Remotely Run Commands on an EC2 Instance with AWS Systems Manager

Project Overview

This hands-on tutorial demonstrates how to securely manage and remotely execute commands on an EC2 instance using **AWS Systems Manager (SSM)** — without using **SSH**, **bastion hosts**, or **remote PowerShell**. This is particularly useful in environments with strict security policies that restrict direct server access.

Prerequisites

- AWS Account (Free Tier eligible)
- Recommended Browser: Chrome or Firefox
- EC2-supported Region selected in the AWS Console

Time to Complete

Approximate duration: 10–15 minutes
Cost: Free Tier Eligible

Use Case

As a **System Administrator**, you are required to perform maintenance tasks like **package updates** on production EC2 servers. However, **SSH access is restricted**. You will:

1. Create an IAM Role for Systems Manager.
2. Launch an EC2 instance with the role attached.
3. Use Systems Manager to:
    - Update the SSM Agent.
    - Run shell commands remotely.
4. Terminate the instance to prevent future costs.

Step-by-Step Implementation

Step 1: Create an IAM Role for Systems Manager

1. Go to the IAM Console.
2. Navigate to **Roles** > **Create role**.
3. Choose:
   - **Trusted Entity**: AWS Service
   - **Use Case**: EC2
   - Click **Next**.
4. Under **Permissions**, search and select:
   - AmazonEC2RoleforSSM
5. Click **Next**, then name your role:
   - **Name**: EnablesEC2ToAccessSystemsManagerRole
   - **Description**: Enables an EC2 instance to access Systems Manager
6. Click **Create role**.

Step 2: Launch an EC2 Instance with the IAM Role

1. Go to the EC2 Console.
2. Click **Launch Instance**:
   - **Name**: MyEC2Tutorial
   - **AMI**: Amazon Linux 2 AMI (default)
   - **Instance type**: t2.micro (Free Tier)
   - **Key pair**: Choose "**Proceed without key pair**"
   - **Network settings**: Leave default
3. Under **Advanced Details**, assign IAM Role:
   - **IAM instance profile**: EnablesEC2ToAccessSystemsManagerRole
4. Click **Launch Instance**.

Step 3: Update the Systems Manager Agent (SSM Agent)

1. Go to the **Systems Manager Console**.
2. On the left panel under **Node Management**, click **Fleet Manager**.
3. Select your instance MyEC2.
4. Click **Node actions** > **Execute run command**.
5. Under the **Run command** page:
   - Filter documents using:
     - Document name prefix → Equals → AWS-UpdateSSMAgent
   - Select **AWS-UpdateSSMAgent**
6. Scroll to **Targets** and select your instance.
7. Click **Run**.

Expected Output: Command should succeed with **"Success"** status. Agent is now updated.

Step 4: Remotely Run a Shell Script (Package Update)

1. In **Fleet Manager**, select your instance again.

2. Click **Node actions** > **Execute run command**.
3. Filter documents:
   - Document name prefix → Equals → AWS-RunShellScript
   - Select **AWS-RunShellScript**
4. Scroll to **Command Parameters**:
   - Paste this command: sudo yum update -y
5. Scroll to **Targets** and select your instance.
6. Click **Run**.

Expected Output:

- Status: **Success**
- Command Output: Package updates logged and completed successfully.

Step 5: Terminate Resources

1. Go to the **EC2 Console**.
2. Under **Instances**, select the instance MyEC2Tutorial.
3. Click **Instance State** > **Terminate instance**.
4. Confirm termination.

Best Practice: Always terminate unused resources to avoid unexpected billing.

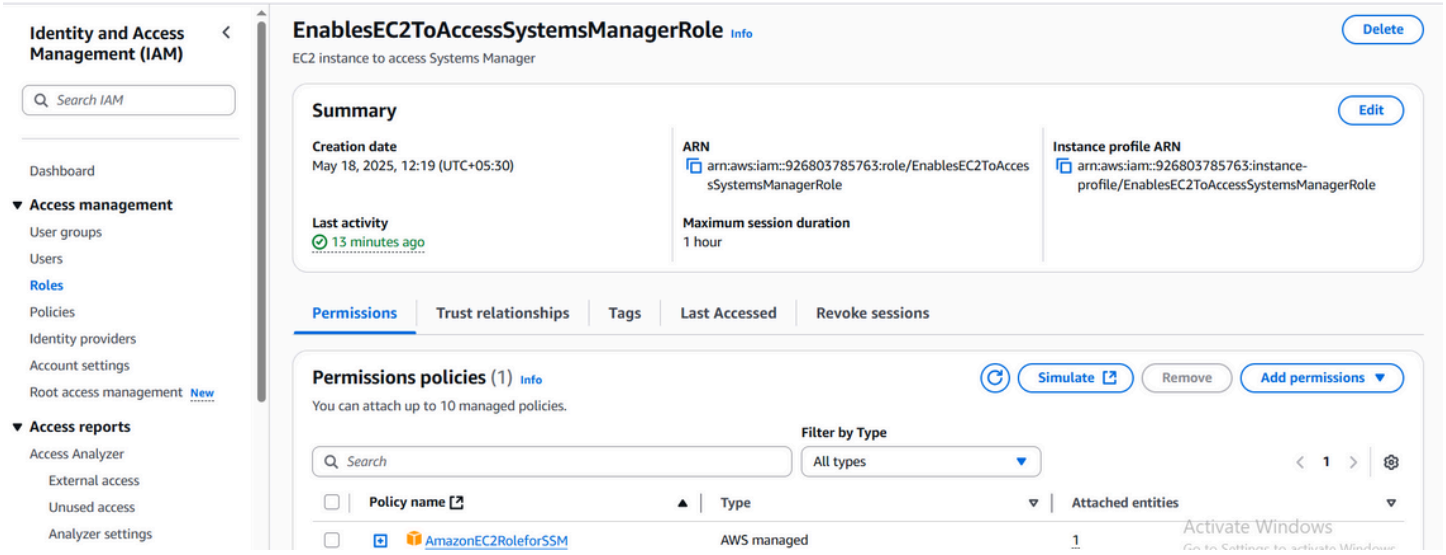

Fig 1: IAM Role

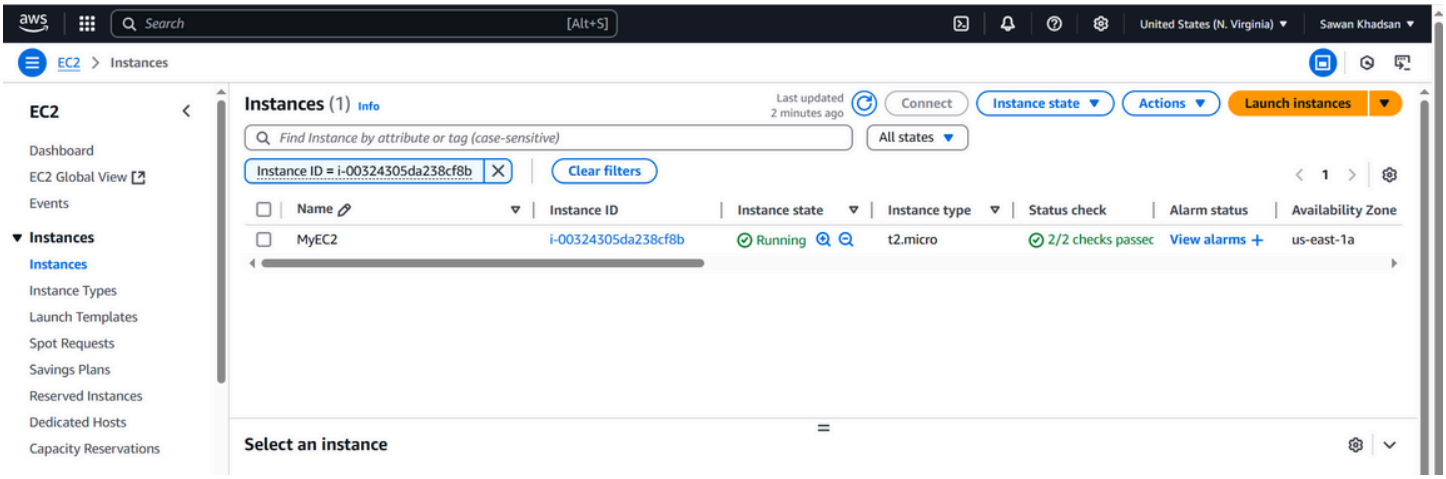

Fig 2: EC2 instance

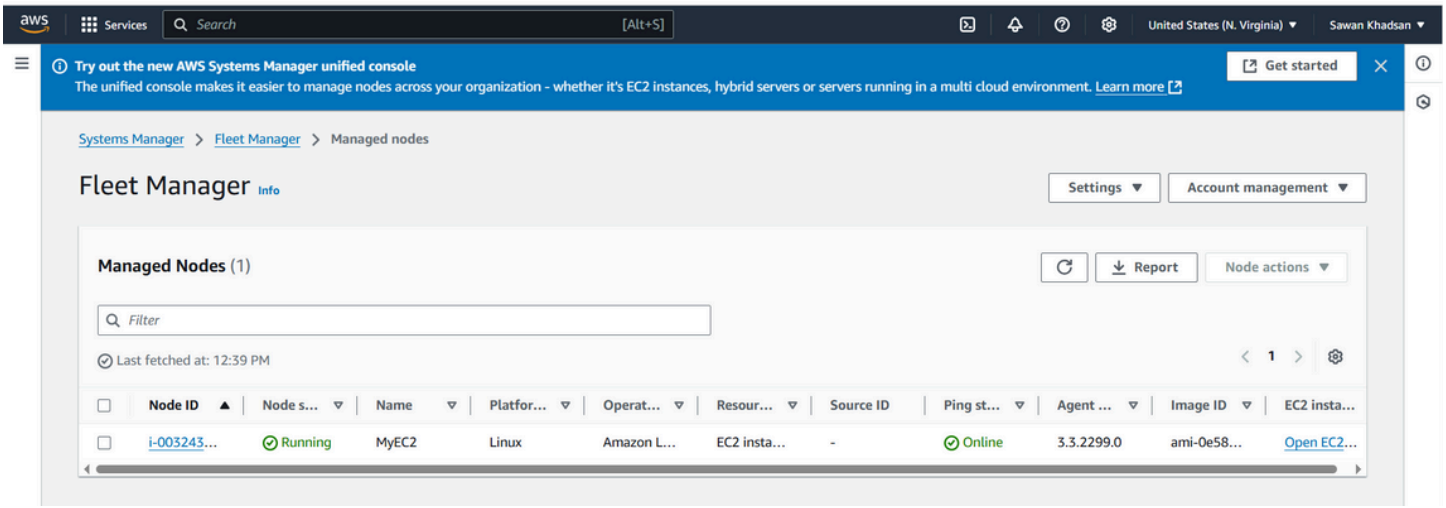

Fig3: system manager

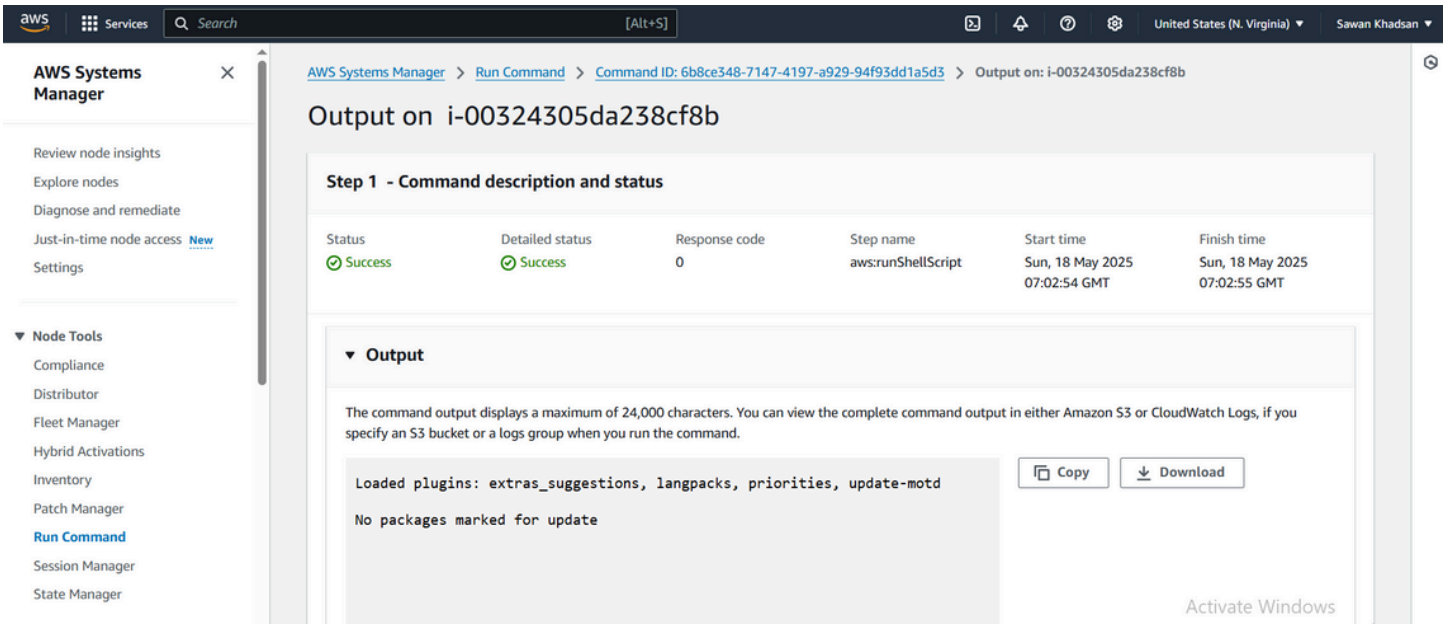

Fig4: Output

Reference :

🌐 How to Remotely Run Commands on an EC2 Instance with AWS Systems Manager | AWS