**Patch Management**

**Contents**

[Scope 2](#_Toc115190395)

[Problem Statement 2](#_Toc115190396)

[Introduction 3](#_Toc115190397)

[AWS System Manager Patch Manager 3](#_Toc115190398)

[About Patch Baselines 3](#_Toc115190399)

[About Patch Groups 4](#_Toc115190400)

[Viewing Available Patches 5](#_Toc115190401)

[Creating Patching Configuration](#_Toc115190401) 6

[Implementation 6](#_Toc115190402)

[Patch Now 6](#_Toc115190399)

[Patch Baselines 12](#_Toc115190399)

[Available Patches 18](#_Toc115190399)

[Patch Configuration 19](#_Toc115190399)

[Patch Groups 22](#_Toc115190399)

[Advantages](#_Toc115190413) 28

[Limitations 28](#_Toc115190413)

**Patch Management**

**Document Name:Patch Management**

**Owner: Hema Paul**

**Scope**

This section provides technical details that explain how Patch Manager, a capability of AWS Systems Manager, determines which patches to install and how it installs them on each supported operating system. Patch Manager automates the process of patching managed nodes with both security related and other types of updates. We can use Patch Manager to apply patches for both operating systems and applications.

**Problem Statement**

Patch management fixes vulnerabilities on software and applications that are susceptible to cyber-attacks, helping the organization reduce its security risk. Patch management ensures your software and applications are kept up-to-date and run smoothly, supporting system uptime.

**Introduction**

# AWS Systems Manager Patch Manager

Patch Manager, a capability of AWS Systems Manager, automates the process of patching managed nodes 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 applications released by Microsoft.) You can use Patch Manager to install Service Packs on Windows nodes and perform minor version upgrades on Linux nodes. You can patch fleets of Amazon Elastic Compute Cloud (Amazon EC2) instances, edge devices, 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, Raspberry Pi OS (formerly Raspbian), 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.

Patch Manager uses **patch baselines**, which include rules for auto-approving patches within days of their release, in addition to 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 managed nodes by using 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 managed nodes and report compliance on a schedule, install available patches on a schedule, and patch or scan targets 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 managed node, reports include details of all patches for the node. For a report on all managed nodes, only a summary of how many patches are missing is provided.

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.

# About patch baselines

Patch Manager, a capability of AWS Systems Manager, provides predefined patch baselines for each of the operating systems supported by Patch Manager. You can use these baselines as they are currently configured (you can't customize them) or you can create your own custom patch baselines. Custom patch baselines allows you greater control over which patches are approved or rejected for your environment. Also, the predefined baselines assign a compliance level of *Unspecified* to all patches installed using those baselines. For compliance values to be assigned, you can create a copy of a predefined baseline and specify the compliance values you want to assign to patches.

**Types of Patch baselines**

1. Predefined Patch baselines: provides predefined patch baselines for each of the operating systems supported by Patch Manager.
2. Custom Patch baselines: If you create your own patch baseline, you can choose which patches to auto-approve by using the following categories.

* Operating system: Windows, Amazon Linux, Ubuntu Server, and so on.
* Product name (for operating systems): For example, RHEL 6.5, Amazon Linux 2014.09, Windows Server 2012, Windows Server 2012 R2, and so on.
* Product name (for applications released by Microsoft on Windows Server only): For example, Word 2016, BizTalk Server, and so on.
* Classification: For example, critical updates, security updates, and so on.
* Severity: For example, critical, important, and so on.

https://docs.aws.amazon.com/systems-manager/latest/userguide/sysman-patch-baselines.html#patch-manager-baselines-custom

**About Patch Groups**

You can use a patch group to associate managed nodes with a specific patch baseline in Patch Manager, a capability of AWS Systems Manager. Patch groups help ensure that you're deploying the appropriate patches, based on the associated patch baseline rules, to the correct set of nodes. Patch groups can also help you avoid deploying patches before they have been adequately tested. For example, you can create patch groups for different environments (such as Development, Test, and Production) and register each patch group to an appropriate patch baseline.

When you run AWS-RunPatchBaseline, you can target managed nodes using their ID or tags. SSM Agent and Patch Manager then evaluate which patch baseline to use based on the patch group value that you added to the managed node.

You create a patch group by using Amazon Elastic Compute Cloud (Amazon EC2) tags. Unlike other tagging scenarios across Systems Manager, a patch group must be defined with the either the tag key Patch Group or PatchGroup. The key is case-sensitive. You can specify any value to help you identify and target the resources in that group, for example "web servers" or "US-EAST-PROD", but the key must be Patch Group or PatchGroup.

After you create a patch group and tag managed nodes, you can register the patch group with a patch baseline. Registering the patch group with a patch baseline ensures that the nodes within the patch group use the rules defined in the associated patch baseline.

**Viewing available patches**

With Patch Manager, a capability of AWS Systems Manager, you can view all available patches for a specified operating system and, optionally, a specific operating system version.

<https://docs.aws.amazon.com/systems-manager/latest/userguide/viewing-available-patches.html>

# Creating patching configuration

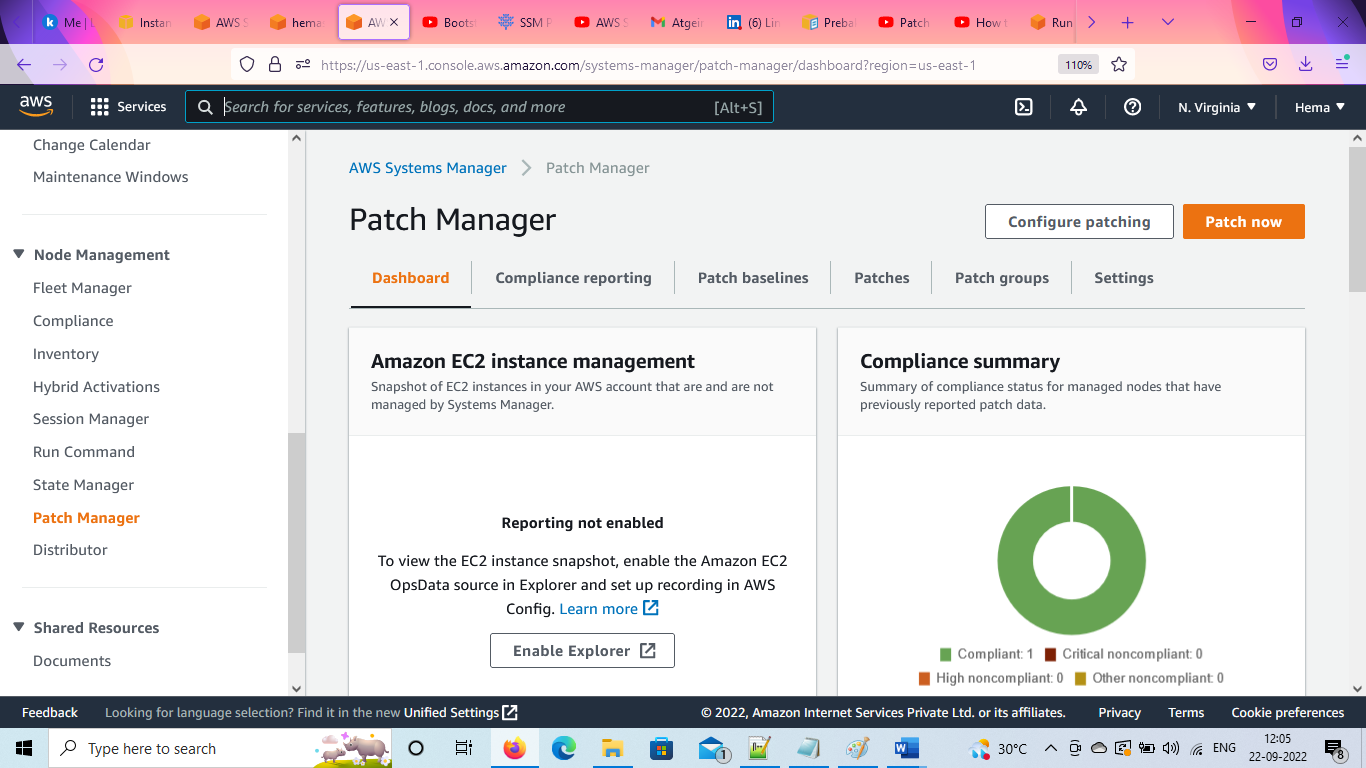
A patching configuration defines a unique patching operation. The configuration specifies the managed nodes for patching, which patch baseline is to be applied, the schedule for patching, and typically, the maintenance window that the configuration is to be associated with.

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

**Implementation**

To get started with Patch Manager, open the [**Systems Manager console**](https://console.aws.amazon.com/systems-manager/patch-manager)

In the navigation pane, choose **Patch Manager**.

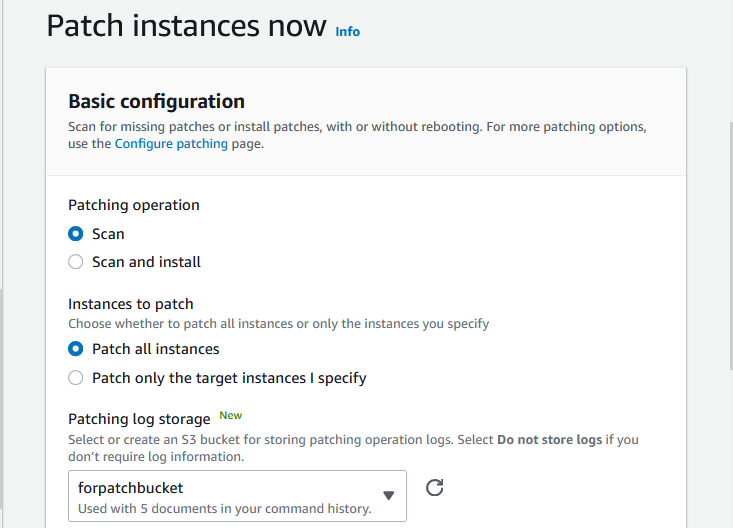


**Click on patch now**

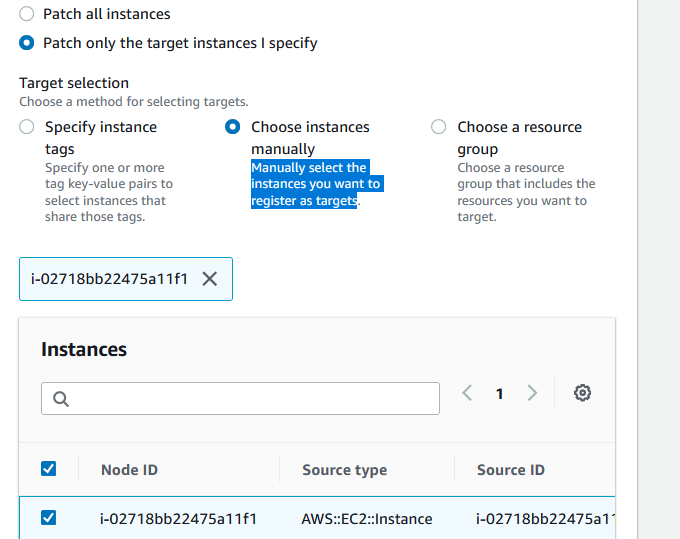
The **Patch now** option lets you run an on-demand patching operation from the console. This bypasses the requirement of creating a schedule to update the compliance status of your instances or install patches on non-compliant instances.

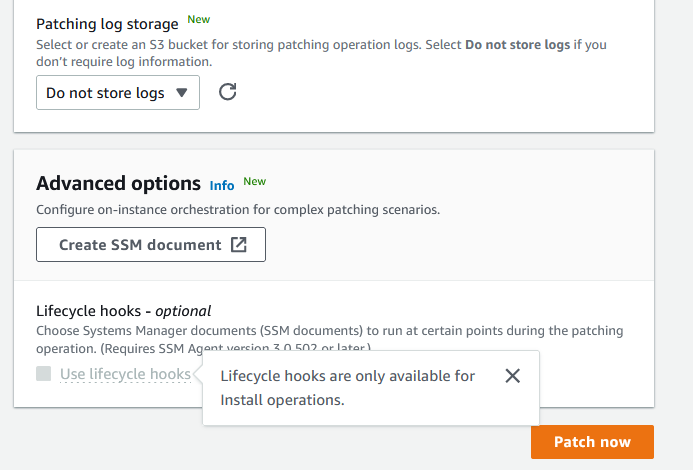
As part of the **Patch now** workflow, you can run Systems Manager documents (SSM documents) as lifecycle hooks at specific points during the patching operation, such as before patch installation or after instance reboot.

Patch now uses AWS recommended best practices for concurrency and error threshold options.

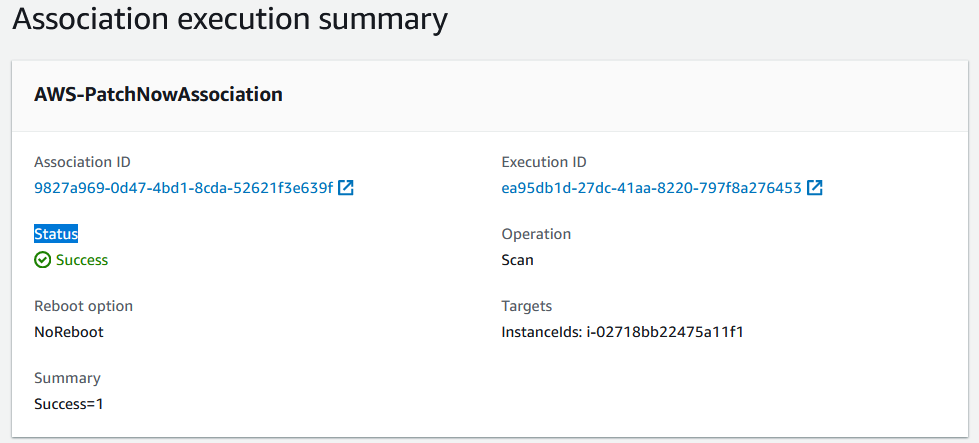


**Choose whether to patch all instances or only the instances you specify**



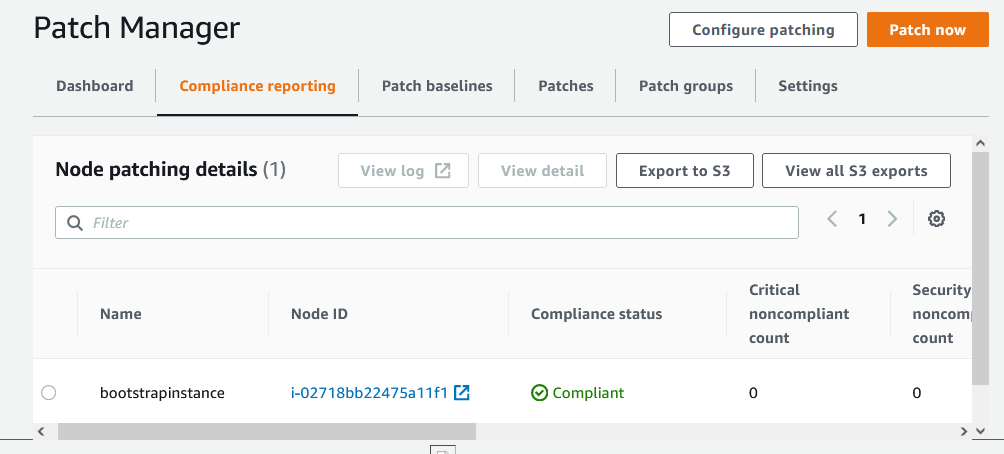


Execution summary shows the status as “Success” , when association is done

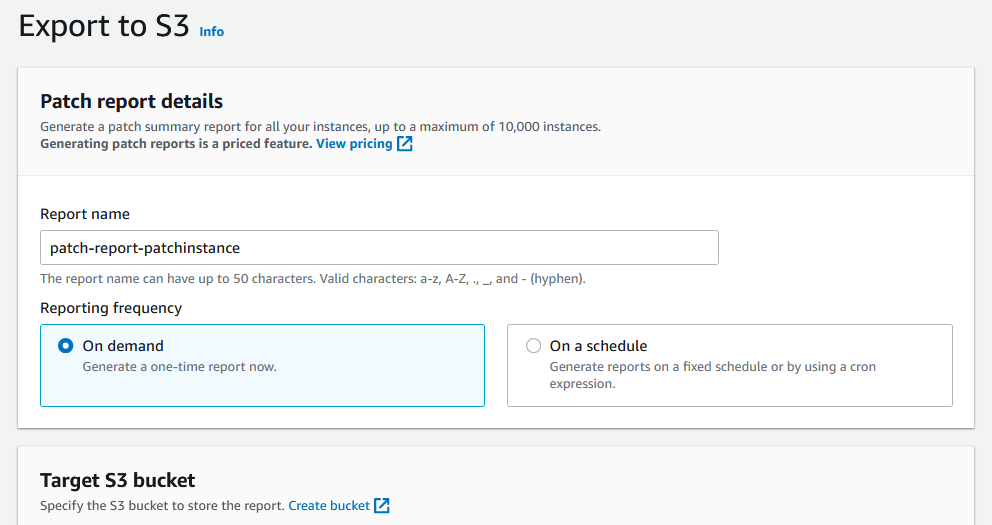


**Now go to Patch Manager**

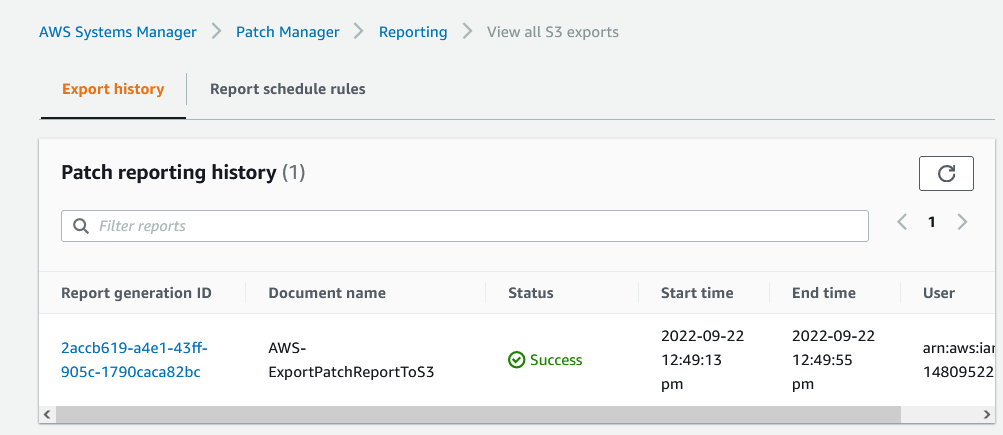
Click on Compliance reporting tab to see whether the patch is complaint or not.



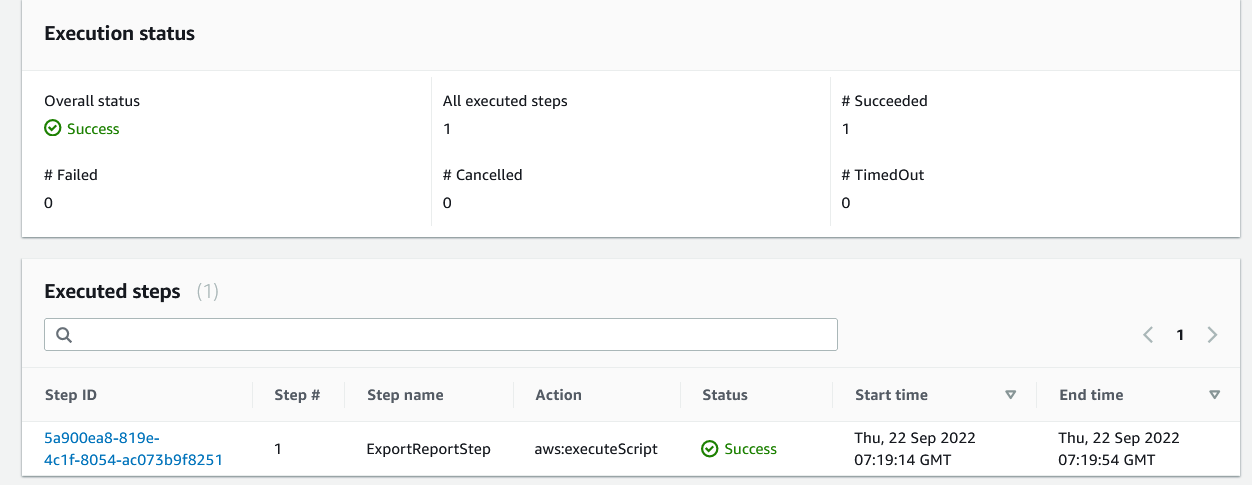
In order to get the log in S3, click on export to S3.



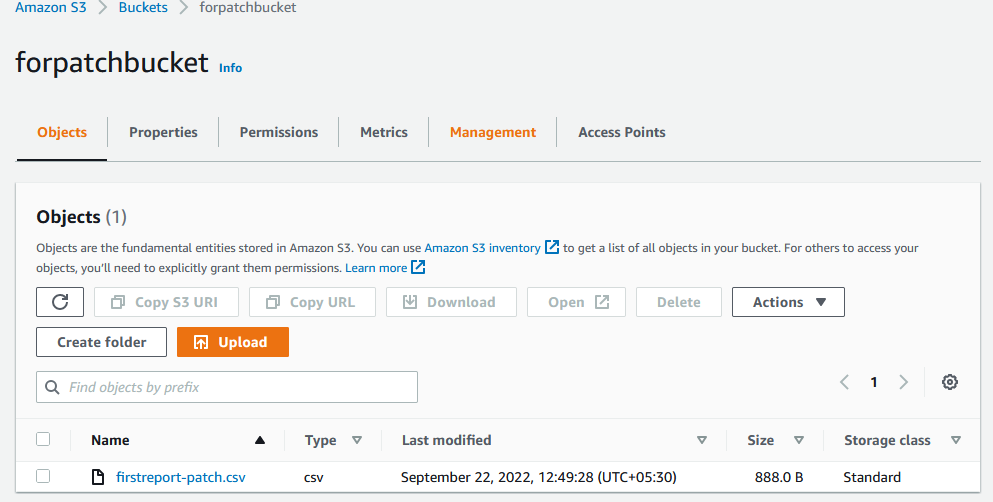
**Note : Generating patch reports is a priced feature.**



The report can be viewed on clicking the Report ID

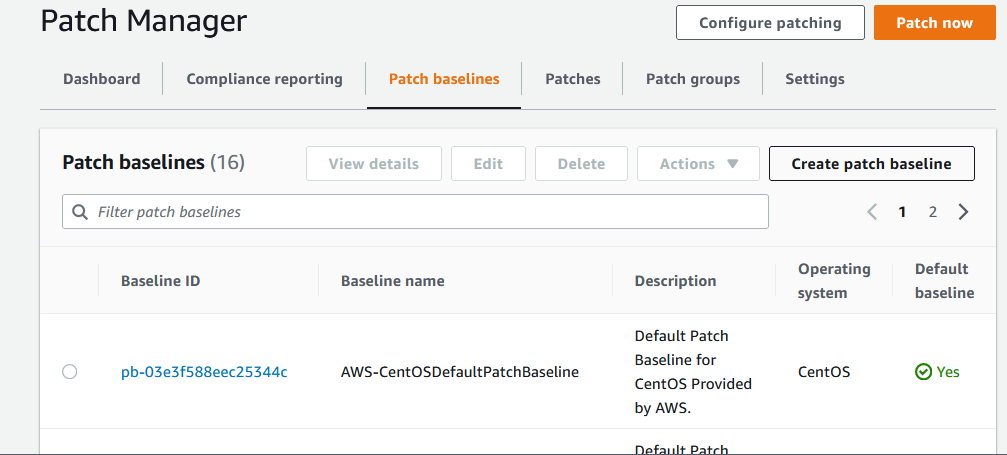


Since the log is exported to S3, it is present in the chosen bucket



# Patch baselines

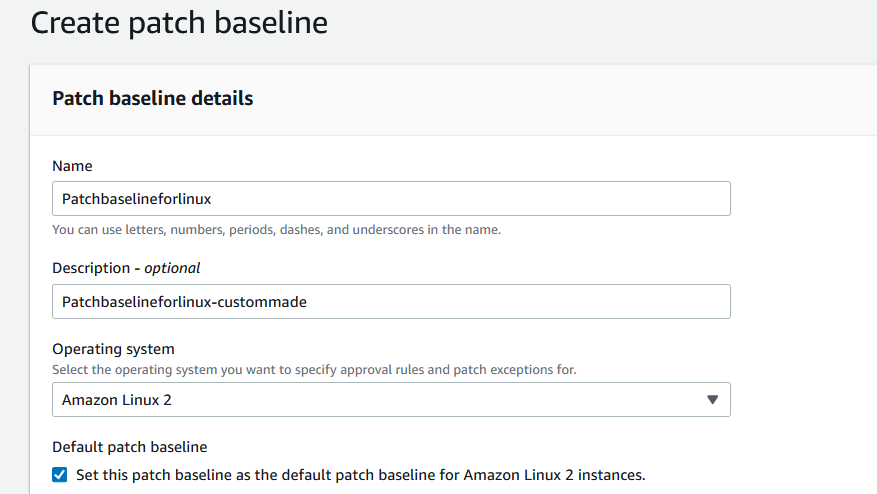
1. Predefined patch baselines : are provided with Patch Manager



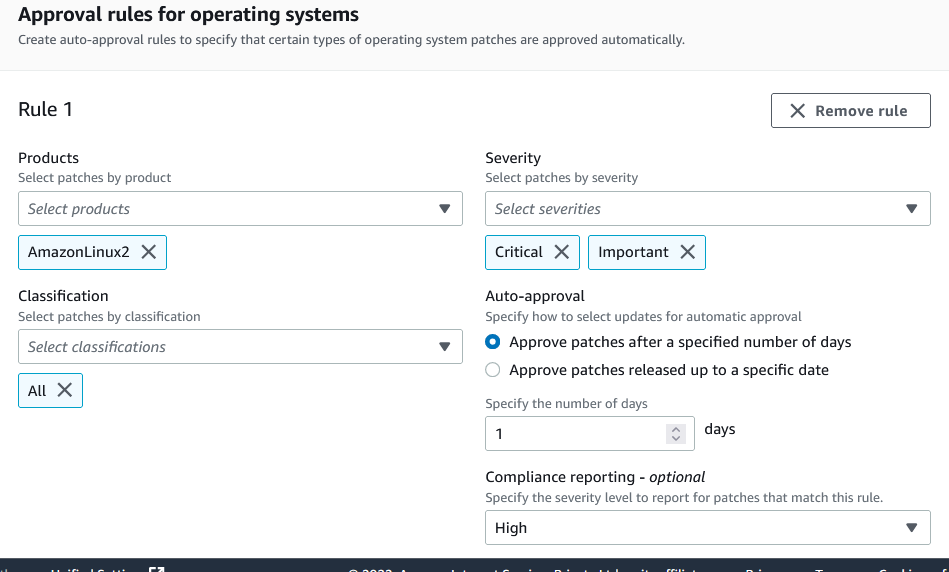
1. Custom patch baselines : allows you greater control over which patches are approved or rejected for your environment.

# Creating a custom patch baseline (Linux)

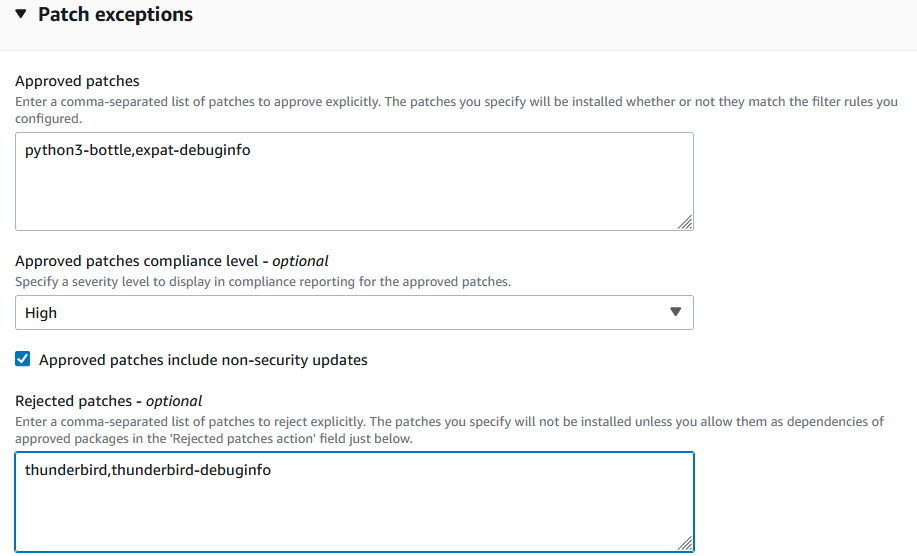
1. Open the AWS Systems Manager console
2. Choose **Create patch baseline**.
3. For **Name**, enter a name for your new patch baseline, for example, *Patchbaselineforlinux*
4. (Optional) For **Description**, enter a description for this patch baseline.
5. For **Operating system**, choose an operating system.



1. If you want to begin using this patch baseline as the default for the selected operating system as soon as you create it, check the box next to **Set this patch baseline as the default patch baseline for operating system name instances**.
2. In the **Approval rules for operating-systems** section, use the fields to create one or more auto-approval rules.
   1. **Product**: The version of the operating systems the approval rule applies to. The default selection is *All*
   2. **Classification**: The type of patches the approval rule applies to, such as Security or Enhancement. The default selection is *All*.
   3. **Severity**: The severity value of patches the rule is to apply to, such as Critical. The default selection is *All*.
   4. **Auto-approval**: The method for selecting patches for automatic approval.
   5. (Optional) **Compliance reporting**: The severity level you want to assign to patches approved by the baseline, such as *High*.
   6. **Include non-security updates**: Select the check box to install nonsecurity Linux operating system patches made available in the source repository, in addition to the security-related patches.



1. If you want to explicitly approve any patches in addition to those meeting your approval rules, do the following in the **Patch exceptions** section:
   1. For **Approved patches**, enter a comma-separated list of the patches you want to approve.
   2. (Optional) For **Approved patches compliance level**, assign a compliance level to the patches in the list.
   3. If any approved patches you specify aren't related to security, select the **Approved patches include non-security updates** check box for these patches to be installed on your Linux operating system as well.
2. If you want to explicitly reject any patches that otherwise meet your approval rules, do the following in the **Patch exceptions** section:
   1. For **Rejected patches**, enter a comma-separated list of the patches you want to reject.
   2. For **Rejected patches action**, select the action for Patch Manager to take on patches included in the **Rejected patches** list.



1. (Optional) If you want to specify alternative patch repositories for different versions of an operating system, such as AmazonLinux2016.03 and AmazonLinux2017.09, do the following for each product in the **Patch sources** section:
   1. n **Name**, enter a name to help you identify the source configuration.
   2. In **Product**, select the version of the operating systems the patch source repository is for, such as RedhatEnterpriseLinux7.4.
   3. In **Configuration**, enter the value of the yum repository configuration to use in the following format:

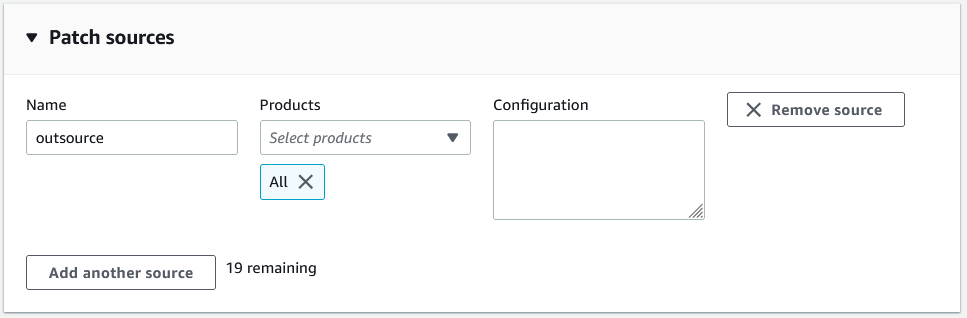
*[main]*

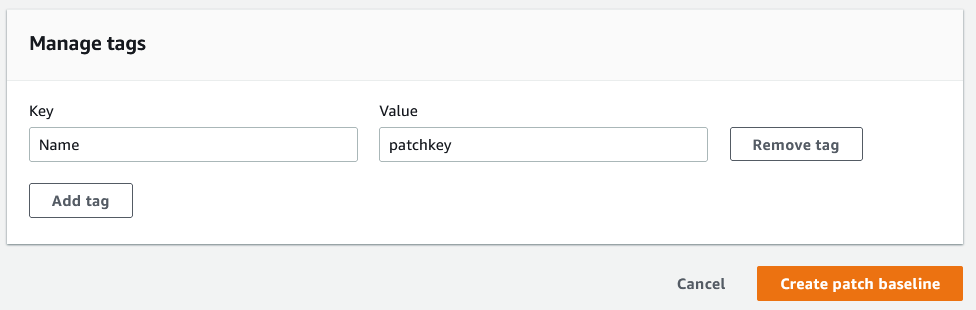
*name=MyCustomRepository*

*baseurl=https://my-custom-repository*

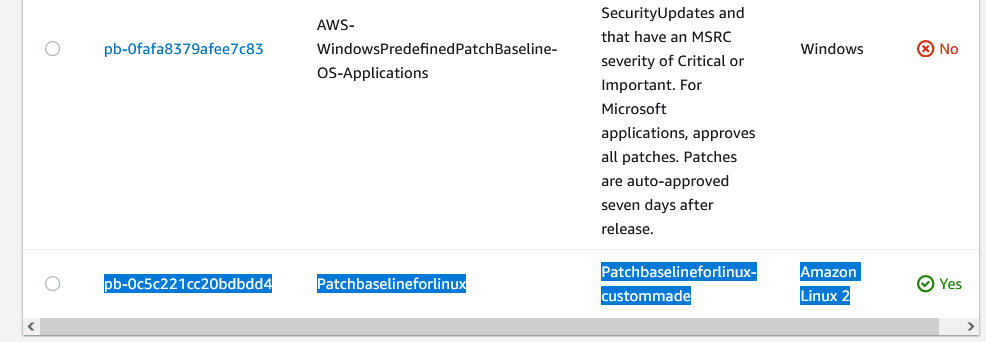
*enabled=1*

1. (Optional) For **Manage tags**, apply one or more tag key name/value pairs to the patch baseline. Tags are optional metadata that you assign to a resource.
2. Choose **Create patch baseline**.

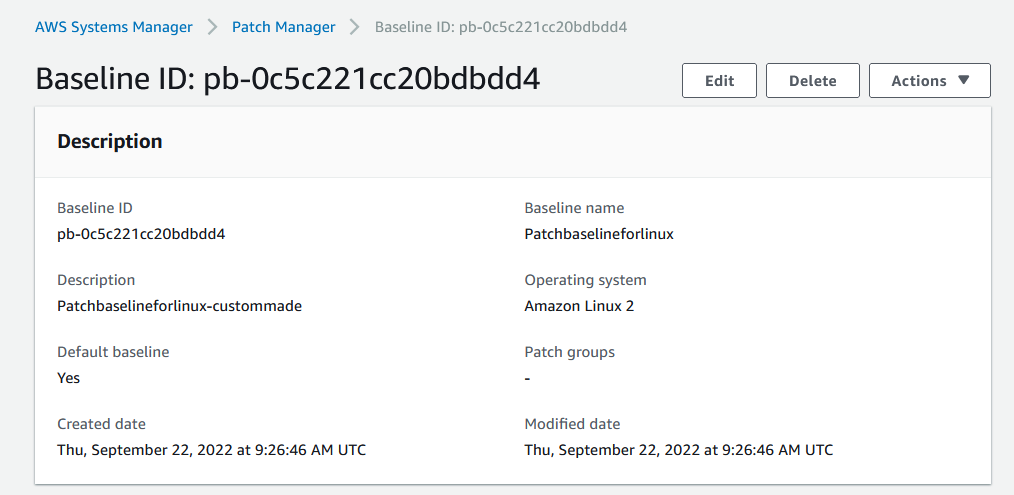


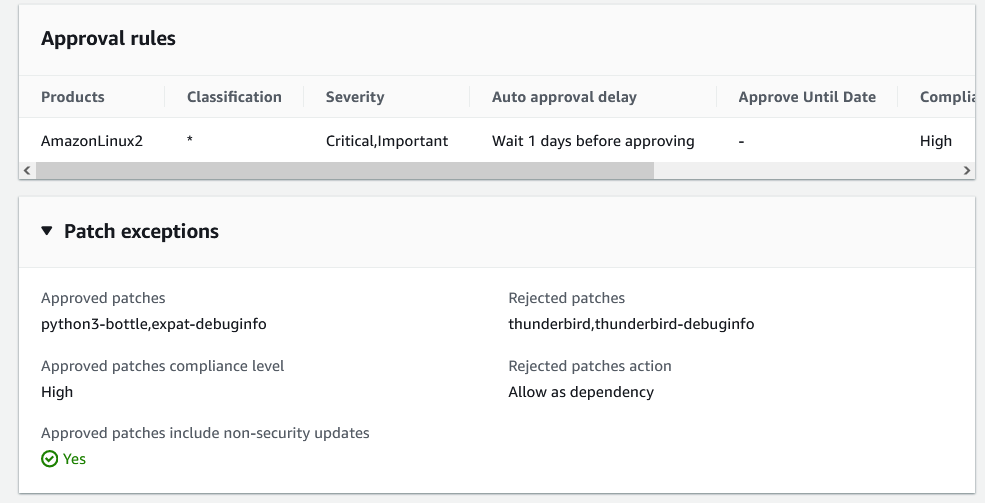


The custom baseline is created.



Clicking on the baseline ID, we can view description of the created baseline.





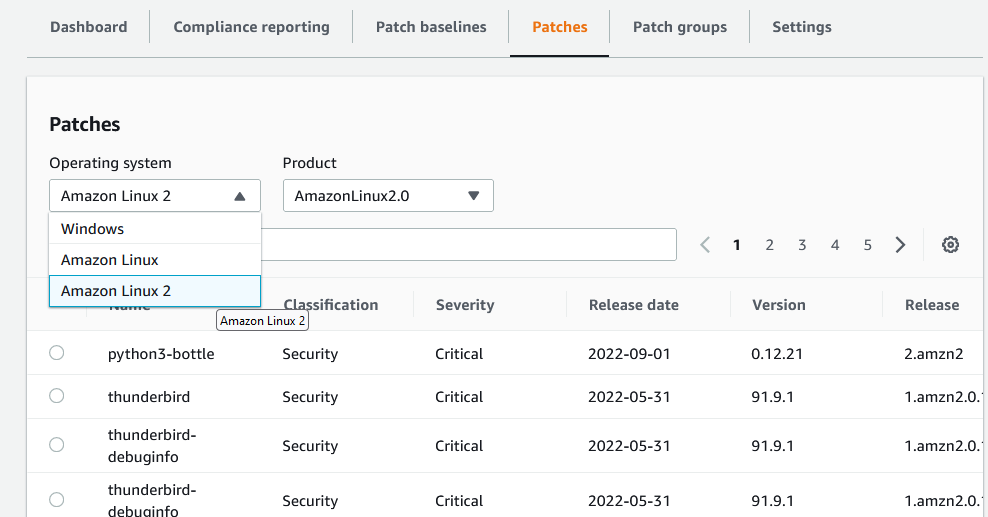
## **Updating or deleting a patch baseline**

Choose the patch baseline from Patch Manager tab that you want to update or delete, and then do one of the following:

* To remove the patch baseline from your AWS account, choose **Delete**. The system prompts you to confirm your actions.
* To make changes to the patch baseline name or description, approval rules, or patch exceptions, choose **Edit**. On the **Edit patch baseline** page, change the values and options that you want, and then choose **Save changes**.
* To add, change, or delete tags applied to the patch baseline, choose the **Tags** tab, and then choose **Edit tags**. On the **Edit patch baseline tags** page, make updates to the patch baseline tags, and then choose **Save changes**.

**View available patches**

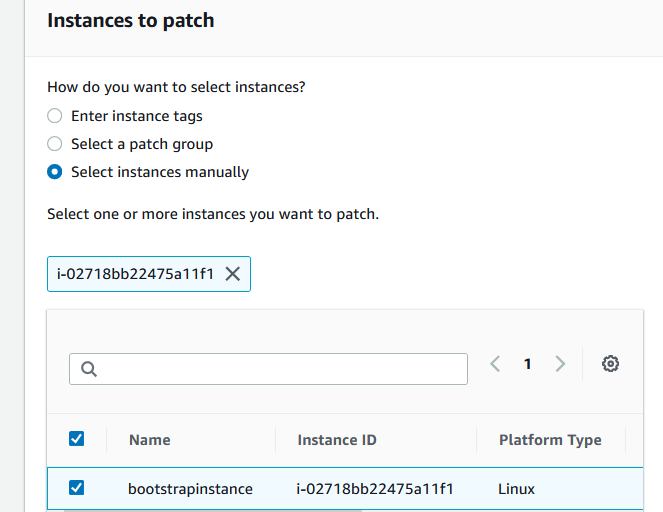
1. Open the AWS Systems Manager console.
2. In the navigation pane, choose **Patch Manager**.
3. Choose the **Patches** tab.
4. For **Operating system**, choose the operating system for which you want to view available patches, such as Windows or Amazon Linux.
5. (Optional) For **Product**, choose an OS version, such as WindowsServer2019 or AmazonLinux2018.03.

****

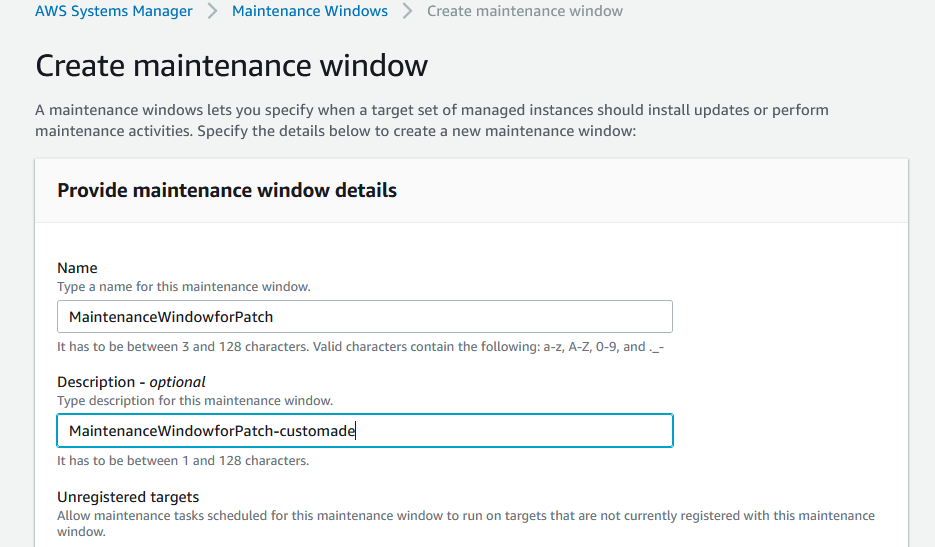
**Note:** There are thousands of in-built patches are available in AWS for different Operating systems and cannot customized.

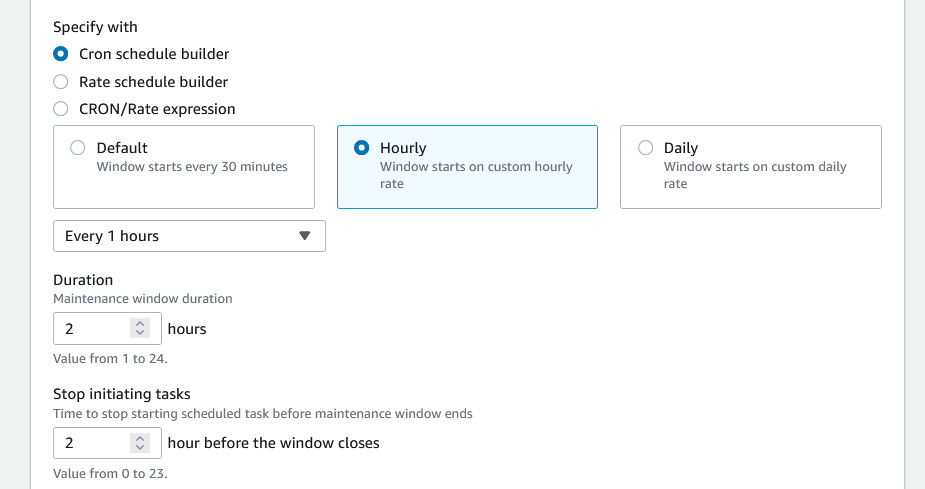
**To create a patching configuration**

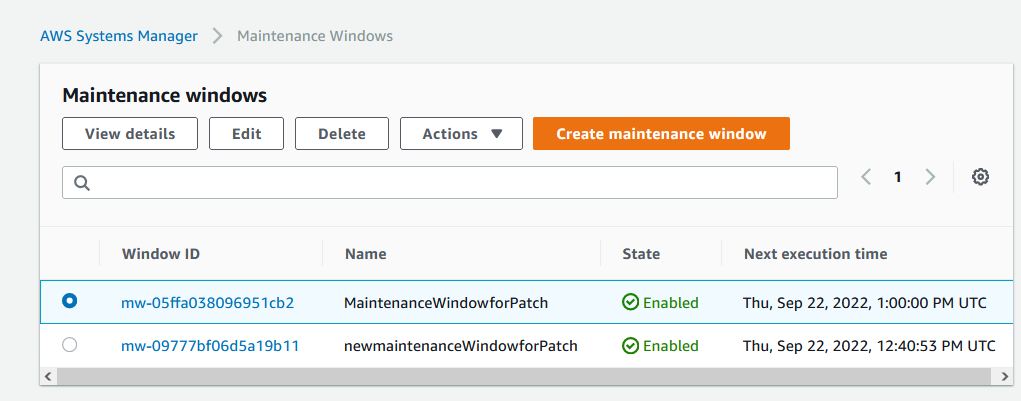
1. Open the AWS Systems Manager console.
2. In the navigation pane, choose **Patch Manager**.
3. Choose **Configure patching**
4. In the **Instances to patch** section, choose one of the following:
   * **Enter instance tags**: Enter a tag key and optional tag value to specify the tagged managed node to patch. Select **Add** to include additional tagged managed nodes.
   * **Select a patch group**: Choose the name of an existing patch group that includes the managed nodes you want to patch.
   * **Select instances manually**: Select the check box next to the name of each managed node you want to patch.

****

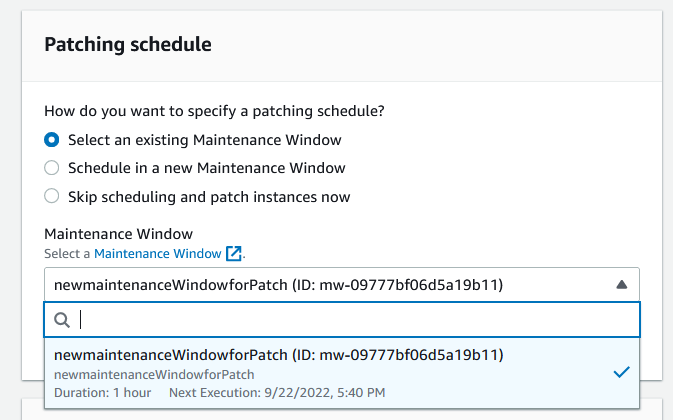
1. In the **Patching schedule** section, choose one of the following:
   * **Select an existing maintenance window**: From the list, select a maintenance window you have already created, and then continue to Step 7.
   * **Schedule in a new maintenance window**: Create a new maintenance window to associate with this patching configuration.
   * **Skip scheduling and patch now**: Run a one-time manual patching operation without a schedule or maintenance window. Continue to Step 7.

****

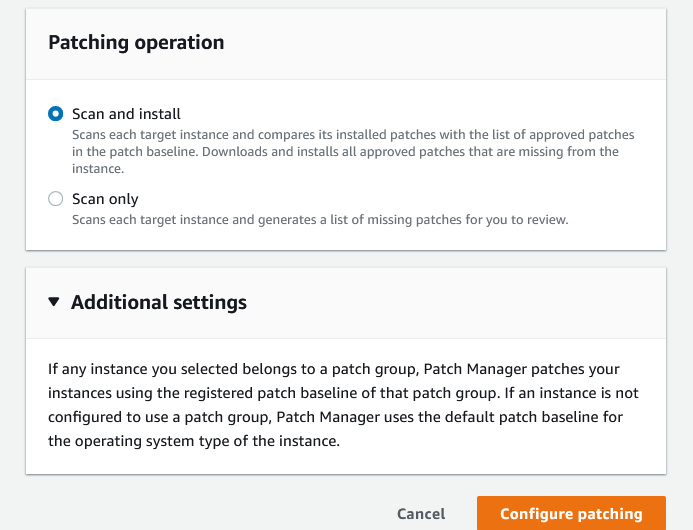
****

****

1. If you chose **Schedule in a new maintenance window** in Step 5, then under **How do you want to specify a patching schedule?**, do the following:
   * Under **How do you want to specify a maintenance window schedule?**, choose a schedule builder or expression option.
   * Under **maintenance window run frequency**, specify how frequently the maintenance window runs.
   * For **Maintenance window duration**, specify the number of hours the maintenance window is permitted to run before timing out.
   * For **Maintenance window name**, enter a name to identify the maintenance window.

****

1. In the **Patching operation** area, choose whether to scan managed nodes for missing patches and apply them as needed, or to scan only and generate a list of missing patches.



1. (Optional) In the **Additional settings** area, if any target managed nodes you selected belong to a patch group, you can change the patch baseline that is associated with the patch group. To do so, follow these steps:
   * Choose the button next to the name of the associated patch baseline.
   * Choose **Change patch baseline registration**.
   * Choose the patch baselines you want to specify for this configuration by clearing and selecting check boxes next to the patch baseline names.
   * Choose **Close**.
2. Choose **Configure patching**.

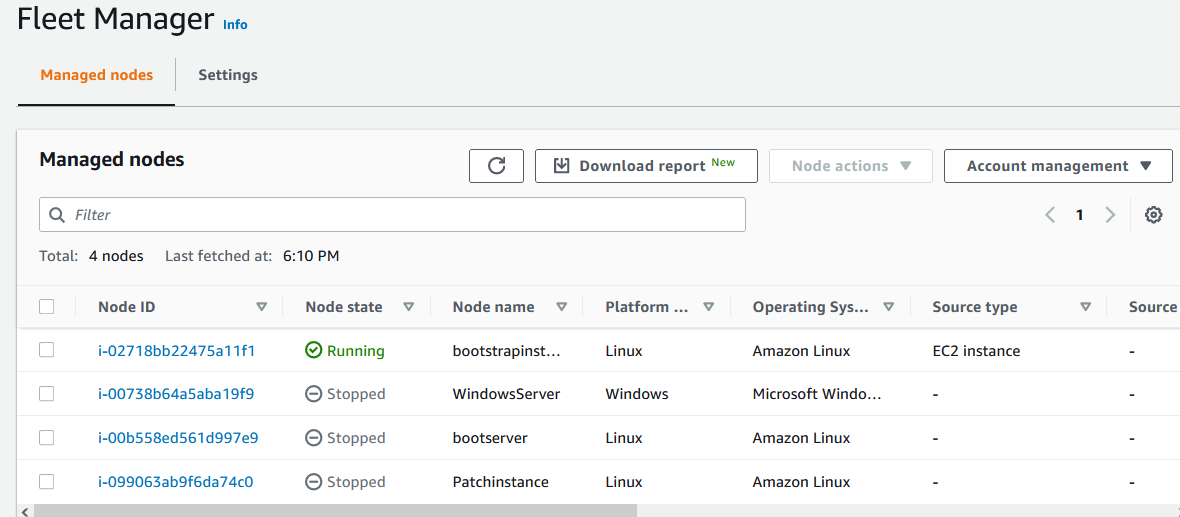
If you created a new maintenance window for this patching configuration, you can add to it or make patching configuration changes in the **Maintenance Windows** area of Systems Manager.

## **How patch group works**

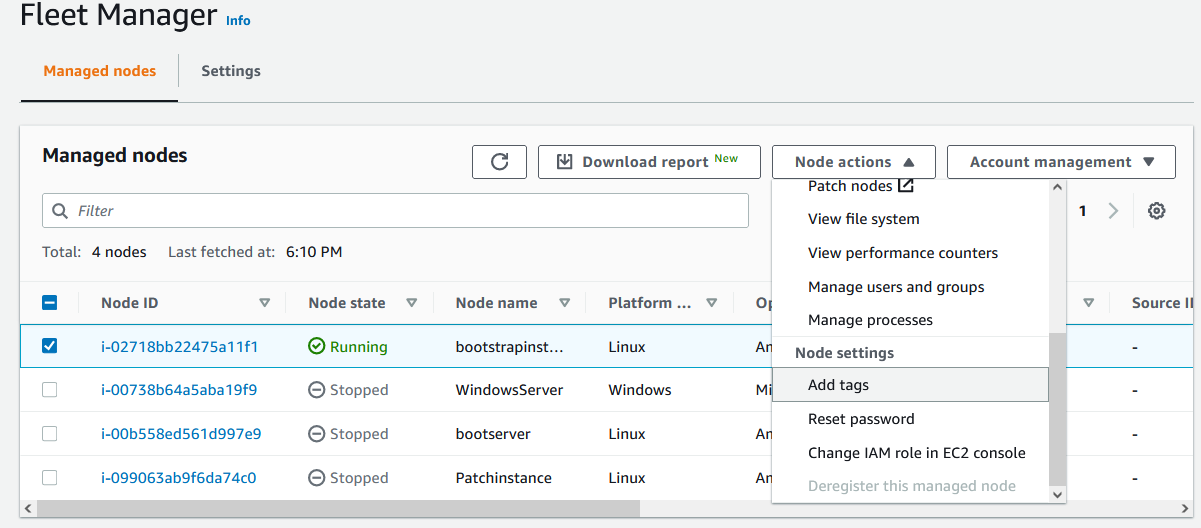
When the system runs the task to apply a patch baseline to a managed node, SSM Agent verifies that a patch group value is defined for the node. If the node is assigned to a patch group, Patch Manager then verifies which patch baseline is registered to that group. If a patch baseline is found for that group, Patch Manager notifies SSM Agent to use the associated patch baseline. If a node isn't configured for a patch group, Patch Manager automatically notifies SSM Agent to use the currently configured default patch baseline.

## **Task 1: Add EC2 instances to a patch group using tags**

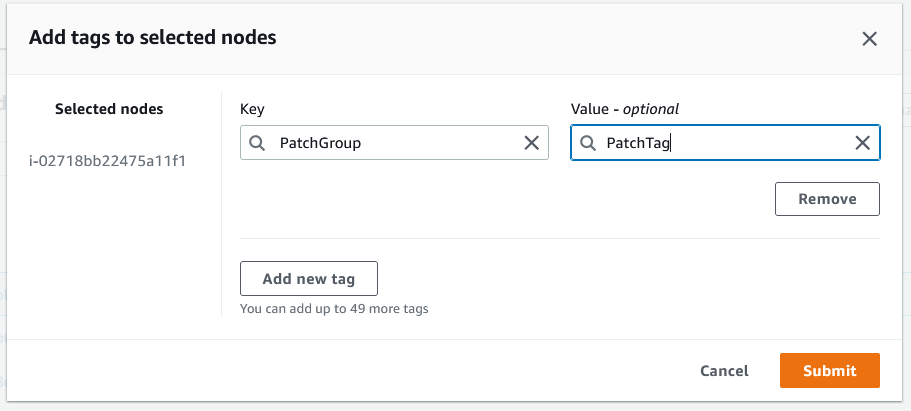
1. Open the AWS Systems Manager console
2. In the navigation pane, choose **Fleet Manager**



1. In the **Managed instances** list, choose the ID of a managed EC2 instance that you want to configure for patching.
2. Select the **Tags** tab, then choose **Edit**.



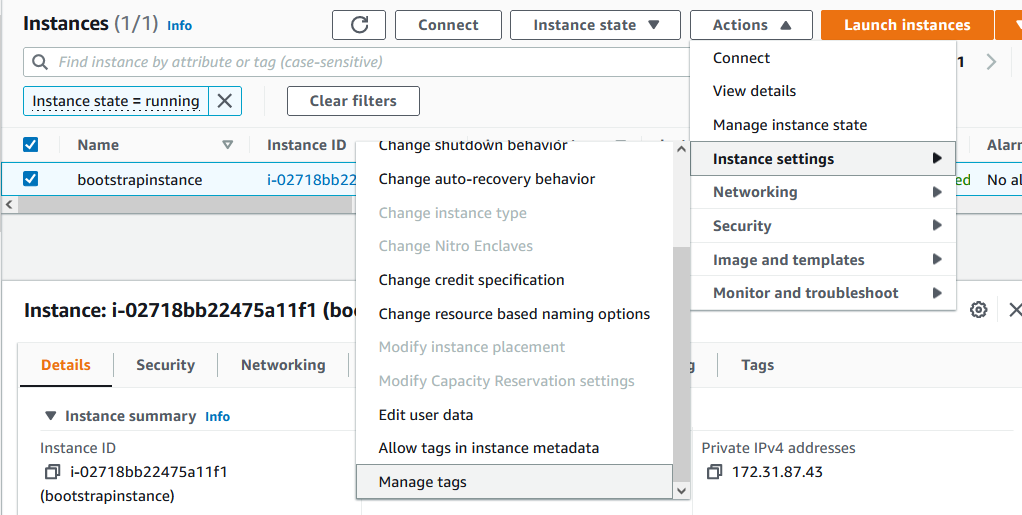
1. In the left column, enter Patch Group or PatchGroup.



1. In the right column, enter a tag value to serve as the name for this patch group.
2. Choose **Save**.
3. Repeat this procedure to add other managed instances to the same patch group.

**To add EC2 instances to a patch group**

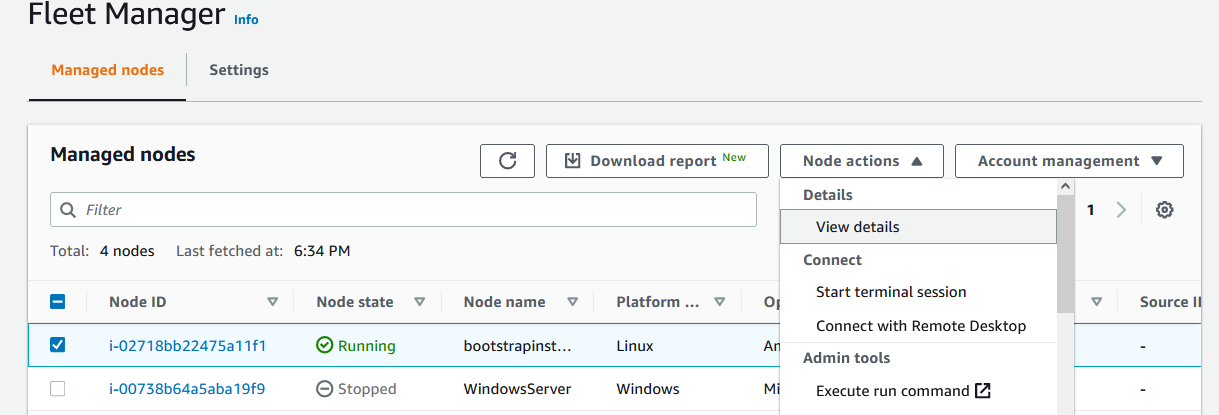
1. Open the [Amazon EC2 console](https://console.aws.amazon.com/ec2/), and then choose **Instances** in the navigation pane.
2. In the list of instances, choose an instance that you want to configure for patching.
3. In the **Actions** menu, choose **Instance Settings**, **Add/Edit Tags**.



1. If the instance already has one or more tags applied, choose **Create Tag**.
2. For **Key**, enter Patch Group or PatchGroup.
3. For **Value**, enter a value to serve as the name for this patch group
4. Repeat this procedure to add other instances to the same patch group.

## **Task 2: Add managed nodes to a patch group using tags**

1. Open the AWS Systems Manager console
2. In the navigation pane, choose **Fleet Manager**.
3. In the **Managed instances** list, choose a managed node that you want to configure for patching.
4. Choose **View details**.

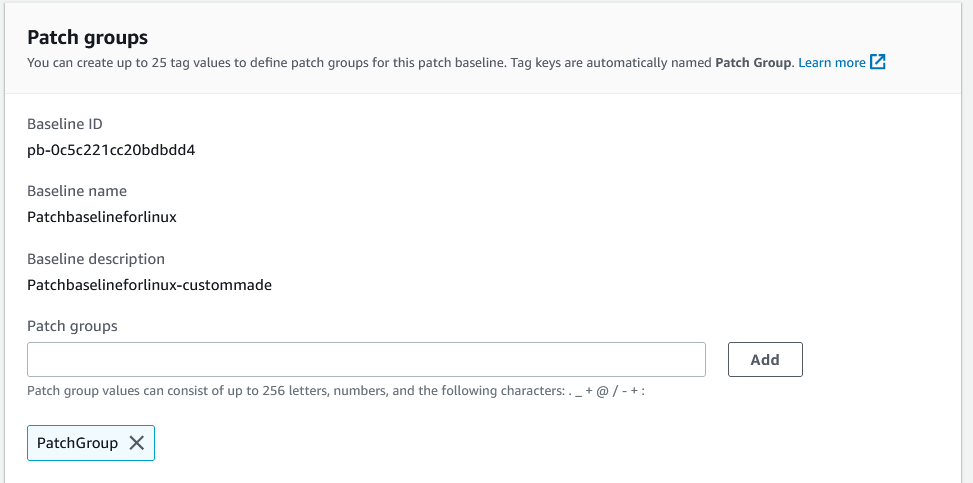


1. Select the **Tags** tab, then choose **Edit.**
2. In the left column, enter Patch Group or PatchGroup.
3. In the right column, enter a tag value to serve as the name for this patch group.
4. Choose **Save**.
5. Repeat this procedure to add other managed nodes to the same patch group.

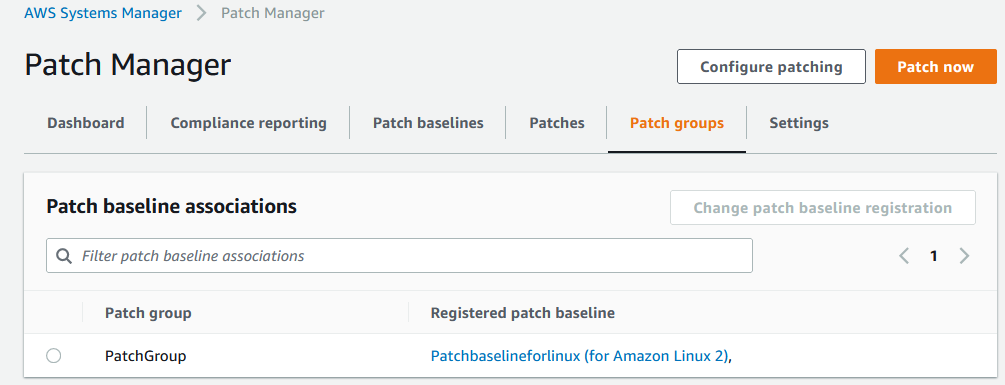
## **Add a patch group to a patch baseline**

To associate a specific patch baseline with your managed nodes, you must add the patch group value to the patch baseline. By registering the patch group with a patch baseline, you can ensure that the correct patches are installed during a patching operation

1. Open the AWS Systems Manager console
2. In the navigation pane, choose **Patch Manager**.
3. In the **Patch baselines** list, choose the patch baseline you want to configure for your patch group.
4. Choose **Actions**, then **Modify patch groups**.
5. Enter the tag value you added to your managed nodes in the previous section, then choose **Add**.



Now Patch Group has the created patchgroup.



From here patching can be done.

**Advantages**

* Protect every endpoint - workstations, laptops, servers and more
* Heterogeneous platform support - Windows, Mac & Linux
* Patches over 850 Applications, including 350+ 3rd party applications
* Scalable distributed architecture suitable for enterprises of all size
* Ensure compliance with real-time reports
* Perform patch management on the go from your Smartphone

**Limitations**

* AWS doesn't test patches before making them available in Patch Manager.
* Patch Manager doesn't support upgrading major versions of operating systems, such as Windows Server 2016 to Windows Server 2019, or SUSE Linux Enterprise Server (SLES) 12.0 to SLES 15.0.