Patching - Strategy

Using the AWS Systems Manager service,

Approach: OS-based Patching

- Tag each instance based on its environment and OS.
- Create a patch baseline in AWS Systems Manager Patch Manager for each environment.
- Categorize EC2 instances based on their tags using Patch Groups and apply the patches specified in the corresponding patch baseline to each Patch Group.

Approach: ZERO down-time

This is to avoid any loss of revenue that could be caused by any unavailability issues of their systems.

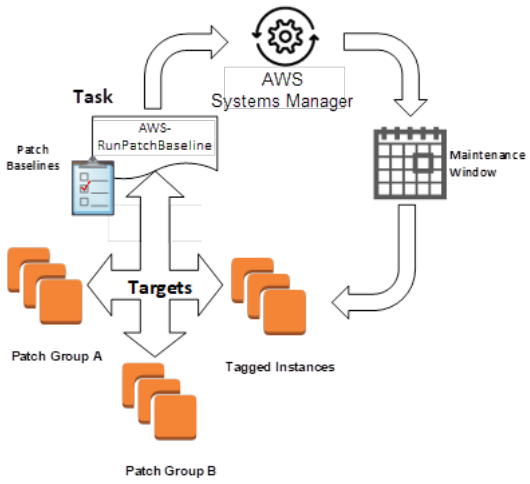
- Create two Patch Groups with unique tags that you will assign to all of your EC2 Windows Instances.
- Associate the predefined AWS-DefaultPatchBaseline baseline on both patch groups.
- Set up two non-overlapping maintenance windows and associate each with a different patch group.
- Using Patch Group tags, register targets with specific maintenance windows and lastly, assign the AWS-RunPatchBaseline document as a task within each maintenance window which has a different processing start time.

AWS Systems Manager Patch Manager automates the process of patching managed instances with security-related updates. For Linux-based instances, you can also install patches for non-security updates.

You can patch fleets of Amazon EC2 instances or your on-premises servers and virtual machines (VMs) by operating system type. This includes supported versions of Windows Server, Ubuntu Server, Red Hat Enterprise Linux (RHEL), SUSE Linux Enterprise Server (SLES), CentOS, Amazon Linux, and Amazon Linux 2. You can scan instances to see only a report of missing patches, or you can scan and automatically install all missing patches.

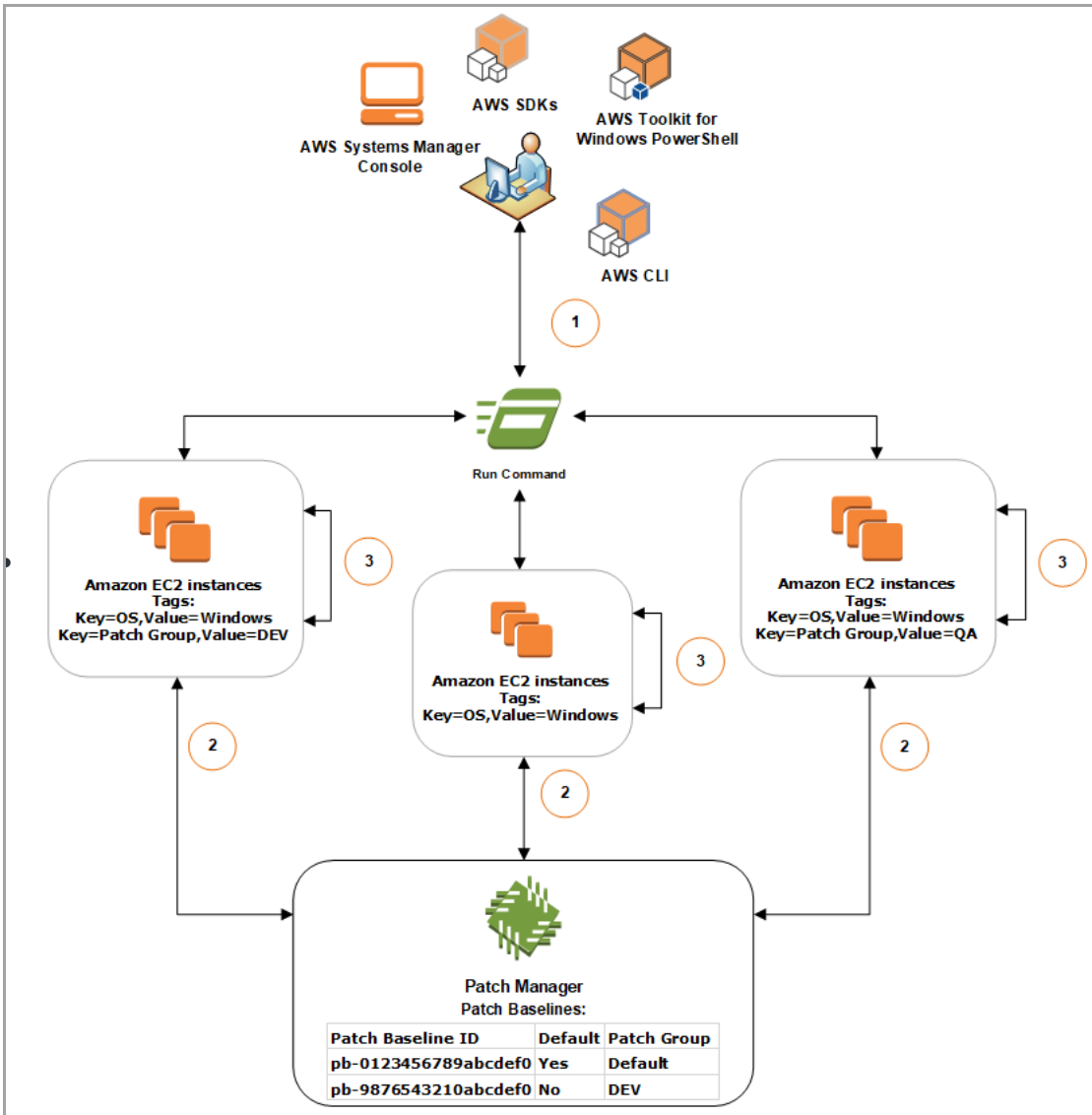
Patch baseline

- *Patch Manager* uses ***patch baselines,*** which include rules for auto-approving patches within days of their release, as well as 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 instances by using Amazon EC2 tags.
- For each auto-approval rule that you create, you can specify an auto-approval delay.
- This delay is the number of days to wait after the patch was released, before the patch is automatically approved for patching.



Patch group

- You can use a *patch group* to associate instances with a specific patch baseline. A *patch group* is an optional means of organizing instances for patching.
- Patch groups help ensure that you are deploying the appropriate patches, based on the associated patch baseline rules, to the correct set of instances.
- 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.
- For example, you can create patch groups for different operating systems (Linux or Windows), different environments (Development, Test, and Production), or different server functions (web servers, file servers, databases).
- Patch groups can help you avoid deploying patches to the wrong set of instances.
- They can also help you avoid deploying patches before they have been adequately tested. You create a patch group by using Amazon EC2 tags.
- Unlike other tagging scenarios across Systems Manager, a patch group must be defined with the tag key: **Patch Group**.
- After you create a patch group and tag instances, you can register the patch group with a patch baseline. By registering the patch group with a patch baseline, you ensure that the correct patches are installed during the patching execution.



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

You create a patch group by using Amazon EC2 tags. Unlike other tagging scenarios across Systems Manager, a patch group *must* be defined with the tag key: **Patch Group**. Note that the key is case-sensitive. You can specify any value, for example, "web servers," but the key must be **Patch Group**.

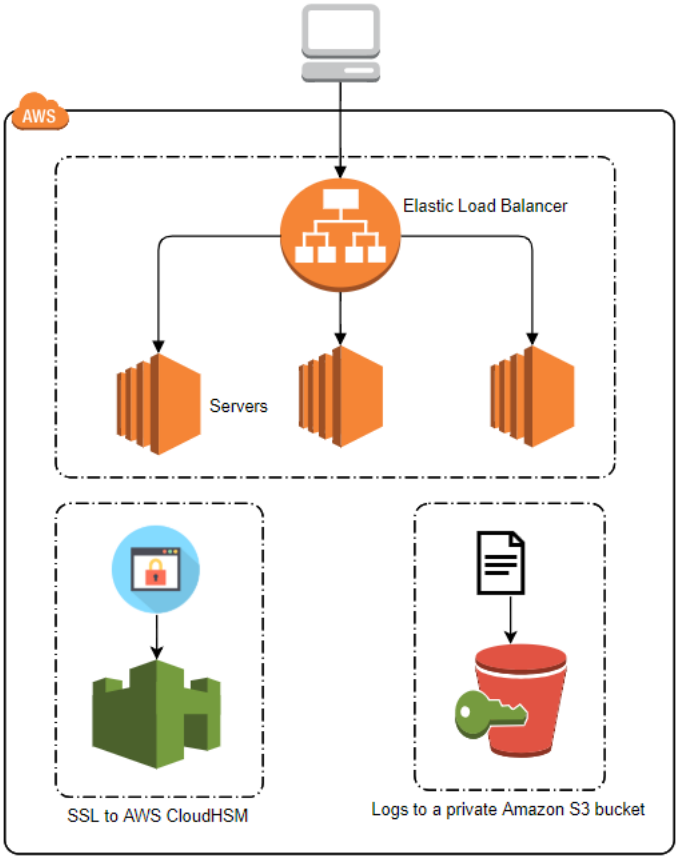
The AWS-DefaultPatchBaseline baseline is primarily used to approve all Windows Server operating system patches that are classified as "CriticalUpdates" or "SecurityUpdates" and that have an MSRC severity of "Critical" or "Important". Patches are auto-approved seven days after release.

SSL - Store/Automation

Cloud HSM

AWS CloudHSM is a cloud-based hardware security module (HSM) that enables you to easily generate and use your own encryption keys on the AWS Cloud.

With CloudHSM, you can manage your own encryption keys and automate time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.



The option that says:

Distribute traffic to a set of web servers using an Elastic Load Balancer that performs TCP load balancing. Use CloudHSM deployed to two Availability Zones to perform the SSL transactions and deliver your application logs to a private Amazon S3 bucket using server-side encryption is correct because it uses CloudHSM for performing the SSL transaction without requiring any additional way of storing or managing the SSL private key.

This is the most secure way of ensuring that the key will not be moved outside of the AWS environment. Also, it uses the highly available and durable S3 service for storing the logs. Take note that this option says "*server-side encryption*" and not "*Amazon S3-Managed Encryption Keys*", which are two different things.

DB - Backup and Recovery

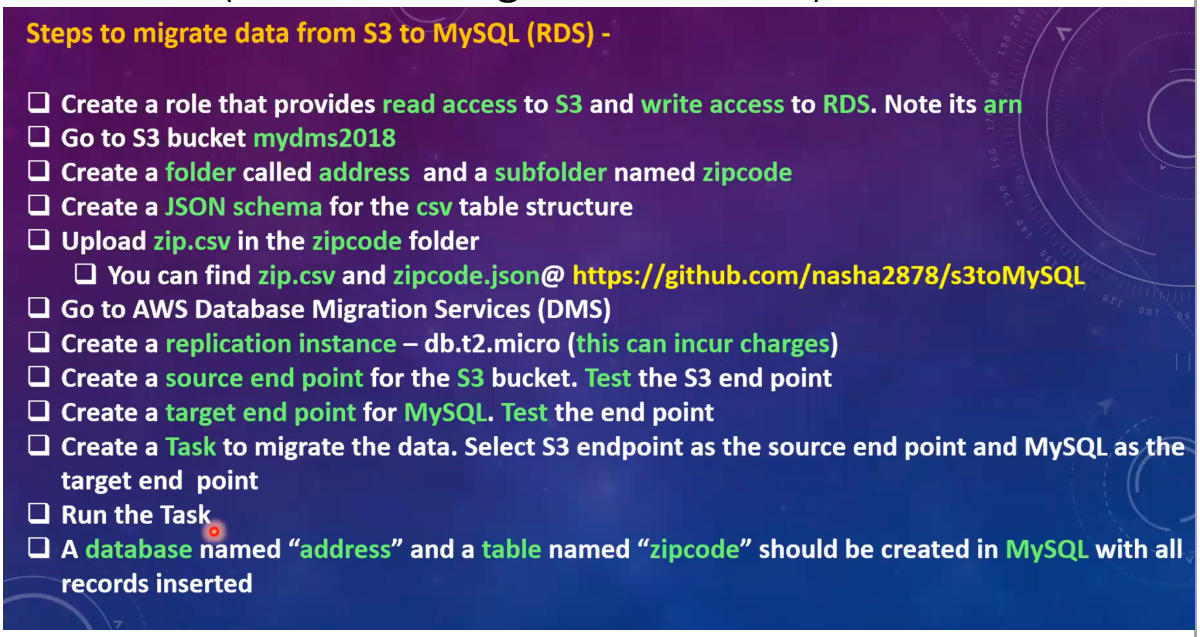
Oracle RMAN

Recovery Manager (RMAN) is an Oracle Database client that performs backup and recovery tasks on your databases and automates administration of your backup strategies. It greatly simplifies backing up, restoring, and recovering database files.

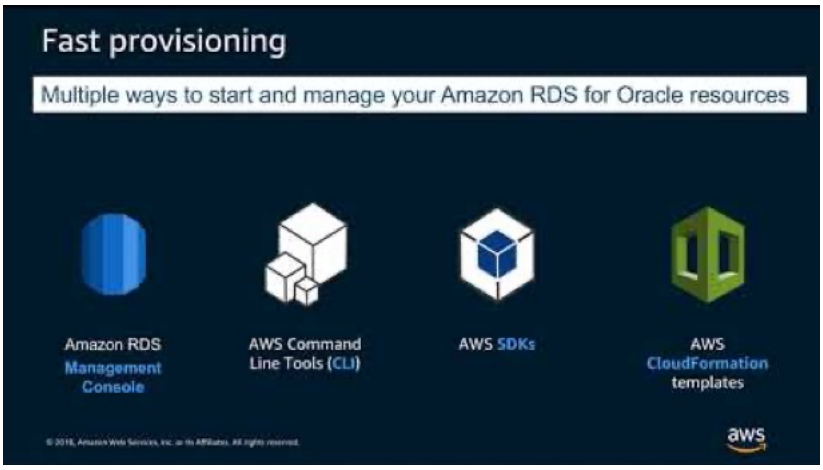
The option that says: ***Provision EC2 servers for both your JBoss application and Oracle database, and then restore the database backups from an S3 bucket. Also provision an EBS volume containing static content obtained from Storage Gateway, and attach the volume to the JBoss EC2 server*** is correct because it deploys the Oracle database on an EC2 instance by restoring the backups from S3 which can provide a faster recovery time, and it generates the EBS volume of static content from Storage Gateway.

https://aws.amazon.com/backup-recovery/gsg-oracle-rman/

DB - DMS (database migration service)



Best Practices for Migrating Oracle Databases to the Cloud - AWS Online Tech Talks



[Amazon RDS Snapshot Export to S3]

[AWS RDS SQL Server Database Restore using S3]