# SOP: AMI Creation and AWS Infrastructure Patching Process

## 1. Purpose

To outline the standard procedure for creating Amazon Machine Images (AMIs) and maintaining secure and compliant Linux Golden Images in the AWS environment.

## 2. Scope

This SOP applies to the creation, validation, and maintenance of AMIs to ensure secure infrastructure patching and compliance with organizational policies.

## 3. Prerequisites

* • Access to AWS Management Console with permissions for EC2, AMI, and KMS operations.
* • CIS-compliant base AMIs pulled from the AWS Marketplace.
* • AWS EC2 inventory file and AMI release schedule.
* • Ensure the environment is configured for RHEL8, AL2, and OEL7 as required.

## 4. Procedure

### 4.1 AMI Release Schedule

AMIs are released based on a pre-defined schedule (refer to internal release schedule documentation).

Every Monday, a Linux administrator initiates the process:

* • Validate that there are no vulnerabilities.
* • Ensure the common configuration is applied across all instances.

### 4.2 High-Level AMI Build Process

* • Take an AMI backup of the source EC2 instance before patching (retention: 60 days).
* • Apply necessary OS and security updates.
* • Perform a Qualys or other vulnerability scan to ensure compliance.
* • Run TVM (Threat and Vulnerability Management) scan to ensure no security issues post-patching.
* • Create an updated AMI for each instance as per the release schedule and name it following the naming convention.
* • Share or copy the updated AMI to the required AWS accounts and verify regional availability.

### 4.3 Initial AMI Image Source

Base AMIs are pulled from the AWS Marketplace. Supported environments:

* • RHEL8
* • AL2 (Amazon Linux 2)
* • OEL7 (Oracle Enterprise Linux 7)

### 4.4 Security and Configuration Requirements

Ensure the following security and operational tools are installed and active:

* • Qualys Agent (VM and EDR)
* • Splunk
* • Dynatrace
* • CloudWatch
* • ATOP
* • LSOF

User Configuration:

* • Remove default EC2-USER.
* • Add application-specific users as required.
* • Configure Qualys user only on DBA servers to allow database scans.

### 4.5 Volume Encryption

Encryption Policies:

* • Enable encryption for EBS volumes.
* • Use the custom KMS key (ec2-goldami-crossaccount-key, Key ID: mrk-36dc33fa58374c50bfba79c99302d8) for cross-account sharing.
* • Avoid using AWS default KMS keys for cross-account sharing.

### 4.6 Pre-Configured AMIs for Autoscaling Applications

* • CALSAWS-BASE-AL2
* • CALSAWS-SPRINGBOOT-AL2
* • CALSAWS-FORGEROCK-AL2-NON-PROD
* • CALSAWS-FORGEROCK-AL2-PRODUCTION
* • CALSAWS-DBA-OEL7
* • CALSAWS-AL2-SQUID
* • CALSAWS-BASE-RHEL8
* • CALSAWS-BASE-AL2-NTP
* • CALSAWS-BASE-ONLINE-RHEL8
* • CALSAWS-DBA-RHEL8

### 4.7 AMI Tagging Standards

Key: PatchGroup  
Value: PG-BASE-AMI

### 4.8 Post-Creation Actions

* • Go to Actions → Edit Permissions and add required AWS accounts for sharing.
* • Select AMI → Copy AMI and choose the Destination Region.
* • Verify encryption settings and click Copy AMI to replicate the image in other regions.

### 4.9 Backup and Retention Policies

• Weekly AMI backups are created before each patch release.

• Backups are retained for 60 days.

## 5. Maintenance Windows and Systems Manager

Schedule patching during designated maintenance windows using AWS Systems Manager.  
Perform on-demand vulnerability scans as necessary.

## 6. Summary of Key Actions

* • Ensure all AMIs follow the organization’s tagging and encryption standards.
* • Verify backup creation and retention policies before releasing patched AMIs.
* • Ensure all instances pass vulnerability scans and are configured correctly.