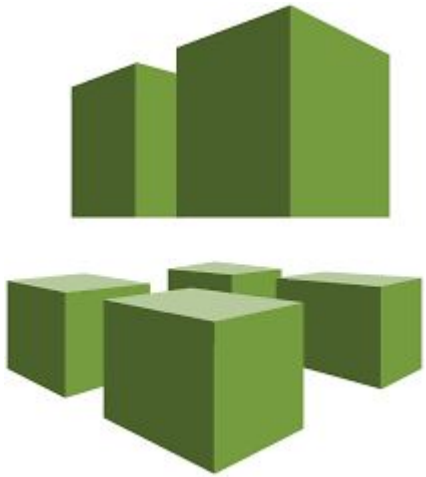
AWS System Manager



AWS Systems Manager is an AWS service that you can use to view and control your infrastructure on AWS. Using the Systems Manager console, you can view operational data from multiple AWS services and automate operational tasks across your AWS resources. Systems Manager helps you maintain security and compliance by scanning your *managed instances* and reporting on (or taking corrective action on) any policy violations it detects.

Managed Instances

A managed instance is a machine that has been configured for use with Systems Manager. Systems Manager also helps you configure and maintain your managed instances. Supported machine types include Amazon EC2 instances, on-premises servers, and virtual machines (VMs), including VMs in other cloud environments. Supported operating system types include Windows Server, multiple distributions of Linux, and Raspbian.

SSM agent

AWS Systems Manager Agent (SSM Agent) is Amazon software that can be installed and configured on an Amazon EC2 instance, an on-premises server, or a virtual machine (VM). SSM Agent makes it possible for Systems Manager to update, manage, and configure these resources. The agent processes requests from the Systems Manager service in the AWS Cloud, and then runs them as specified in the request. SSM Agent then sends status and execution information back to the Systems Manager service by using the Amazon Message Delivery Service
SSM Agent must be installed on each instance you want to use with Systems Manager. SSM Agent is preinstalled, by default, on instances created from the following Amazon Machine Images (AMIs):

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

Windows Server 2016 and 2019

Amazon Linux

Amazon Linux 2

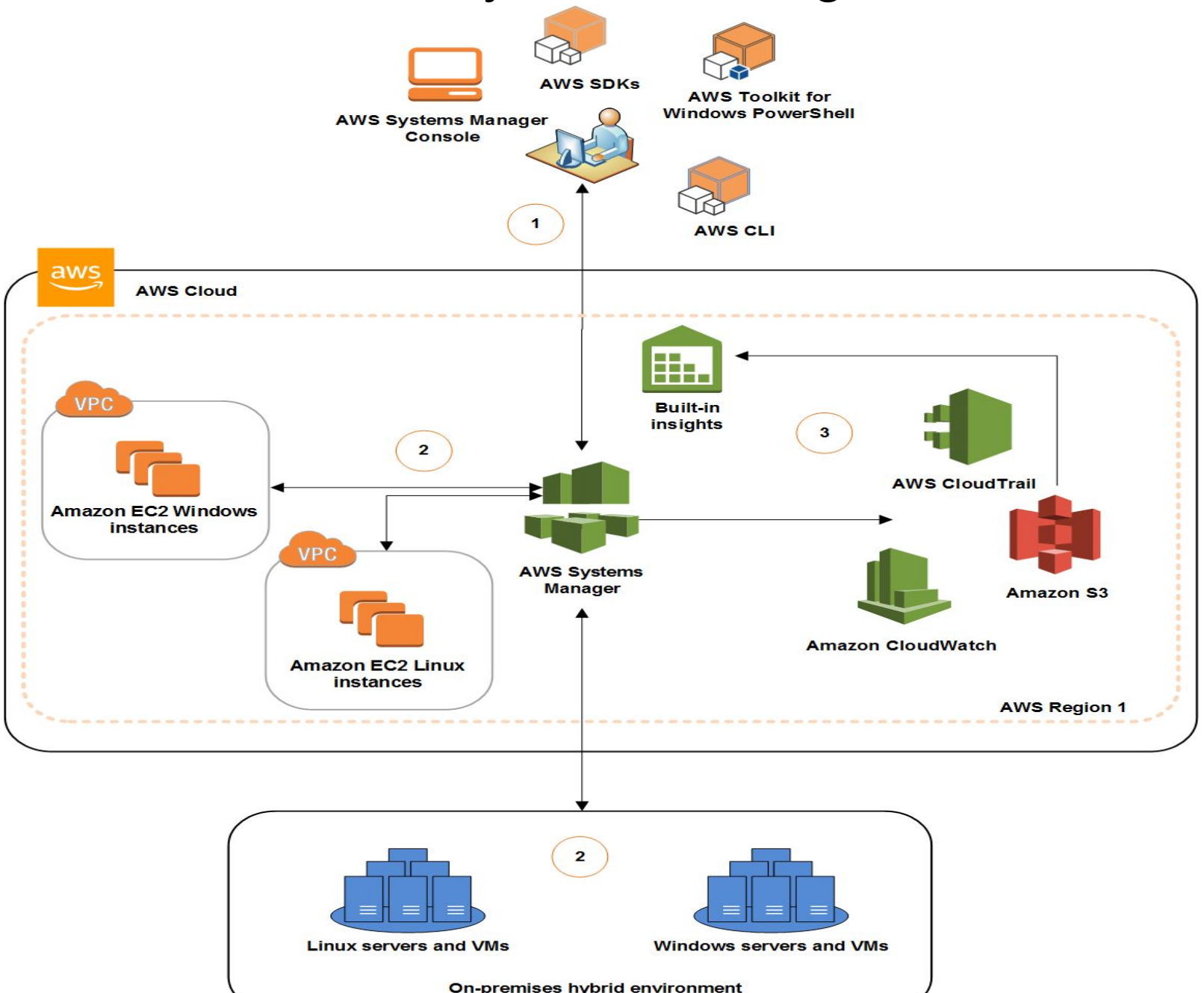
Ubuntu Server 16.04

Ubuntu Server 18.04

Amazon ECS-Optimized

On other AMIs, and on on-premises servers and virtual machines for your hybrid environment, you must install the agent manually
For ex Installing and Configuring SSM Agent on Amazon EC2 Linux Instances.

How does systems manager work?



Run command

AWS Systems Manager Run Command lets you remotely and securely manage the configuration of your managed instances. A managed instance is any Amazon EC2 instance or on-premises machine in your hybrid environment that has been configured for Systems Manager. Run Command enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. You can use Run Command from the AWS console, the AWS Command Line Interface, AWS Tools for Windows PowerShell, or the AWS SDKs. Run Command is offered at no additional cost.
Prerequisite to using a run command is making sure the instance is managed by SSM
Run command can be used to enforce standards ,running mandatory bootstrap action and it can be operated on hundreds of instances at one go.
Output of run command can be saved in an S3 bucket , the logs can be sent to cloudwatch logs also we can send notifications to SNS to know the status of the command

Session manager

Session Manager is a fully managed AWS Systems Manager capability that lets you manage your Amazon EC2 instances, on-premises instances, and virtual machines (VMs) through an interactive one-click browser-based shell or through the AWS CLI. Session Manager provides secure and auditable instance management without the need to open inbound ports, maintain bastion hosts, or manage SSH keys. Session Manager also makes it easy to comply with corporate policies that require controlled access to instances, strict security practices, and fully auditable logs with instance access details, while still providing end users with simple one-click cross-platform access to your managed instances.
One can send the output of the session to the S3 bucket as well as Cloudwatch logs

SSM patch manager

AWS Systems Manager Patch Manager automates the process of patching managed instances with both security related and other types of updates. You can use Patch Manager to apply patches for both operating systems and applications. (On Windows Server, application support is limited to updates for Microsoft applications.)

patch baselines- rules for auto-approving patches within days of their release,

as well as a list of approved and rejected patches

Patch group – Patch group represents a group of instances using EC2 tags which can be used for patching .

These can be used with Key “Patch Group”

Approval rules- Approval rules define which patches are approved and can be installed using the patch manager

Any questions ?

ssm.txt