AUTOMATE OPERATING SYSTEMS PATCHES AND SECURITY PATCHES USING AWS SSM

KEY POINTS

Important

Beginning December 22, 2022, Systems Manager provides support for *patch policies*, which are the new and recommended method for configuring your patching operations. Using a single patch policy configuration, you can define patching for all accounts in all Regions in your organization, for only the accounts and Regions you choose, or for a single account-Region pair. For more information, see Using Quick Setup patch policies.

Note

AWS doesn't test patches before making them available in Patch Manager. Also, 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.

For Linux-based operating system types that report a severity level for patches, Patch Manager uses the severity level reported by the software publisher for the update notice or individual patch. Patch Manager doesn't derive severity levels from third-party sources, such as the Common Vulnerability Scoring System (CVSS), or from metrics released by the National Vulnerability Database (NVD).

Integrates With AWS Services

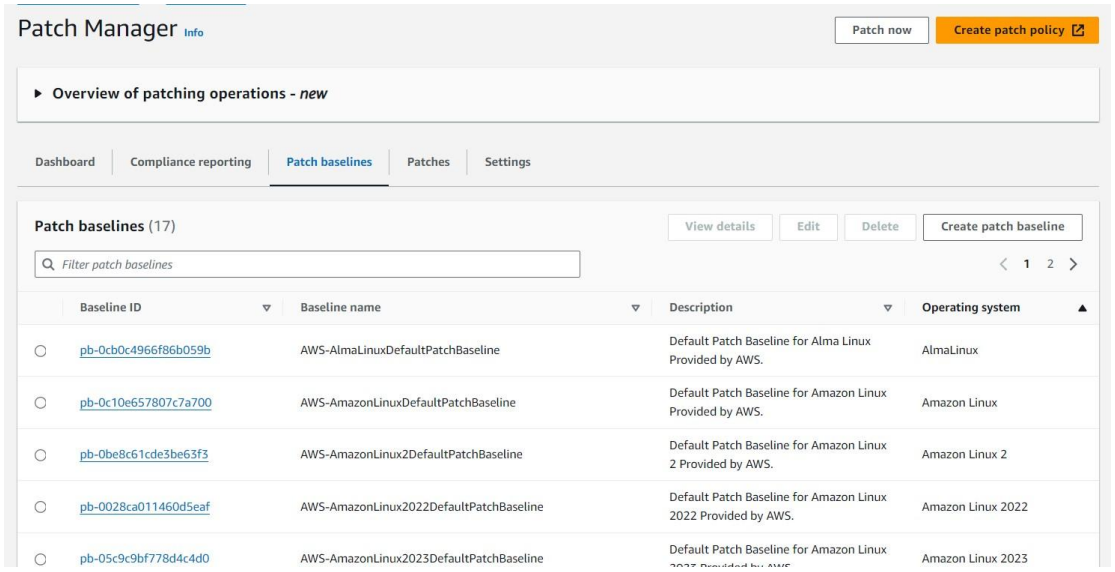
Integrations

Patch Manager integrates with the following other AWS services:

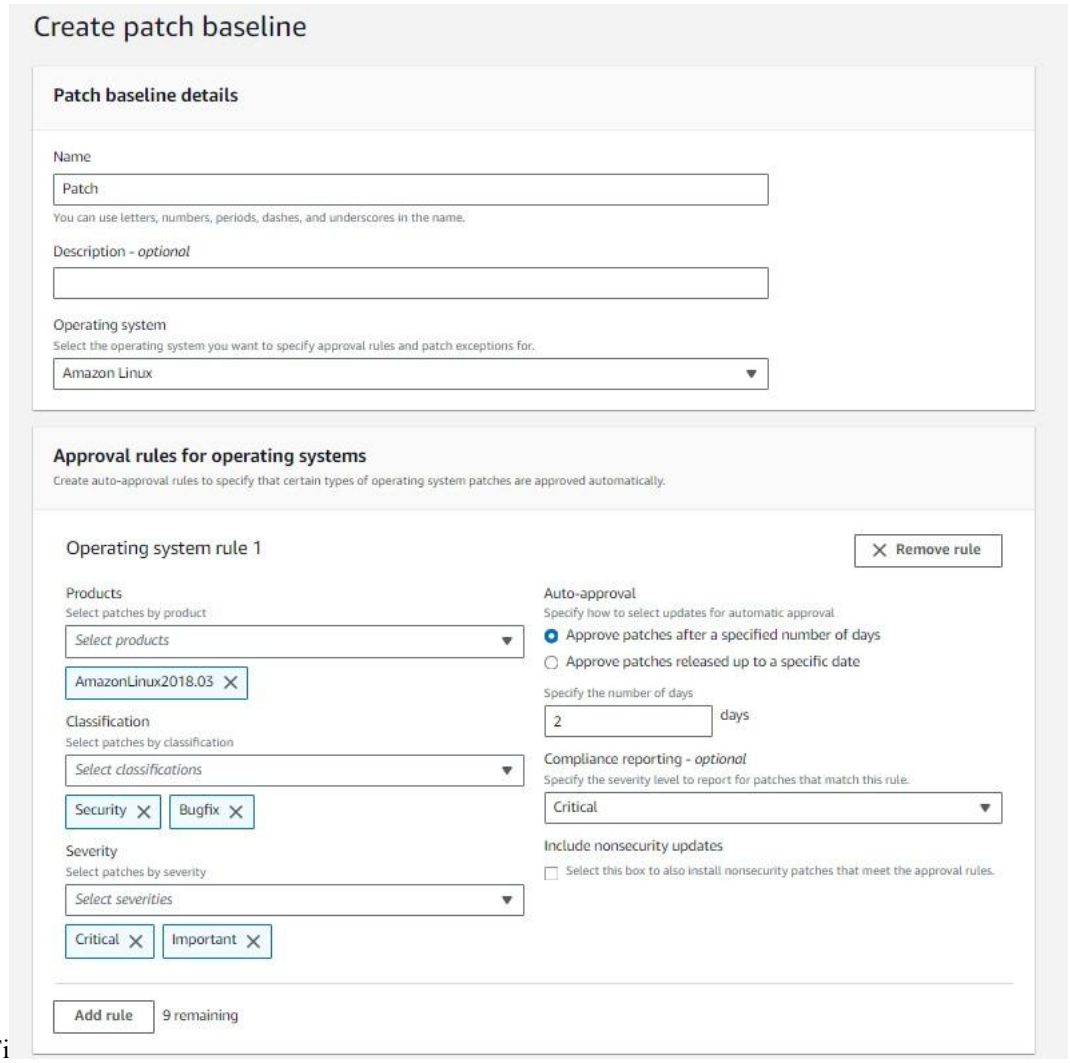
- **AWS Identity and Access Management (IAM)** – Use IAM to control which users, groups, and roles have access to Patch Manager operations. For more information, see How AWS Systems Manager works with IAM and Configure instance permissions required for Systems Manager.
- **AWS CloudTrail** – Use CloudTrail to record an auditable history of patching operation events initiated by users, roles, or groups. For more information, see Logging AWS Systems Manager API calls with AWS CloudTrail.
- **AWS Security Hub** – Patch compliance data from Patch Manager can be sent to AWS Security Hub. Security Hub gives you a comprehensive view of your high-priority security alerts and compliance status. It also monitors the patching status of your fleet. For more information, see Integrating Patch Manager with AWS Security Hub.
- **AWS Config** – Set up recording in AWS Config to view Amazon EC2 instance management data in the Patch Manager Dashboard. For more information, see Viewing patch Dashboard summaries.

STEP 1 :- Visit AWS System Manager Dashboard.

STEP 2 :- Patch Manager

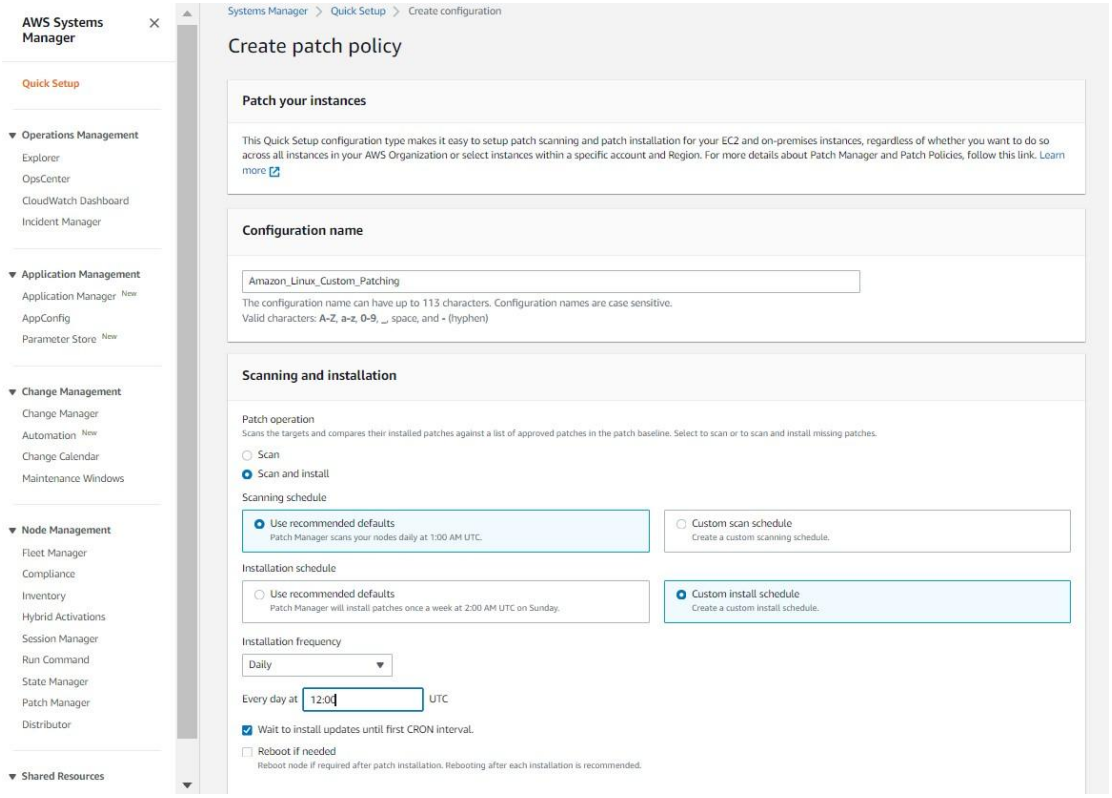


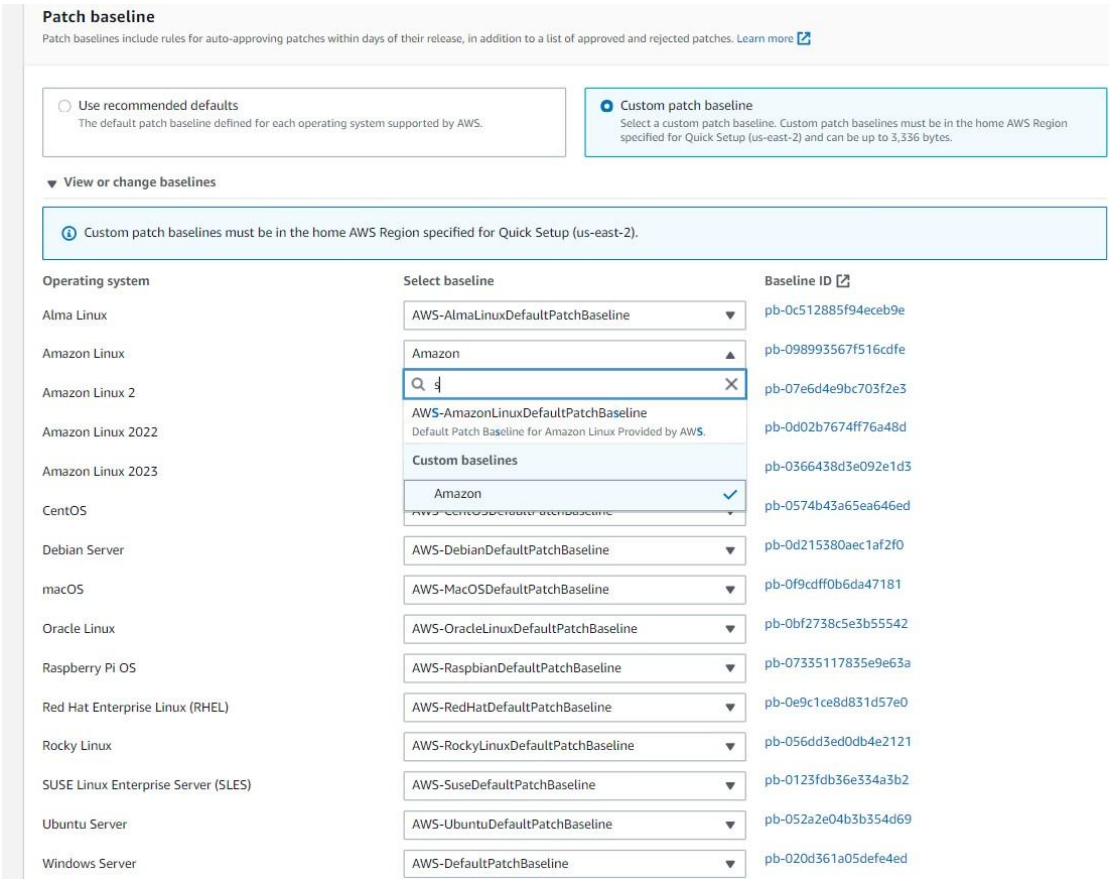
STEP 3 :- Creating Patch Baseline

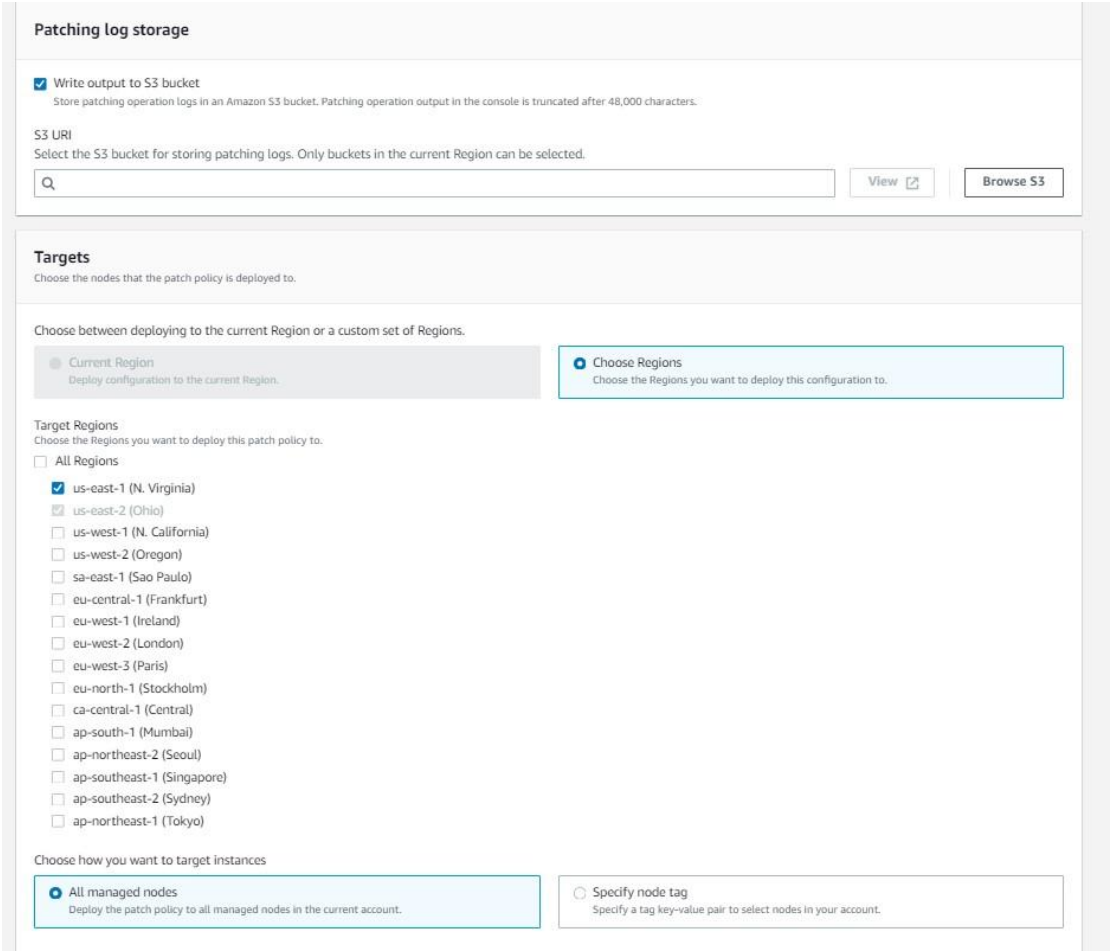


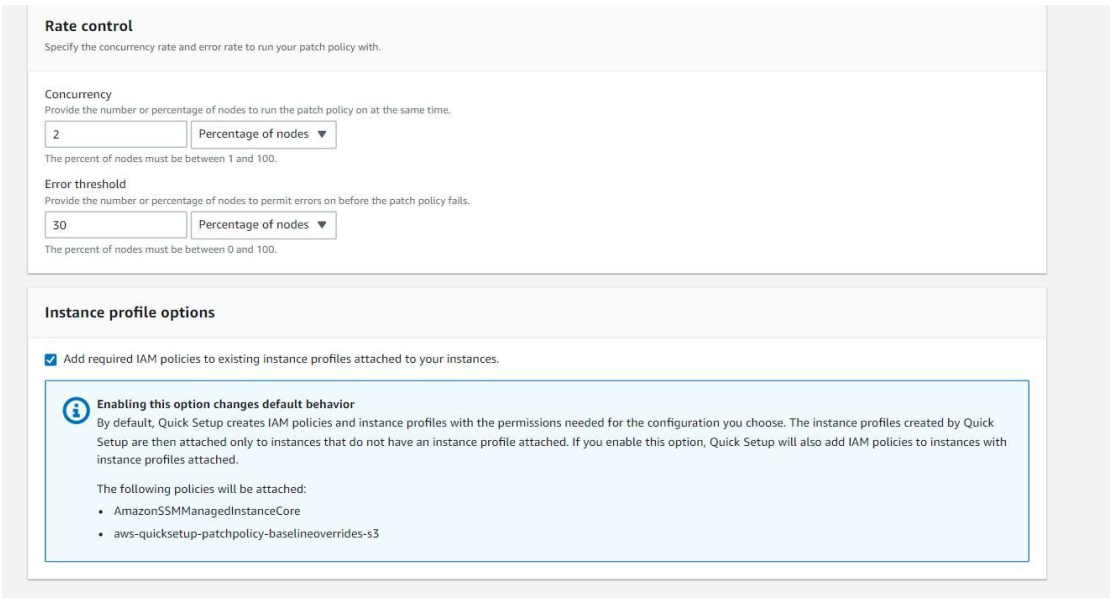
Fi

STEP 4 :- Creating Patch Policy.






Patching log storage
Write output to S3 bucket
Store patching operation logs in an Amazon S3 bucket. Patching operation output in the console is truncated after 48,000 characters.
S3 URI
Select the S3 bucket for storing patching logs. Only buckets in the current Region can be selected.
View
Browse S3
Targets
Choose the nodes that the patch policy is deployed to.
Choose between deploying to the current Region or a custom set of Regions.
Current Region
Deploy configuration to the current Region.
Choose Regions
Choose the Regions you want to deploy this configuration to.
Target Regions
Choose the Regions you want to deploy this patch policy to.
All Regions
us-east-1 (N. Virginia)
us-east-2 (Ohio)
us-west-1 (N. California)
us-west-2 (Oregon)
sa-east-1 (Sao Paulo)
eu-central-1 (Frankfurt)
eu-west-1 (Ireland)
eu-west-2 (London)
eu-west-3 (Paris)
eu-north-1 (Stockholm)
ca-central-1 (Central)
ap-south-1 (Mumbai)
ap-northeast-2 (Seoul)
ap-southeast-1 (Singapore)
ap-southeast-2 (Sydney)
ap-northeast-1 (Tokyo)
Choose how you want to target instances
All managed nodes
Deploy the patch policy to all managed nodes in the current account.
Specify node tag
Specify a tag key-value pair to select nodes in your account.


Rate control
Specify the concurrency rate and error rate to run your patch policy with.
Concurrency
Provide the number or percentage of nodes to run the patch policy on at the same time.
2
Percentage of nodes
The percent of nodes must be between 1 and 100.
Error threshold
Provide the number or percentage of nodes to permit errors on before the patch policy fails.
30
Percentage of nodes
The percent of nodes must be between 0 and 100.
Instance profile options
Add required IAM policies to existing instance profiles attached to your instances.
Enabling this option changes default behavior
By default, Quick Setup creates IAM policies and instance profiles with the permissions needed for the configuration you choose. The instance profiles created by Quick Setup are then attached only to instances that do not have an instance profile attached. If you enable this option, Quick Setup will also add IAM policies to instances with instance profiles attached.
The following policies will be attached:
AmazonSSMManagedInstanceCore
aws-quicksetup-patchpolicy-baselineoverrides-s3