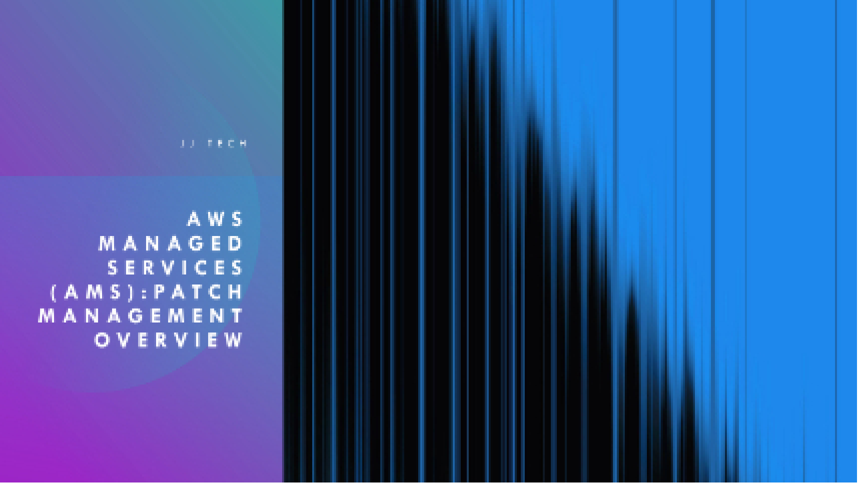

JJ TECH

AWS MANAGED SERVICES (AMS):PATCH MANAGEMENT OVERVIEW

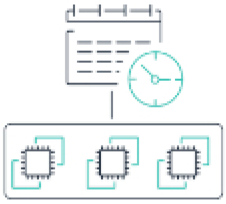
AMS TAG-BASED PATCH MANAGEMENT PROCESS

What is tag-based patching?

- A tag-based patching model allows you to use tags to apply your patch configuration to a precise set of resources, called a patch group, ranging from one instance to all instances.
- Patches are installed during the patch windows and defined using the AMS console, AMS API, or the AMS Command Line Interface (AMS CLI). After patches are installed on an instance, it is rebooted. Patch notifications are sent before and after patching.

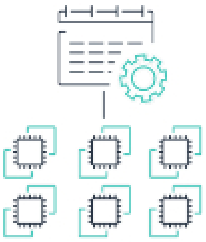
WHAT IS A PATCH WINDOW?

- A *patch window* is a scheduled time interval when patches are installed to a patch group. When a patch window is created for a patch group, those instances are no longer part of the default maintenance window. Instances that are not part of an explicit patch window are patched during the default maintenance window.



WHAT IS THE DEFAULT MAINTENANCE WINDOW?

- Instances that are not part of an explicit patch window are patched during the default maintenance window. You define this when you set up your other tag-based patching windows.



A patch window can be assigned during instance creation if you have decided to enable the auto-tagging feature but can also be done using the console if you have Developer Mode.

NOTE

BEST PRACTICES

Consider the following as you build your patching strategy.

NUMBER OF INSTANCES

- If multiple patch maintenance windows are scheduled to run at the same time, they must have fewer than 1,001 instances being processed at any given time. This is an AWS Systems Manager limitation. AMS recommends at least 1 hour per every 50 instances.

OPERATING SYSTEMS

- Be mindful of completion times for different operating systems when setting cutoffs. For example, a Windows instance takes on average 1.5 hours to complete, whereas a Linux instance will take on average 1 hour.

MAX CONCURRENCY

- AMS has a maximum number of concurrently executing automations of 25. Consider setting the max concurrency to 100 percent to maximize the number of instances that are being patched at one time.

AWS SMS TOPIC NOTIFICATIONS

- Up to five email addresses can subscribe to topic notifications for AWS Server Migration Service (AWS SMS) maintenance windows. Consider using email groups rather than individual email addresses to ensure the best communication.

WHAT ARE ON-DEMAND PATCHES AND DEFAULT PATCH BASELINE?

- Customers can run a patch for instances on demand by using an AMS change type. For example, if a customer requires a one-off patch on a patch group that normally is maintained the third Thursday at 2 AM, they can schedule a maintenance window with a start date and an end date while leaving the existing maintenance window in place. The on-demand patch window will run along with the other maintenance window until the end date of the on-demand patch.
- AMS default patch baseline will install critical and important security patches, as well as critical OS patches. Custom patch baseline can add or limit those default settings and also add exclusions or allowances.

LEGACY AMS PATCH MANAGEMENT PROCESS

- **How does standard patching happen in the legacy AMS patch management process?**

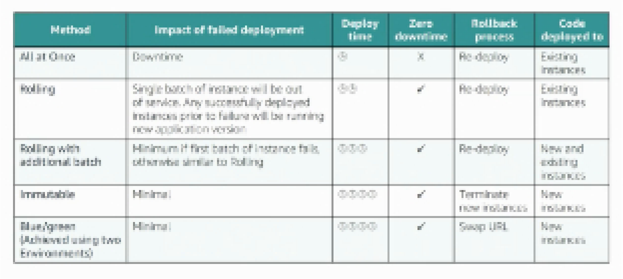
- **Mutable**
  - Standard patching occurs on the agreed-to patch schedule and includes regular patch updates that are not deemed critical.
- **Immutable**
  - Every month, AMS releases new AMIs with service improvements and applicable patches. This new AMI will be referenced in the Amazon EC2 Auto Scaling group during the agreed-to patch schedule.

WHAT ARE THE DIFFERENT PATCH TYPES FOR THE LEGACY AMS PATCH MANAGEMENT PROCESS?

- **Critical patches**
  - When an OS vendor releases a critical security update, we notify the customer within 8-10 days through a service notification.
- **Important patches**
  - When an OS vendor releases a critical security update, we notify the customer within 2 months through a service notification.

WHY IS PATCH MANAGEMENT IMPORTANT?

- Patch management is a critical part of keeping customer environments safe and secure. You can likely think of a company that was recently in the news for a major data breach caused by the company's failure to patch a critical vulnerability. AMS works with customers to schedule patch updates to infrastructure on a regular cadence for standard patching. For critical patching, AMS schedules a patch update within 14 days after notifying the customer.



Method	Impact of failed deployment	Deploy time	Zero downtime	Rollback process	Code deployed to
All at Once	Downtime	🕒	X	Re-deploy	Existing instances
Rolling	Single batch of instance will be out of service. Any successfully deployed instances prior to failure will be running new application version	🕒🕒	✓	Re-deploy	Existing instances
Rolling with additional batch	Minimum if first batch of instance fails, otherwise similar to Rolling	🕒🕒🕒	✓	Re-deploy	New and existing instances
Immutable	Minimal	🕒🕒🕒🕒	✓	Terminate new instances	New instances
Blue/green (Achieved using two Environments)	Minimal	🕒🕒🕒🕒	✓	Swap URL	New instances