Table of contents

AWS SSM

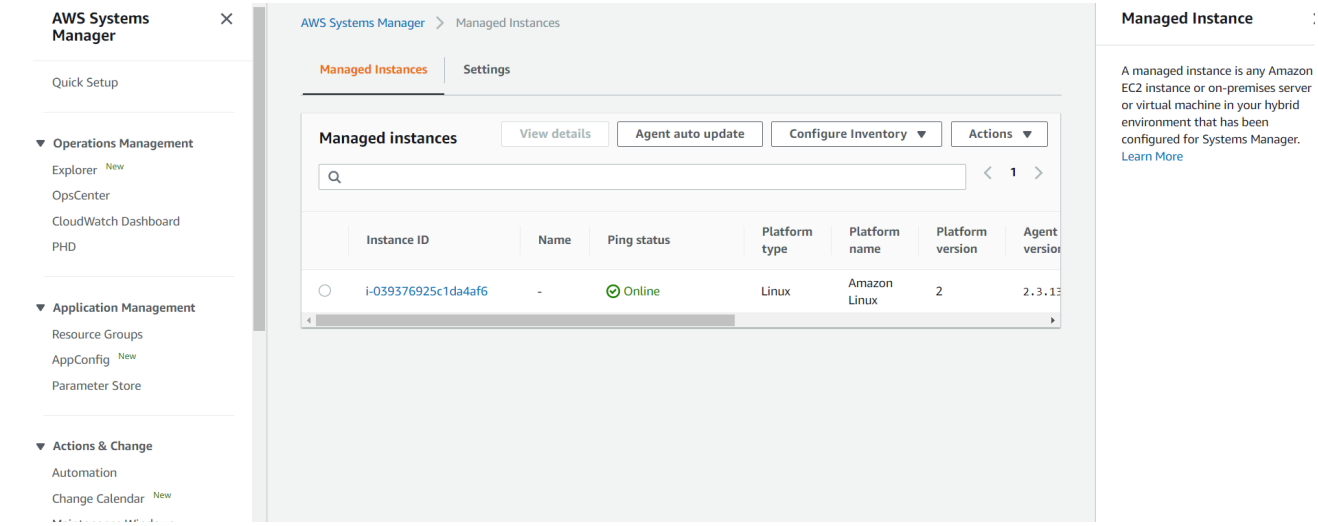
- AWS Systems Manager is an AWS service that you can use to view and control your infrastructure on AWS

Managed instances

- A managed instance is a machine that has been configured for use with Systems Manager
- If the server is managed , we can log in the server from the console itself without using any third party tool
- Also remote commands can be run over the instance from ssm if it is managed

Creating a managed instance

- In order to make sure our instances are managed , we need to have IAM role attached to the ec2 instances which has necessart permissions to send data to ssm
- Create an ec2 service role , attach AmazonEC2RoleforSSM to the said role and attach it to your instance
- Verify if the instances are managed by logging on to ssm and going in managed instances



Run command

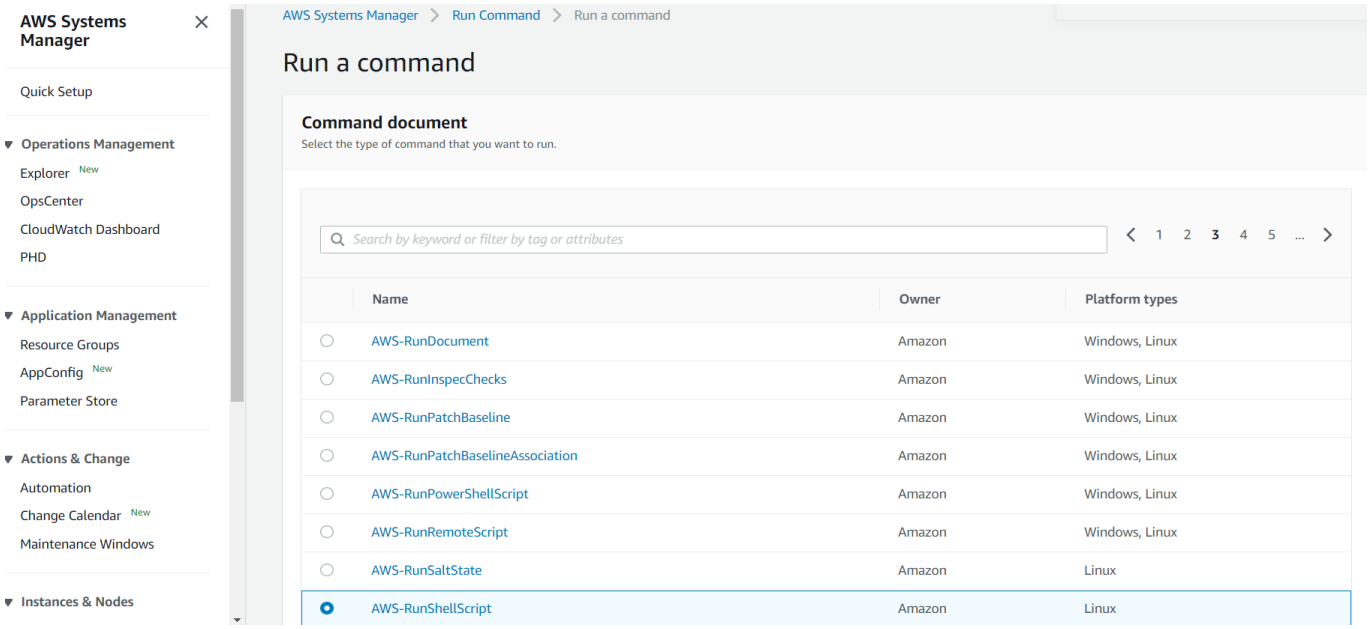
- If the instances are managed , we can run remote commands from the console by going in run command option in ssm
- Click on run comand and chose module AWS-Runshellscript which is on 3rd index page .
- Type the shell commands or a shell script and chose the instance you want to run it on .for ex.

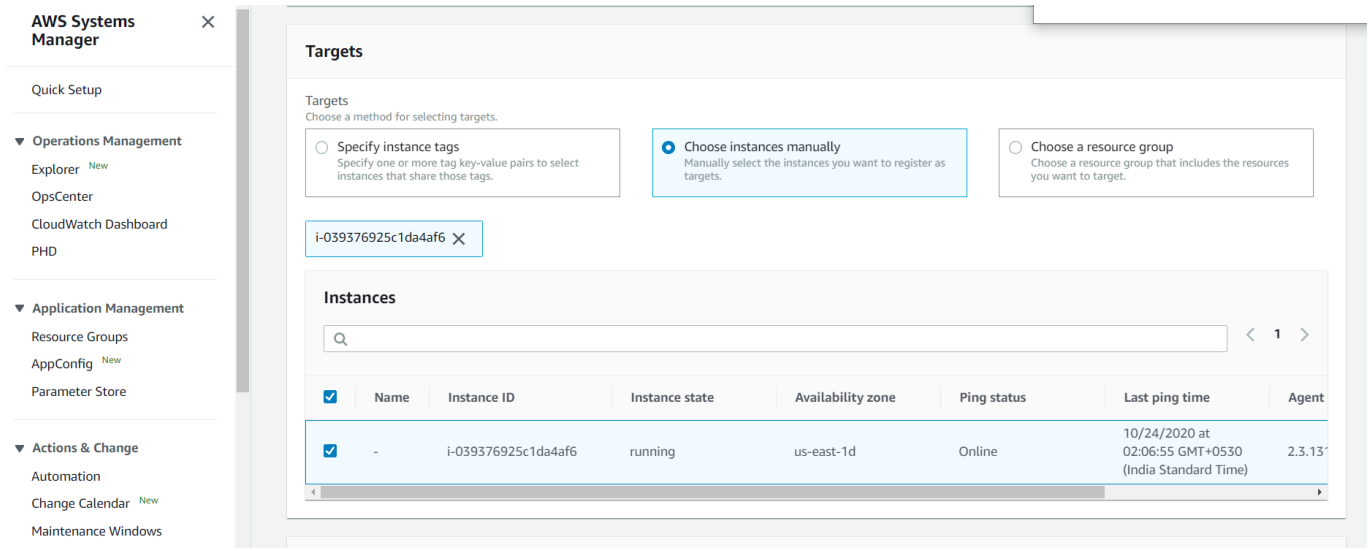
```
#!/bin/bash

# Adding two values
((sum=25+35))

#Print the result
echo $sum
```

- There is another way of running shell scripts on ec2 . That is by using ec2 user data . It is a bootstrap script that we can pass to an ec2 while launching which we want to get executed during instance startup. for ex-

```
#!/bin/bash
sudo yum update -y
sudo yum install httpd -y
sudo service httpd start
```

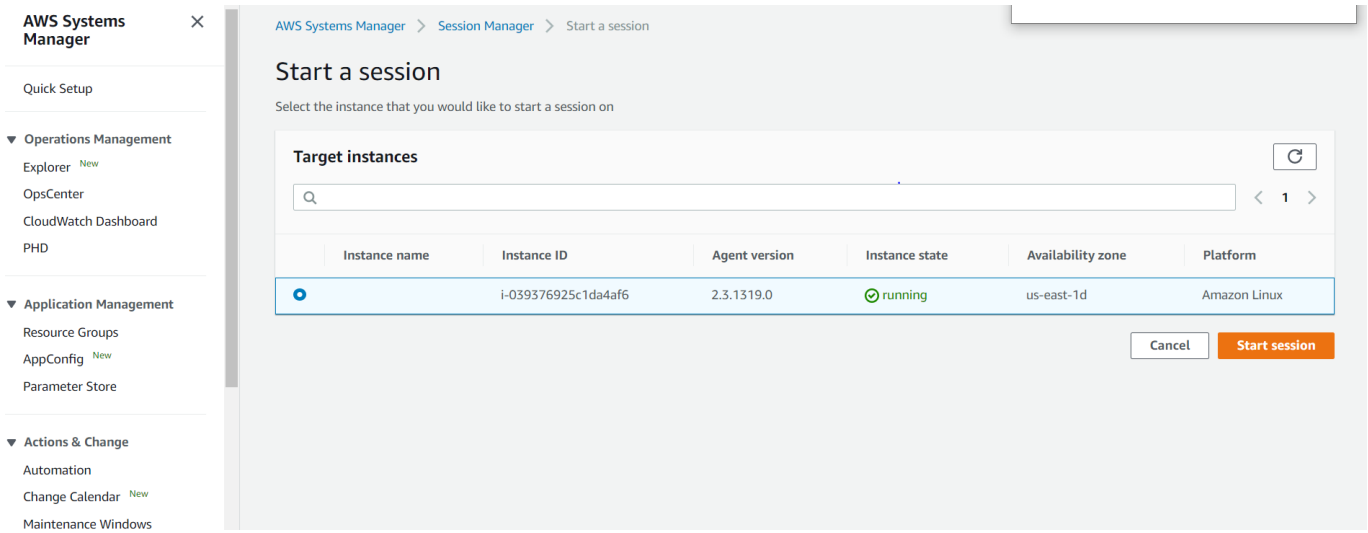
- You can also chose multiple targets by utilizing the ec2 tags

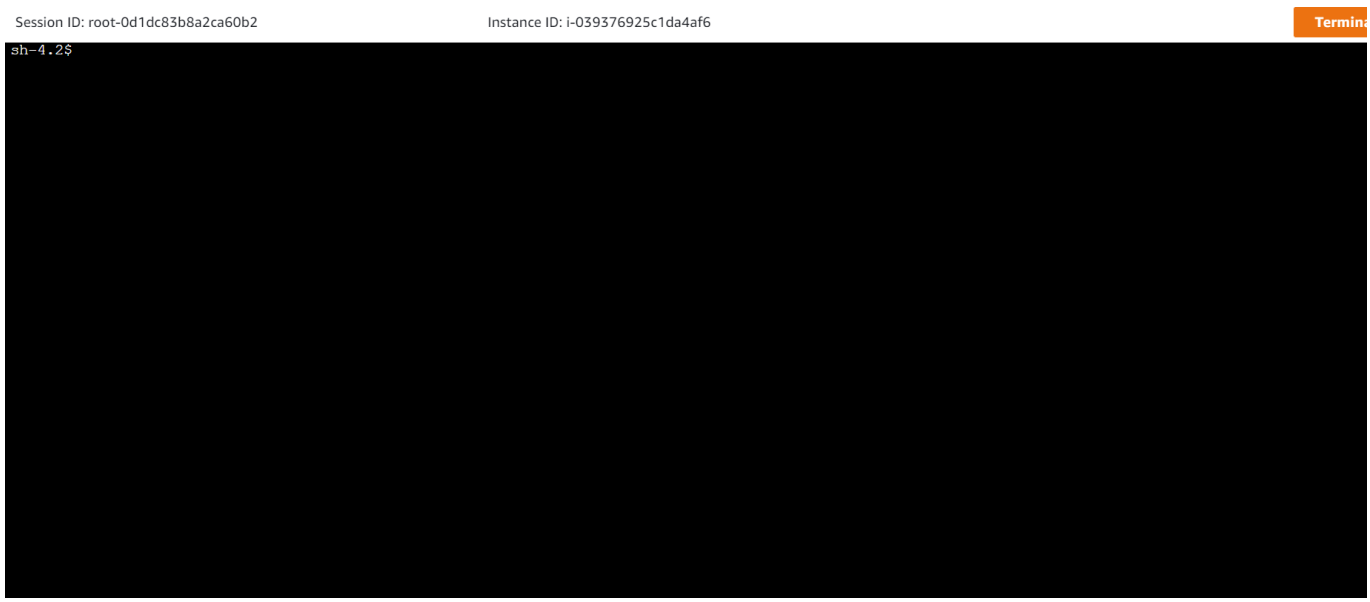




Session manager

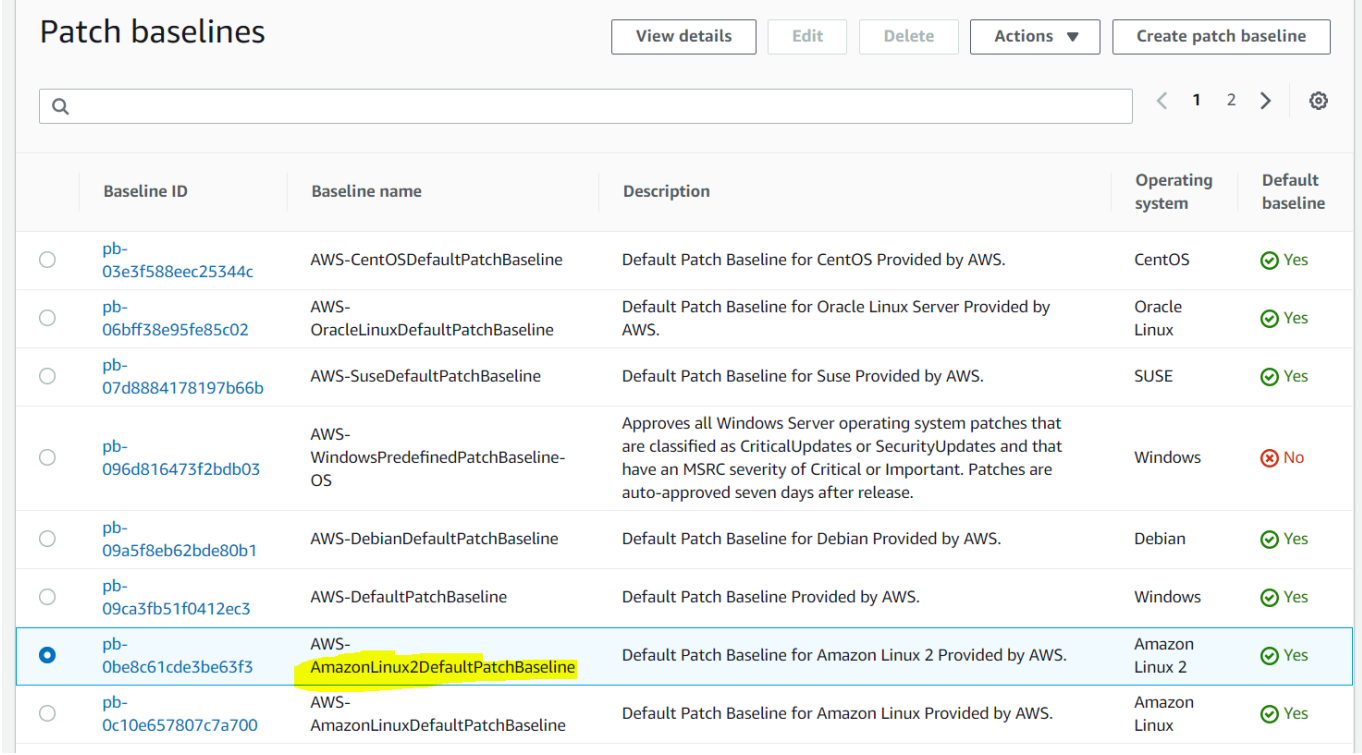
- Session manager lets us spawn a console shell for the managed instaces without having to logging into them .
- Navigate to session manager and click on start session
- select the target instance and click on start session .





Patch-manager

- a. patch baseline - Which patches are approved for installation on your instances.
- b. Patch group - Organise group of instances for patching
    - use EC2 tags to define the same Key - Patch Group Value - anyvalue
- c. Approval rules - Defines which pathaces should be automatically be approved and installed
- AWS provides default patch groups for various OS .
- Navigate to patch manager in ssm .
- Select view Patch baselines



Patch baselines

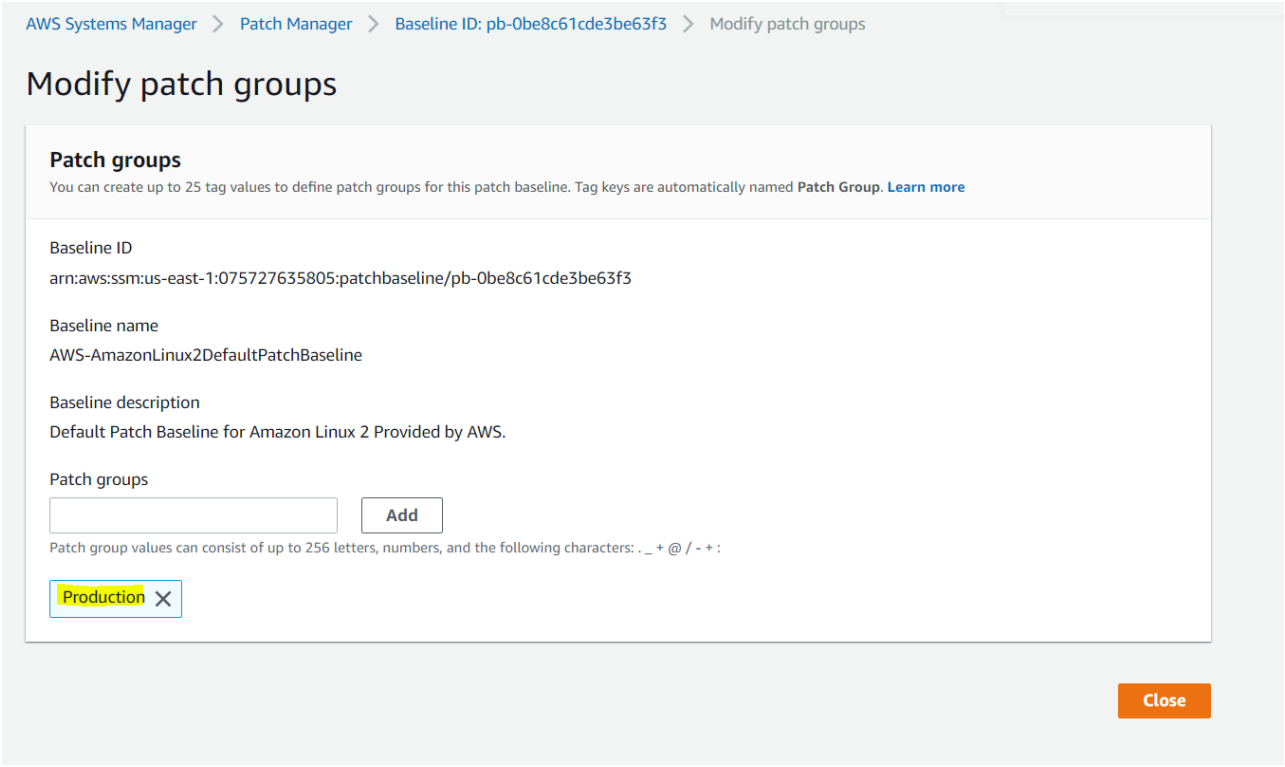
View details | Edit | Delete | Actions | Create patch baseline

1 2

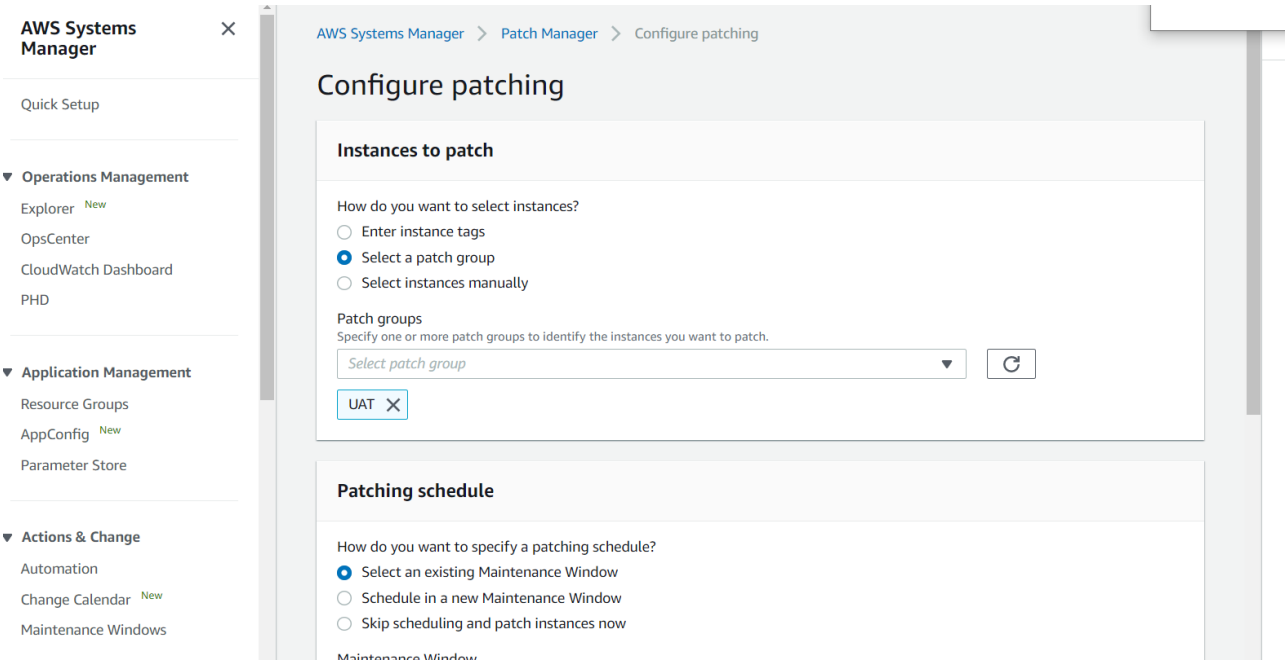
Baseline ID	Baseline name	Description	Operating system	Default baseline
pb-03e3f588eec25344c	AWS-CentOSDefaultPatchBaseline	Default Patch Baseline for CentOS Provided by AWS.	CentOS	Yes
pb-06bff38e95fe85c02	AWS-OracleLinuxDefaultPatchBaseline	Default Patch Baseline for Oracle Linux Server Provided by AWS.	Oracle Linux	Yes
pb-07d8884178197b66b	AWS-SuseDefaultPatchBaseline	Default Patch Baseline for Suse Provided by AWS.	SUSE	Yes
pb-096d816473f2bdb03	AWS-WindowsPredefinedPatchBaseline-OS	Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of Critical or Important. Patches are auto-approved seven days after release.	Windows	No
pb-09a5f8eb62bde80b1	AWS-DebianDefaultPatchBaseline	Default Patch Baseline for Debian Provided by AWS.	Debian	Yes
pb-09ca3fb51f0412ec3	AWS-DefaultPatchBaseline	Default Patch Baseline Provided by AWS.	Windows	Yes
pb-0be8c61cde3be63f3	AWS-AmazonLinux2DefaultPatchBaseline	Default Patch Baseline for Amazon Linux 2 Provided by AWS.	Amazon Linux 2	Yes
pb-0c10e657807c7a700	AWS-AmazonLinuxDefaultPatchBaseline	Default Patch Baseline for Amazon Linux Provided by AWS.	Amazon Linux	Yes

- Select one for amazon linux 2 , go to actions and click on modify patch group.

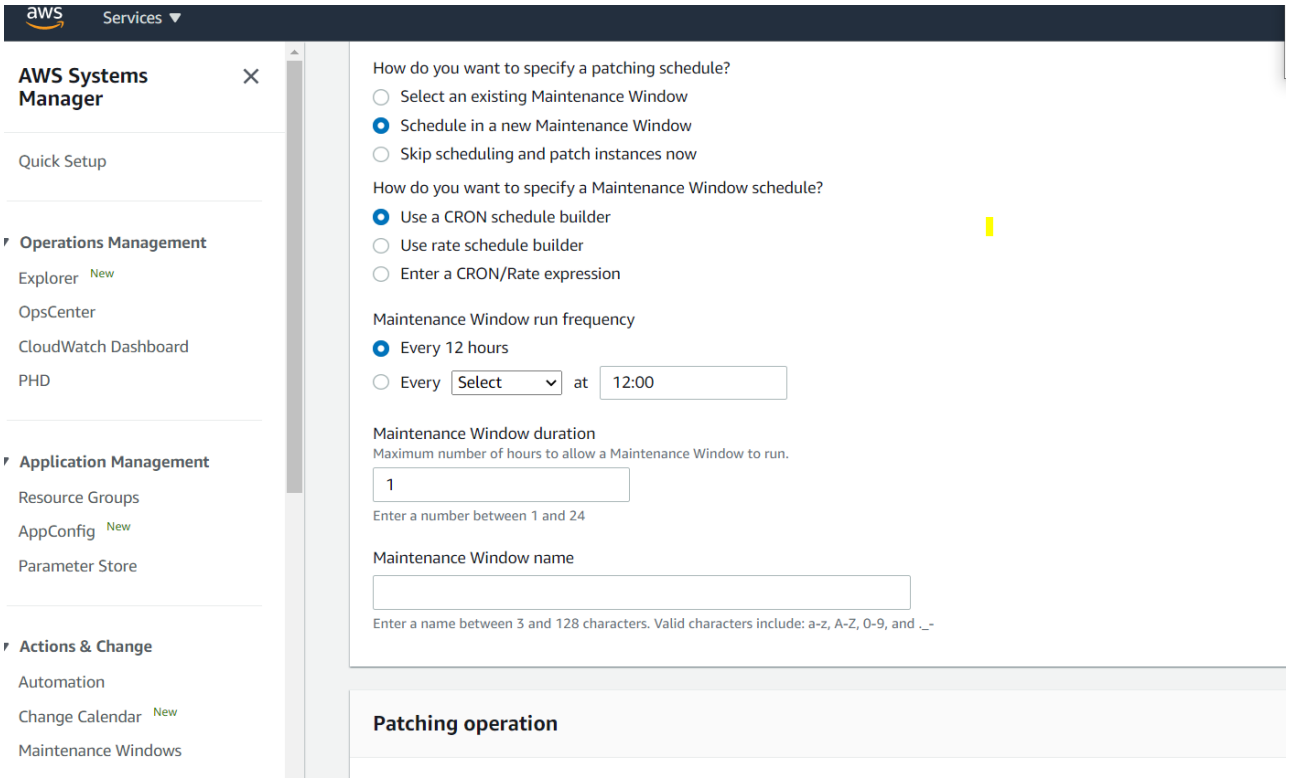
- Mention the tag value and click on save .



- We can repeat the above action for Windows instance as well, we just have to change the patch baseline and use the default windows baseline
- Click on configure patching in the patch baslines dashboard
- Select the patch group from the Instance tags box



- In patching schedule , we can use existing patching window , create a new window using cron expressions or we can patch the instances on demand by selecting skip scheduling .



- In the upper part of the screen we can click on View details to see the output
- We can also create our own patch baseline based on operating system and appication .