End-to-End Process: Automating Patching Using AWS Systems Manager Patch Manager

# 1. Introduction

This document outlines the complete, step-by-step procedure to automate patching of EC2 instances, on-premise virtual machines, and other supported nodes using AWS Systems Manager Patch Manager.

# 2. Prerequisites

Ensure the following requirements are met:

* - AWS Systems Manager (SSM) Agent must be installed on all managed nodes.
* - Appropriate IAM roles/policies must be attached to EC2 instances or configured for on-prem VMs.
* - Outbound internet access or VPC endpoints must be configured for communication with SSM.

- Nodes must appear as 'Managed Instances' in Systems Manager.

# 3. High-Level Steps

## 3.1 Create Patch Baseline

Define the patching rules based on OS type, severity, and classification. You can create separate baselines for OS and applications.

* - Go to Systems Manager → Patch Manager → Create Patch Baseline
* - Select OS (e.g., Amazon Linux 2, Windows Server 2012)
* - Set approval rules (e.g., apply patches after 2 days)
* - Optionally define patch exceptions

## 3.2 Create Patch Group

Tag EC2 instances using a common tag key-value pair (e.g., Patch Group=critical).

* - Go to EC2 → Select Instances → Add Tag (e.g., Key=Patch Group, Value=critical)
* - Go back to Patch Manager → Assign Patch Group to Baseline

## 3.3 Create Maintenance Window

Define a recurring schedule for patching operations.

* - Go to Systems Manager → Maintenance Windows → Create Maintenance Window
* - Configure CRON or rate-based schedule (e.g., every 7 days at 11 PM)
* - Define duration and stop initiation time

## 3.4 Configure Patch Task

Attach tasks to the maintenance window for automated patching.

* - Go to Patch Manager → Configure Patching
* - Choose targeting method: tag-based, patch group, or manual instance selection
* - Select patch operation: Scan, Install, or both
* - Choose reboot behavior: If needed, No reboot, or Scheduled reboot

# 4. Execution Options

* - Manual Execution: Trigger patching immediately via 'Patch Now'.
* - Scheduled Execution: Wait for Maintenance Window to initiate the patching.

# 5. Monitoring & Reporting

* - Use Systems Manager dashboards to view patch compliance.
* - Logs can optionally be stored in S3.

# 6. Best Practices

* - Use tag-based approach for auto-scaling environments.
* - Create separate baselines and maintenance windows for Dev, UAT, and Prod.
* - Apply critical patches first and delay lower severity patches for testing.