Systems Hardening with Patch Manager via AWS Systems Manager

Lab overview

In organizations with hundreds and often thousands of workstations, it can be logistically challenging to keep all the operating system (OS) and application software up to date. In most cases, OS updates on workstations can be automatically applied via the network. However, administrators must have a clear security policy and baseline plan to ensure that all workstations are running a certain minimum version of software.

In this lab, you use Patch Manager, a capability of AWS Systems Manager, to create a patch baseline. You then use the patch baseline that you created to scan the Amazon Elastic Compute Cloud (Amazon EC2) instances for Linux and Windows that were pre-created for this lab. You also learn how to create a maintenance window to automate the scanning and patching process.

The primary focus of Patch Manager is to install OS security-related updates on managed nodes.

Objectives

After completing this lab, you should be able to:

- Create a custom patch baseline
- Modify patch groups
- Configure patching
- Schedule a maintenance window
- Perform an instant scan
- Verify patch compliance

Duration

This lab requires approximately **60 minutes** to complete.

Lab environment

The current environment has six EC2 instances: three instances with the Linux OS and three with the Windows OS.

All backend components, such as EC2 instances, AWS Identity and Access Management (IAM) roles, and some AWS services, have been built into your lab already.

Accessing the AWS Management Console

1. At the upper-right corner of these instructions, choose ▶ **Start Lab**

   Troubleshooting tip: If you get an **Access Denied** error, close the error box, and choose ▶ **Start Lab** again.

2. The following information indicates the lab status:
   - A red circle next to **AWS** 🔴 at the upper-left corner of this page indicates that the lab has not been started.
   - A yellow circle next to **AWS** 🟡 at the upper-left corner of this page indicates that the lab is starting.
   - A green circle next to **AWS** 🟢 at the upper-left corner of this page indicates that the lab is ready.

Wait for the lab to be ready before proceeding.

3. At the top of these instructions, choose the green circle next to **AWS** ●

   This option opens the AWS Management Console in a new browser tab. The system automatically sign you in.

   Tip: If a new browser tab does not open, a banner or icon at the top of your browser might indicate that your browser is preventing the site from opening pop-up windows. Choose the banner or icon, and choose **Allow pop-ups**.

4. If you see a dialog prompting you to switch to the new console home, choose **Switch to the new Console Home**.
5. Arrange the AWS Management Console tab so that it displays along side these instructions. Ideally, you should be able to see both browser tabs at the same time so that you can follow the lab steps.

   ⚠ **Do not change the lab Region unless specifically instructed to do so**.

Task 1: Select patch baselines

In this task, you select a patch baseline to apply to the Linux EC2 instances. You then create a custom patch baseline for the Windows server EC2 instances.

Patch Manager provides predefined patch baselines for each of the operating systems that it supports. You can use these baselines as they are currently configured (you can't customize them), or you can create your own custom patch baselines. You can use custom patch baselines for greater control over which patches are approved or rejected for your environment.

6. In the AWS Management Console, in the search 🔍 box, enter `Systems Manager` and select it. This option takes you to the Systems Manager console page.

7. In the left navigation pane, under **Node Management**, choose **Fleet Manager**.
   Here are the pre-configured EC2 instances. There are three Linux instances and three Windows instances. These EC2 instances need a specific IAM role to activate Systems Manager on the instances, which is why you can view them in the Fleet Manager section. This is also part of the lab setup.

8. Select the check box next to **Linux-1**. Then choose the **Node actions** ▾ dropdown list, and choose **View details**.
   Here you can view details about the specific instance, such as **Platform type**, **Node type**, **OS name**, and the **IAM role** that allows you to use Systems Manager.

9. At the top of the page, choose **AWS Systems Manager** to go back to the Systems Manager homepage.
10. In the left navigation pane, under **Node Management**, choose **Patch Manager**.
11. Choose the **View predefined patch baselines** button.
12. Choose the **Patch baselines** tab. This tab includes the default patch baselines that you can select.
13. In the search bar, enter `AWS-AmazonLinux2DefaultPatchBaseline` and press Enter. Then select the radio button ○ next to the baseline that is listed.
14. Choose the **Actions** ▾ dropdown list, and choose **Modify patch groups**.
    ℹ You can use a patch group to associate managed nodes with a specific patch baseline in Patch Manager. Patch groups help ensure that you're deploying the appropriate patches based on the associated patch baseline rules to the correct set of nodes.

15. In the **Modify patch groups** section under **Patch groups**, enter `LinuxProd` and then choose the **Add** button.
16. Choose **Close**.

Task 1.1: Tag instances

In this task, you tag your Windows instances. Later in the lab, you create a patch group and associate it with these tags.

💬 *The Linux instances were pre-configured during lab setup with LinuxProd tags and do not need any added tags.*

17. In the AWS Management Console, in the search 🔍 bar, enter `EC2` and select it.
18. Select the check box next to the **Windows-1** instance, and then choose the **Tags** tab.
19. Choose the **Manage tags** button, choose **Add tag**, and configure the following options:
    - **Key**: Enter `Patch Group`
    - **Value**: Enter `WindowsProd`
20. Choose **Save**.
21. Repeat the previous steps to tag the **Windows-2** and **Windows-3** instances with the same tags.

Task 1.2: Create a custom patch baseline

Next, you create a custom patch baseline for the Windows instances. Although Windows has default patch baselines that you can use, for this use case, you set up a baseline for Windows security updates.

22. Return to the Systems Manager console. In the search bar at the top, enter `Systems Manager` and then select it.
23. In the left navigation pane, under **Node Management**, choose **Patch Manager**.
24. In the **Patch your instances** section, choose **View predefined patch baselines**.
25. Choose the **Patch baselines** tab.
26. Choose the **Create patch baseline** button.
27. For **Patch baseline details**, configure the following options:
    - For **Name**, enter `WindowsServerSecurityUpdates`
    - For **Description - *optional***, enter `Windows security baseline patch`
    - For **Operating system**, choose **Windows**.
    - Leave the check box for **Default patch baseline** unselected.
28. In the **Approval rules for operating systems** section, configure the following options:
    - **Product**: From the dropdown list, choose **WindowsServer2019**.
    - **Severity**: This option indicates the severity value of the patches that the rule applies to. To ensure that all service packs are included by the rule, choose **Critical** from the dropdown list.
    - **Classification**: From the dropdown list, choose **SecurityUpdates**.
    - **Auto-approval**: Enter `3` days.
    - **Compliance reporting - *optional***: From the dropdown list, choose **Critical**.
29. Choose **Add rule** to add a second rule to this patch baseline, and configure the following options:
    - **Product**: From the dropdown list, choose **WindowsServer2019**.
    - **Severity**: From the dropdown list, choose **Important**.
    - **Classification**: From the dropdown list, choose **SecurityUpdates**.
    - **Auto-approval**: Enter `3` days.
    - **Compliance reporting - *optional***: From the dropdown list, choose **High**.
30. Choose **Create patch baseline**.

    Next, modify a patch group for the Windows patch baseline that you just created.

31. In the **Patch baselines** section, select the button for the **WindowsServerSecurityUpdates** patch baseline that you just created.
    Note: The patch baseline that you created may be on the second page of the baselines list.
32. Choose the **Actions** dropdown list, and then choose **Modify patch groups**.
33. In the **Modify patch groups** section under **Patch groups**, enter `WindowsProd`
34. Choose the **Add** button, and then choose **Close**.

Summary of task 1

In this task, you used a default Linux Amazon patch baseline and modified a patch group for the LinuxProd group. You then tagged your Windows instances so that they could be associated with the WindowsProd patch group. You learned how to create a custom patch baseline for the Windows instances.

Task 2: Configure patching

In this task, you configure patching for the Linux instances and create a scheduled maintenance window. You then patch the Windows instances manually.

After configuration, Patch Manager uses the **Run Command** to call the **RunPatchBaseline** document to evaluate which patches should be installed on target instances according to each instance's operating system type directly or during the defined schedule (maintenance window).

35. From the **Patch Manager** console page, choose the **Configure patching** button.
36. In the **Instances to patch** section, choose **Select a patch group**, and then choose **LinuxProd** from the dropdown list.
37. Under **Patching schedule**, choose **Schedule in a new Maintenance Window**, and then configure the following options:
    - **How do you want to specify a Maintenance Window schedule?**: Choose **Use a CRON schedule builder**.
    - **Maintenance Window run frequency**: Choose the radio button for **Every**. From the **Select** dropdown list, choose **Every Day** and enter `02:00`
    - **Maintenance Window duration**: Enter `1`
    - **Maintenance Window name**: Enter `Linux-Maintenance`
38. In the **Patching operation** section, choose **Scan and install**, and then choose the **Configure patching** button.

Task 2.1: Patch instances instantly

39. From the **Patch Manager** console page, choose the **Patch baselines** tab, and then choose the button for the **WindowsServerSecurityUpdates** baseline that you created previously.
40. Choose **Configure patching**.
41. For the **Configure patching** section, configure the following options:
    - **How do you want to select instances?**: Choose **Select a patch group**.
    - **Patch groups**: Choose **WindowsProd**.
    - **How do you want to specify a patching schedule?**: Choose **Skip scheduling and patch instances now**.
    - **Patching operation**: Choose **Scan and install**.
42. Choose the **Configure patching** button.
43. At the top of the page, you should see a green banner that says **Successfully configured patching**. Choose the **View details** button.

    ℹ Behind the scenes, Patch Manager uses the **Run Command** to run the **AWS-RunPatchBaseline** document. You can now see the Windows instances in progress.

    A Systems Manager document (SSM document) defines the actions that Systems Manager performs on your managed instances.
44. Choose the refresh button inside the AWS console.

    Wait until you see ✓**Success** for the **Status** of all of the instances.
45. Select the radio button ○ for one of the instances that was just scanned, and then choose the **View output** button.

46. In the **Step 1 - Command description and status** section, expand the ▸ **Output**. As the **Step name** indicates, this step patches Windows instances (**PatchWindows**).

47. Scroll through the output, and find **InstalledCount** to see how many patches were installed.

    The following is other key information available in the output:

    - PatchGroup
    - BaselineId
    - OperationStartTime
    - OperationEndTime
    - FailedCount

    Although you have set up a scheduled maintenance window for the **LinuxProd** patch group, you still want to patch now just to be sure.

48. In the left navigation pane, under **Node Management**, choose **Patch Manager**.

49. Choose **Configure patching**.

50. For the **Configure patching** section, configure the following options:

    - **How do you want to select instances?**: Choose **Select a patch group**.
    - **Patch groups**: Choose **LinuxProd**.
    - **How do you want to specify a patching schedule?**: Choose **Skip scheduling and patch instances now**.
    - **Patching operation**: Choose **Scan and install**.

51. Choose the **Configure patching** button.

Task 2.2: Verify compliance

52. In the left navigation pane, under **Node Management**, choose **Patch Manager**.
53. Choose the **Dashboard** tab. Under **Compliance summary**, you should now see **Compliant: 6**, which verifies that all Windows and Linux instances are compliant.
54. Choose the **Compliance reporting** tab.
    💬 This tab provides an overview of all running instances with SSM. You should be able to verify that the **Compliance status** of all Linux and Windows instances is ✔**Compliant**.

Summary of task 2

In this task, you configured patching and created a scheduled maintenance window for the LinuxProd group. This will now scan and install patches (if available) every day at 2 AM.

You then learned how to scan and install patches instantly and analyze the output from the Run command to see the patch updates. You verified through compliance reporting that all EC2 instances have been scanned and updated and are compliant.

Conclusion

🏁 Congratulations! You now have successfully:

- Created a custom patch baseline
- Modified two patch groups
- Configured patching
- Scheduled a maintenance window
- Performed an instant scan, and verified patch compliance