Cloudwatch Logs Labs

In the lab, you will deploy an EC2 instance with Apache and PHP installed. The web server will host a very simple website. You will configure a CloudWatch Agent on the instance via Amazon Systems Manager (SSM). This agent will collect log files from services running on the EC2 instance, such as Apache access and error logs, yum logs, SSH logs, and CloudWatch agent logs. These logs are exported from the EC2 instance to the CloudWatch logs service for centralized storage. You will export these logs to an S3 bucket for long term storage and archival. These logs will then be queried via Athena, so people are kept away from accessing the log files directly. This data will be visually represented in a QuickSight dashboard.

Deploy the CloudFormation Stack

1. Download the CloudFormation template provided in this lab .
2. Go to CloudFormation console , click **Create Stack**, and select **With new resources (standard)**.
3. In the **Specify Template** menu, choose **Upload a template file**, then **Choose file**, and select the security-lab-stack.yaml template you downloaded.
4. In the **Specify Stack Details** menu:
    a. Enter a stack name, such as security-cw-lab. Note the name down, as you will need to re-visit this stack for Outputs later on.
    b. Enter your name in the DisplayedName field, this will be the name that appears on your sample website!
    c. Enter an S3 bucket name in the BucketName field. Amazon S3 bucket names are globally unique, and the namespace is shared by all AWS accounts, so make sure your bucket is names as uniquely as possible. For example: wa-lab-<your-account-id>-<date>.
    d. Do not modify the LatestAmiId field. This uses a public parameter stored in Systems Manager Parameter Store that will automatically use the latest Amazon Machine Image (AMI) for the EC2 instance.
5. No changes are needed on the **Configure Stack Options** page. Click through **Next.**
6. On the **Review** page, check the box in the **Capabilities** section to allow the creation of an IAM role. This selection gives the CloudFormation template permission to create IAM roles - in particular, the role used to allow the EC2 instance to interact with SSM and CloudWatch. Click **Create Stack**. You will be taken back to the CloudFormation console, where your stack will be launched.
7. Once the stack shows CREATE COMPLETE, click on the **Outputs** tab and click on the WebsiteURL, you will be brought to your sample web server.

Install the CloudWatch Agent

1. Open the Systems Manager console .
2. Choose **Run Command** from the left side menu under **Nodes Management.** Click **Run Command** on the page that opens up.
3. In the **Command document** box, click in the search bar. Select "**Document name prefix"**, then "**Equals**", and enter **AWS-ConfigureAWSPackage**. Select the command that appears below. This command allows you to install packages on EC2 instances without directly accessing the instance; the AmazonCloudWatchAgent package we will use in this lab is one of these packages.
4. Under **Command parameters:**
    a. Set **Action** to **Install**
    b. Set **Installation Type** to **Uninstall and Reinstall**
    c. In the **Name field,** enter AmazonCloudWatchAgent
    d. In the **Version** field, enter latest
    e. Do not modify the **Additional Arguments** field
5. Under **Targets**:
    a. Select Choose instances manually.
        i. For the purpose of this lab, there is only one EC2 Instance you need to run a command on. If you have a large fleet of EC2 instances, you can assign a tag to those instances and choose Specify instance tags to run a command on many tagged instances easily.
        ii. You should see a list of running instances. Select the instance that was launched by the CloudFormation template you deployed for this lab, which will be named Security-CW-Lab-Instance.
        iii. In order to use Systems Manager with an instance, the instance needs certain IAM permissions. The initial CloudFormation stack you deployed created and assigned an IAM role to this instance. The policy document AmazonSSMManagedInstanceCore is attached to this role, allowing Systems Manager to perform operations on the instance.
6. Under **Output Options**, deselect **Enable writing to an S3 bucket**.
7. Choose **Run**.
8. Optionally, in the **Targets and outputs** areas, select the button next to an instance name and choose **View output**. Systems Manager should show that the agent was successfully installed.

Store the CloudWatch Config File in Parameter Store

You will use Parameter Store, a tool in Systems Manager, to store the CloudWatch agent configuration. Parameter store allows you to securely store configuration data and secrets for reusability. You can re-use configuration data that is well controlled and consistent. In this case, you need to store the configuration file for CloudWatch Agent on your EC2 instance.

The CloudWatch agent configuration data specifies which logs and metrics will be sent to CloudWatch as well as the source of this data.

1. Open the Systems Manager console .
2. Choose **Parameter Store** from the left side menu under **Application Management.** Choose **Create parameter** from that screen.
3. Enter the parameter name AmazonCloudWatch-securitylab-cw-config. You may use a different name, but it *must* begin with AmazonCloudWatch``- in order to be recognized by CloudWatch as a valid configuration file.
4. Give your parameter a description, such as “This is a CloudWatch Agent config file for use in the Well Architected security lab”.
5. Set **Tier** to **Standard.**
6. Set **Type** to **String.**
7. Set **Data type** to **text.**
8. In the **Value** field, copy and paste the contents of the config.json file found in the lab assets. This config file specifies which metrics and logs to collect.
    a. The agent section specifies which user to run the logs agent as, and how frequently to collect logs.
    b. The logs section specifies which log files to monitor and which log group and stream to place those logs in. This information can be seen in collect_list. For this lab, you are collecting SSH logs, Apache Web Server logs, and logs for the CloudWatch Agent itself. We will examine these logs more closely in a later step
    c. The metrics section specifies which metrics are collected (in metrics_collected), the frequency of collection, measurement, and other details.
    d. To learn more about creating config files, see this link .
9. Click **Create parameter**.

Start the CloudWatch Agent

1. Open the Systems Manager console .
2. Choose **Run command** from the left side menu under **Node Management.** Click **Run Command** on the page that opens up.
3. In the **Command document** box, click in the search bar. Select “**Document name prefix”**, then “**equals**”, and enter **AmazonCloudWatch-ManageAgent**. Select the command that appears in the results. This command sends commands directly to the CloudWatch agent on your instances by remotely running scripts on the instance. You will be sending a “configure” command with the created parameter from Parameter Store to instruct the CloudWatch agent installed on the EC2 instance to use this configuration and start collecting logs.

4. Under **Command parameters:**
    a. Set **Action** to **Configure**.
    b. Set **Mode** to **ec2**.
    c. Set **Optional Configuration Source** to **ssm**.
    d. Set **Optional Configuration Location** to the name of the parameter you created in **Parameter Store**. If you used the name provided above, it should be called AmazonCloudWatch-securitylab-cw-config.
    e. Set **Optional Restart** to **yes**.
5. Under **Targets**:
    a. Select **Choose instances manually**.
    b. You should see a list of running instances. Select the instance that was launched by the CloudFormation template you deployed for this lab. This will be named Security-CW-Lab-Instance.
6. Under **Output Options**, deselect **Enable writing to an S3 bucket**.
7. Choose **Run**.
8. Optionally, in the **Targets and outputs** areas, select the button next to an instance name and choose **View output**. Systems Manager should show that the agent was successfully installed in a few seconds.

Generate Logs

In order to populate the logs you are collecting, you need to interact with the deployed website. The Apache web server service being used to host your website generates access logs. In the following steps, you will visit the website to generate these access logs.

1. Go to the CloudFormation console .
2. Select the stack you deployed for this lab, called security-cw-lab.
3. Click on **Outputs**, then click on **WebsiteURL**.
4. Refresh the page a few time to generate some activity on your website.
5. Repeat steps 1-4, but add /example to the end of the website url. This will generate a 404 error, which is expected.

View your CloudWatch Logs

Now that the CloudWatch Agent is up and running on your EC2 Instance, let's go ahead and view those logs and metrics from the Console. CloudWatch is a useful place to view logs because it is centralized, meaning you can switch between examining logs from many sources.

Viewing Logs:

1. Open the CloudWatch console .
2. On the left side menu, choose **Log groups** under **Logs.** On that screen, enter securitylablogs in the search bar. Click on the log group that appears in the results.
3. You will see these log streams: cw-agent-logs, apache-access-logs, apache-error-logs, yum-logs, and ssh-logs. Click through all of them to view the logs from each of these services.
4. You should see a record of log events. This is the data being collected on your EC2 instance, and then sent to CloudWatch by the CloudWatch Agent installed on the instance.

Export Logs to S3

After collecting logs, you may want to export logs from CloudWatch to an S3 Bucket. This is useful as storing data in S3 is more cost effective and reliable than storing it in CloudWatch, making S3 a good option for long-term storage and archival of log files.

1. Open up the CloudWatch console .
2. On the left side menu, choose **Log groups** under **Logs.** On that screen, enter securitylablogs in the search bar. Click on the log group that appears in the results.
3. Click **Actions** and **Export data to Amazon S3** in the top menu.
4. You will have to fill out information about what data to export.
    a. In the **From** field, set the YYYY/MM/DD field to today's date (the date you are doing this lab). This is the earliest creation date of logs you want to export.
    b. In the **To** field, set set the YYYY/MM/DD field to tomorrow's date (the date after the day you are doing this lab). This is the latest creation date of logs you want to export.
    c. Leave the **Stream prefix** field blank, as we want to export all logs. This field allows you to select which logs you want to export.
    d. Set **S3BucketName** to the bucket name you entered in your CloudFormation stack, likely wa-lab-<your-account-id>-<date>. This is the bucket your logs will be exported to.
    e. Set **S3 bucket prefix** to lablogs. This is the subdirectory your exported logs will be stored in.
5. Click **Export**
6. Click on the **View export tasks** in the pop up box that appears. This will bring you to a list of **Export tasks** performed from CloudWatch
7. Click the radio bubble next to the most recent export. Click **View in Amazon S3** to open these logs in the S3 bucket you created.
8. You should now see folders corresponding to all of the log streams you viewed earlier. You can explore these logs and download the .gz files if you'd like to see their contents.

Lab Teardown

Deleting the Systems Manager stored parameter

1. Visit the Systems Manager console .
2. In the left side menu, click on **Parameter store**.
3. Click the box next to your created parameter, likely called AmazonCloudWatch-securitylab-cw-config.
4. Click **Delete**. Click **Delete parameters** on the pop up that appears.

Deleting the S3 Bucket

1. Visit the S3 console .
2. Click the button next to your created bucket, likely called wa-lab-<your-last-name>-<date>.
3. Click **Delete**, follow the instructions in the pop-up to delete your bucket.

Tearing down the CloudFormation stack.

1. Visit the CloudFormation console .
2. Click on the stack you created for this lab, likely called security-cw-lab.
3. Click **Delete** and then **Delete stack** on the window that pops up.