

Additional Education

Although not a requirement, we've included a few additional 'labs' for you to work on after today's Innovation Day was complete. The labs will build upon what you've learned during today's session and will further display how you can easily integrate multiple AWS services to build and accomplish amazing things. While not as detailed as the labs above, feel free to experiment with the concepts behind these 'take-a-way' labs as you continue to educate yourself and gain experience on the AWS platform. Enjoy!

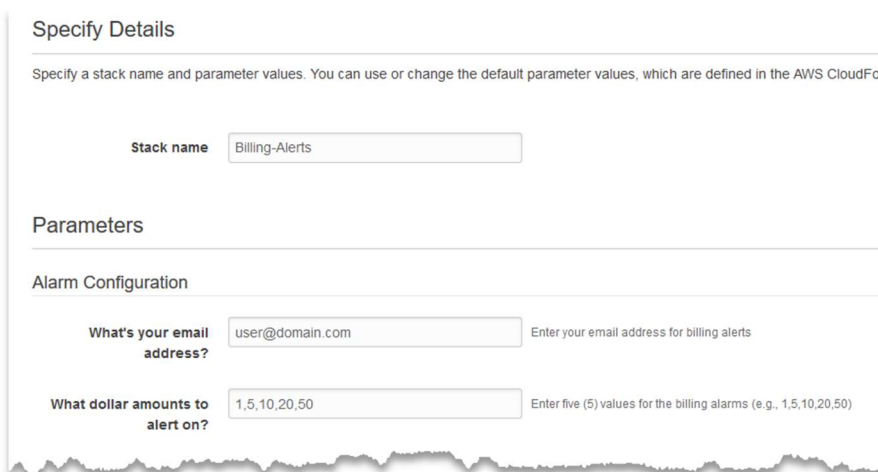
Lab 1 – Billing Alerts

During the process of experimentation and learning something new, the last thing you want to worry about is what your bill will be at the end of the month. Sure, you can check your account often to ensure your bill doesn't unexpectedly increase, but why not use the AWS platform to protect yourself from an unexpected bill. With the combined use of CloudWatch and SNS, you can configure billing alarms to send out notifications when your bill hits certain thresholds.

Goal – Go beyond the guided labs above and experiment with additional services on the AWS platform.

Prerequisites – A desire to learn and expand your skillset. You'll need an AWS account as well!

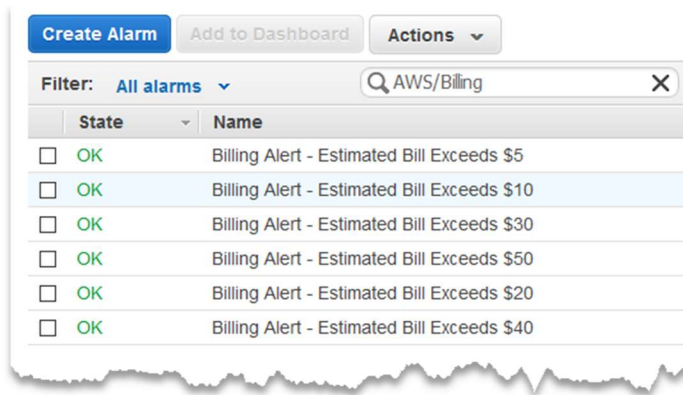
1. Using CloudFormation, **create a new stack** using the template found at the following URL:
<https://s3.us-east-2.amazonaws.com/ahead-innovation-days/aws201/billingalerts.yml>
2. Enter the desired billing alert thresholds for your account. For example, if you want to be notified when your estimated monthly bill exceeds \$1, \$5, \$10, \$20, and \$50, enter **1,5,10,20,50**.



The screenshot shows the AWS CloudFormation console interface for creating a new stack. The 'Specify Details' section is active, showing the stack name 'Billing-Alerts'. Below this, the 'Parameters' section is visible, containing an 'Alarm Configuration' subsection. In this subsection, there are two input fields: 'What's your email address?' with the value 'user@domain.com' and 'What dollar amounts to alert on?' with the value '1,5,10,20,50'. Both fields have placeholder text explaining their purpose.

3. Enter your **email address**.

4. Click **Next**, **Next**, and **Create**.
5. **Confirm your subscription** to the SNS topic using the link in the confirmation email.
6. To see the billing alerts created, navigate to the **CloudWatch** console.
7. Click on **Billing** in the navigation pane to view the new alarms created. Feel free to review or modify the alarms as needed.



8. Navigate to the **Simple Notification Service (SNS)** console.
9. Click **Topics** on the left.
10. Click the **Billing-Alerts** topic to view the email subscription already created by the template.

You did it. You are done with this lab.

Conclusion: In this lab, participants created billing alarms to ensure there are no unexpected bills from experimentation and exploration of the AWS platform.

Lab 2 – Creating a Backup Retention Schedule

In Lab 2, you deployed two AWS Lambda functions to take and delete snapshots of EBS volumes attached to your EC2 instances. However, everything you did was manual, meaning there was no scheduler that executed the Lambda functions automatically. This lab will walk you through the use of CloudWatch Events to schedule the execution of the two Lambda functions for a more comprehensive backup strategy.

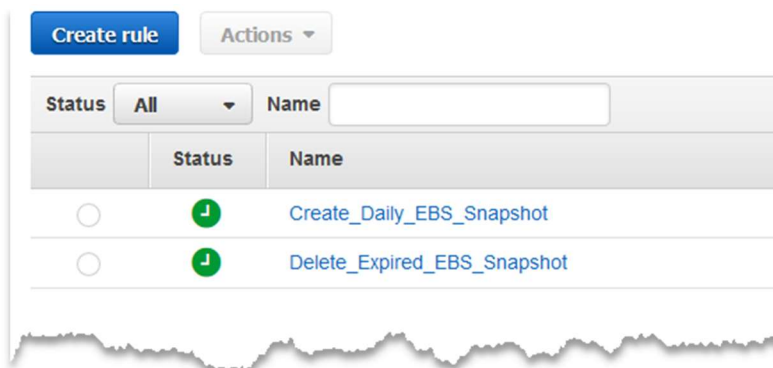
1. Using AWS **CloudFormation**, deploy the **EBS-Snapshots** stack again. Use the same CloudFormation template used in Lab 2:

https://s3.us-east-2.amazonaws.com/ahead-innovation-days/aws201/lab1/ebs_snapshots.yml

2. Navigate to the **CloudWatch** console. Select **Events** on the left.
3. Click **Create Rule**.
4. In the **Event Source** section, select **Schedule**.
5. Select the radio button for **Cron expression** and type the following: **0 2 * * ? ***

Note: This Cron expression states that the rule will run every day at 2:00 UTC, which is 10:00PM EST. Once you enter the expression, it will display the next 10 events to ensure your command is correct. Cron expressions are written as: Minutes | Hours | Day of Month | Month | Day of Week | Year.

6. On the right, click the **Add target** button.
7. Select **Lambda function** from the drop-down. Select **EBS-Snapshot>Create-Function** from the Function* drop-down.
8. Click **Configure Details**.
9. Enter a name for the rule, perhaps **Create_Daily_EBS_Snapshot**. Enter a Description if you'd like.
10. Click **Create rule**.



11. Create a second rule for the **EBS-Snapshot-Delete-Function**, but use the Cron expression:

0 1 * * ? *

Note: *This will execute the EBS-Snapshot-Delete-Function every day at 1:00 UTC, which is 9:00PM EST.*

12. Give the rule the name **Delete_Expired_EBS_Snapshot**.
13. In the **EC2** console, **tag any instances** that you want snapshots with the **backup** and **Retention** tag, as you did in Lab 2.



That's it. You are done with this lab.

Conclusion: In this lab, participants created CloudWatch Events to schedule the AWS Lambda functions to automatically execute at certain times of the day. This will help create a more comprehensive backup strategy for EC2 instances.

Lab 3 – Using Snapshots to Restore Files

In Lab 2, you took snapshots of an EC2 instance using the Lambda functions. However, you didn't do anything with the snapshots, such as restore any data. In this lab, you'll manually create a snapshot, delete some data on the EC2 instance, and then try to recover those files using the snapshot.

1. Using **CloudFormation**, deploy the initial stack as you did in Lab 1 using the following URL. This will deploy all the resources needed for this lab.

<https://s3.us-east-2.amazonaws.com/ahead-innovation-days/aws201/lab1/toplevel.yml>
2. Navigate the **EC2** console. Click on **Volumes**.
3. Select the **Volume** attached to the **Windows Instance – Lab 2** instance. You can find information on the volumes by selecting them and viewing the information in the bottom pane.
4. Under the Action menu, select **Create Snapshot**.
5. Enter the name of **Manual Snapshot**.
6. Click on **Snapshots** in the navigation pane and **refresh** the list until the snapshot changes from a status of  Pending to  Completed.
7. In the EC2 console, select **Security Groups** in the navigation pane.
8. Select the **ahead-lab-rep-access** security group and click the **Inbound** tab at the bottom.
9. Click **Edit**.
10. Modify the existing rule so the source is **0.0.0.0/0** rather than 10.0.0.0/16.
11. Click **Save**.
12. Using **Remote Desktop**, connect to the **EC2** instance. Don't forget to grab the administrator password by decrypting it using the EC2 Key Pair. For a refresher, check out Lab 2.
13. Open **File Explorer** and view the files located in C:\AHEAD-Lab-Files.

***Note:** These are photos of our amazing office in downtown Chicago. Make sure to connect with your account rep to schedule some time in our office and to check out our incredible briefing center.*
14. Delete the folder **C:\AHEAD-Lab-Files**.
15. In the EC2 console, click **Snapshots**
16. Select the snapshot, and click **Create Volume** from the Actions menu.
17. Leave all the defaults and click **Create Volume**.

18. Click the volume name in the confirmation box or select Volumes in the EC2 console and **select the new volume**.
19. From the Actions Menu, select **Attach Volume**.
20. In the Instance field, select **Windows Instance – Lab 2**. Leave the device field as the default.
21. Click **Attach**.
22. Open your **Remote Desktop** connection to the instance and open **Disk Management**. This can be done by right-clicking the Start Menu and selecting Disk Management.
23. You should have a second disk listed as Disk 1.
24. Right click Disk 1 and choose **Online**.

***Note:** You have to click the left-side, the gray box where it says Disk 1.*
25. The disk should come **online** and Windows will likely assign it as D: drive.
26. Using **File Explorer**, browse to D: drive and see that the AHEAD-Lab-Files folder still exists, as you took the snapshot before you deleted the folder.
27. Copy the files from **D:\AHEAD-Lab-Files** back to the original location of **C:\AHEAD-Lab-Files**.
28. Now that you've restored the files, feel free to **view** those photos of the beautiful **AHEAD** office again!

That's it. You are done with this lab.

Conclusion: In this lab, participants took a manual snapshot of a running instance, purposely deleted files on the instance, and using the snapshot to restore the original files.

Lab Cleanup:

Don't forget to detach the additional volume, delete the volume, and delete the snapshot. Then delete the CloudFormation stack. If you need help, refer to Lab 6.