Systems Hardening with Patch Manager via AWS Systems Manager

Lab Overview:

This lab guides you through using Patch Manager, a capability of AWS Systems Manager, to create patch baselines and patch EC2 instances for Linux and Windows.

Objectives:

- Create a custom patch baseline
- Modify patch groups
- Configure patching
- Verify patch compliance

Lab Environment:

The lab environment has six pre-created EC2 instances: three Linux and three Windows.

Task 1: Select Patch Baselines

1. In the AWS Management Console, search for and select **Systems Manager**.
2. Under **Node Management**, choose **Patch Manager**.
3. Choose **Start with an overview**.
4. Select the **Patch baselines** tab.
5. Choose the **AWS-AmazonLinux2DefaultPatchBaseline** baseline and modify its patch groups to include **LinuxProd**.

Task 1.1: Tag Windows Instances

1. Search for and select **EC2**.
2. Choose **Instances**.
3. Tag the Windows instances with the key **Patch Group** and value **WindowsProd**.

Task 1.2: Create a Custom Patch Baseline for Windows

1. In the Systems Manager console, search for and select **Systems Manager**.
2. Under **Node Management**, choose **Patch Manager**.
3. Choose **Start with an overview**.
4. Select the **Patch baselines** tab and click **Create patch baseline**.

5. Configure the following options:
    - **Name:** WindowsServerSecurityUpdates
    - **Description:** Windows security baseline patch
    - **Operating system:** Windows
    - **Approval rules:**
        - Products: WindowsServer2019 (excluding All)
        - Severity: Critical
        - Classification: SecurityUpdates
        - Auto-approval: 3 days
        - (Add another rule with the same Products, Severity: Important, Classification: SecurityUpdates, and Auto-approval: 3 days)
6. Click **Create patch baseline**.
7. Modify the patch groups for the **WindowsServerSecurityUpdates** baseline to include **WindowsProd**.

Task 2: Configure Patching

Task 2.1: Patch the Linux Instances

1. In the Patch Manager console, choose **Patch now**.
2. Configure the following options:
    - 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
3. Click **Patch now** and monitor the progress.

Task 2.2: Patch the Windows Instances

1. Repeat the steps in **Task 2.1**, replacing **LinuxProd** with **WindowsProd**.
2. In the **AWS-PatchNowAssociation** panel, click the **Execution ID** link.
3. In the **State Manager** page, click the **Output** link for an instance with the status **InProgress**.

4. Observe the output details, including the **PatchGroup: WindowsProd**.

Task 2.3: Verify Compliance

1. In the Patch Manager console, choose **Dashboard**.
2. Verify that **Compliance summary** shows **Compliant: 6**.
3. Choose **Compliance reporting**. Verify that all instances are **Compliant**.

Conclusion:

Congratulations! You have successfully completed the lab.

End Lab:

Choose **End Lab** at the top of the page and confirm.