SSM - Node Management – Patch Manager

## Service Overview

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.) You can use Patch Manager to install Service Packs on Windows instances and perform minor version upgrades on Linux instances. You can patch fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Amazon Linux, Amazon Linux 2, CentOS, Debian Server, macOS, Oracle Linux, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), Ubuntu Server, and Windows Server. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

## Use cases / Considerations

Patch Manager uses *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.

Patch Manager provides options to scan your instances and report compliance on a schedule, install available patches on a schedule, and patch or scan instances on demand whenever you need to. You can also generate patch compliance reports that are sent to an Amazon Simple Storage Service (Amazon S3) bucket of your choice. You can generate one-time reports, or generate reports on a regular schedule. For a single instance, reports include details of all patches for the instance. For a report on all instances, only a summary of how many patches are missing is provided.

## Governance

Patch Manager integrates with AWS Identity and Access Management (IAM), AWS CloudTrail, and Amazon EventBridge to provide a secure patching experience that includes event notifications and the ability to audit usage.

[Logging AWS Systems Manager API calls with AWS CloudTrail](https://docs.aws.amazon.com/systems-manager/latest/userguide/monitoring-cloudtrail-logs.html).

[Monitoring Systems Manager events with Amazon EventBridge](https://docs.aws.amazon.com/systems-manager/latest/userguide/monitoring-eventbridge-events.html).

## Cautions

[Patch Manager prerequisites](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-prerequisites.html)

## Pricing considerations

[Patch Manager pricing](https://aws.amazon.com/systems-manager/pricing/#Patch_Manager)

## More details

* [Patch Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-patch.html)
* [Patch Manager prerequisites](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-prerequisites.html)
* [How Patch Manager operations work](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-how-it-works.html)
* [About patching operations](https://docs.aws.amazon.com/systems-manager/latest/userguide/about-patching-operations.html)
* [About patch baselines](https://docs.aws.amazon.com/systems-manager/latest/userguide/about-patch-baselines.html)
* [Remediating out-of-compliance instances (Patch Manager)](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-compliance-remediation.html)
* [Use Kernel Live Patching on Amazon Linux 2 instances](https://docs.aws.amazon.com/systems-manager/latest/userguide/kernel-live-patching.html)
* [Working with Patch Manager (console)](https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-working.html)
* [Working with Patch Manager (AWS CLI)](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-cli-commands.html)
* [AWS Systems Manager Patch Manager walkthroughs](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-walkthroughs.html)
* [Troubleshooting Patch Manager](https://docs.aws.amazon.com/systems-manager/latest/userguide/patch-manager-troubleshooting.html)
* [Patching for your Amazon EC2 Instances (video)](https://www.youtube.com/watch?v=ABtwRb9BFY4)
* [AWS Systems Manager - Automate Patching for Amazon EC2 Instances (video)](https://www.youtube.com/watch?v=Dm4id0FVhtc)