# **CloudPatchPro: A Cloud Formation Based Systems Manager Automation for Security Patching and More!**

## **v1.0.0**

## **February 8, 2023**

### Basic Info

At the time this document was written; SSM Agent is preinstalled on AMIs provided by AWS for the following operating systems (OSs):

Amazon Linux Base AMIs dated 2017.09 and later

Amazon Linux 2

Amazon Linux 2 ECS-Optimized Base AMIs

Amazon EKS-Optimized Amazon Linux AMIs

macOS 10.14.x (Mojave), 10.15.x (Catalina), and 11.x (Big Sur)

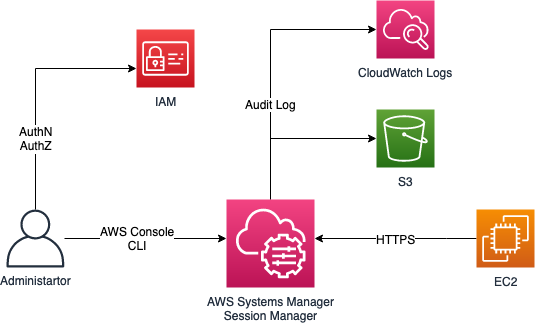
SUSE Linux Enterprise Server (SLES) 12 and 15

Ubuntu Server 16.04, 18.04, and 20.04

Windows Server 2008-2012 R2 AMIs published in November 2016 or later

Windows Server 2016, 2019, and 2022

You must manually install SSM Agent on Amazon EC2 instances created from other Linux AMIs.



[*https://catalog.workshops.aws/cfn101/en-US/basics/operations/session-manager#how-session-manager-works*](https://catalog.workshops.aws/cfn101/en-US/basics/operations/session-manager#how-session-manager-works)

### Before you Begin

You must make note of the AMI/Instance ID of the instance that you wish to use, this is because cloudformation does not have the capability to list the AMI IDs.

### Anatomy of the template

Parameters:

We have listed a few parameters that may or may not be needed for your instance, you should feel free to edit as needed for your environment.

Properties:

UserData

The easiest way to achieve the installation of the ssm agent is through the use of a helper script in the user data section of the template. You will have to modify this depending on your OS.

SSMIAMRole:

The AWS managed policy, AmazonSSMManagedInstanceCore, allows an instance to use AWS Systems Manager service core functionality. This will allow you to connect to the EC2 instance using Systems Manager Session Manager.

Frequently Assked Questions

What if I want my EC2 instance to be in a custom VPC or to not be publicly available upon initial setup?

The intent of this template is not to solve for all possible use cases of where/how these instances could be configured. Our suggestion is to create the base image you seek with a regular instance and get SSM installed using this template, then use that image to clone and put in the proper final resting place as you see fit.

What version of SSM is being installed?

We install the latest stable version as you are running the template.

What permissions are being granted to SSM using the role in this template?

We use AmazonSSMManagedInstanceCore and it provides minimum permissions which allow the instance to:

* Register as a managed instance
* Send heartbeat information
* Send and receive messages for Run Command and Session Manager
* Retrieve State Manager association details
* Read parameters in Parameter Store

If this is not acceptable we suggest using a custom role and updating the template to reflect this.