June 25, 2019

Patch Management in EC2 for Immutable & in-place architectures

Amrith Raj Radhakrishnan
Sr AWS Architect | DXC Connect - AWS Practice

Sudev Kurur
AWS DevOps Engineer | DXC Connect - AWS Practice

What we will cover today

- Operating System Patching
- In-place patching
- AWS Systems Manager
- Immutable servers
- Gold AMI
- Step Functions

What is Patching?

- ✓ Applying fixes
  - ✓ for Software flaws
    - ✓ to a large software → Operating System

- ✓ Incorporate new features

The Famous Flaws of the OS

Eternal Blue

RDP CVE-2019-0708

June 25, 2019

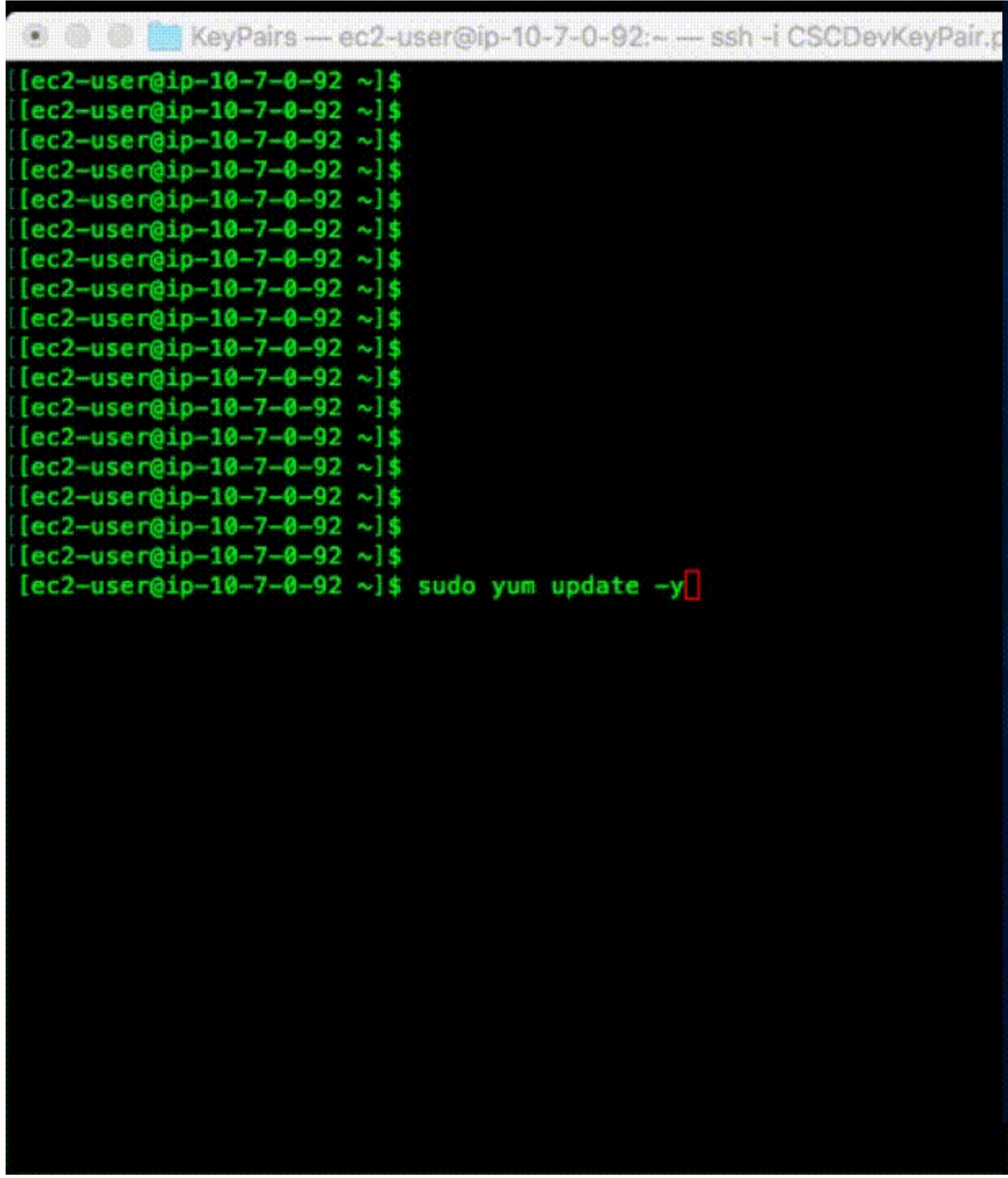
Amazon EC2

Amazon Elastic Compute Cloud (Amazon EC2) is a web service that provides secure, resizable ***compute capacity*** *in the cloud.*

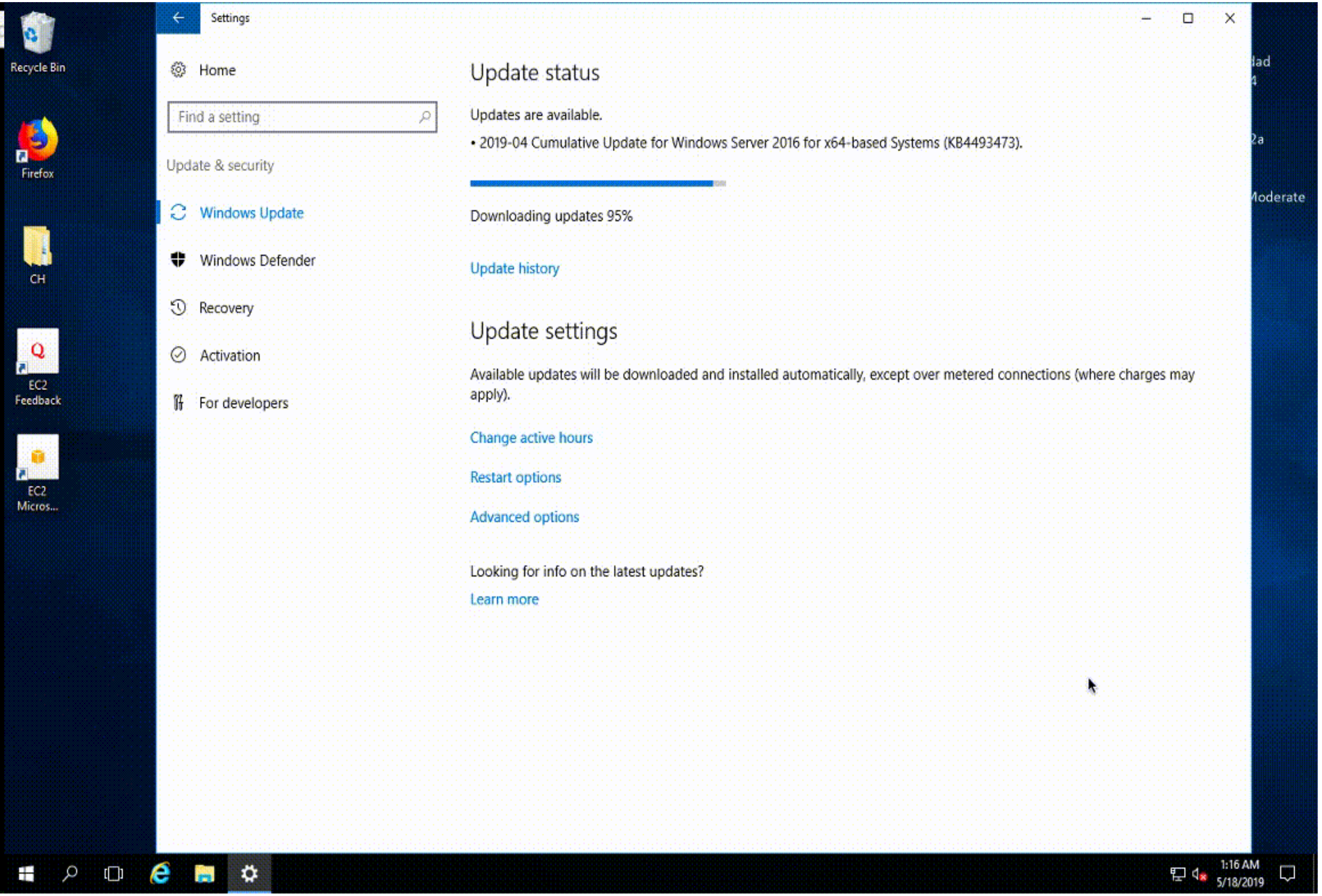
Operating system patching is not Amazon’s responsibility!

Its your responsibility.

How to (not) patch an EC2 Machine?



```
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$
[ec2-user@ip-10-7-0-92 ~]$ sudo yum update -y
```



Update status

Updates are available.

• 2019-04 Cumulative Update for Windows Server 2016 for x64-based Systems (KB4493473).

Downloading updates 95%

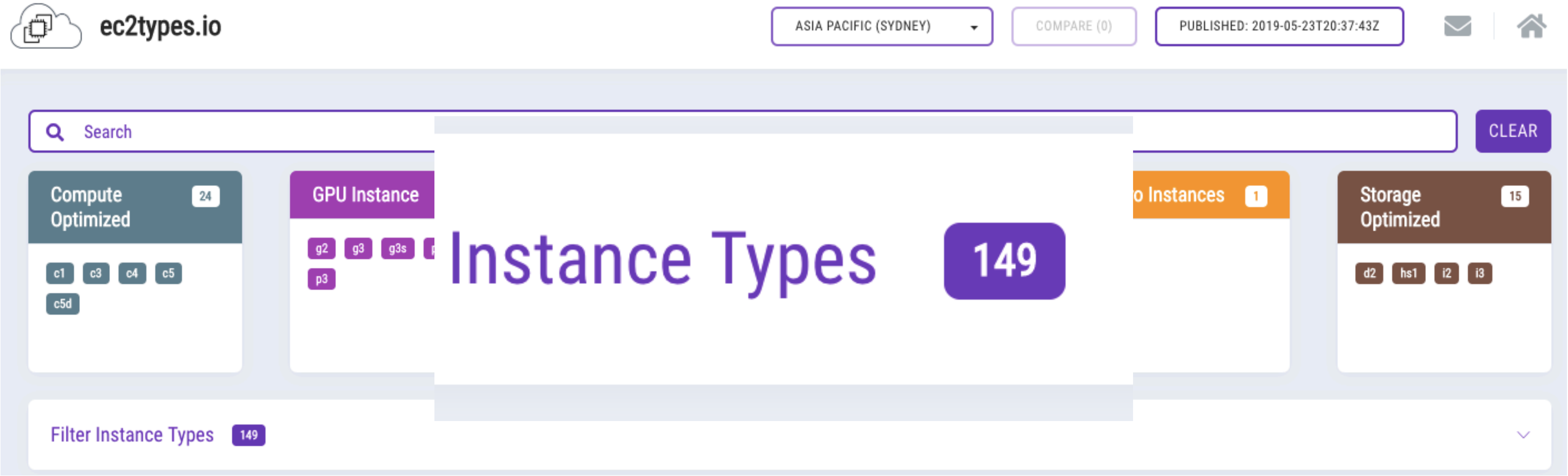
Update settings

Available updates will be downloaded and installed automatically, except over metered connections (where charges may apply).

Looking for info on the latest updates?

June 25, 2019

EC2 is still heavily used for Compute work



ec2types.io

ASIA PACIFIC (SYDNEY)

COMPARE (0)

PUBLISHED: 2019-05-23T20:37:43Z

Search

CLEAR

Compute Optimized 24

c1 c3 c4 c5 c5d

GPU Instance

g2 g3 g3s p3

o Instances 1

Storage Optimized 15

d2 hs1 i2 i3

Instance Types 149

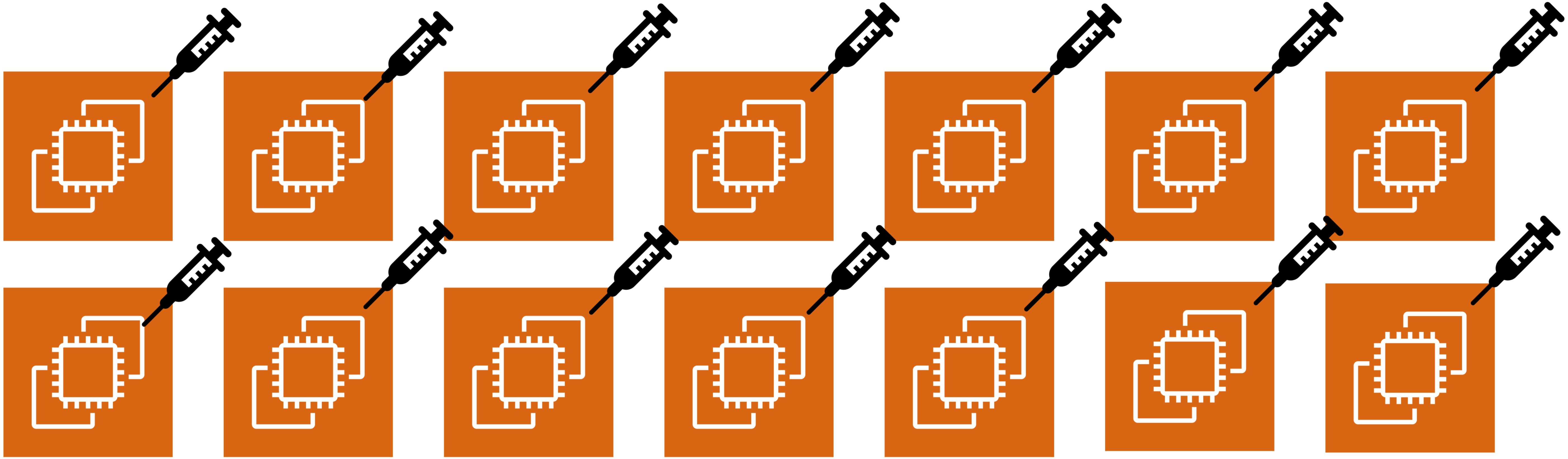
Filter Instance Types 149

https://ec2types.io/

In-place Patching

What is in-place patching?

Patching of an operating system or application on the server without removing the older version first and without saving any data beyond normal precautions.

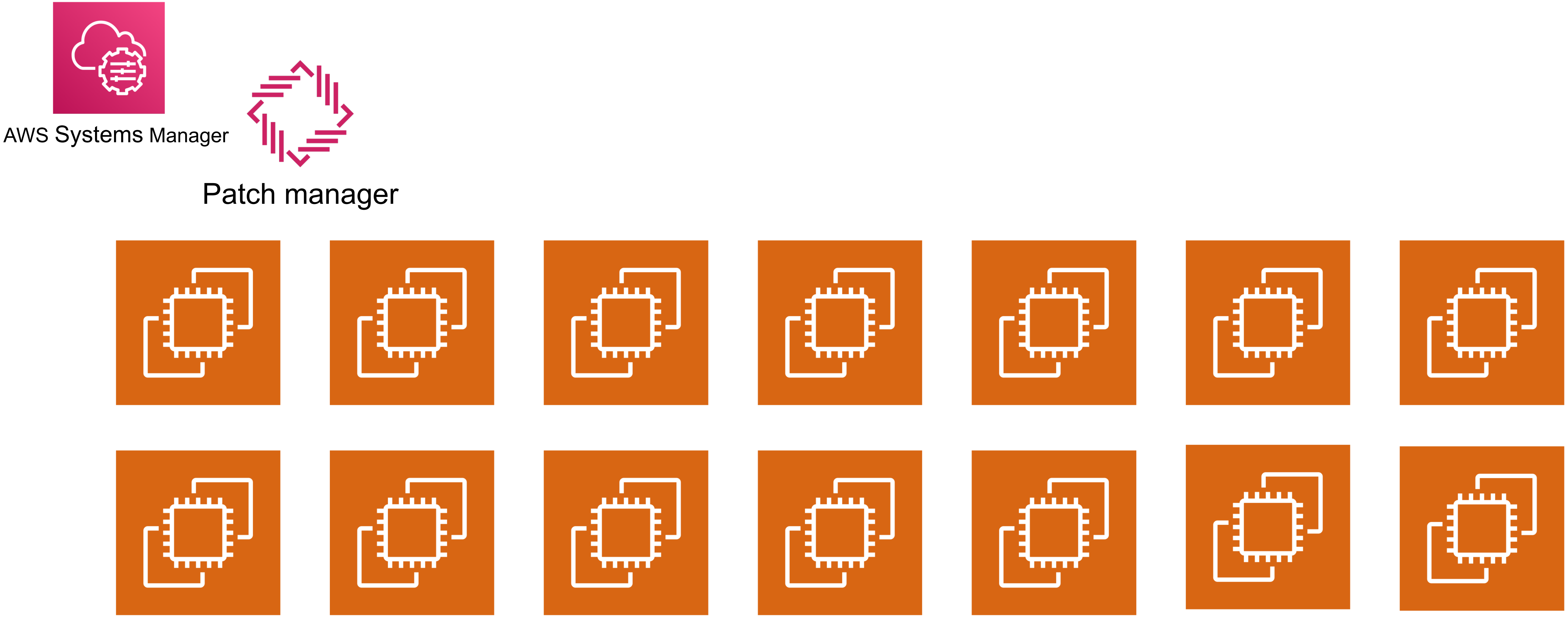


How do you automate in-place patching?

"Doing Automation is very easy,
especially when done through PowerPoint."

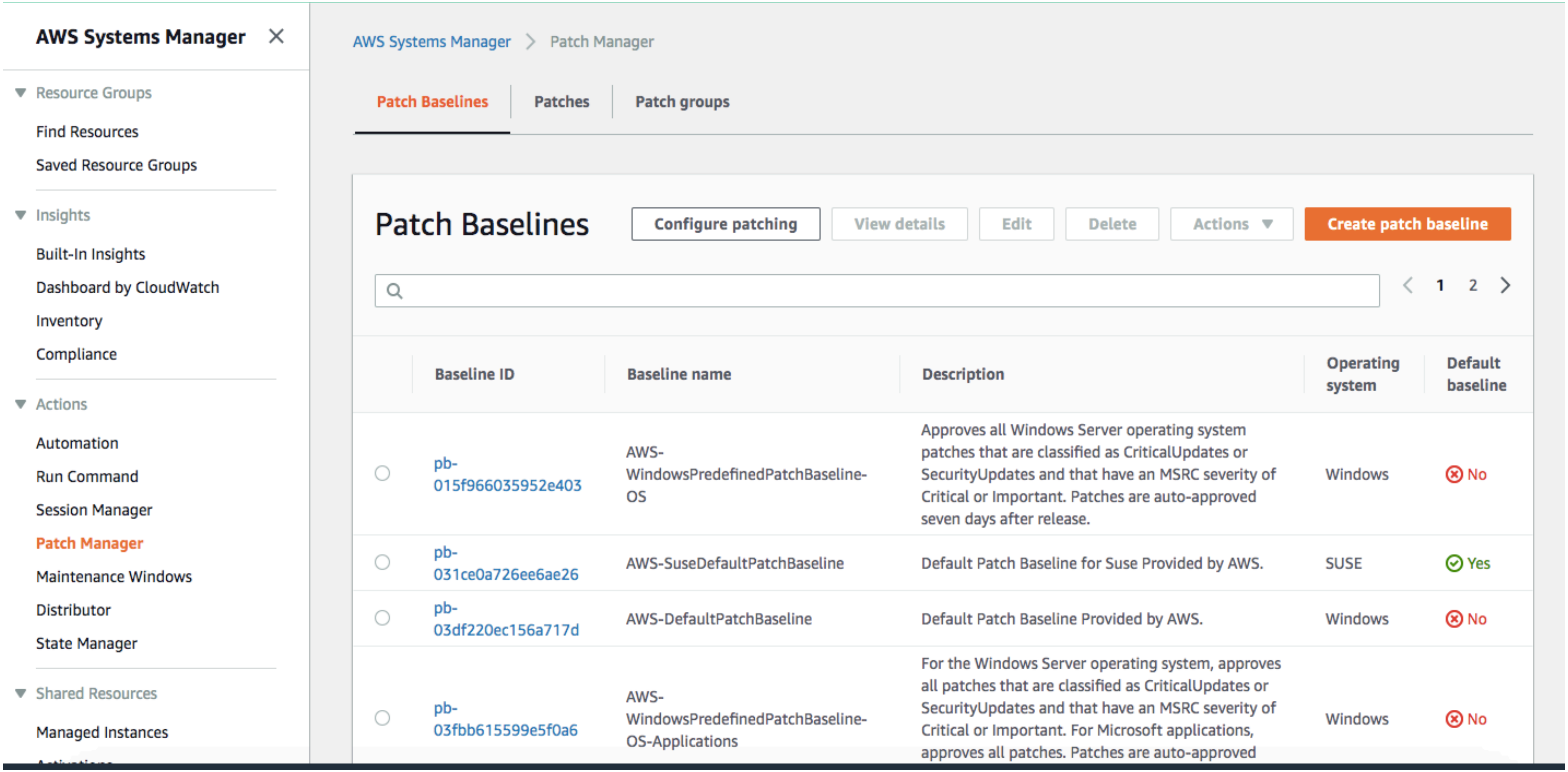
https://www.rajeshvu.com/cartoons/tag/all/39

AWS Systems Manager – Patch Manager



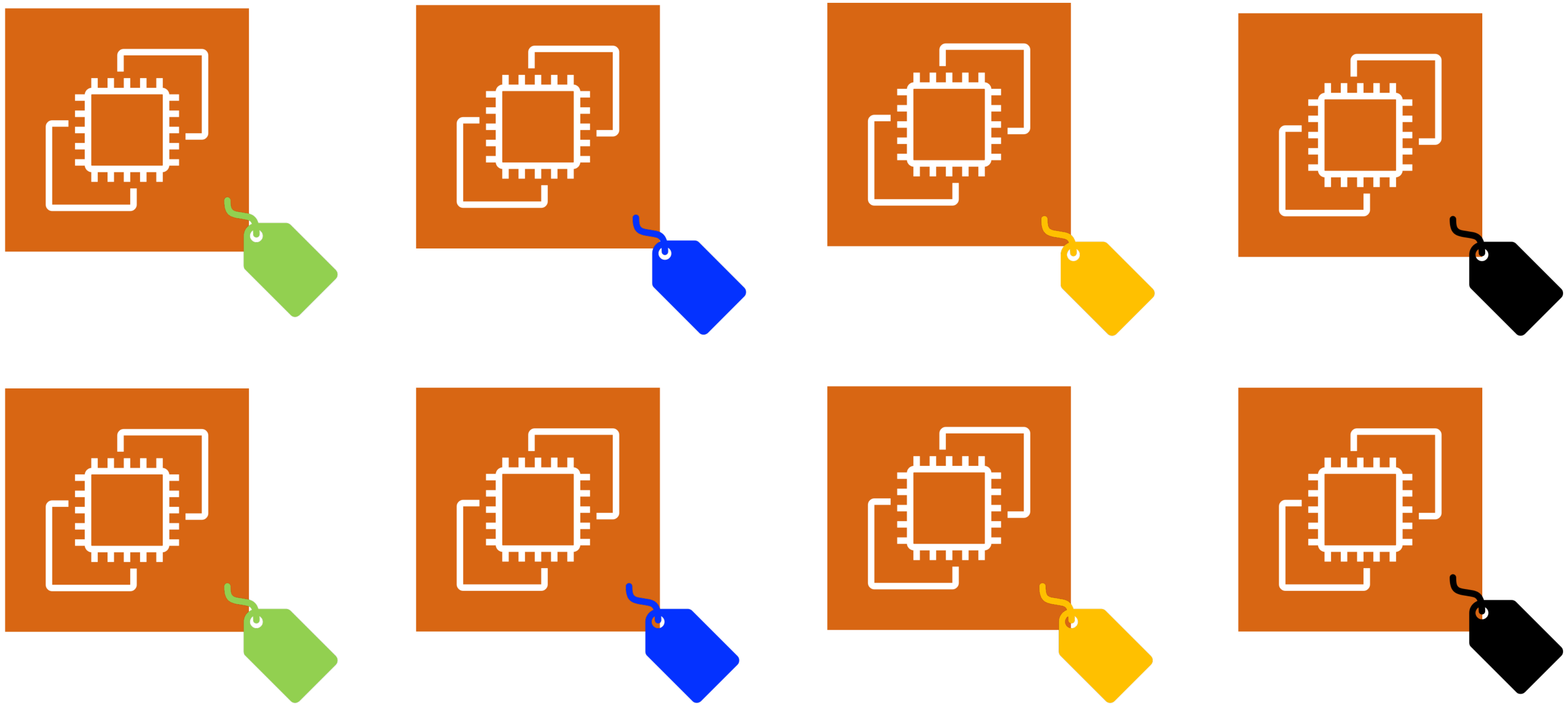
AWS Systems Manager

Patch manager



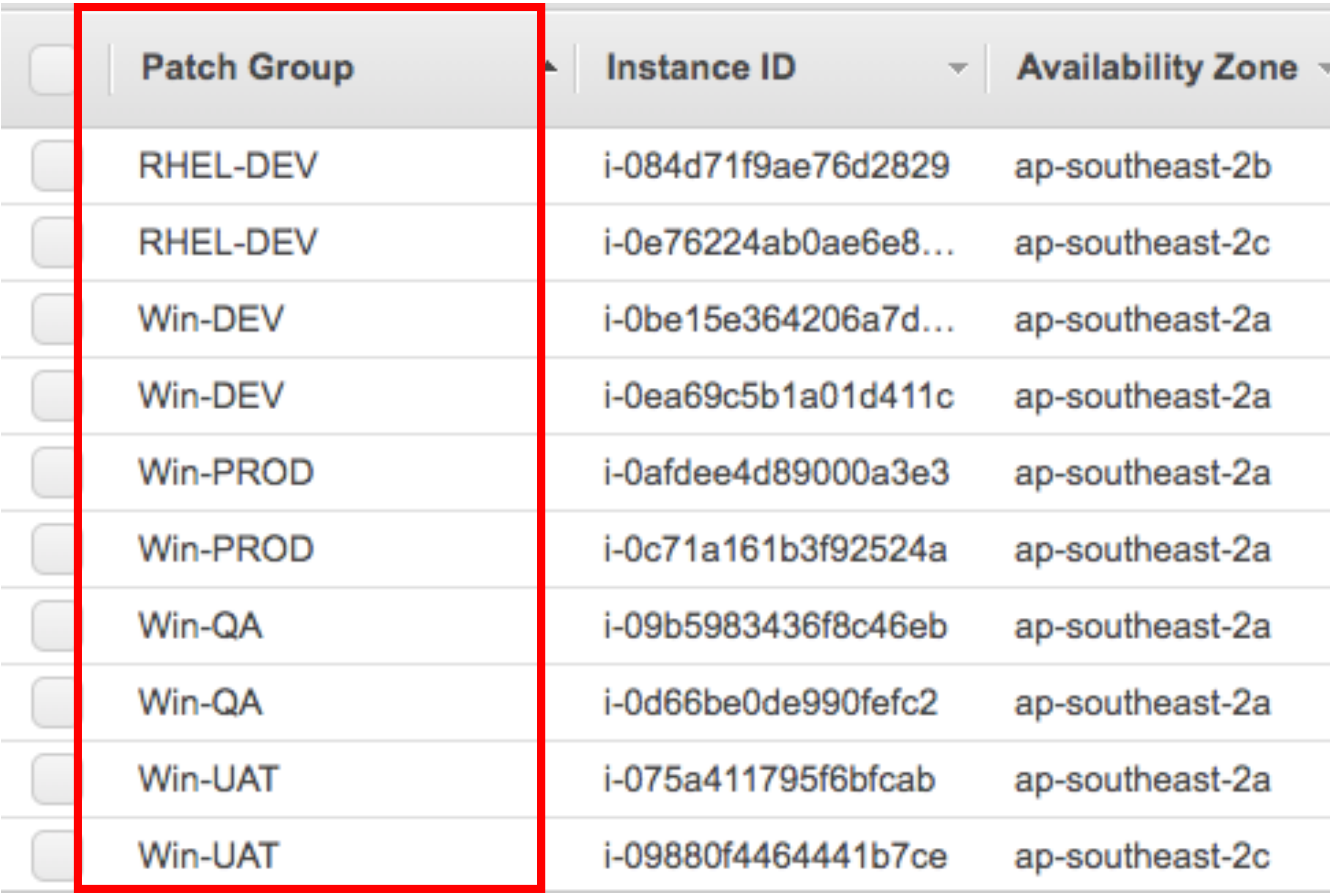
	Baseline ID	Baseline name	Description	Operating system	Default baseline
○	pb-015f966035952e403	AWS-WindowsPredefinedPatchBaseline-OS	Approves all Windows Server operating system patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of Critical or Important. Patches are auto-approved seven days after release.	Windows	⊗ No
○	pb-031ce0a726ee6ae26	AWS-SuseDefaultPatchBaseline	Default Patch Baseline for Suse Provided by AWS.	SUSE	✓ Yes
○	pb-03df220ec156a717d	AWS-DefaultPatchBaseline	Default Patch Baseline Provided by AWS.	Windows	⊗ No
○	pb-03fbb615599e5f0a6	AWS-WindowsPredefinedPatchBaseline-OS-Applications	For the Windows Server operating system, approves all patches that are classified as CriticalUpdates or SecurityUpdates and that have an MSRC severity of Critical or Important. For Microsoft applications, approves all patches. Patches are auto-approved	Windows	⊗ No

1. Tag instances with the Patch Group Tag



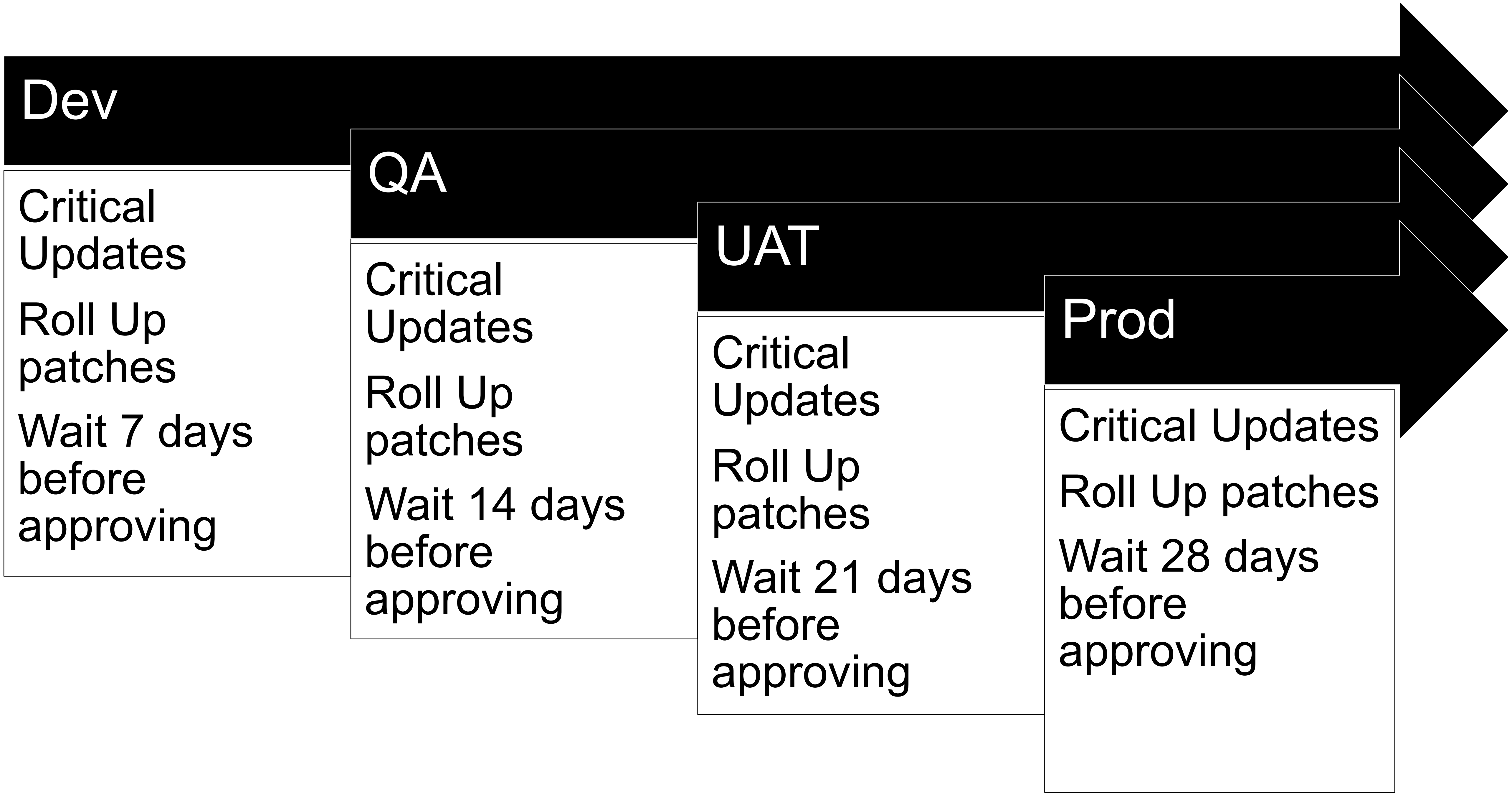
Patch Group	Value
🟩	Dev
🟦	QA
🟨	UAT
⬛	Prod

1. Tag instances with the Patch Group Tag



Patch Group	Instance ID	Availability Zone
RHEL-DEV	i-084d71f9ae76d2829	ap-southeast-2b
RHEL-DEV	i-0e76224ab0ae6e8…	ap-southeast-2c
Win-DEV	i-0be15e364206a7d…	ap-southeast-2a
Win-DEV	i-0ea69c5b1a01d411c	ap-southeast-2a
Win-PROD	i-0afdee4d89000a3e3	ap-southeast-2a
Win-PROD	i-0c71a161b3f92524a	ap-southeast-2a
Win-QA	i-09b5983436f8c46eb	ap-southeast-2a
Win-QA	i-0d66be0de990fefc2	ap-southeast-2a
Win-UAT	i-075a411795f6bfcab	ap-southeast-2a
Win-UAT	i-09880f4464441b7ce	ap-southeast-2c

2. Create a Patch Baseline for each set of Patch Groups (e.g)



Dev

- Critical Updates
- Roll Up patches
- Wait 7 days before approving

QA

- Critical Updates
- Roll Up patches
- Wait 14 days before approving

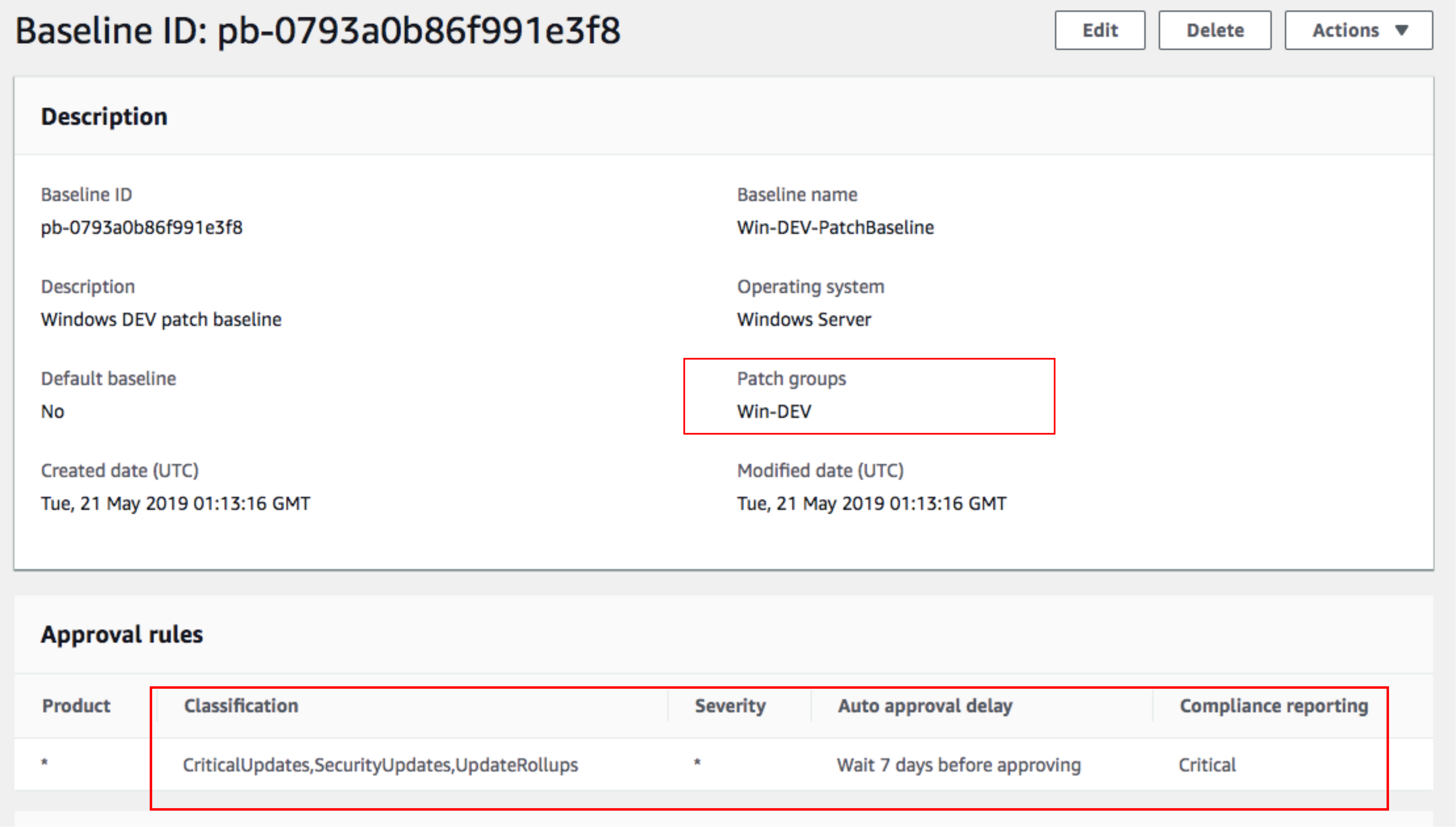
UAT

- Critical Updates
- Roll Up patches
- Wait 21 days before approving

Prod

- Critical Updates
- Roll Up patches
- Wait 28 days before approving

2. Create a Patch Baseline for each set of Patch Groups



Baseline ID: pb-0793a0b86f991e3f8

Description

Baseline ID
pb-0793a0b86f991e3f8

Baseline name
Win-DEV-PatchBaseline

Description
Windows DEV patch baseline

Operating system
Windows Server

Default baseline
No

Patch groups
Win-DEV

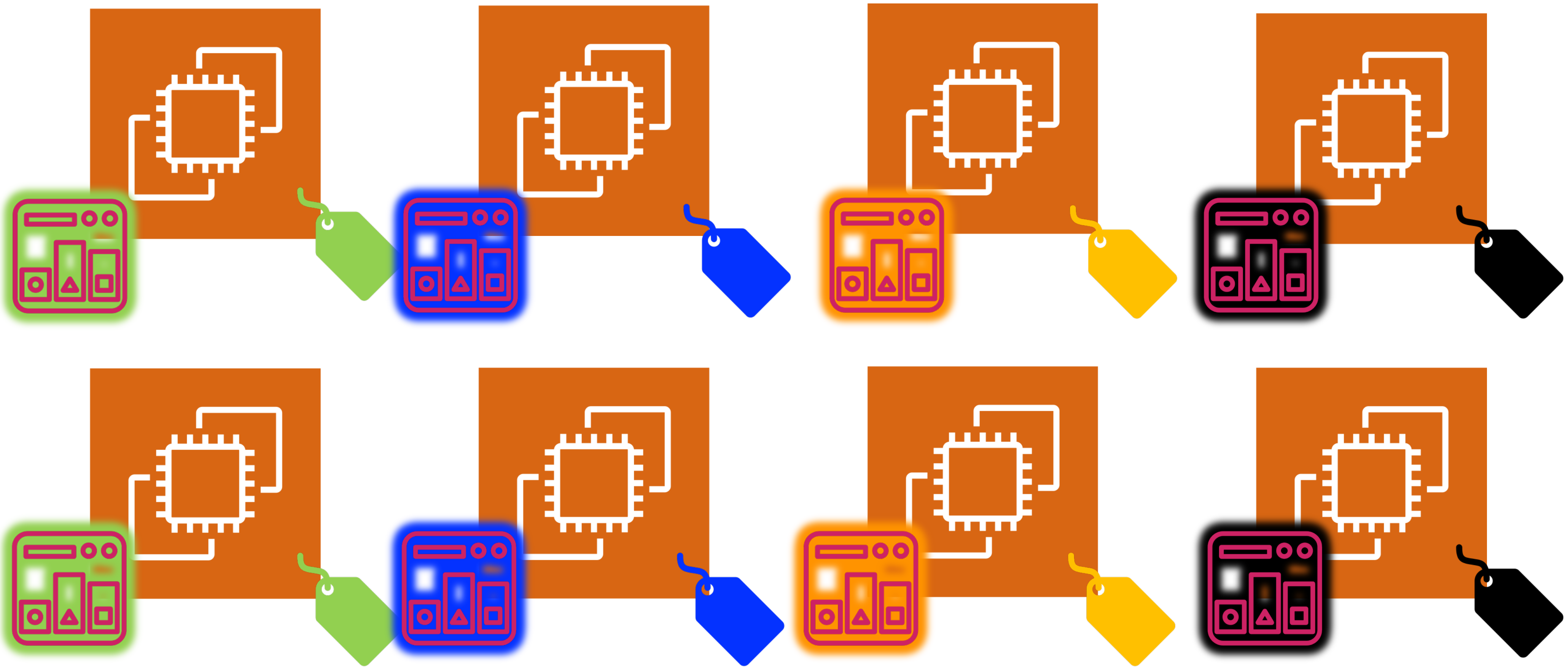
Created date (UTC)
Tue, 21 May 2019 01:13:16 GMT

Modified date (UTC)
Tue, 21 May 2019 01:13:16 GMT

Approval rules

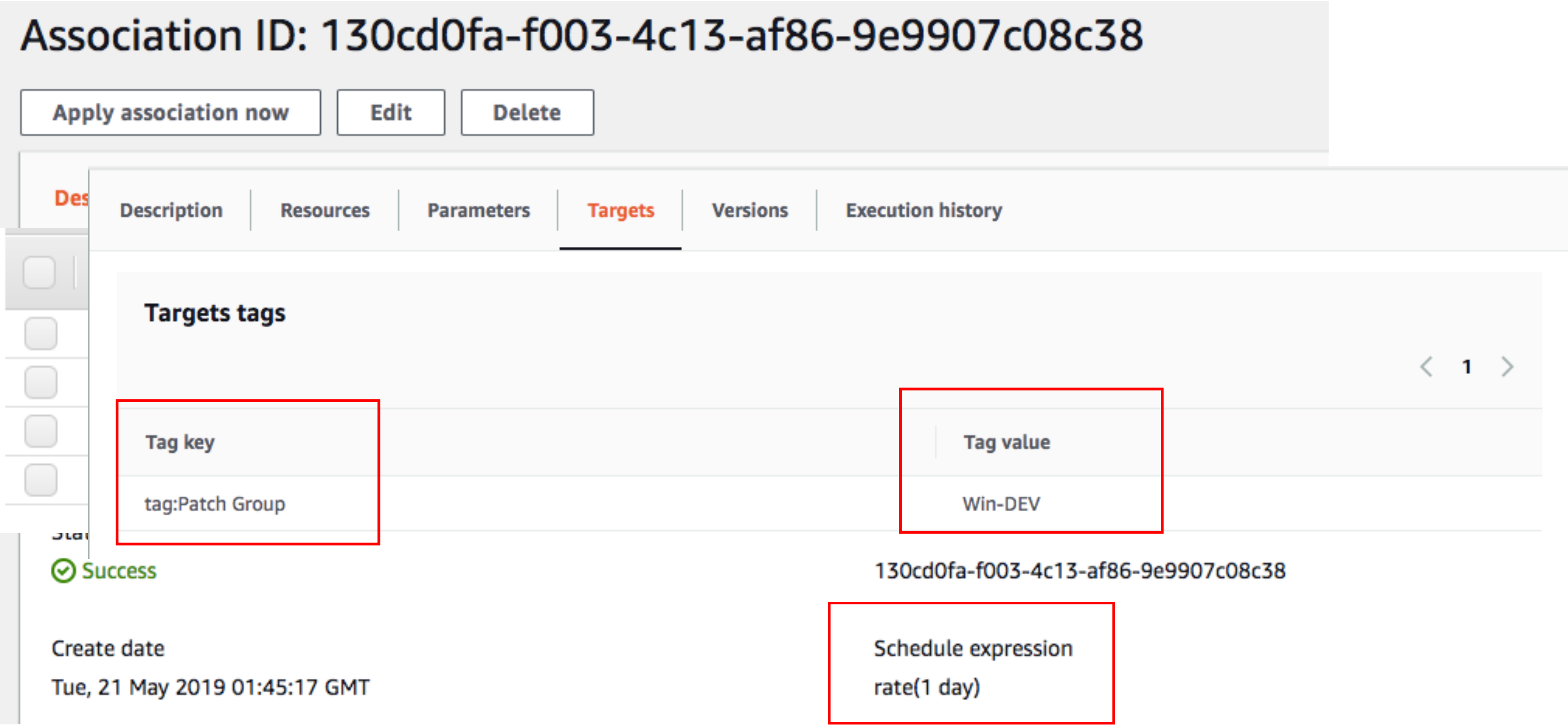
Product	Classification	Severity	Auto approval delay	Compliance reporting
*	CriticalUpdates,SecurityUpdates,UpdateRollups	*	Wait 7 days before approving	Critical

3a. Create Association to schedule periodic scans for compliance



Patch Group	Value
🟩	Dev
🟦	QA
🟨	UAT
⬛	Prod

3a. Create Association to check patch status against the baseline



Association ID: 130cd0fa-f003-4c13-af86-9e9907c08c38

Targets tags

Tag key	Tag value
tag:Patch Group	Win-DEV

Stat

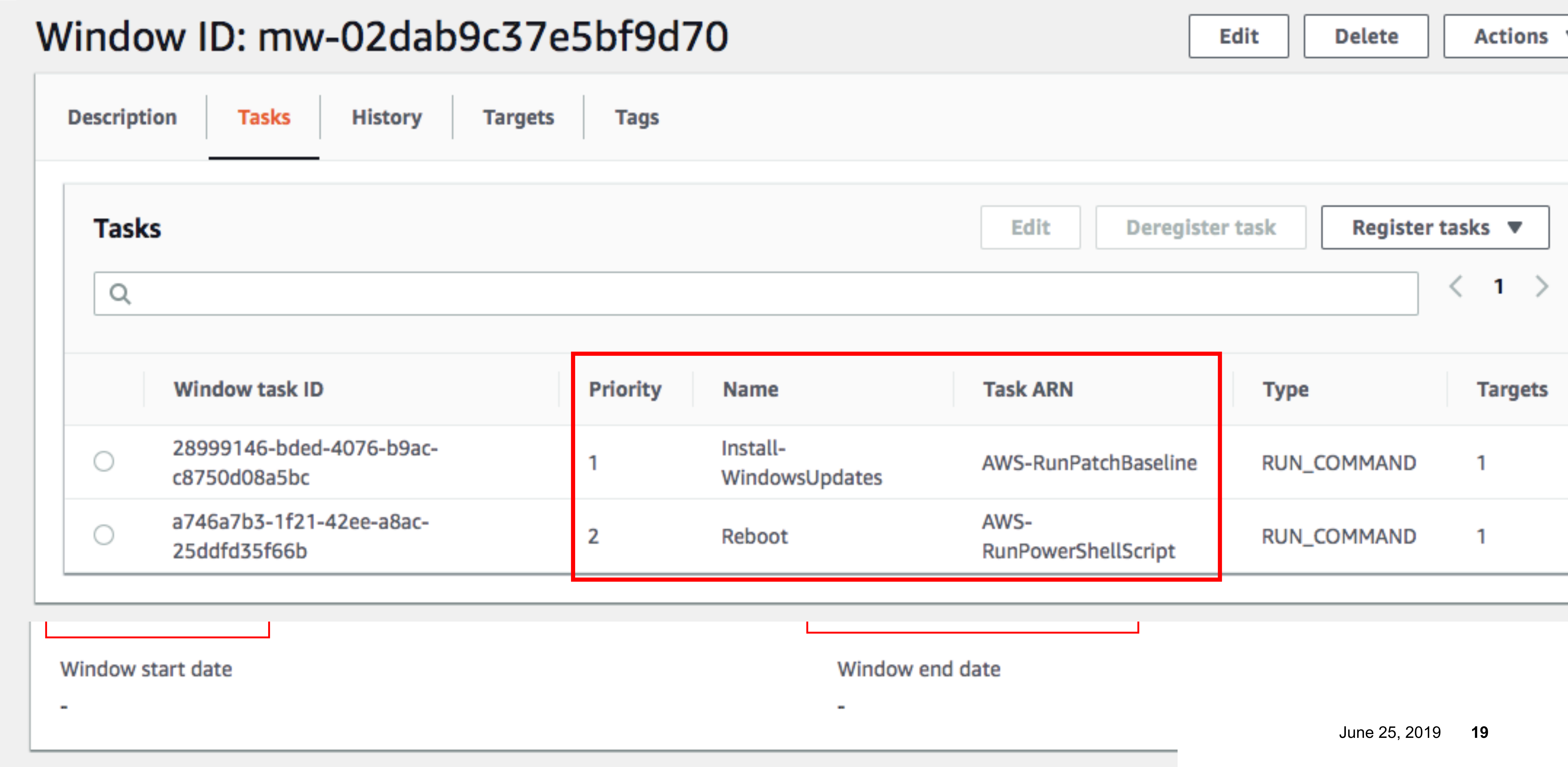
✓ Success

130cd0fa-f003-4c13-af86-9e9907c08c38

Create date
Tue, 21 May 2019 01:45:17 GMT

Schedule expression
rate(1 day)

4. Create a Maintenance Window to Schedule patching



Window ID: mw-02dab9c37e5bf9d70

Tasks

	Window task ID	Priority	Name	Task ARN	Type	Targets
○	28999146-bded-4076-b9ac-c8750d08a5bc	1	Install-WindowsUpdates	AWS-RunPatchBaseline	RUN_COMMAND	1
○	a746a7b3-1f21-42ee-a8ac-25ddfd35f66b	2	Reboot	AWS-RunPowerShellScript	RUN_COMMAND	1

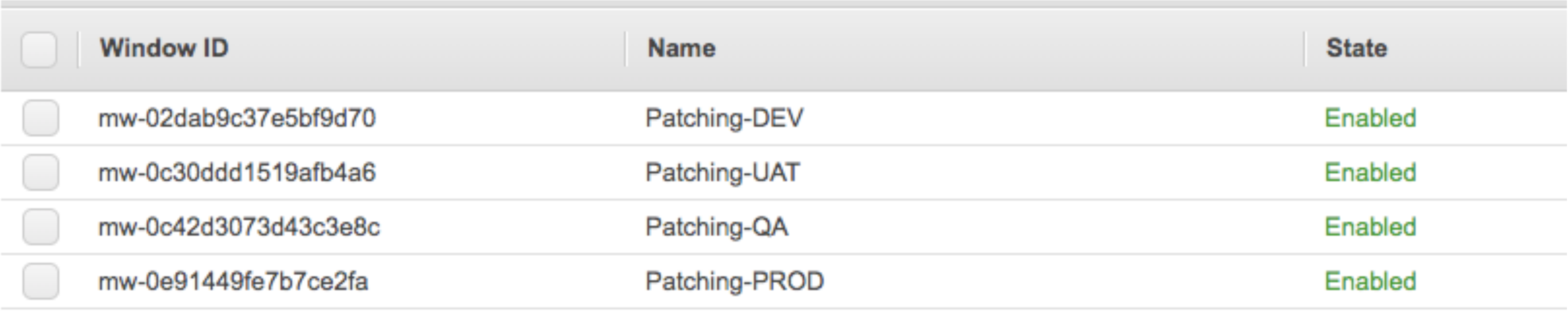
Window start date

-

Window end date

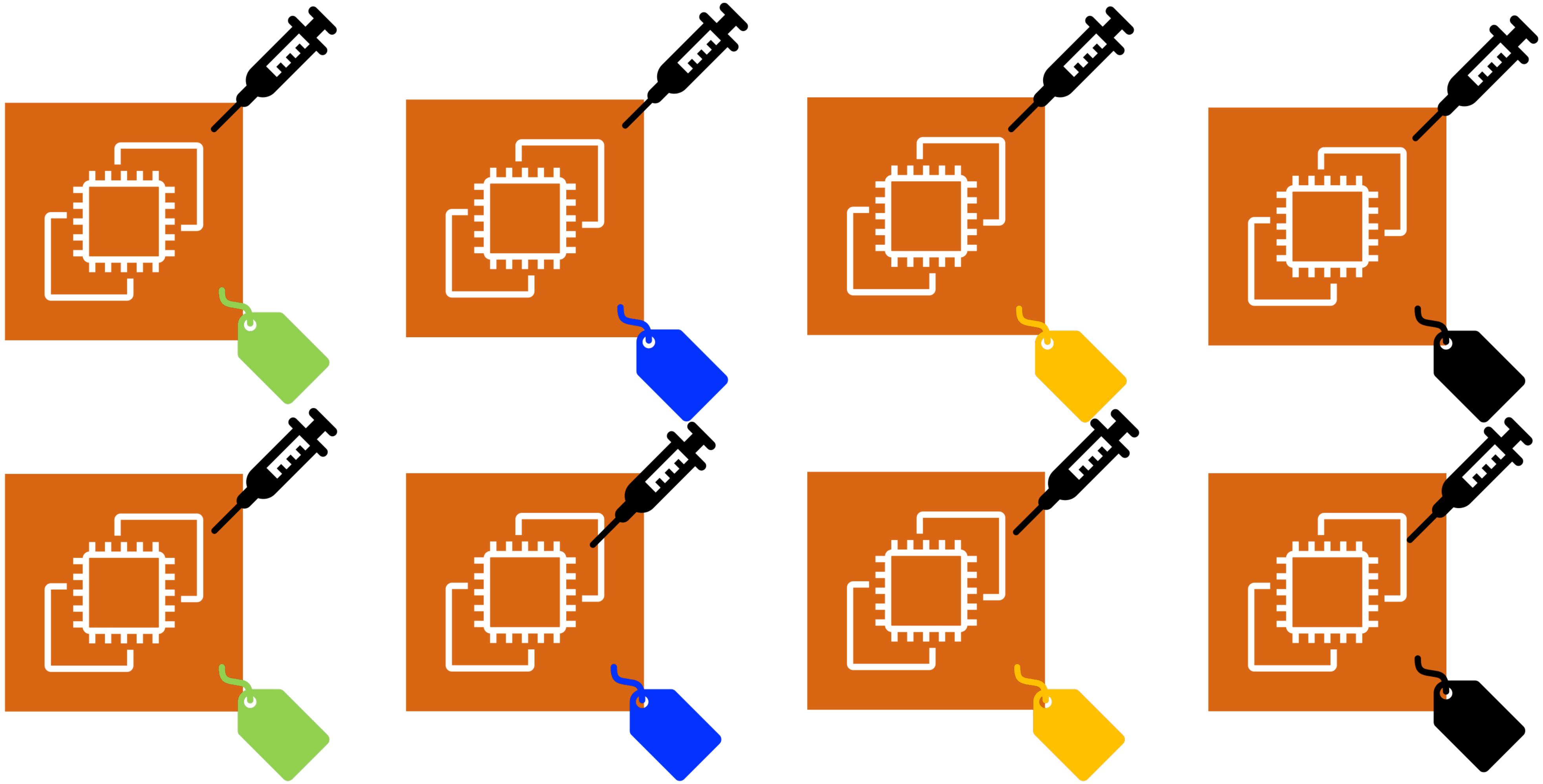
-

4b Create Maintenance Windows for all environments



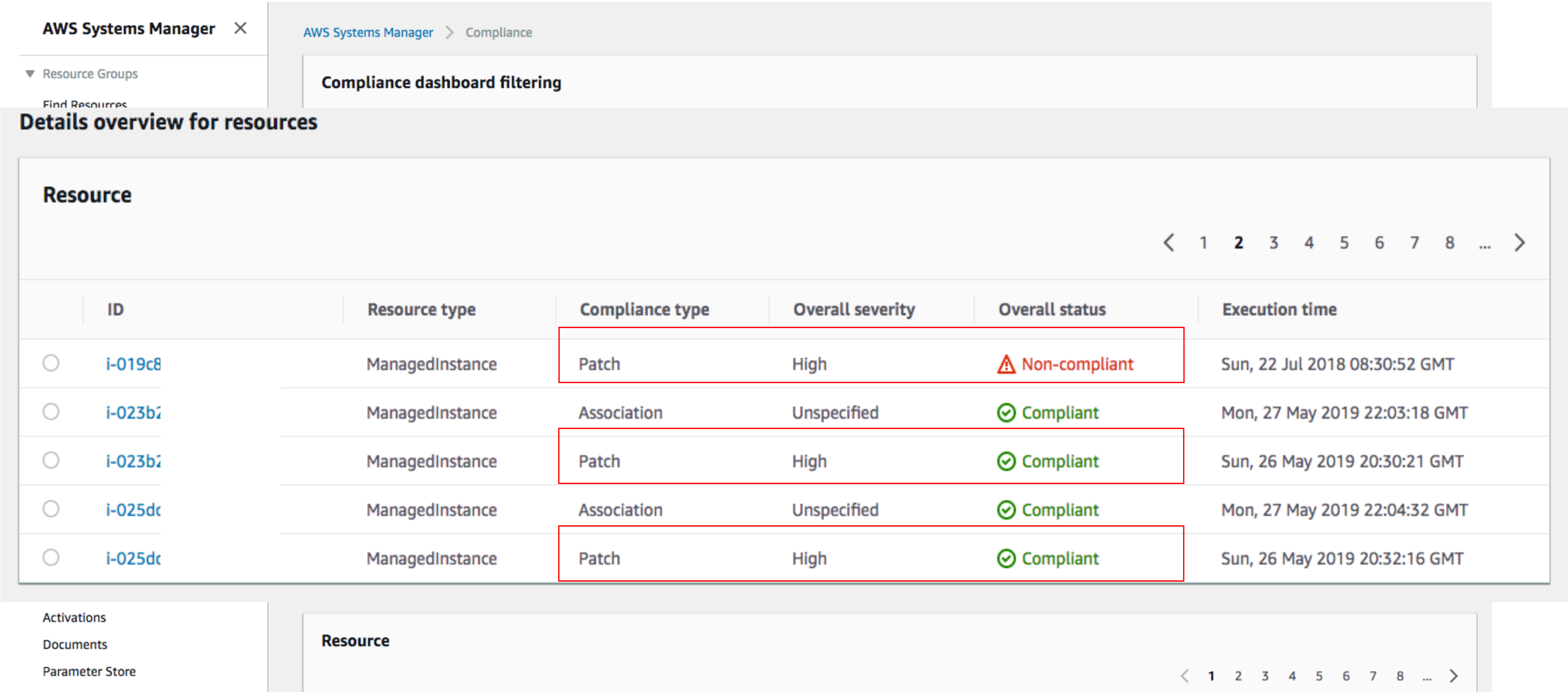
□	Window ID	Name	State
□	mw-02dab9c37e5bf9d70	Patching-DEV	Enabled
□	mw-0c30ddd1519afb4a6	Patching-UAT	Enabled
□	mw-0c42d3073d43c3e8c	Patching-QA	Enabled
□	mw-0e91449fe7b7ce2fa	Patching-PROD	Enabled

Set Maintenance Windows (example)



Patch Group	MW
Dev	1st Week
QA	2nd Week
UAT	3rd Week
Prod	4th Week

Patch Compliance



AWS Systems Manager ×

▼ Resource Groups

Find Resources

AWS Systems Manager > Compliance

Compliance dashboard filtering

Details overview for resources

Resource

< 1 **2** 3 4 5 6 7 8 ... >

	ID	Resource type	Compliance type	Overall severity	Overall status	Execution time
○	i-019c8	ManagedInstance	Patch	High	⚠ Non-compliant	Sun, 22 Jul 2018 08:30:52 GMT
○	i-023b2	ManagedInstance	Association	Unspecified	✓ Compliant	Mon, 27 May 2019 22:03:18 GMT
○	i-023b2	ManagedInstance	Patch	High	✓ Compliant	Sun, 26 May 2019 20:30:21 GMT
○	i-025dc	ManagedInstance	Association	Unspecified	✓ Compliant	Mon, 27 May 2019 22:04:32 GMT
○	i-025dc	ManagedInstance	Patch	High	✓ Compliant	Sun, 26 May 2019 20:32:16 GMT

Activations

Documents

Parameter Store

Resource

< **1** 2 3 4 5 6 7 8 ... >

In Place Patching using AWS Systems Manager

Patch Compliance:

- Tag instances using Patch Group
- Create Patch Baseline and associate it with the Patch Groups
- Create Association to RunPatchBaseline SSM Document with Scan
  - This populates the Patch Compliance Section

Patching:

- Create a SSM Maintenance Window – Defines when your instances are patched
- Run the RunPatchBaseline SSM Document with Install and Reboot as tasks

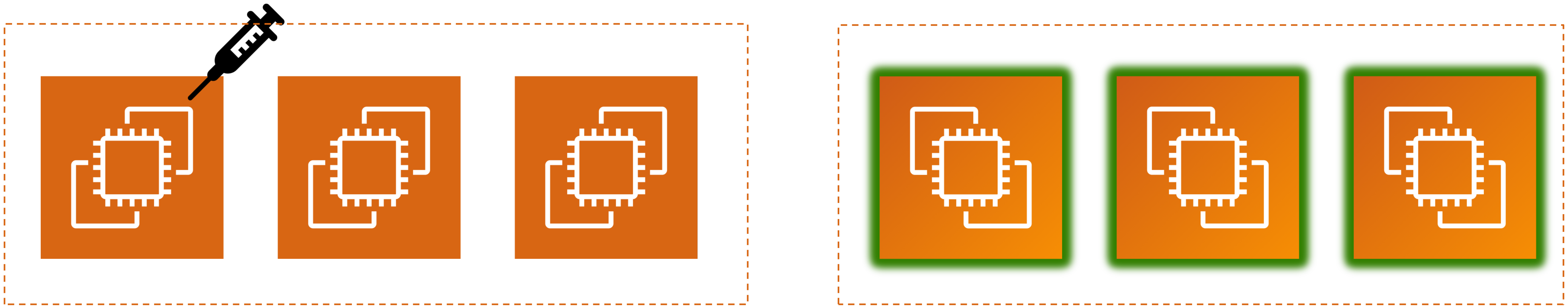
Patching Immutable Servers

What are immutable servers / architectures?

✓ Servers that have no reason to change

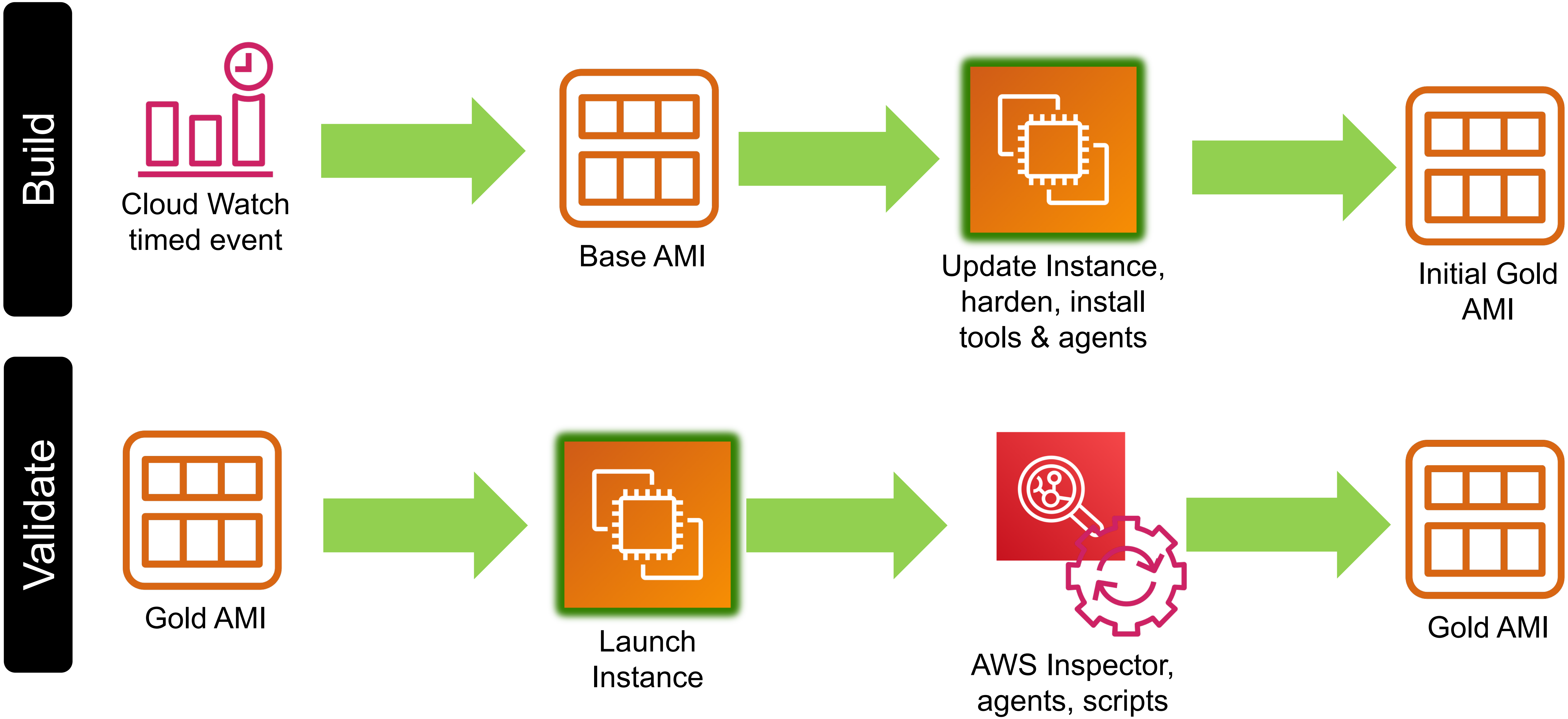
Q. What if its needs to be changed?

A. A new server image needs to be created



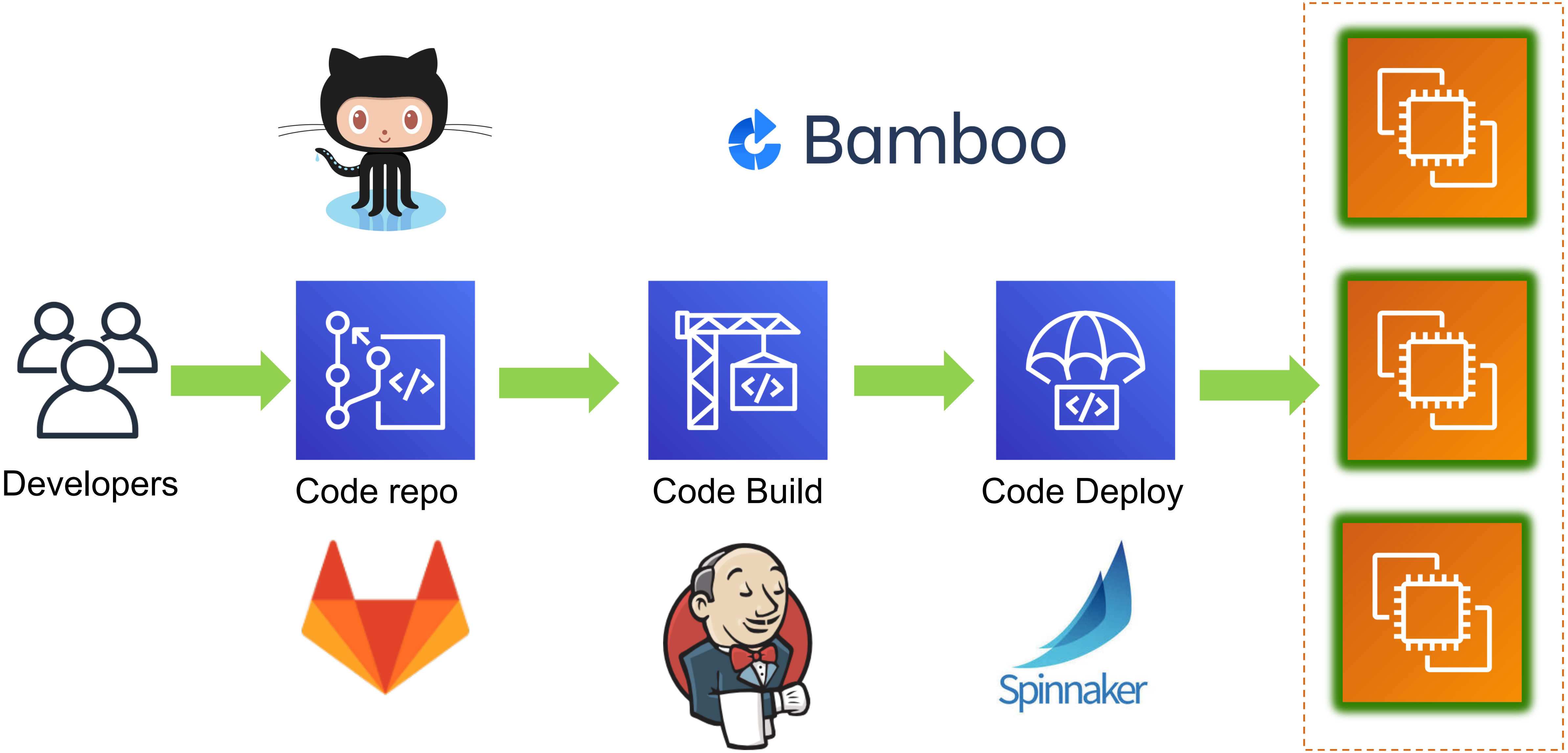
How do you automate patching your AMI?

Create an AMI Baking Pipeline



E.g: https://github.com/aws-samples/aws-golden-ami-pipeline-sample

In real world, a Continuous Deployment pipeline manages the ASGs



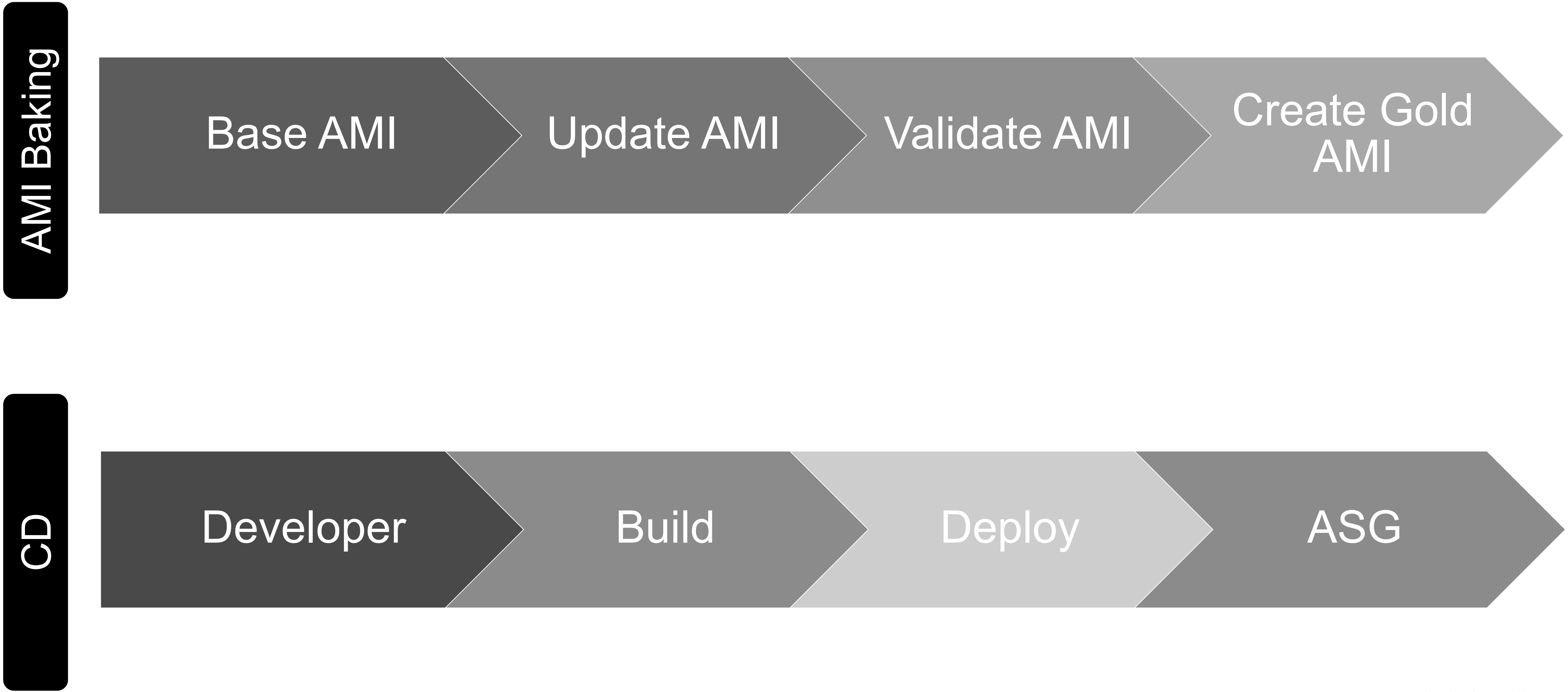
Developers

Code repo

Code Build

Code Deploy

Ensuring your CD Pipeline uses only $latestAmi



June 25, 2019

Step Functions for patching immutable architecture

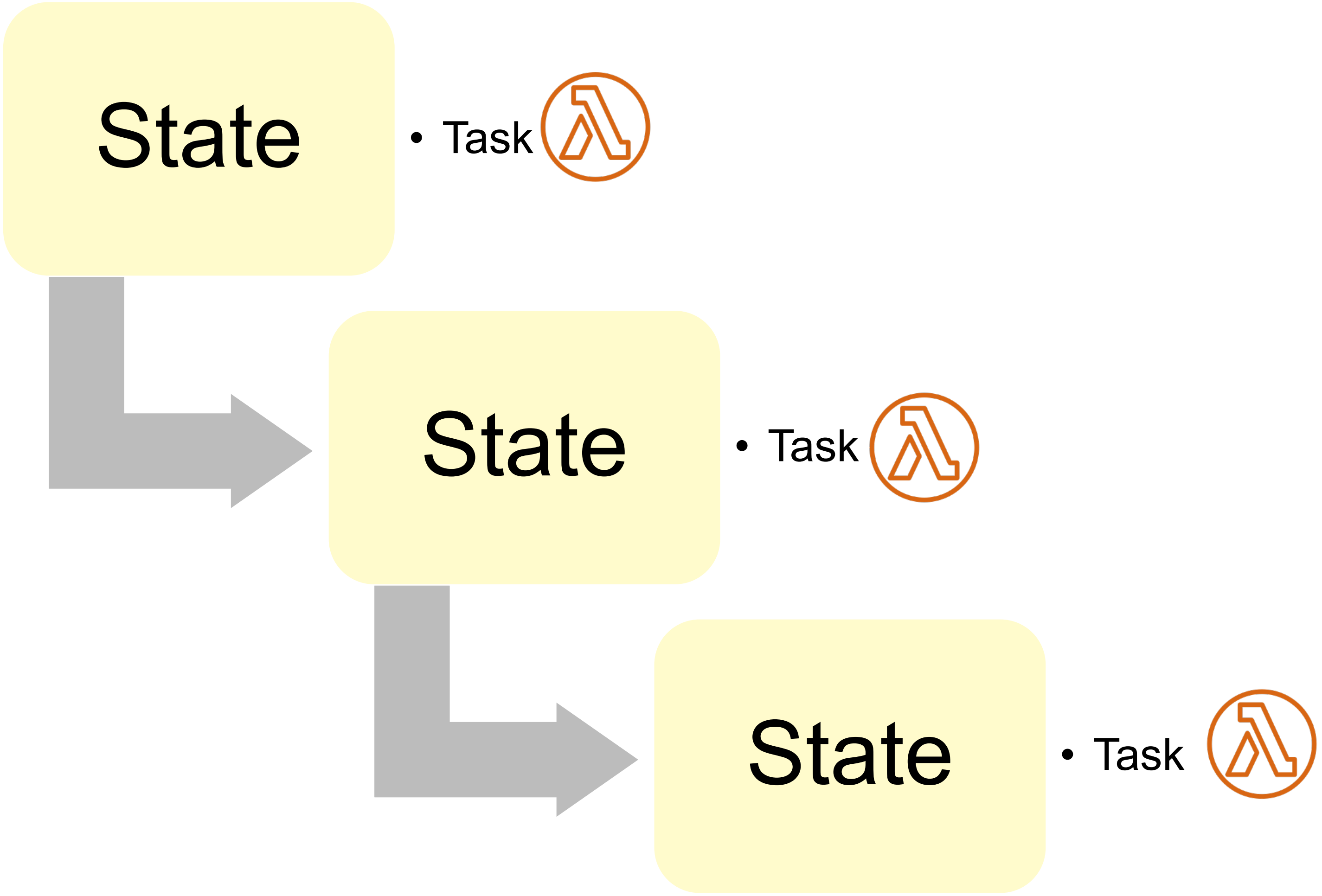
Sudev Kurur
AWS DevOps Engineer

What is AWS Step Functions?

✓ Coordinate multiple AWS services
✓ To produce a desired outcome

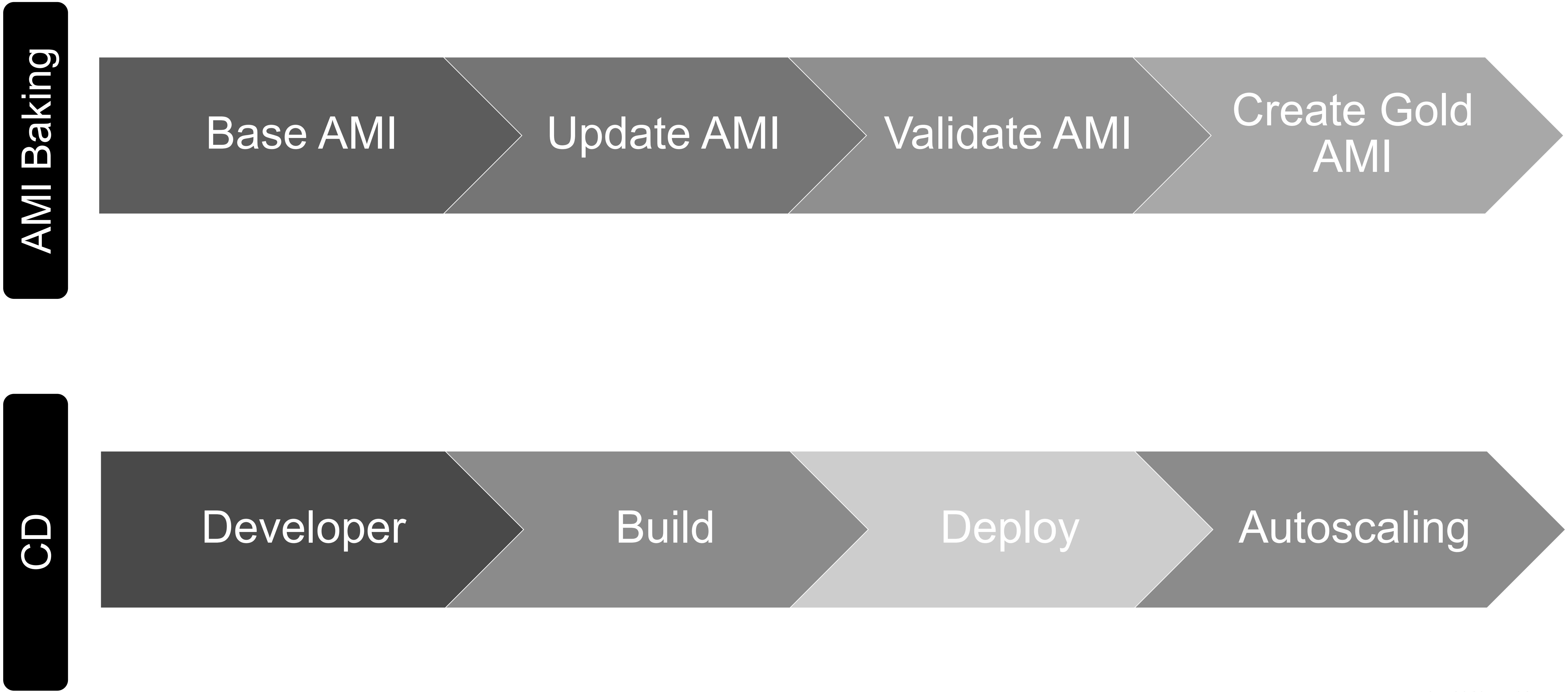
Step functions helps in:

- Sequence functions
- Run functions in parallel
- Select functions based on data
- Retry functions
- Error handling - Try/Catch/Finally
- Code that runs for hours



June 25, 2019

Ensuring your CD Pipeline uses only $latestAmi

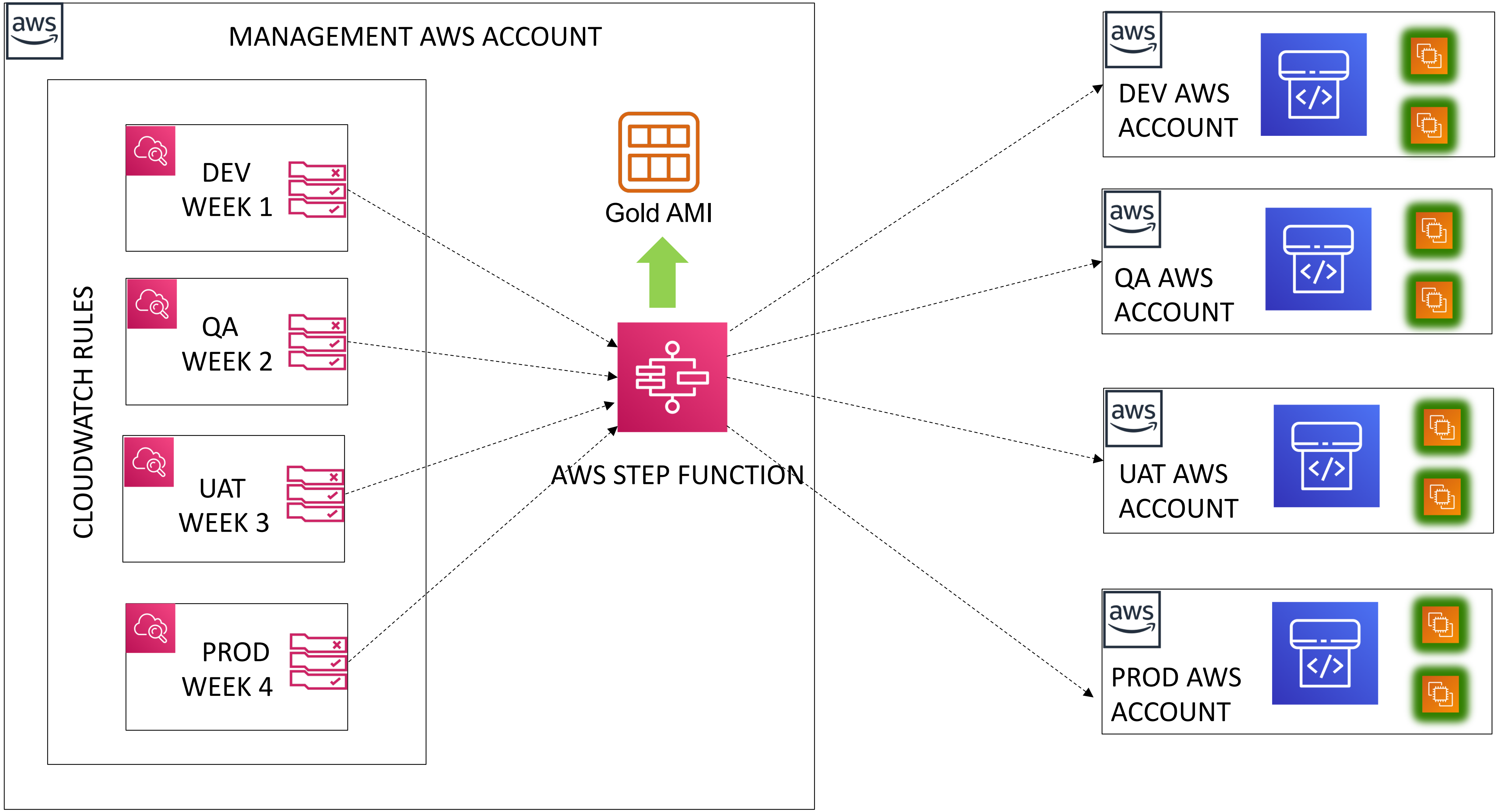


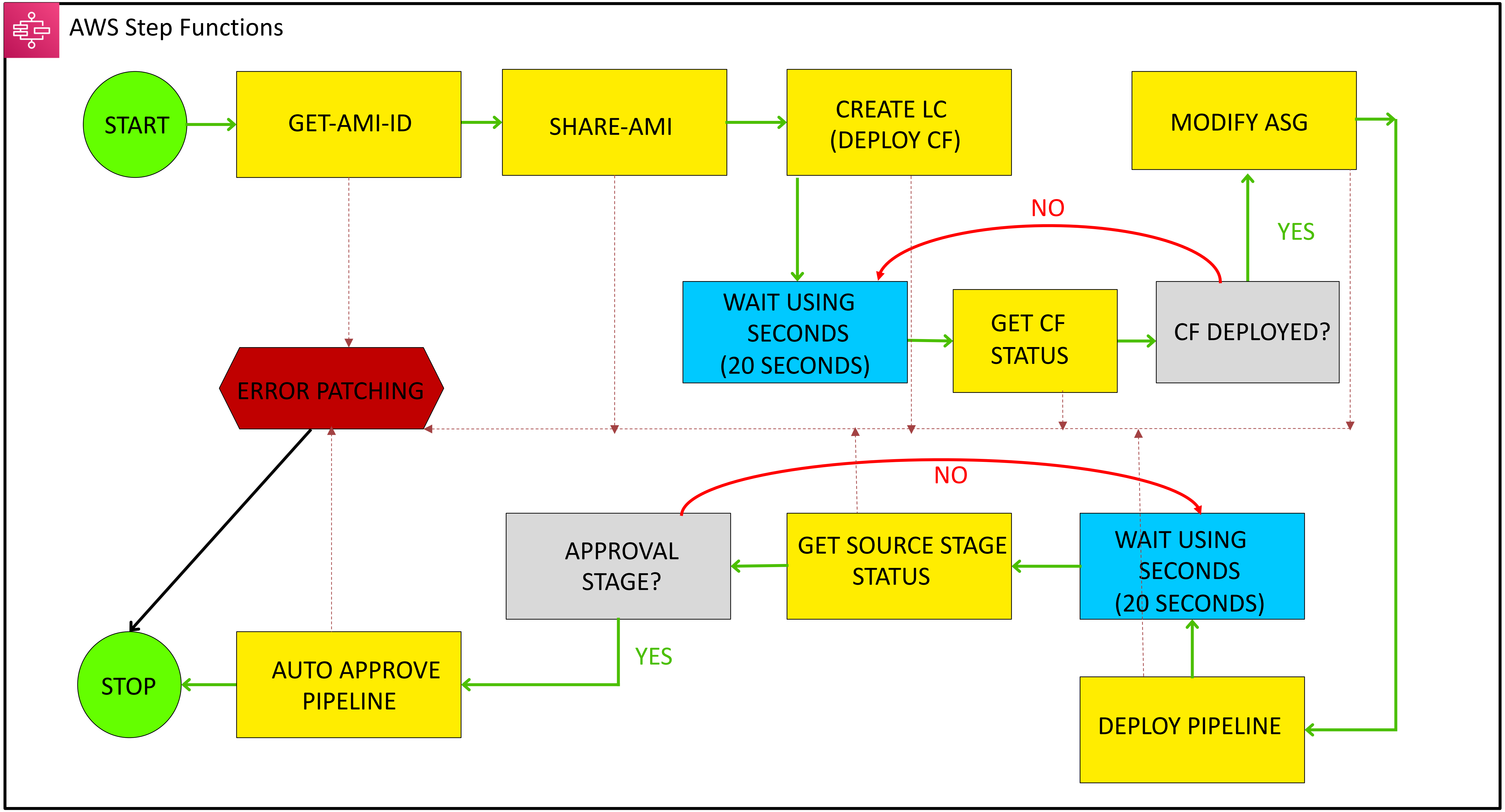
AMI Baking

Base AMI → Update AMI → Validate AMI → Create Gold AMI

CD

Developer → Build → Deploy → Autoscaling


MANAGEMENT AWS ACCOUNT
CLOUDWATCH RULES
DEV WEEK 1
QA WEEK 2
UAT WEEK 3
PROD WEEK 4
Gold AMI
AWS STEP FUNCTION
DEV AWS ACCOUNT
QA AWS ACCOUNT
UAT AWS ACCOUNT
PROD AWS ACCOUNT


AWS Step Functions
START
GET-AMI-ID
SHARE-AMI
CREATE LC (DEPLOY CF)
MODIFY ASG
NO
YES
WAIT USING SECONDS (20 SECONDS)
GET CF STATUS
CF DEPLOYED?
ERROR PATCHING
NO
APPROVAL STAGE?
GET SOURCE STAGE STATUS
WAIT USING SECONDS (20 SECONDS)
YES
STOP
AUTO APPROVE PIPELINE
DEPLOY PIPELINE

Demo

Life of your EC2 instance and patch approach

Situation	EC2 Pricing Model	Life expectancy	Example	Patching approach
Monolithic Workloads	RI / On-demand	Long term	Traditional Monolithic Application	In-place
CI CD Workloads	RI / On-demand	Short to Long term	DevOps Workloads	AMI Baking Pipeline
Short term compute operations	Spot instance	Short Term	Fault tolerant and Flexible Application	AMI Baking Pipeline / Latest Image

EC2 Patch Management - Endgame

- Rapid developments mean more possibility of new flaws
- Patching is more important today than ever before
- There is no one size fits all for patch management
- Reduce your blast radius at all times
- If you can’t patch, destroy your server

Questions?

Thank you.