



re:Invent 2019

ARC319

Security Vulnerability Identification and Remediation

Copyright © 2019 Amazon Web Services, Inc. or its affiliates. All rights reserved.

This work may not be reproduced or redistributed, in whole or in part, without prior written permission from Amazon Web Services, Inc. Commercial copying, lending, or selling is prohibited.

All trademarks are the property of their owners.

Table of Contents

Prerequisites	4
Problem Statement	5
Solution Overview	6
Task 1 – Enable AWS Config and AWS Security Hub	7
Task 2 – Deploy the Three Tier Web App CloudFormation Template	10
Task 3 – Check your security findings	11
Task 3 – Create AWS Config rules/remediations	11
Task 4 – Review the AWS Config deployed rules	12
Task 5 – Review the Security Hub findings – Needs Screenshots	13
Task 6 – Create a new AWS Config Rule	13
Task 7 – Additional Testing	16
Task 8 – Cleanup	17
Task 9 – Optional (further reading/discussion)	17
Appendix A: Troubleshooting common issues	17

Prerequisites

This exercise requires access to Amazon Web Services (AWS) console. You will be provided with a pre-provisioned AWS account and console access. As this is a 300-level workshop, it is assumed that you already have the knowledge required to satisfy the prerequisites for the workshop.

In the event you are conducting this exercise without a pre-provisioned account ensure the IAM user you are leveraging has full admin rights.

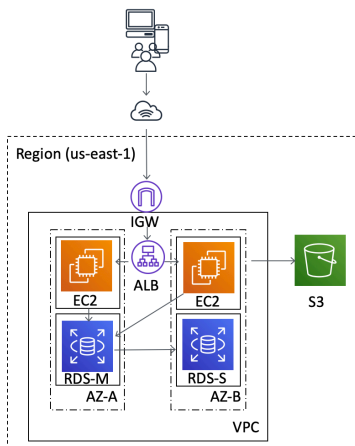
Problem Statement

You are the lead DevSecOps engineer for a large global conglomerate. Various business lines are grown primarily through mergers and acquisitions. Your company just bought a new startup that specializes in an online blogging platform; and you have been asked to implement the technology stack that was acquired. The technology stack was done as infrastructure as code in a CloudFormation Template. This will be cake.... Right?

This workshop focuses on integrating the new web platform and ensuring a proper security posture is maintained. The lab will involve learning how to monitor, alert, and remediate security events in your AWS environments; primarily focusing on [AWS Config](#) and [AWS Security Hub](#).

*****ARC319 will provide scripts and templates that intentionally create security holes, to be remediated. These templates should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

Solution Overview



The solution diagram, shown above, is to be deployed into the AWS region –us-east-1 (N. Virginia); and

The architecture provides a WordPress environment to host the online blogging platform. AWS services included are [Amazon EC2](#), [Amazon S3](#), and [Amazon RDS](#).

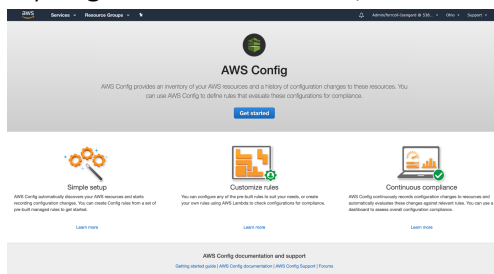
In the workshop, you will need to ensure that the new technology stack fits within your company's security posture. Your company is fairly new to AWS but has heard about services like [AWS Config](#), [AWS Security Hub](#), [Amazon GuardDuty](#), and [Amazon Macie](#) to help secure their environment. This lab will focus on the **AWS Config** and **AWS Security Hub** for detective controls and remediation.

Task 1 – Enable AWS Config and AWS Security Hub

AWS Security Hub requires AWS Config to be turned on. Let's do that first.

Enable AWS Config

1. Log into the AWS console with the link and credentials provided by the lab instructor
2. Ensure your region is US East - N. Virginia (in the top right navigation bar)
3. Navigate to the AWS Config service (click services at the top; Config is under 'Management & Governance')
4. If you get the screen below, click 'Get Started'



5. In 'Step 1: Settings' leave the settings as default
 - a. Resource types to record; "Record all resources supported in this region" Checked
 - b. Amazon S3 bucket; 'Create Bucket' Checked

Settings ?

Specify the types of AWS resources you want AWS Config to record, the Amazon S3 bucket to which it sends files, and the Amazon SNS topic to which it sends notifications. Review the [pricing page](#) before you start.

Resource types to record

Select the types of AWS resources for which you want AWS Config to record configuration changes. By default, AWS Config records configuration changes for all supported resources. You can also choose to record configuration changes for supported global resources in this region.

All resources ☒ Record all resources supported in this region ?
☐ Include global resources (e.g., AWS IAM resources) ?

Specific types

Amazon S3 bucket*

Your bucket receives configuration history and configuration snapshot files, which contain details for the resources that AWS Config records.


☒ Create a bucket
☐ Choose a bucket from your account
☐ Choose a bucket from another account ?

Bucket name* / /

6. Continue configuring settings as indicated below
 - a. Amazon SNS topic; "Create a topic" checked; leave the "Topic name" as default
 - b. AWS Config role; "Create AWS Config service-linked role"


Amazon SNS topic

☒ Stream configuration changes and notifications to an Amazon SNS topic.

 If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. [Learn more.](#)

☒ Create a topic

☐ Choose a topic from your account

☐ Choose a topic from another account 

Topic name*

AWS Config role*

Grant AWS Config read-only access to your AWS resources so that it can record configuration information, and grant it permission to send this information to Amazon S3 and Amazon SNS.


☒ Create AWS Config service-linked role

☐ Choose a role from your account

7. Click “Next”
8. On “Step 2: Rules” don’t select any (we’ll create these later)
9. Click “Skip”
10. On “Step 3: Review” click “Confirm”

OR

11. Choose to use the redesigned interface, if prompted

 **The redesigned AWS Config console is now available for use.**
We've completely redesigned the console to improve the overall look and feel. [Try it out now.](#)

12. Click the navigation icon in the top left (≡) and choose Settings
13. Click ‘Edit’ in the top right of the Settings page
14. Enable the AWS Config Recorder
 - a. Under Recorder select ‘Enable Recording’

Recorder

☒ Enable recording

- b. Under General Settings change the AWS Config Role option to ‘Use an existing AWS Config service-linked role’

▼ General settings

Resource types to record

- ☒ Record all resources supported in this region
To learn more, see [Supported AWS Resource Types](#).
- ☐ Record specific resource types

☒ Include global resources (e.g., AWS IAM resources)

Supported global resource types are IAM users, groups, roles, and customer managed policies.

Data retention period

- ☒ Retain AWS Config data for 7 years (2557 days)
- ☐ Set a custom retention period for configuration items recorded by AWS Config.

AWS Config role

- ☒ Use an existing AWS Config service-linked role
- ☐ Choose a role from your account

c. Under Delivery Method -> S3 Bucket chose 'Create a bucket'

▼ Delivery method

S3 bucket

- ☒ Create a bucket
- ☐ Choose a bucket from your account
- ☐ Choose a bucket from another account
Ensure appropriate permissions are available in this S3 bucket's policy. [Learn more](#).

S3 bucket name

/ AWSLogs/309852070700/Config/us-east-1

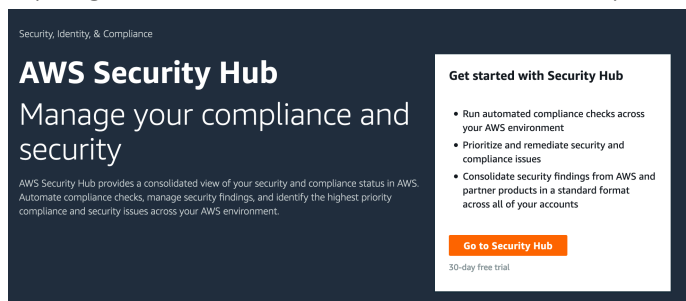
SNS topic

- ☐ Stream configuration changes and notifications to an Amazon SNS topic.
If you choose email as the notification endpoint for your SNS topic, this can cause a high volume of email. [Learn more](#).

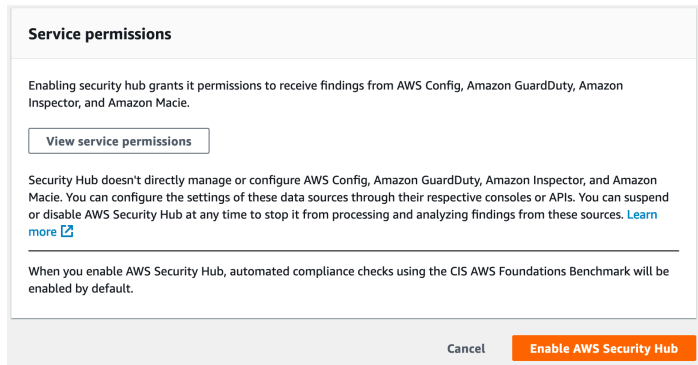
d. Click Save

Enable AWS Security Hub

1. Navigate to the AWS Security Hub service (click services at the top; Security Hub is under 'Security, Identity, & Compliance')
2. If you get the screen below, click 'Go to Security Hub'



3. On the next screen click 'Enable AWS Security Hub'



Task 2 – Deploy the Three Tier Web App CloudFormation Template

*****The steps below will deploy an environment with intentional security vulnerabilities, this template should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

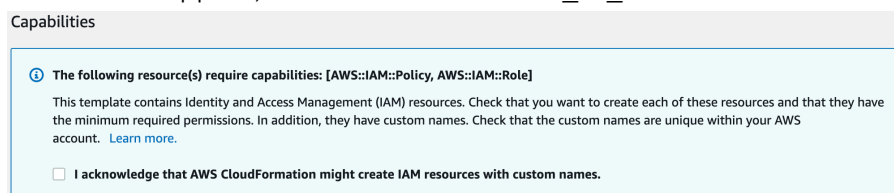
Launch the AWS Three Tier Web App CloudFormation stack in us-east-1 (N. Virginia):



Will need to add the hyperlink

The link opens the CloudFormation console in your account in us-east-1 region.

1. In 'Select Template', click Next.
2. Under 'Specify Details', enter a 'Stack Name' of your choice, click Next
3. In the Options section, scroll down to the bottom and click Next.
4. In the Review section, scroll down to the bottom, check the "I acknowledge..." checkbox and click Create. You may have to click the refresh button in CloudFormation console for the stack to appear; it should show CREATE_IN_PROGRESS under Status.



The creation of this stack can take up to 10 minutes. While the CloudFormation stack is being created open the CloudFormation Template in the editor of your choice.

Discussion: Do you see anything that might generate security concerns?

Task 3 – Check your security findings

1. Navigate to the AWS Security Hub service (click services at the top; Security Hub is under 'Security, Identity, & Compliance')
2. Click on Findings

We can see that several findings are listed. This is great for an environment that is regularly monitored, unfortunately yours is not.

Discussion: How could you enable automated remediation for these findings?

Task 3 – Create AWS Config rules/remediations

Launch the AWS Config CloudFormation stack in us-east-1 (N. Virginia):



The link opens the CloudFormation console in your account in us-east-1 region.

1. In 'Select Template', click Next.
2. Under 'Specify Details'
 - a. Change MyIPAddress (enter your current IP Address; from <https://whatismyipaddress.com>)
 - b. Enter an email that you have access to in MyEmailAddress; this will be used for remediation notifications
 - c. Leave the defaults for TagCostCenterValue, TagWorkloadValue, and TagOwnerValue
3. In the Options section, scroll down to the bottom and click Next.
4. In the Review section, scroll down to the bottom, check the "I acknowledge..." checkbox and click Create. You may have to click the refresh button in CloudFormation console for the stack to appear; it should show CREATE_IN_PROGRESS under Status.

Capabilities

i The following resource(s) require capabilities: [AWS::IAM::Policy, AWS::IAM::Role]

This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. [Learn more.](#)


☐ I acknowledge that AWS CloudFormation might create IAM resources with custom names.

While the stacks are being built, we will discuss details around creating AWS Config rules and options that exist for remediation.

Once the stack creation has completed, do the following;

1. Check the resources output within the CloudFormation stack and copy the 'IAMRoleArn' (you will need this later)
2. check the email addressed you entered in the stack details. You should see an email from AWS Notifications titled 'AWS Notification – Subscription Confirmation.' Open this email and click 'Confirm subscription.'

AWS Notification - Subscription Confirmation

 **AWS Notifications** <no-reply@sns.amazonaws.com>
Monday, October 21, 2019 at 2:22 PM
Strader, Eric
[Show Details](#)

You have chosen to subscribe to the topic:
~~arn:aws:sns:us-east-1:339852070700:339852070700-custom-remediation-topic~~

To confirm this subscription, click or visit the link below (If this was in error no action is necessary):
[Confirm subscription](#)

Please do not reply directly to this email. If you wish to remove yourself from receiving all future SNS subscription confirmation requests please send an email to [sns-opt-out](#)

Task 4 – Review the AWS Config deployed rules

When the CloudFormation stack is complete:

1. Click the 'outputs' tab within the CloudFormation stack and make note of the *IAMRoleArn* value (you will need this later)
2. Navigate to the AWS Config service (click services at the top; Config is under 'Management & Governance')
3. Choose to use the redesigned interface if prompted

i The redesigned AWS Config console is now available for use.
We've completely redesigned the console to improve the overall look and feel. [Try it out now.](#)

4. Click the navigation icon in the top left (≡) and choose Rules
5. Look at the rule titled 'S3_BUCKET_PUBLIC_READ_PROHIBITED'
 - a. Click the rule name

- b. In the rule window click on Remediation Actions
 - c. We see that this rule is being remediated with a Systems Manager pre-defined remediation
 - d. **The rule shows ‘remediation successful’ but still shows non-compliant. Why would this be?**
6. Now look at the rule titled ‘IAM_POLICY_NO_STATEMENTS_WITH_ADMIN_ACCESS’
 - a. Click the rule name
 - b. In the rule window click on the rule name
 - i. Click Edit for the rule (top right)
 - ii. Notice that the remediation is ‘AWS-PublisSNSNotification’
 - iii. This rule doesn’t have a corresponding AWS Systems Manager pre-defined remediation; it is being remediated with a custom Lambda Function triggered via an SNS topic.
7. Open AWS Lambda (click services at the top; Lambda is under ‘Compute’)
 - a. Open the Lambda function where the name includes ‘IAMRemediationLambdaFunction’
 - b. Review the Lambda function to understand how it is remediating the overly permissive security groups

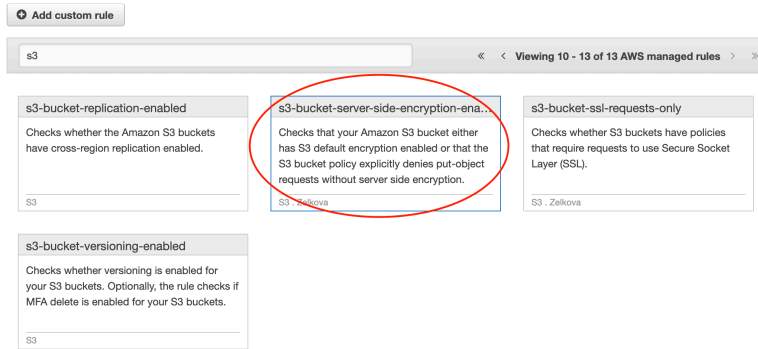
Task 5 – Review the Security Hub findings – Needs Screenshots

1. Navigate to the AWS Security Hub service (click services at the top; Security Hub is under ‘Security, Identity, & Compliance’)
2. Click on Findings
3. Notice the additional findings that are represented based on the newly deployed AWS Config rules as well as those enabled by default with Security Hub

Discussion – AWS Security Hub is a centralized service to review aggregated and normalized findings. What other AWS Security services (and 3rd party solutions) could integrate?

Task 6 – Create a new AWS Config Rule

1. Navigate to the AWS Config service (click services at the top; Config is under ‘Management & Governance’)
2. Search for ‘s3-bucket-server’ and select ‘s3-bucket-server-side-encryption-ena...’



3. Leave the defaults up until the 'Choose Remediation Section'
4. Modify the following settings
 - a. Remediation Action: choose 'AWS-EnableS3BucketEncryption'
 - b. Change Auto Remediation to 'Yes'
 - c. Resource ID Parameter: choose 'BucketName'

Remediation action AWS-EnableS3BucketEncryption
Enables Encryption on S3 Bucket

Auto remediation ☒ Yes ☐ No
If a resource is still non-compliant after auto-remediation, you can set this rule to try again. Note, there are costs associated with running a remediation script.

Retries in Seconds

Rate Limits You can specify the percentage of resources against which SSM documents are executed at a time and also the percentage of failed SSM executions for which the entire batch is marked as failed

Concurrent Execution Rate Error Rate

Resource ID parameter BucketName

5. In the parameters section change Automation Assume Role to the arn of the IAM role created in the [Task 3](#) ('IAMRoleArn' Noted earlier)
6. Leave SSE Algorithm as 'AES256'

Parameters Every parameter has either a static value or a dynamic value. By default, the dynamic value is no-resource type. Only when the dynamic value is no-resource type, you can enter a static value. Alternatively, you can choose a resource type from the dynamic value drop-down list. Upon choosing a dynamic value, the static value is cleared (if present) and grayed. Depending on the remediation action, you will see either specific parameters or no parameters.

Key	Value
AutomationAssumeRole	ARNfromCloudFormation
BucketName*	
SSEAlgorithm	AES256

* Required fields

7. Click Save
8. Check the rule status and verify that encryption was turned on for your S3 Bucket

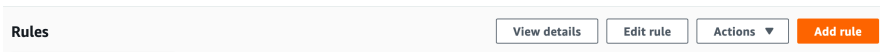
OR

9. Choose to use the redesigned interface if prompted

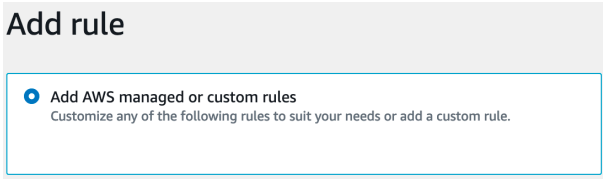
i The redesigned AWS Config console is now available for use.
We've completely redesigned the console to improve the overall look and feel. [Try it out now.](#)

10. Click the navigation icon in the top left (≡) and choose Rules

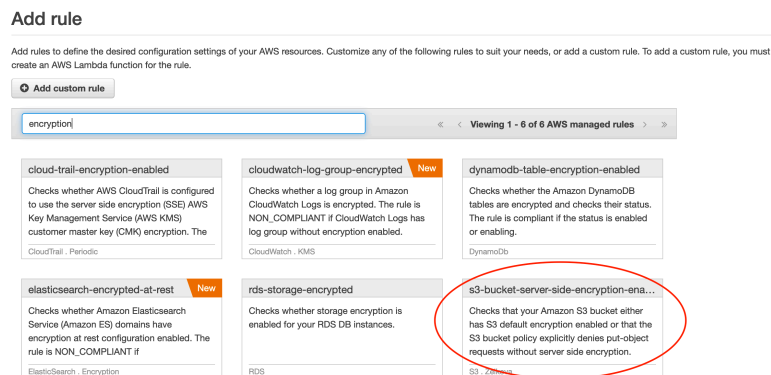
11. Click 'Add Rule'



12. Select the 'Add AWS managed or custom rules' option



13. Search for Encryption and select 's3-bucket-server-side-encryption-ena...'



14. Leave the defaults up until the 'Choose Remediation Section'

15. Modify the following settings

- a. Remediation Action: choose 'AWS-EnableS3BucketEncryption'
- b. Change Auto Remediation to 'Yes'
- c. Resource ID Parameter: choose 'BucketName'

Remediation action AWS-EnableS3BucketEncryption
Enables Encryption on S3 Bucket

Auto remediation ☒ Yes ☐ No
If a resource is still non-compliant after auto-remediation, you can set this rule to try again. Note, there are costs associated with running a remediation script.

Retries in Seconds

Rate Limits You can specify the percentage of resources against which SSM documents are executed at a time and also the percentage of failed SSM executions for which the entire batch is marked as failed

Concurrent Execution Rate Error Rate

Resource ID parameter BucketName

- d. In the parameters section change Automation Assume Role to the arn of the IAM role created in the [Task 3](#) ('IAMRoleArn' Noted earlier)
- e. Leave SSE Algorithm as 'AES256'

Parameters Every parameter has either a static value or a dynamic value. By default, the dynamic value is no-resource type. Only when the dynamic value is no-resource type, you can enter a static value. Alternatively, you can choose a resource type from the dynamic value drop-down list. Upon choosing a dynamic value, the static value is cleared (if present) and grayed. Depending on the remediation action, you will see either specific parameters or no parameters.

Key	Value
AutomationAssumeRole	ARNfromCloudFormation
BucketName*	
SSEAlgorithm	AES256

* Required fields

- f. Click Save
- g. Check the rule status and verify that encryption was turned on for your S3 Bucket

Task 7 – Additional Testing

Now that you have deployed the environment and remediated the security vulnerabilities through a combination of AWS Config and AWS Security Hub test out deploying resources with known vulnerabilities.

Examples

- Create a new EC2 instance with SSH open to the public internet
- Create a new S3 bucket not encrypted with public read/write settings

Once deployed go back in and check the settings.

Do the vulnerabilities still exist?

Task 8 – Cleanup

As these are temporary accounts, environments will be deleted upon completion. However; best practices would indicate to delete each deployed CloudFormation stack to avoid incurring additional costs. If you encounter errors with deleting the Config.yaml CloudFormation Stack, go to AWS config open any rule that hasn't been deleted > click edit > click delete rule (bottom of page). Once you have done this try to delete the CloudFormation Stack again.

Manually disable Security Hub and Config as follows

- Disable Security Hub (settings > general > disable)
- Disable Config (settings > edit > uncheck Enable Recorder > save)

Task 9 – Optional (further reading/discussion)

Appendix A: Troubleshooting common issues

Problem: My CloudFormation stack shows failed after I attempt to delete it.

Fix: Sometimes Config Rules with remediations fail to delete through the CloudFormation process. If you experience this, go into AWS Config and delete the rules, then delete the CloudFormation stack; it will then succeed.

Problem: I created a new AWS Config rule but the remediation isn't working.

Fix: Verify that you used the IAMRoleArn from the Config CloudFormation deployment. Additionally, if you chose a different remediation you will need to update the IAM role with proper policies.

Problem: I don't see the stack that I deployed.

Fix: Verify that you are working in the US-East-1 region.