re:Invent 2019

ARC319

Security Vulnerability Identification and Remediation

Table of Contents

Prerequisites 4
Problem Statement 5
Solution Overview 6
Task 1 – Enable AWS Config 7
Task 2 – Deploy AWS Config rules/remediations 8
Task 3 – Deploy the Three Tier Web App 9
Task 4 – Create AWS Resources (manual) 10
Task 5 – Create a new AWS Config Rule (manual) 12
Task 6 – Enable Security Hub and Check your security findings 13
Task 7 – Review the AWS Config deployed rules 15
Task 8 – Validate Remediation 15
Task 9 – Cleanup 17
Task 10 – 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.

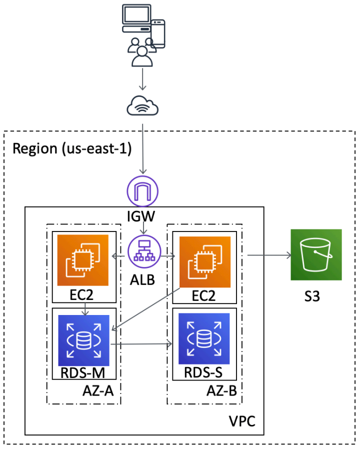
Problem Statement

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 eu-central-1 (Frankfurt); and the architecture provides a WordPress environment to host the online blogging platform. AWS services included are Amazon EC2, Amazon S3, and Amazon RDS.

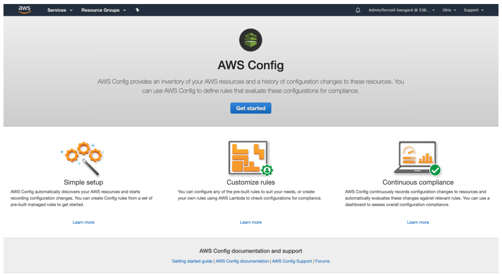
In the workshop, you will need to ensure that the new technology stack fits within your company's security posture. Your company is fairly new to AWS but has heard about services like AWS Config, AWS Security Hub, Amazon GuardDuty, and Amazon Macie to help secure their environment. This lab will focus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

Task 1 – Enable AWS Config

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 eu-central-1 (Frankfurt); (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'


aws
Services
Resource Groups
Admin/forrcoll-Isengard @ 538...
Ohio
Support
Get started
Learn more
Learn more
Learn more
Getting started guide | AWS Config documentation | AWS Config Support | Forums

AWS Config

AWS Config provides an inventory of your AWS resources and a history of configuration changes to these resources. You can use AWS Config to define rules that evaluate these configurations for compliance.

Simple setup

AWS Config automatically discovers your AWS resources and starts recording configuration changes. You can create Config rules from a set of pre-built managed rules to get started.

Customize rules

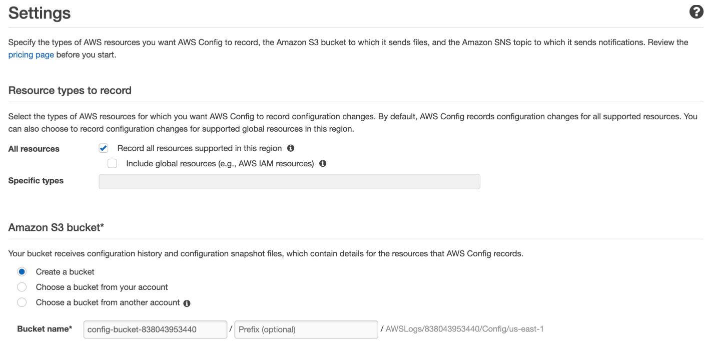
You can configure any of the pre-built rules to suit your needs, or create your own rules using AWS Lambda to check configurations for compliance.

Continuous compliance

AWS Config continuously records configuration changes to resources and automatically evaluates these changes against relevant rules. You can use a dashboard to assess overall configuration compliance.

AWS Config documentation and support

5. In 'Step 1: Settings' ensure the following options are configured
   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

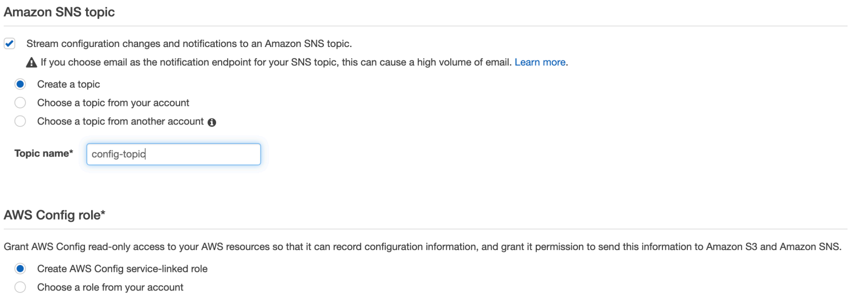
Amazon S3 bucket*

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* config-bucket-838043953440 / Prefix (optional) / AWSLogs/838043953440/Config/us-east-1

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* config-topic

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”

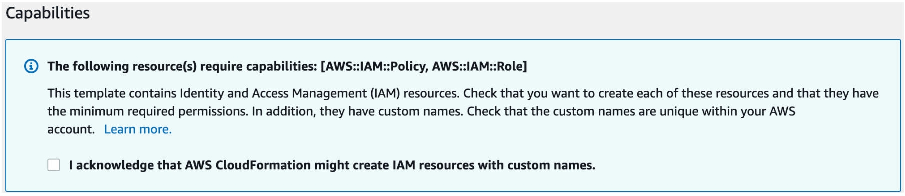
Task 2 – Deploy AWS Config rules/remediations

Launch the AWS Config CloudFormation stack in eu-central-1 (Frankfurt):

Launch Stack

The link opens the CloudFormation console in your account eu-central-1 region.

1. In ‘Specify Template’, click Next. (details should be pre-populated)
2. Under ‘Specify Stack Details’
    a. Enter an email that you have access to in MyEmailAddress; this will be used for remediation notifications
    b. Review, but 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

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

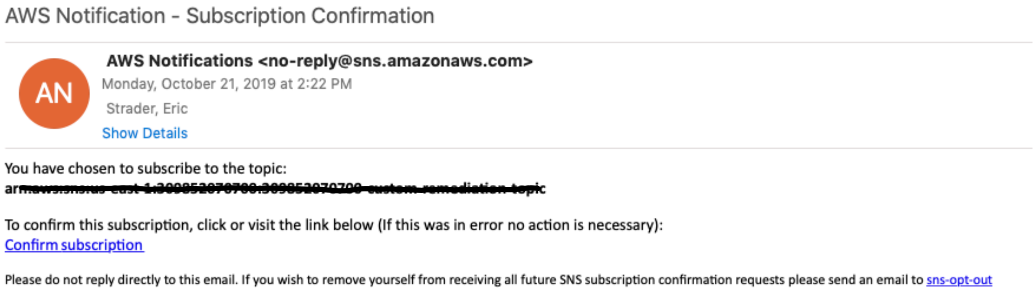
This template contains Identity and Access Management (IAM) resources. Check that you want to create each of these resources and that they have the minimum required permissions. In addition, they have custom names. Check that the custom names are unique within your AWS account. Learn more.

□ **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:
[redacted]

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 3 – Deploy the Three Tier Web App

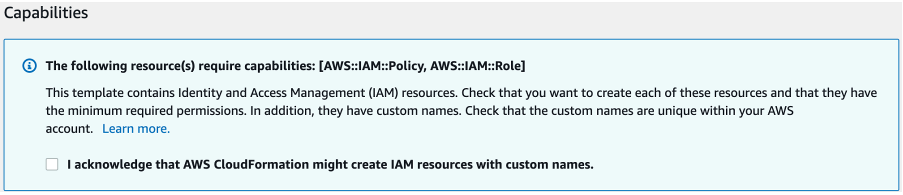
*****The steps below will deploy an environment with intentional security vulnerabilities, this template should ONLY be deployed into temporary/sandbox AWS accounts and not into your corporate environment or anywhere with sensitive data.**

Launch the AWS Three Tier Web App CloudFormation stack in eu-central-1 (Frankfurt):

Launch Stack ▶

The link opens the CloudFormation console in your account in eu-central-1 region.

1. In 'Specify Template', click Next.
2. In 'Specify Stack Details' 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.



Capabilities

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.

The creation of this stack can take up to 5 minutes. While the CloudFormation stack is being created we'll review the CloudFormation Template.

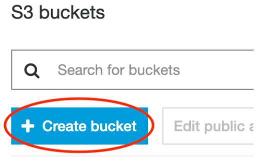
<u>Discussion: Do you see anything that might generate security concerns? (Hint… Hint… Look at lines 295 and 350.)</u>

Task 4 – Create AWS Resources (manual)

Now we are going to manually create some resources as well to illustrate how we can detect and remediate findings that were deployed via CloudFormation (previously) and manually (this step).

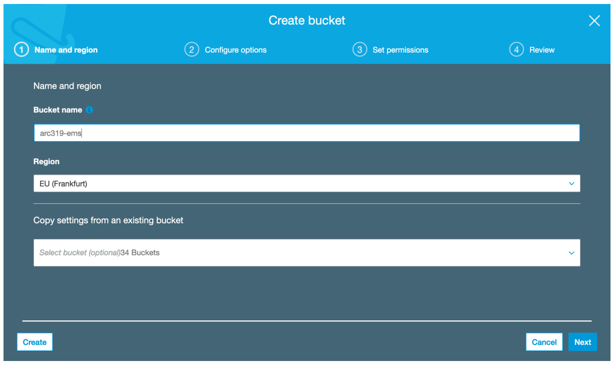
Create an S3 bucket

1. Navigate to the S3 service (click services at the top; S3 is under 'storage')
2. Click the 'Create bucket' button



S3 buckets

3. In the 'create bucket' screen give your bucket a name (recommend arc319-'your initials' to ensure it is uniquely named)
4. Leave the Region default and click 'Next'



Create bucket

Name and region

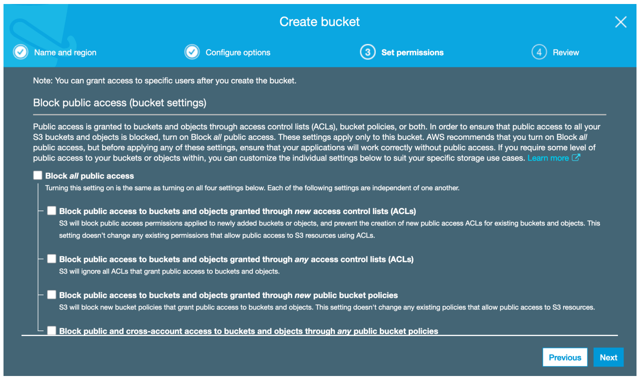
Bucket name: arc319-ems

Region: EU (Frankfurt)

Copy settings from an existing bucket

Select bucket (optional)34 Buckets

5. On the 'Create bucket' tab leave the defaults and click 'Next'
6. On the 'Set Permissions' tab uncheck 'Block all public access' click 'next'



Note: You can grant access to specific users after you create the bucket.

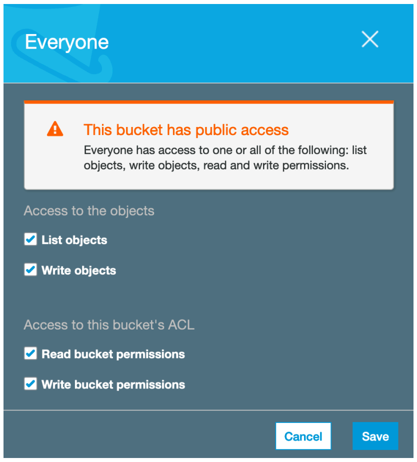
Block public access (bucket settings)

Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, or both. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block *all* public access. These settings apply only to this bucket. AWS recommends that you turn on Block *all* public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more

□ **Block *all* public access**
Turning this setting on is the same as turning on all four settings below. Each of the following settings are independent of one another.

- □ **Block public access to buckets and objects granted through *new* access control lists (ACLs)**
  S3 will block public access permissions applied to newly added buckets or objects, and prevent the creation of new public access ACLs for existing buckets and objects. This setting doesn't change any existing permissions that allow public access to S3 resources using ACLs.
- □ **Block public access to buckets and objects granted through *any* access control lists (ACLs)**
  S3 will ignore all ACLs that grant public access to buckets and objects.
- □ **Block public access to buckets and objects granted through *new* public bucket policies**
  S3 will block new bucket policies that grant public access to buckets and objects. This setting doesn't change any existing policies that allow public access to S3 resources.
- □ **Block public and cross-account access to buckets and objects through *any* public bucket policies**

7. On the ‘Review’ tab, click ‘Create bucket’
8. Once created click the bucket name and go to the ‘Permissions’ tab, Select ‘Access Control List’
9. Under ‘Public Access’ click the radio button next to ‘Everyone’
10. In the ‘Everyone box’ that pops up check all four options and click ‘Save’



This bucket has public access
Everyone has access to one or all of the following: list objects, write objects, read and write permissions.

Access to the objects

☑ **List objects**

☑ **Write objects**

Access to this bucket's ACL

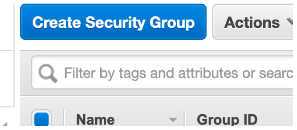
☑ **Read bucket permissions**

☑ **Write bucket permissions**

*****You should never open an S3 bucket to public access unless it is required, we have made this bucket public to allow us to see the remediation from resources deployed via CloudFormation and Manually.**

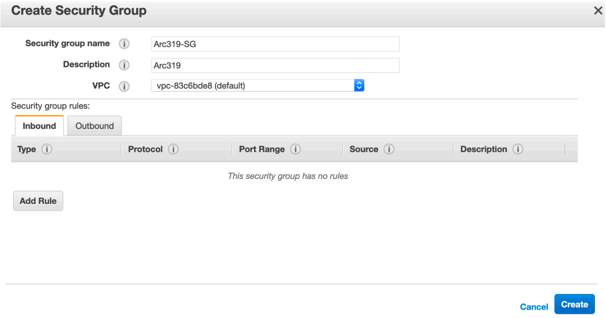
Create a Security Group

1. Navigate to the EC2 service (click services at the top; EC2 is under ‘Compute’)
2. In the left navigation pane under ‘Network & Security’ click on ‘Security Groups’
3. In the Security Group window click on the ‘Create Security Group’ button



4. In the ‘Create Security Group’ window change the following

   a. Name the Security Group (recommend Arc319-SG)
   b. Provide a Description (recommend Arc319)
   c. Then click ‘Create’



Create Security Group

Security group name: Arc319-SG

Description: Arc319

VPC: vpc-83c6bde8 (default)

Security group rules:

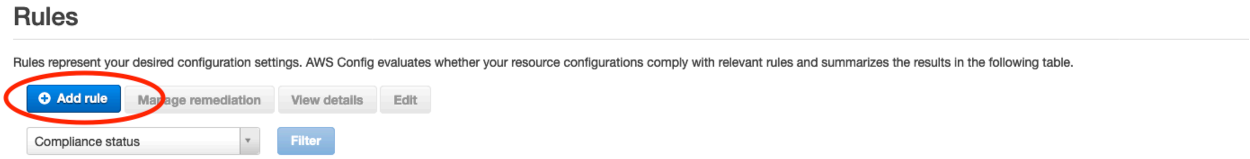
Type	Protocol	Port Range	Source	Description

This security group has no rules

5. Once created make note of the las three digits of the ‘Group ID’ for your newly created security group (this will help you identify it later)

Task 5 – Create a new AWS Config Rule (manual)

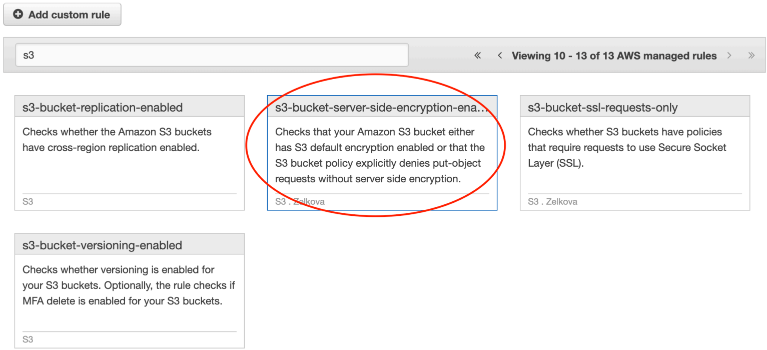
1. Navigate to the AWS Config service (click services at the top; Config is under ‘Management & Governance’)
2. In the left side navigation pane, select rules
3. Select ‘Add Rule’



Rules

Rules represent your desired configuration settings. AWS Config evaluates whether your resource configurations comply with relevant rules and summarizes the results in the following table.

4. Search for ‘s3-bucket-server’ and select ‘s3-bucket-server-side-encryption-ena…’



s3

Viewing 10 - 13 of 13 AWS managed rules

s3-bucket-replication-enabled

Checks whether the Amazon S3 buckets have cross-region replication enabled.

S3

s3-bucket-server-side-encryption-ena…

Checks that your Amazon S3 bucket either has S3 default encryption enabled or that the S3 bucket policy explicitly denies put-object requests without server side encryption.

S3 . Zelkova

s3-bucket-ssl-requests-only

Checks whether S3 buckets have policies that require requests to use Secure Socket Layer (SSL).

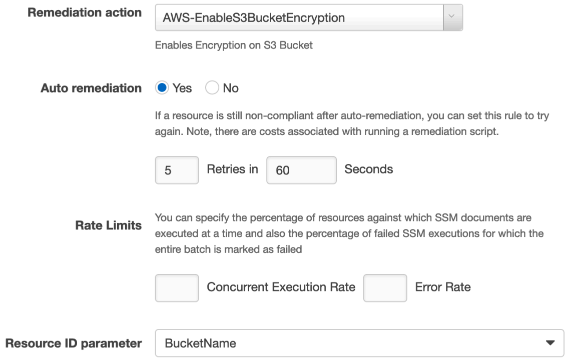
S3 . Zelkova

s3-bucket-versioning-enabled

Checks whether versioning is enabled for your S3 buckets. Optionally, the rule checks if MFA delete is enabled for your S3 buckets.

S3

5. Leave the defaults up until the ‘Choose Remediation’ Section
6. 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.

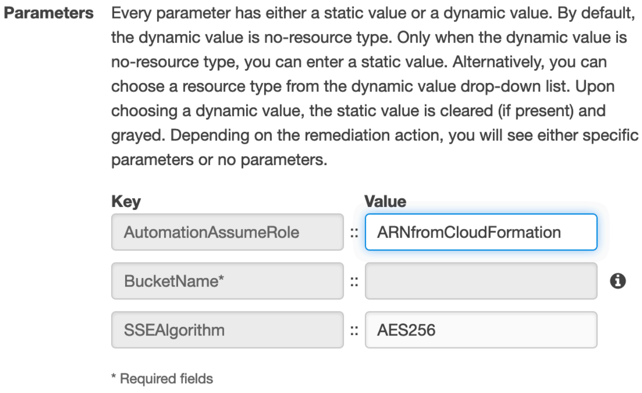
5 Retries in 60 Seconds

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

7. In the parameters section change AutomationAssumeRole to the arn of the IAM role created in the Task 3 ('**IAMRoleArn'** Noted earlier)
8. 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.

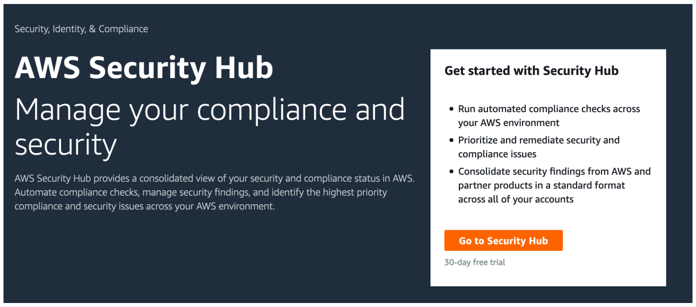
Key	Value
AutomationAssumeRole	ARNfromCloudFormation
BucketName*	
SSEAlgorithm	AES256

* Required fields

9. Click Save
10. In the 'rules' window select the rule titled 'S3-bucket-server-side-encryption-enabled'
11. We will check on this rule in a subsequent step as it can take a few minutes for it to trigger

Task 6 – Enable Security Hub and 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. Ensure your region is eu-central-1 (Frankfurt); (in the top right navigation bar)
3. If you get the screen below, click 'Go to Security Hub'



Security, Identity, & Compliance

AWS Security Hub

Manage your compliance and security

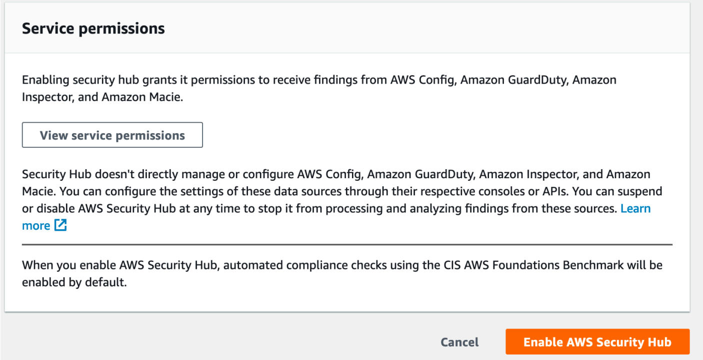
AWS Security Hub provides a consolidated view of your security and compliance status in AWS. Automate compliance checks, manage security findings, and identify the highest priority compliance and security issues across your AWS environment.

Get started with Security Hub

- Run automated compliance checks across your AWS environment
- Prioritize and remediate security and compliance issues
- Consolidate security findings from AWS and partner products in a standard format across all of your accounts

30-day free trial

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



Service permissions

Enabling security hub grants it permissions to receive findings from AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie.

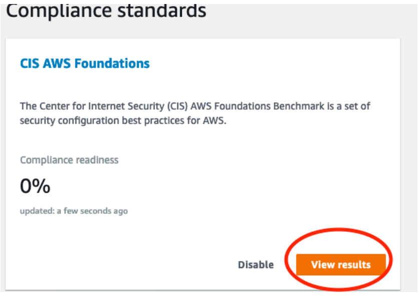
Security Hub doesn't directly manage or configure AWS Config, Amazon GuardDuty, Amazon Inspector, and Amazon Macie. You can configure the settings of these data sources through their respective consoles or APIs. You can suspend or disable AWS Security Hub at any time to stop it from processing and analyzing findings from these sources. Learn more

When you enable AWS Security Hub, automated compliance checks using the CIS AWS Foundations Benchmark will be enabled by default.

5. Scroll through the 'Summary' section
6. Click on the 'Integrations' link on the left side and explore the different AWS Services and 3rd party solutions that integrate with Security Hub.

<u>**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?**</u>

7. Click on 'Compliance Standards'
8. Click on View Results



Compliance standards

CIS AWS Foundations

The Center for Internet Security (CIS) AWS Foundations Benchmark is a set of security configuration best practices for AWS.

Compliance readiness

0%

updated: a few seconds ago

9. The foundational controls that are displayed are based on CIS Hardening; providing greater visibility and allowing you to identify additional vulnerabilities. (actual findings related to these controls will show up in the 'Findings' section)
10. In the 'Filter Controls' search box type 'S3'

We can see a large number of findings are listed. This is great for an environment that is regularly monitored, unfortunately yours is not. In addition, what about internally mandated controls (versus CIS) like encrypted S3 buckets?

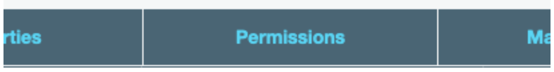
Discussion: How could you enable automated remediation for these findings or add new controls?

Task 7 – Review the AWS Config deployed rules

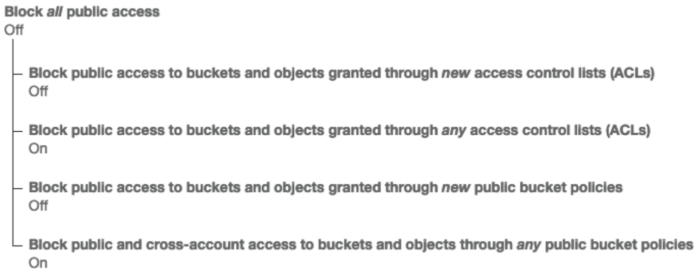
1. Navigate to the AWS Config service (click services at the top; Config is under 'Management & Governance')
2. In the left navigation pane click on Rules
3. Look at the rule titled 'S3_BUCKET_PUBLIC_READ_PROHIBITED'
    a. Click the rule name
    b. Click Edit
    c. Explore the remediation actions
    d. We see that this rule is being remediated with a Systems Manager pre-defined remediation
    e. Click Cancel
4. Now look at the rule that includes 'REQUIRED_TAGS' in the name
    a. Click 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.
5. Open AWS Lambda (click services at the top; Lambda is under 'Compute')
    a. Open the Lambda function where the name includes 'RequiredTags'
    b. Review the Lambda function to understand how it is remediating inconsistent/non-existent tags

Task 8 – Validate Remediation

1. Go back into the rule titled S3_BUCKET_PUBLIC_READ_PROHIBITED'and check the 'Compliance Status' section at the bottom
    a. Click on the name of the bucket you created (Arc319-'your initials')
    b. Click the 'Manage Resource' button in the top right
    c. Once in the corresponding S3 bucket, click the 'Permissions' tab



d. View the 'Block public access' rule and validate that it looks like the following screenshot



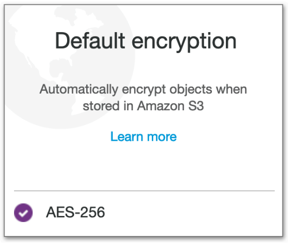
Block *all* public access
Off

- Block public access to buckets and objects granted through *new* access control lists (ACLs)
  Off
- Block public access to buckets and objects granted through *any* access control lists (ACLs)
  On
- Block public access to buckets and objects granted through *new* public bucket policies
  Off
- Block public and cross-account access to buckets and objects through *any* public bucket policies
  On

e. While were here let's also validate that the bucket is encrypted (based on the rule we manually created)

f. Click on the Properties tab

g. There should be a checkbox in the 'Default encrption' box like the image below



Default encryption

Automatically encrypt objects when stored in Amazon S3

Learn more

☑ AES-256

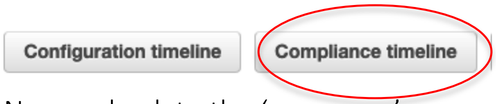
h. Go ahead and validate these same settings on the S3 bucket that was created by the CloudFormation template

i. Congratulations, your config rules has blocked public access and enabled encryption!

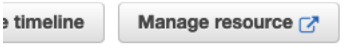
6. Go back to the config look at the rule that includes 'REQUIRED_TAGS' in the name

a. In the compliance status section click on one of the resource names (either the security group you manually created or one of the resources created by CloudFormation)

b. Explore this section by looking at the compliance timelines



c. Now go back to the 'resources' screen for the resource you selected and choose 'Manage Resource' in top right



d. Validate that the tags have been updated in the corresponding resource, they should be as follows (clicking the 'Tags' tab within the resource)

  i. CostCenter = 900124-984
  ii. Owner = Brad Pitt (but not THAT Brad Pitt)
  iii. Workload=WordPress

e. Now check your email (email used when you deployed the CloudFormation Stack) and validate that you received notifications regarding missing required tags.

Task 9 – 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.

If you have the AWS CLI configured or are familiar with a Node JS development environment, you can use the material https://github.com/collinforrester/aws-config-helpers#aws-config-helpers to help clean up.

Manually disable Security Hub and Config as follows

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

Task 10 – Optional (further reading/discussion)

- AWS Config
- AWS Conformance Packs
- AWS Security Hub
- CIS Hardening
- Amazon Macie
- Amazon GuardDuty
- Service Control Policies

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 eu-central-1.

Problem: I have created an AWS Config rule but it is not finding any resources out of compliance?
Fix: Depending on the type of rule and size of the account it can take some time for the rule to evaluate/remediate. Check back in later.