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 Windows that were pre-created for this lab. You also use default patch baseline to patch EC2 Linux instances.

Objectives

After completing this lab, you should be able to:

- Patch Linux instances using default baseline
- Create custom patch baseline
- Use patch groups to to patch Windows instances using custom patch baseline
- 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: Patch Linux instances using default baselines

In this task, you patch Linux EC2 instances using default baselines available for the OS.

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 have a specific IAM role associated with them that allows you you managed them using Systems Manager, 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 to manage this instance.
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 **Start with an overview** (Proceed to next step if this option does not appear).
12. Choose **Patch now** to patch the Linux instances with **AWS-AmazonLinux2DefaultPatchBaseline**.

13. Under **Basic configuration**, configure as follows:
    - Patching operation: **Scan and install**
    - Reboot option: **Reboot if needed**
    - Instances to patch: **Patch only the target instances I specify**
    - Target selection: **Specify instance tags**
        - Tag key: `Patch Group`
        - Tag value: `LinuxProd`
    - Choose **Add**
14. Choose **Patch now**
15. Observe the status of the patching.

    A new page displays. In the **AWS-PatchNowAssociation** panel, there is a **Status** field that will show that three instances will be affected and the progress made.

    A Scan/Install operation summary panel also displays the status of the affected EC2 instances visually. Monitor this page until the patch operation on all three instances completes.

Task 2: Create a custom patch baseline for Windows instances

In this task, 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.

16. Return to the Systems Manager console. In the search bar at the top, enter `Systems Manager` and then select it.
17. In the left navigation pane, under **Node Management**, choose **Patch Manager**.
18. Choose **Start with an overview** (Proceed to next step if this option does not appear).
19. Choose the **Patch baselines** tab.
20. Choose the **Create patch baseline** button.
21. 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.

22. In the **Approval rules for operating systems** section, configure the following options:
    - **Products**: From the dropdown list, choose **WindowsServer2019**. Also, *deselect* **All** so that it no longer appears under Products.
    - **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**.
23. Choose **Add rule** to add a second rule to this patch baseline, and configure the following options:
    - **Products**: From the dropdown list, choose **WindowsServer2019**. Also, *deselect* **All** so that it no longer appears under Products.
    - **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**.

24. Choose **Create patch baseline**.

    Next, modify a patch group for the Windows patch baseline that you just created, to associate it with a patch group.

25. 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. You could also use the search bar to locate it and then select it.

26. Choose the **Actions** dropdown list, and then choose **Modify patch groups**.

27. In the **Modify patch groups** section under **Patch groups**, enter `WindowsProd`

28. Choose the **Add** button, and then choose **Close**.

Task 3: Patching the Windows instances

In this task, you patch the Windows instances using the *Patch now* feature based on the tag associated with them.

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).

Task 3.1: Tagging Windows 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.*

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

Task 3.2: Patching Windows instances

34. Return to the Systems Manager console. In the search bar at the top, enter `Systems Manager` and then select it.
35. To Patch the Windows instances:
    - Choose **Patch Manager**
    - Choose **Start with an overview** (Proceed to next step if this option does not appear).
    - Choose **Patch now**.
    - Patching operation: **Scan and install**
    - Reboot option: **Reboot if needed**
    - Instances to patch: **Patch only the target instances I specify**
    - Target selection: **Specify instance tags**
        - Tag key: `Patch Group`
        - Tag value: `WindowsProd`
    - Choose **Add**
    - Choose **Patch now**

36. A new page displays. When it becomes available, choose the link to the **Execution ID**.

    A page in the State Manager part of Systems Manager opens.

37. Choose the **Output** link for one of the managed instances that shows a status of InProgress.

    A page in the Run Command part of Systems Manager opens.

38. *Expand* the Output panel to observe the details.

    ℹ Behind the scenes, Patch Manager uses the **Run Command** to run the PatchBaselineOperations. If you scroll through the output, you should see the **PatchGroup: WindowsProd** details.

    A Systems Manager document (SSM document) defines the actions that Systems Manager performs on your managed instances.

Task 4: Verifying compliance

39. In the left navigation pane, under **Node Management**, choose **Patch Manager**.
40. Choose the **Dashboard** tab. Under **Compliance summary**, you should now see **Compliant: 6**, which verifies that all Windows and Linux instances are compliant.

41. 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**.

    - All six instance (three Linux and three Windows) should show as compliant.
    - Scroll to the right in the *Node patching details* panel to find for each instance:
        - Critical noncompliant count
        - Security noncompliant count
        - Other noncompliant count
        - Last operation date
        - Baseline ID
    - Choose the Node ID for one of the Windows nodes.
    - In the Node ID page that opens, choose the Patch tab.
    - Scroll down and observe what patches were applied to this instance, as well as the Installed Time.