Runbook: Secure EC2 RDP Access via SSM Run Command (Windows Only)

Objective

To securely configure RDP access on a Windows EC2 instance using AWS Systems Manager (SSM) Run Command. This setup eliminates the need to open default RDP ports at launch and enables port customization via SSM, increasing security and flexibility. The system includes:

- Automatic installation of the SSM Agent via PowerShell in EC2 user data
- Using SSM Run Command to change the RDP port securely
- Creating firewall rules for custom RDP access
- Storing command output in S3 and optionally notifying via SNS or CloudWatch
- Removing default RDP access roles after verification

Architecture Overview

1. EC2 Windows instance launched with a role (EC2forSSM) allowing access to SSM.
2. User data installs the SSM Agent automatically at boot.
3. Custom TCP port (e.g., 8090) is opened via a security group.
4. SSM Run Command with AWS-RunPowerShellScript is used to change the RDP port and add a firewall rule.
5. Output is optionally stored in S3, with SNS or CloudWatch for alerting or logging.
6. RDP connection is tested using the new port and then default rules are removed.

1. EC2 Instance Setup

- AMI: Windows Server
- Instance Profile: EC2forSSM (attach or create with AmazonSSMManagedInstanceCore)
- Key Pair: Use existing or generate new
- User Data:

```
<powershell>
# Download and install the latest SSM Agent
$region = "us-east-1"
$ssmInstallerUrl = "https://s3.amazonaws.com/amazon-ssm-
$region/latest/windows_amd64/AmazonSSMAgentSetup.exe"
$installerPath = "$env:USERPROFILE\AmazonSSMAgentSetup.exe"

Invoke-WebRequest -Uri $ssmInstallerUrl -OutFile $installerPath
Start-Process -FilePath $installerPath -ArgumentList "/quiet" -Wait

# Start the service and set it to start automatically
Start-Service AmazonSSMAgent
Set-Service AmazonSSMAgent -StartupType Automatic
</powershell>
```

2. Security Group Rule

- Add Inbound Rule:

  - Protocol: TCP
  - Port Range: e.g., 8090
  - Source: Your IP or 0.0.0.0/0 (for testing only)

3. SSM Run Command to Change RDP Port

- Navigate to Systems Manager > Run Command
- Select AWS-RunPowerShellScript
- Choose instance manually
- Paste this in Command Parameters:

```
$newPort = 8090
$regPath = "HKLM:\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp"
Set-ItemProperty -Path $regPath -Name "PortNumber" -Value $newPort
New-NetFirewallRule -DisplayName "Allow RDP on port $newPort" -Direction Inbound -Protocol TCP -
LocalPort $newPort -Action Allow
Restart-Service -Name TermService -Force
```

- Output options:

  - Store output in an S3 bucket

  - (Optional) Configure SNS for notifications

  - (Optional) Enable CloudWatch Logs

4. Connect via RDP

- Use: EC2-Public-IP:8090

- Authenticate using the credentials from EC2 password reset or domain setup

- Ensure SG allows port 8090 and SSM has completed the command

5. Remove Old RDP Access

- Remove old SG rule for port 3389

- Remove any associated RDP role or firewall rules

Tested Environment

- Windows 10/11 client

- Windows EC2 instance with SSM agent

- SSM Run Command

- AWS CLI / Console

- Port forward via custom SG

Recommendation

Automate this workflow using an SSM Automation Document (Runbook) for repeatable, scalable secure EC2 setup across accounts or environments.