Infrastructure Identity Workshop
Scenario

Your company is new to the cloud and has deployed their first set of development and productions systems in AWS, additionally you still have hosts to manage in your data center.

You are a systems administrator and have been tasked with setting up secure administrative access to your systems in AWS and on-premise.

As part of that configuration you are also responsible for confirm the ability to audit administrative activities.
Lab Activities

Secure Administration using Session Manager and EC2 Instance Connect

1. Configure IAM to enable Session Manager
2. Build and bootstrap instances with SSM Agent
3. Configure the Systems Manager service
4. Configure tag based restrictions
5. Setup logging
6. Confirm appropriate access and review logs
7. Build and bootstrap an instance with EC2 Instance Connect
8. Confirm appropriate access
Lab Architecture – Initial Environment
Lab Architecture – What we’re building?
Purpose

- Hands on experience using IAM to access AWS infrastructure with Systems Manager Session Manager and EC2 Instance Connect
- Immutable central management using ephemeral credentials based on tags
- One tool to manage EC2 + on premise systems
Access the Lab


https://idm-infrastructure.awssecworkshops.com/