**Implement patch management solution using Systems Manager**

**AWS Systems Manager**

AWS Systems Manager is an AWS service that you can use to view and control your infrastructure on AWS. you can view operational data from multiple AWS services and automate operational tasks across your AWS resources.

**prerequisites for using Systems Manager**

1. Create an AWS account and configure the required IAM roles.
2. Verify that Systems Manager is supported in the AWS Regions where you want to use the service.
3. Verify that your instances run a supported operating system.
4. For EC2 instances, create an IAM instance profile and attach it to your machines.
5. For on-premises servers and VMs, create an IAM service role for a hybrid environment.
6. Verify that you are allowing HTTPS (port 443) outbound traffic to the Systems Manager endpoints.
7. (Recommended) Create a VPC endpoint in Amazon Virtual Private Cloud to use with Systems Manager.
8. On on-premises servers, VMs, and EC2 instances created from AMIs that are not supplied by AWS, install a Transport Layer Security (TLS) certificate.
9. For on-premises servers and VMs, register the machines with Systems Manager through the managed instance activation process.
10. Install or verify installation of SSM Agent on each of your managed instances.

**policies for a Systems Manager instance profile**

The following policy to grant permission for Systems Manager to interact with your instances.

**Policy: AmazonSSMManagedInstanceCore**

Required permissions.

This AWS managed policy enables an instance to use Systems Manager service core functionality.

**Managed Instance**

Is a machine that has been configured for use with Systems Manager.

A group of EC2 instances

A group of on-premises servers in your own facility

A Systems Manager patch baseline that specifies which patches to apply to your managed instances.

A Systems Manager maintenance window that specifies the schedule for the patching operation

**Patch Manager**

Automates the process of patching managed instances with both security related and other types of updates.

You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type.

Employs the intrinsic capabilities of AWS Systems Manager

Run command

Documents

Maintenance windows

to enable remediation of OS vulnerabilities in a safe and scalable fashion.

**supported versions**

* Windows Server
* Amazon Linux
* Amazon Linux 2
* CentOS, Debian
* Oracle Linux,
* Red Hat Enterprise Linux (RHEL)
* SUSE Linux Enterprise Server (SLES)
* Ubuntu Server

**Patch Manger workflow Diagram**

![Diagram

Description automatically generated]()

**Patch Group**

Provide an optional means of organizing instances into groups for patching , patch group can help you avoid deploying patches to the wrong set of instances and ensure adequate testing.

You can register patch groups with a patch baseline. By registering the patch group with patch baseline, you ensure that correct patches are installed during the patching execution.

Following link will guide you to create patch group

https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-group-tagging.html

**Patch Approvals**

Automate the approval of patches using patch baseline

**Patch reporting**

Compliance reporting for audit and remediation

**Security Patch Selection**

• The primary focus of Patch Manager is on installing operating

system security-related updates on instances.

• By default, Patch Manager doesn't install all available patches, but rather a smaller set of patches focused on security.

• Patch Manager uses a different process to evaluate which patches should be present on Windows managed instances versus Linux managed instances.

**Patch Baseline**

Defines which patches are approved for installation on your instances. Specify approved or rejected patches one by one or setup auto-approval rules.

A patch is installed on an instance only if it applies to software on the instance, even if the patch has otherwise been approved for the instance.

**Default Baselines**

Systems Manager provides pre-defined patch baselines for each of the operating systems supported by Patch Manager. Use as they are or create your own patch baselines.

**Maintenance Windows**

Reduce the impact on server availability by specifying a time to perform the patching process that doesn't interrupt business operations.

Each Maintenance Window has a schedule, a duration, a set of registered targets, and a set of registered tasks.

**Run Command**

Enables you to automate common administrative tasks and perform ad hoc configuration changes at scale. Leveraged by Patch Manager for patching operations.

**AWS-RunPatchBaseline**

Systems Manager command document that supports executing patch operations on both Windows and Linux managed instances. The document will perform the appropriate actions for each platform.

**Compliance Status**

After you use Patch Manager to install patches on your instances, compliance status information is immediately available to you in the console or in the responses to a set of AWS CLI commands or corresponding Systems Manager API actions.

Installed : Either the patch was already installed, or Patch Manager installed it when the document was run on the instance.

Installed Other : The patch is not in the baseline, but it is installed on the instance. An individual might have installed it manually.

Missing : The patch is approved in the baseline, but it's not installed on the instance.

Not\_Applicable : The patch is approved in the baseline, but the service or feature that uses the patch is not installed on the instance.

Failed: The patch is approved in the baseline, but it could not be installed.

**patch baselines**

which include rules for auto-approving patches within days of their release, as well as a list of approved and rejected patches.

You can install patches on a regular basis by scheduling patching to run as a Systems Manager maintenance window task.

You can also install patches individually or to large groups of instances by using Amazon EC2 tags. (Tags are keys that help identify and sort your resources within your organization.)

You can add tags to your patch baselines themselves when you create or update them.

**patching configuration**

The configuration specifies the instances for patching

Which patch baseline is to be applied

Schedule for patching

Maintenance window that the configuration is to be associated with.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/create-patching-configuration.html>

AWS Systems Manager Automation

- Systems Manager Automation simplifies common maintenance and deployment tasks of EC2 instances and other AWS resources.

5 - Automation enables you to do the following:

6 Build Automation workflows to configure and manage instances and AWS resources.

7 8 Create custom workflows or use pre-defined workflows maintained by AWS.

9 10 Receive notifications about Automation tasks and workflows by using Amazon CloudWatch Events.

11 12 Monitor Automation progress and execution details by using the Amazon EC2 or the AWS Systems Manager console.

13 14 Automation use cases

15 16 17 - Perform common IT tasks 18 - Safely perform disruptive tasks in bulk

19 - Update AMI 20