWS architecture.

Evaluate and implement AWS services and features that align with privacy and data protection requirements.

**7) Why do like to Join IHIS**

Ans) looking for long term opportunity in Singapore

**8) What frustrates you ?**

Ans) I will not be frustrated. Most of the time I will maintain the transference with the team and the management. Its always help me to maintain the positive environment