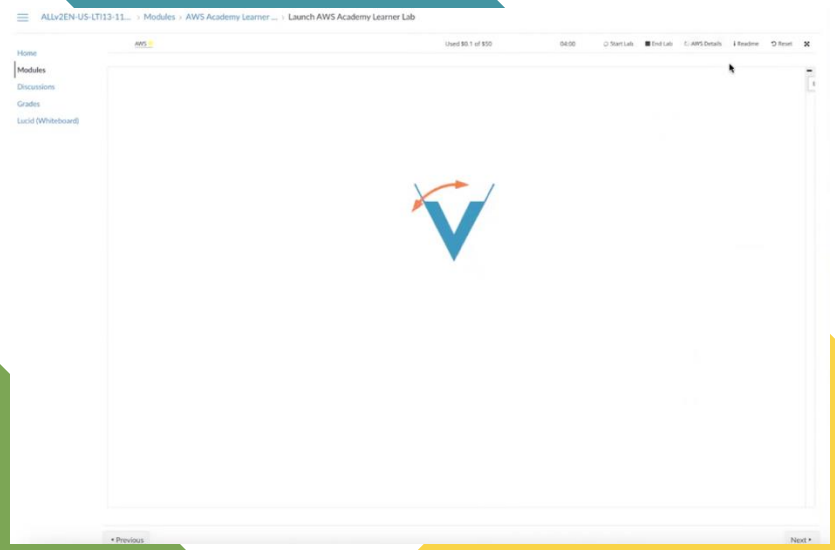
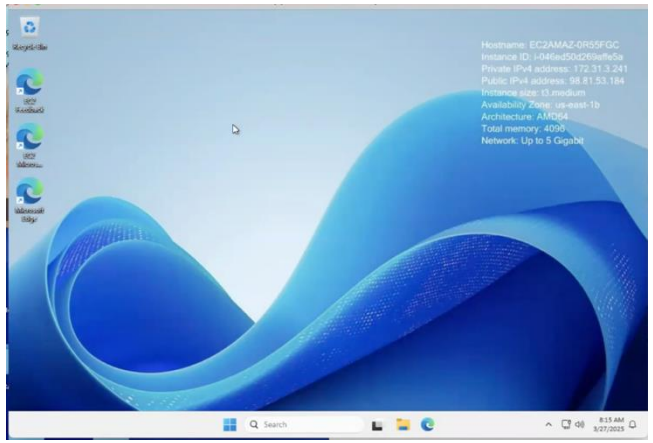
Tishk International University

Week 5: **Windows Server on AWS: Theoretical Foundation**



Class code

gxgxvq4



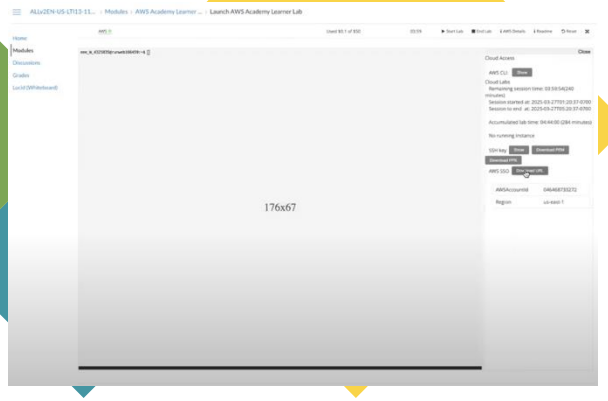
4th Year IT Department, Tishk International University
Lecturer: Mohammad Salim Al-Othman

Outline

- Introduction to AWS Academy Learner Lab
- EC2 Windows Server Instances
- Remote Desktop Protocol (RDP)
- Basic Windows Server Administration
- AWS Cost Management
- Security Fundamentals

1 Introduction to AWS Academy Learner Lab

Tishk International University



AWS Academy Fundamentals

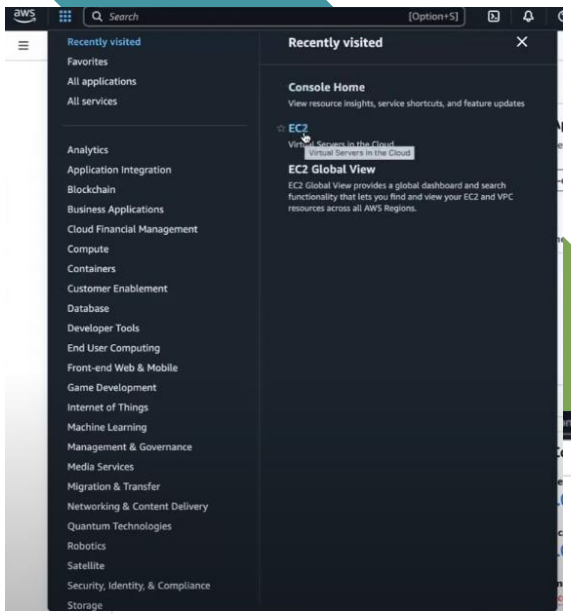
- AWS Academy is Amazon's educational program providing students with hands-on cloud experience
- Learner Lab is a controlled environment with pre-allocated credits for educational purposes
- The AWS Academy portal provides a simplified interface to access AWS services
- Lab environment offers temporary access to AWS resources without billing concerns

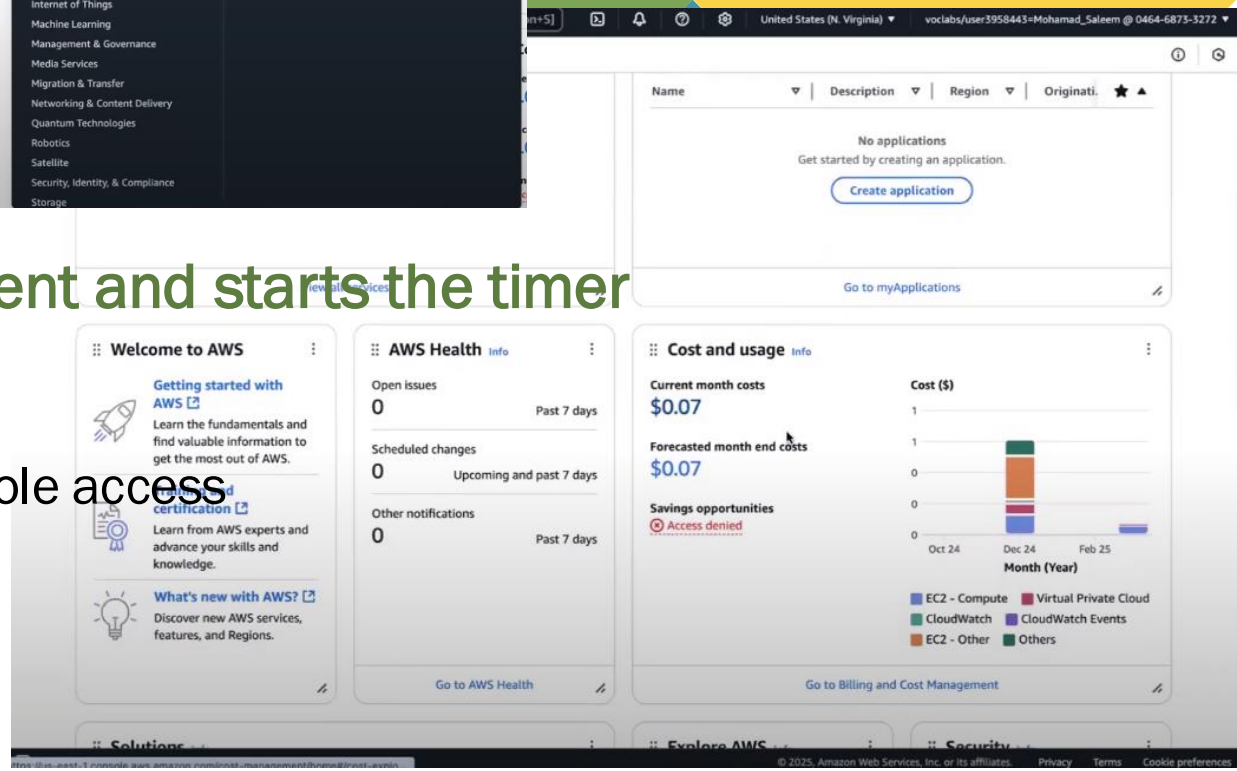
1 Introduction to AWS Academy Learner Lab

Lab Environment Structure

- Lab Timer/Duration: Labs have specific time limits (typically 2-4 hours) Green indicator shows active lab time remaining
- Labs automatically terminate when time expires
- Students should save work regularly and manage time effectively

1 Introduction to AWS Academy Learner Lab



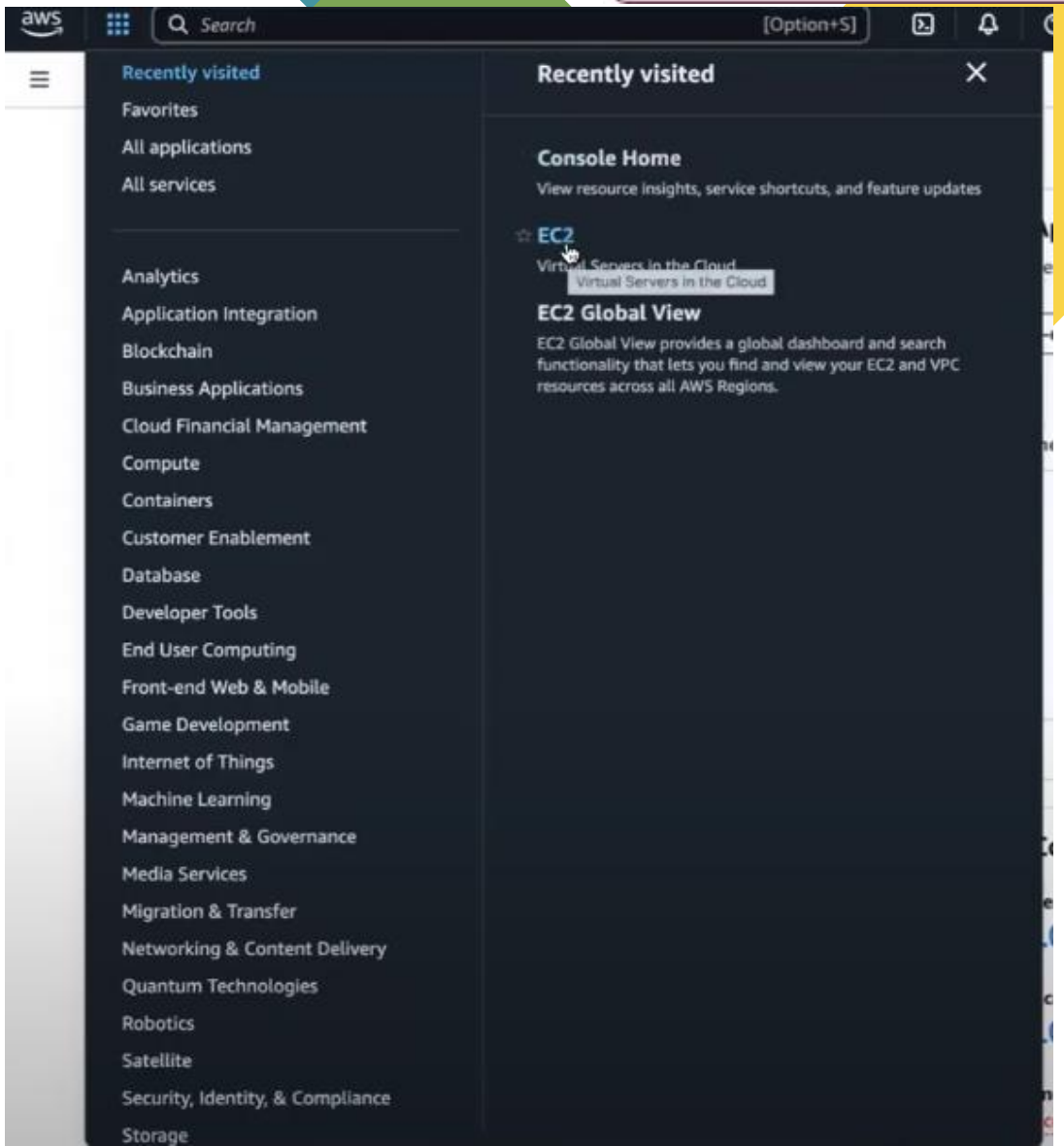


AWS Learner Lab Interface

- Start Lab Button: Initiates the lab environment and starts the timer
- AWS Details Section:
  - Critical panel containing: AWS SSO URL for console access
  - User credentials (username, password)
  - AWS Region information
  - Available credits/budget
- Lab Resources Panel: Shows available services and resource limits

1 Introduction to AWS Academy Learner Lab

- Lab Resources Panel: Shows available services and resource limits



1 Introduction to AWS Academy Learner Lab

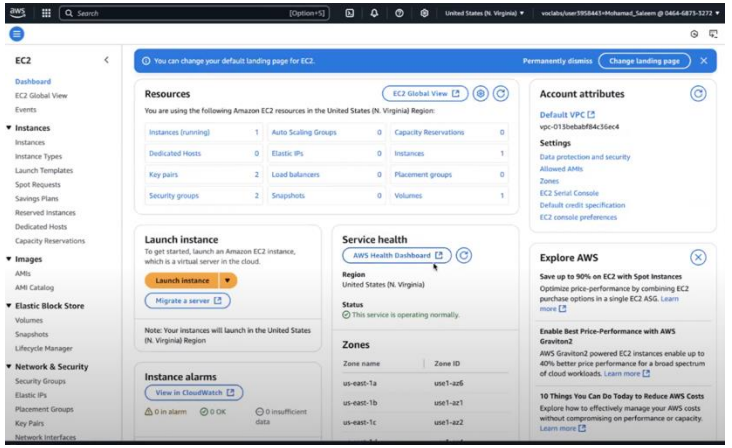
AWS SSO Login Process

1. Single Sign-On (SSO): Simplified authentication method for AWS resources Process flow: Student clicks AWS SSO URL from AWS Details section
2. System opens secure browser session to AWS authentication portal
3. Student enters credentials from AWS Academy (different from personal AWS accounts)
4. Temporary session grants access to specific AWS services with educational permissions
5. Security automatically handles session timeouts and credential rotation

1 Introduction to AWS Academy Learner Lab

AWS Management Console

- Management Console: Web-based interface for accessing all AWS services
- Key components:
  - Service search: Quick access to specific services (used to find EC2)
  - Region selector: Determines geographic location of resources
  - User menu: Shows identity and access information
  - Service dashboard: Primary workspace for each AWS service



Navigation designed for service-specific workflows

Definition:

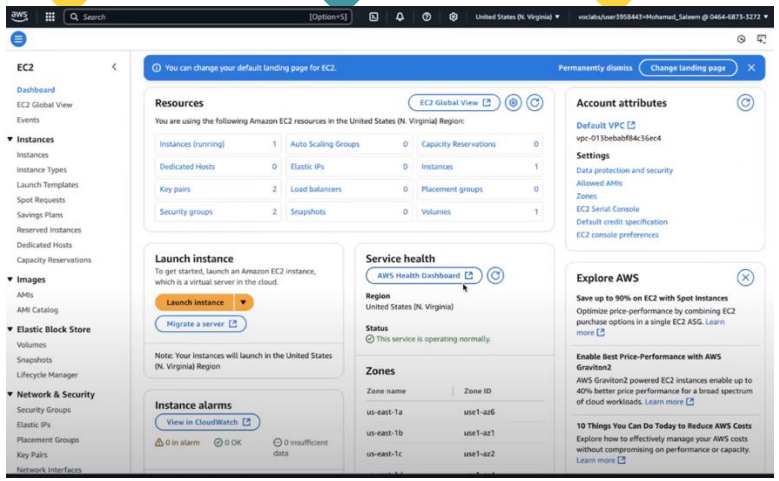
AWS Region is a geographical area containing multiple isolated data centers (Availability Zones) where you can deploy resources, offering lower latency to local users and helping meet data residency requirements.

1 Introduction to AWS Academy Learner Lab

AWS Academy vs. Production Environment

Key differences from standard AWS accounts:

- Limited service selection (education-focused)
- Credit-based instead of payment method-based
- Simplified IAM permissions model
- Automatic cleanup of resources
- Preset service quotas and limits
- No ability to request service limit increases
- Isolated from production AWS infrastructure



Explanation:

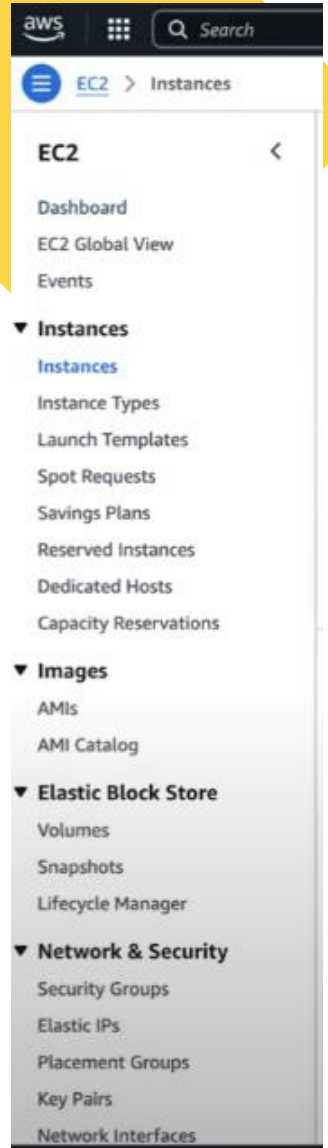
IAM is AWS's permission management system that controls which users can access which resources and what actions they can perform, using users, groups, roles, and policies.

2- EC2 Windows Server Instances

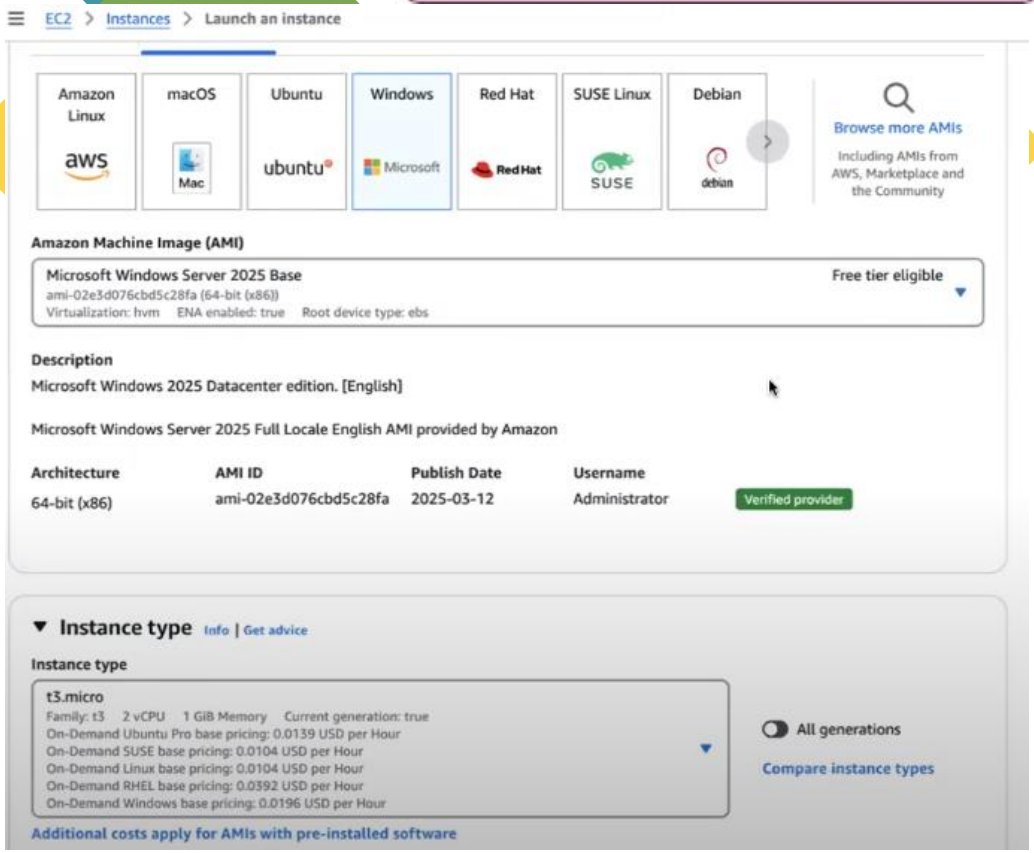
Tishk International University

What is EC2?

- EC2 (Elastic Compute Cloud) is AWS's service that provides resizable computing capacity
- EC2 allows you to launch virtual servers (instances) in the cloud
- Windows Server instances are EC2 instances running Microsoft Windows Server operating system
- AWS supports multiple Windows Server versions (2019, 2022, 2025)



2- EC2 Windows Server Instances



Instance Types Covered in Lab

T3 instance family: Burstable general-purpose instances

- t3.micro: 1 vCPU, 1 GiB memory (minimal resources)
- t3.small: 2 vCPUs, 2 GiB memory (light workloads)
- t3.medium: 2 vCPUs, 4 GiB memory (recommended for Windows Server)

Defnitions:

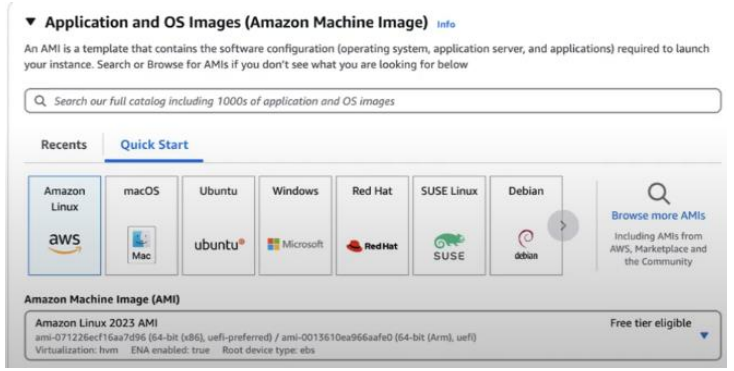
A vCPU (virtual CPU) represents a portion of the underlying physical CPU assigned to a virtual machine, allowing multiple instances to share processing resources of the physical server.

GiB (Gibibyte) is a unit of digital information storage equal to 1,073,741,824 bytes (2^30), slightly larger than a GB (Gigabyte) which equals 1,000,000,000 bytes (10^9).

2- EC2 Windows Server Instances

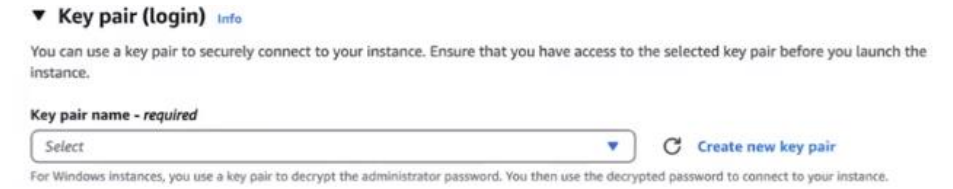
Key Components of EC2 Windows Deployment

- AMI (Amazon Machine Image): An AMI is a pre-configured template containing an operating system, application server, and applications used to launch EC2 instances. AMIs can be AWS-provided, marketplace AMIs, or custom AMIs you create from your instances.
  - Windows Server 2025 Base (GUI version)
  - Windows Server 2025 Core (command-line only)



- Key Pair: Public/private key combination for secure authentication
  - Used to decrypt Windows administrator password
  - PEM file format for the private key

- Security Group: Virtual firewall controlling traffic to the instance
  - RDP port 3389 must be open for remote access
  - Best practice is to limit RDP access to specific IP addresses

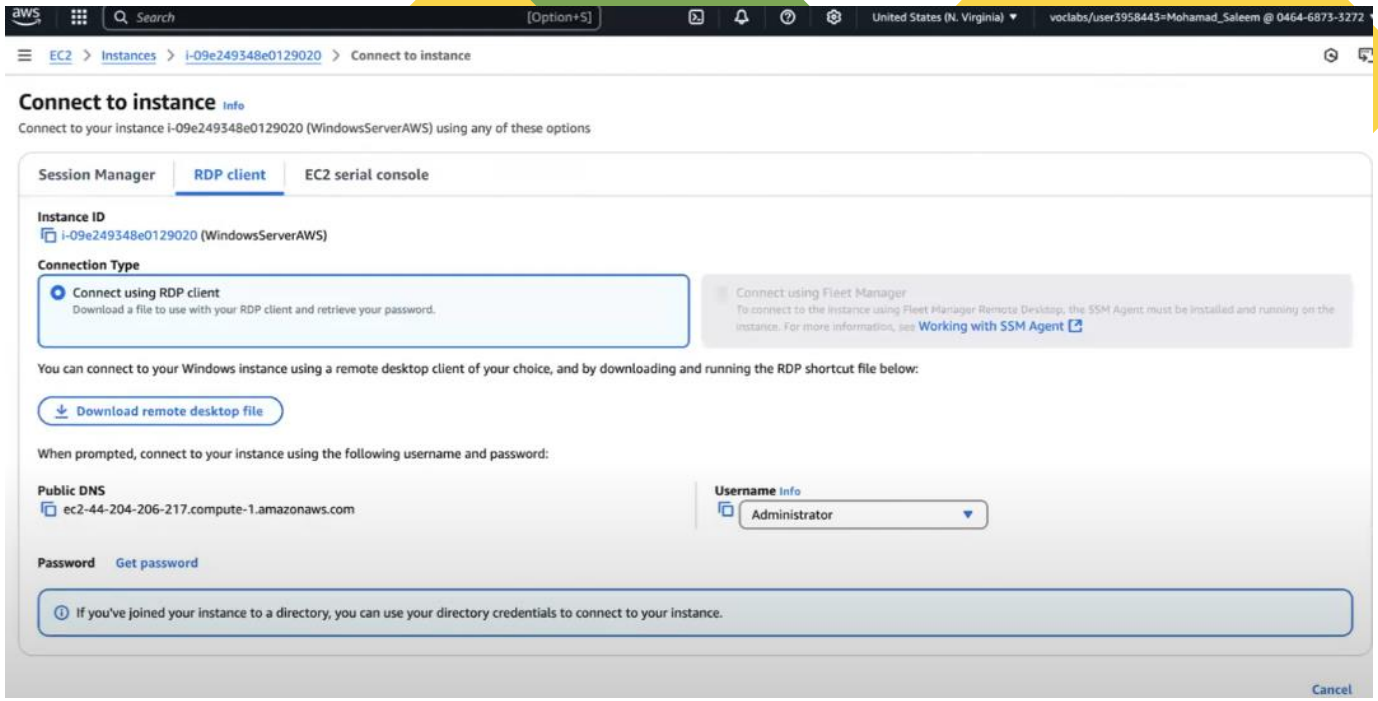


3. Remote Desktop Protocol (RDP)

Tishk International University

RDP Fundamentals

- Remote Desktop Protocol (RDP) is Microsoft's proprietary protocol for remote system access
- Allows administrators to connect to and manage Windows servers from a distance
- Provides a graphical interface identical to being physically at the server
- Operates over TCP port 3389 by default

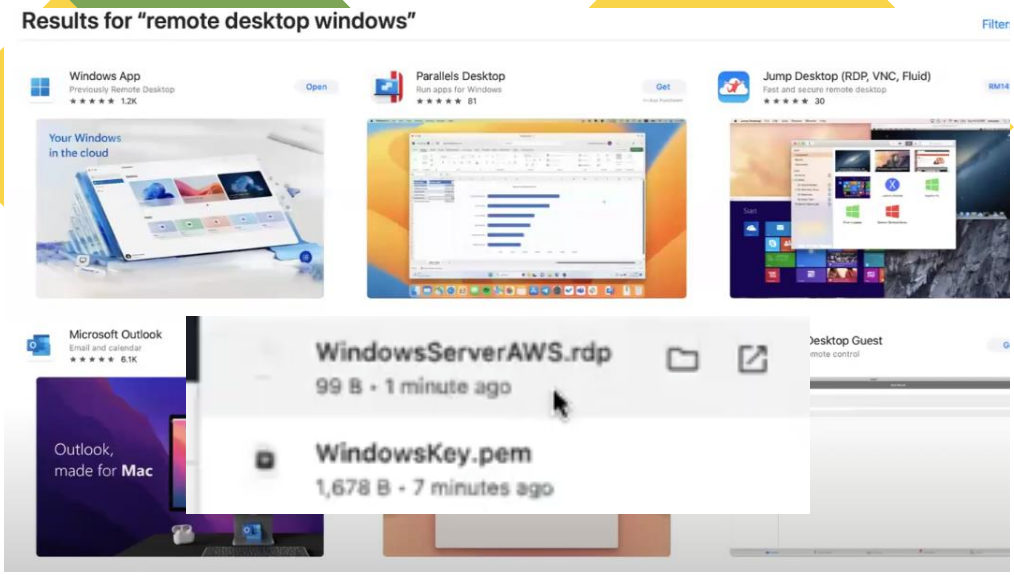


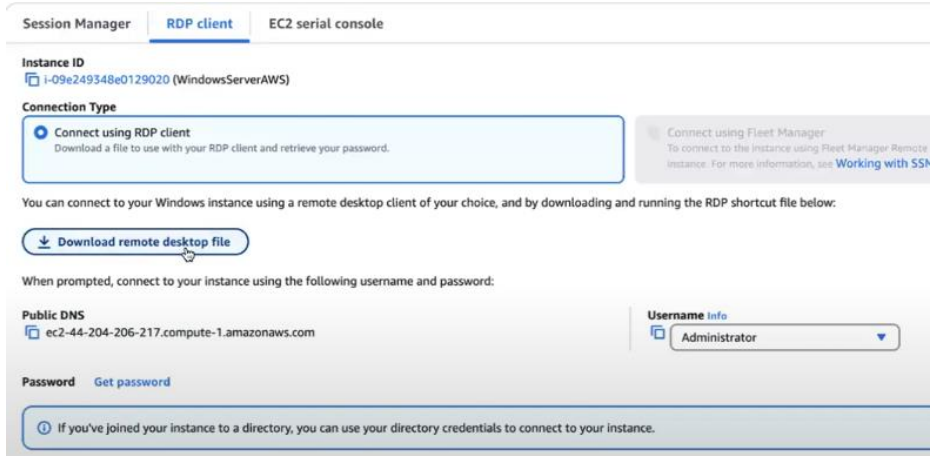
Windows2025-Key.pem

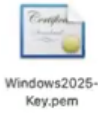
3. Remote Desktop Protocol (RDP)

RDP Connection Process

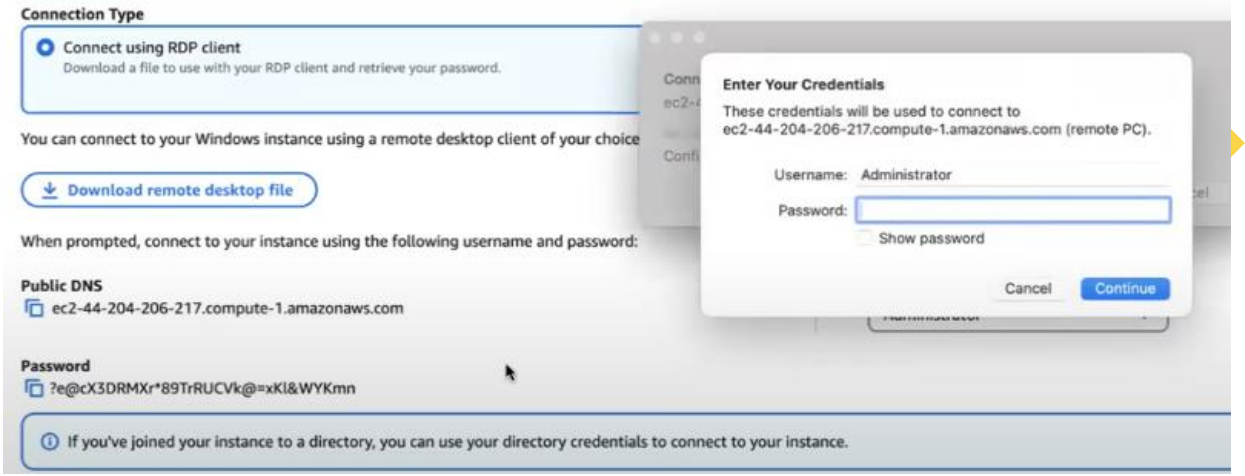
- Administrator downloads RDP file or configures connection manually
- Enters server address, username, and password credentials
- RDP client establishes encrypted connection to server
- Server displays desktop and responds to user input







3. Remote Desktop Protocol (RDP)



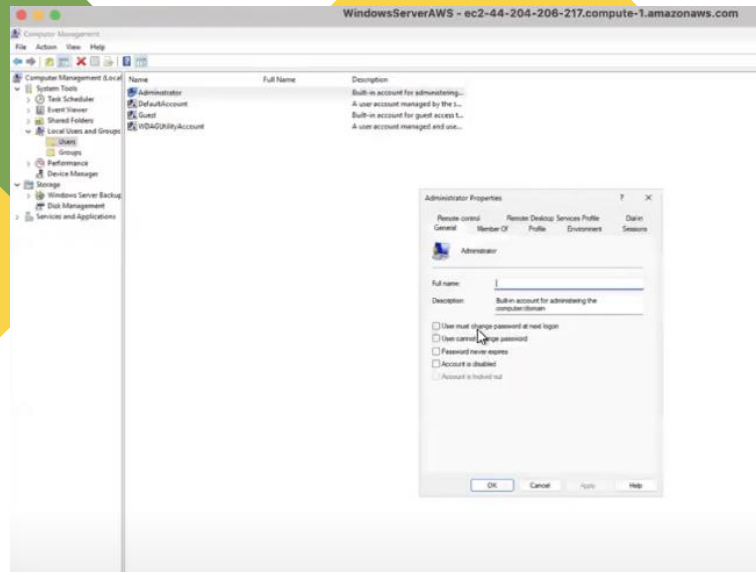
RDP Security Considerations

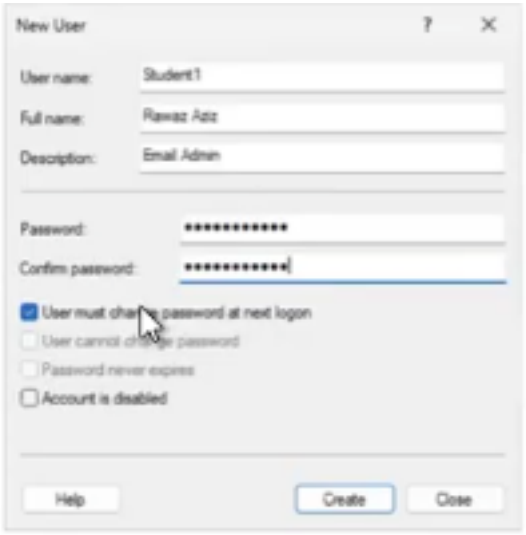
- Password encryption secures authentication process
- Connection to unknown servers presents certificate validation warnings
- Public access to RDP is a security risk (ransomware/brute force attacks)
- Best practice is to use restricted IP ranges and complex passwords

4. Basic Windows Server Administration

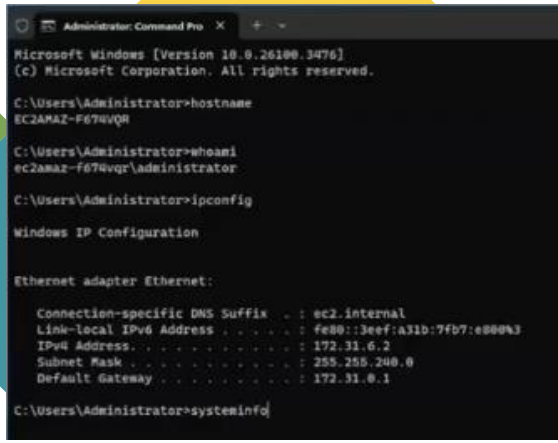
User Management

- Local Users and Groups: Windows tool for managing server accounts
- Administrator: Default administrative account with full system control
- New user creation process:
  - Setting username and password
  - Configuring password policies (expiration, complexity)
  - Assigning group memberships for access control
- Administrative access through "Administrators" group membership





4. Basic Windows Server Administration



Essential Command-Line Tools

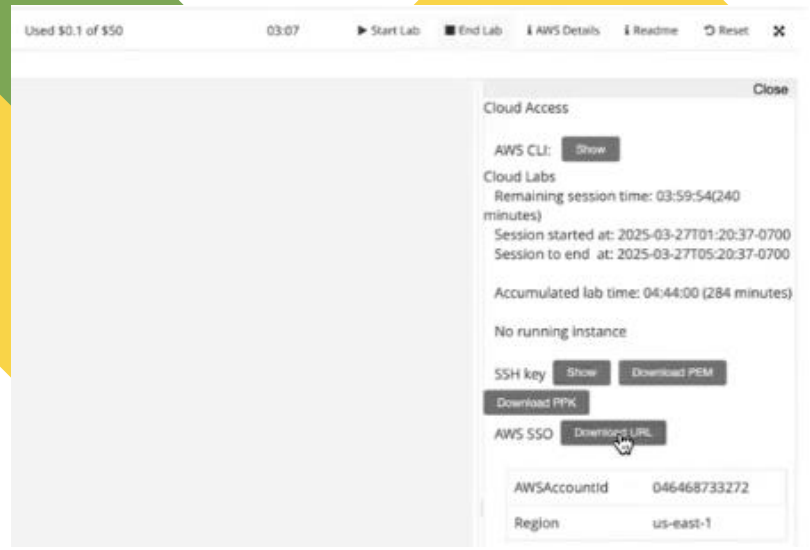
- Command Prompt (cmd.exe): Windows command-line interface
- Key system commands covered in lab:
  - **hostname**: Displays the computer's network name
  - **whoami**: Shows current user context (domain\username)
  - **ipconfig**: Displays network configuration details (IP address, subnet, DNS)
  - **systeminfo**: Provides comprehensive system information (OS, hardware, patches)
- These commands help administrators quickly gather system information

4. Basic Windows Server Administration

System Management

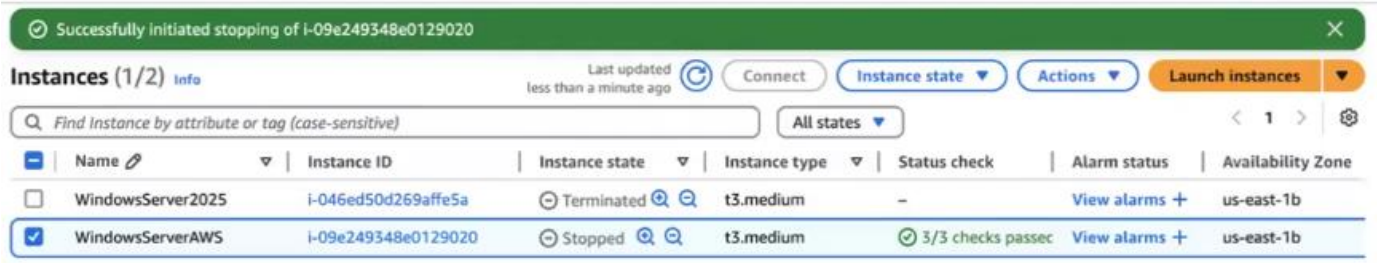
- Shutdown commands: Proper methods to restart or power off servers
  - shutdown /s /t 0: Immediate shutdown
  - shutdown /r /t 0: Immediate restart
- Why controlled shutdown matters:
  - Prevents data corruption
  - Allows services to close gracefully
  - Updates system state properly
- Server shutdowns require careful consideration in production environments

5. AWS Cost Management



AWS Billing Concepts

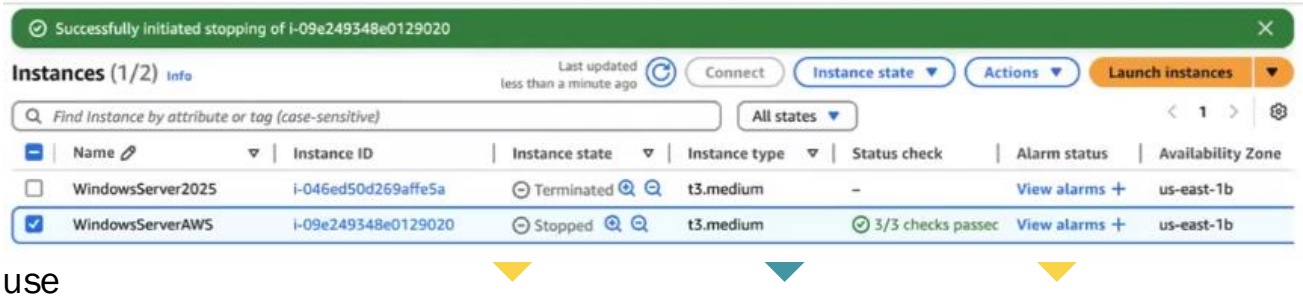
- Pay-as-you-go model: Charges based on actual resource usage
- Hourly billing: Compute resources charged by the hour
- Multiple cost components:
  - EC2 instance runtime (compute)
  - EBS storage (persistent disk): EBS provides persistent block-level storage volumes for EC2 instances. These virtual hard drives can be attached to instances, offer different performance characteristics, and persist independently from the instance lifecycle.
  - Data transfer
  - Elastic IP addresses



Instance States and Billing

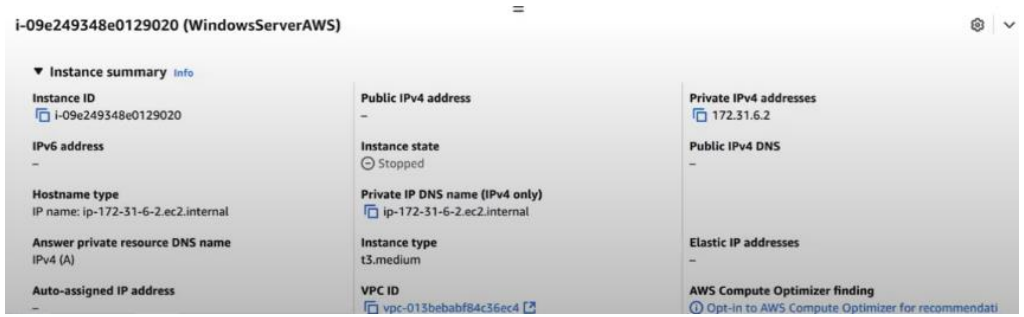
- Running: Full charges for compute and storage
- Stopped: No compute charges, but storage costs continue
- Terminated: All charges cease, instance deleted permanently

5. AWS Cost Management



Proper Instance Shutdown

- Stopping vs. Terminating:
  - **Stop**: Preserves instance configuration and data for later use
  - **Terminate**: Permanently deletes the instance
- EC2 Dashboard workflow for stopping instances
- Importance of verifying instance state to prevent unexpected charges
- EBS storage costs continue even when instances are stopped



Elastic IP Management

- Elastic IP: Static public IP address for EC2 instances
- Unused Elastic IPs incur charges even when instances are stopped
- Proper release procedure to avoid unnecessary billing

6. Security Fundamentals

AWS Security Group Concepts

- Security Groups: Virtual firewalls controlling traffic to/from instances
- Stateful packet filtering automatically allows return traffic for established connections without requiring separate rules, unlike stateless filtering which requires explicit rules for both inbound and outbound traffic. (return traffic automatically allowed)
- Allow rules only (no explicit deny rules)
- Rule components:
  - Protocol (TCP/UDP)
  - Port range
  - Source/destination

6. Security Fundamentals

RDP Security Best Practices

- Restrict RDP access to specific IP addresses
- Use complex passwords for Administrator account
- Consider alternative access methods for production:
  - VPN + RDP : A VPN creates an encrypted connection between remote users and AWS resources, allowing secure access to private instances without exposing them to the public internet.
  - Bastion hosts: Bastion hosts are specially hardened instances placed in public subnets that serve as secure gateways for accessing private instances, adding an additional security layer for remote administration.
  - AWS Systems Manager Session Manager

Key Pair Security

- Private key (.pem file) must be protected
- Never share private keys between users
- Store key files securely
- Different keys for different environments

Conclusion

- AWS Academy Learner Lab provides a controlled environment for hands-on cloud experience
- EC2 Windows Server combines Microsoft's OS with Amazon's scalable infrastructure
- Remote administration via RDP enables secure management from anywhere
- Basic Windows commands (hostname, whoami, ipconfig, systeminfo) provide essential system information
- User management in Windows Server follows same principles across environments
- Cost management requires understanding instance states (Running, Stopped, Terminated)
- Security considerations span multiple layers (Key Pairs, Security Groups, Windows authentication)
- Skills transfer directly to production environments and professional IT roles

Thank you

Mohammad Salim-

IT Dept- Applied Science Faculty- TIU University

Class code

gxgxvq4