

Laboratoire: Sécuriser une application avec plusieurs services AWS

Scénario:

Vous avez été embauché par une entreprise qui a une expérience limitée d'AWS et qui a besoin de votre expertise en tant que **SysOps administrator** pour renforcer la sécurité de ses applications. Vos tâches consistent à supprimer les secrets d'un modèle CloudFormation, à configurer une ACL web et à vous assurer qu'une instance EC2 est configurée pour fonctionner avec Systems Manager, ce qui est une condition préalable pour que les instances fonctionnent avec Amazon Inspector.

Description

Ce laboratoire pratique exige que vous travailliez avec tous les services majeurs suivants : Amazon Inspector, Web Application Firewall et AWS Secrets Manager.

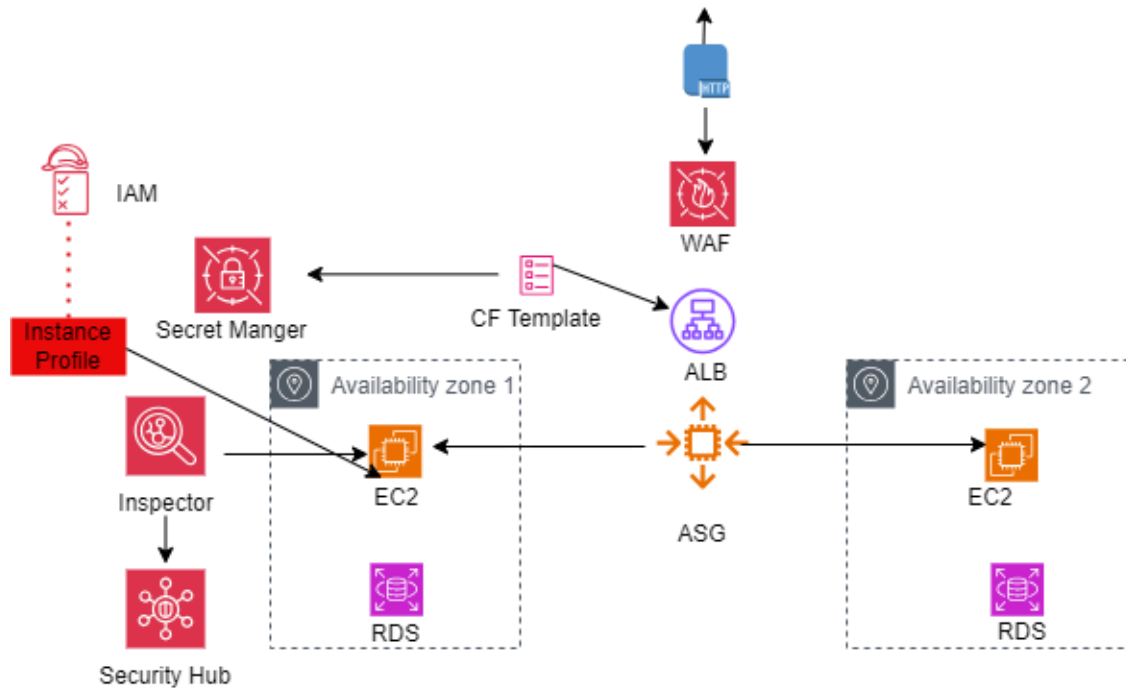
Temps de réalisation: 2h maximum.

Liste des services

- AWS WAF;
- AWS Security Hub;
- AWS IAM
- EC2;
- Amazon Inspector;
- AWS Secret Manager;
- AWS Config;
- AWS CloudFormation

Architecture

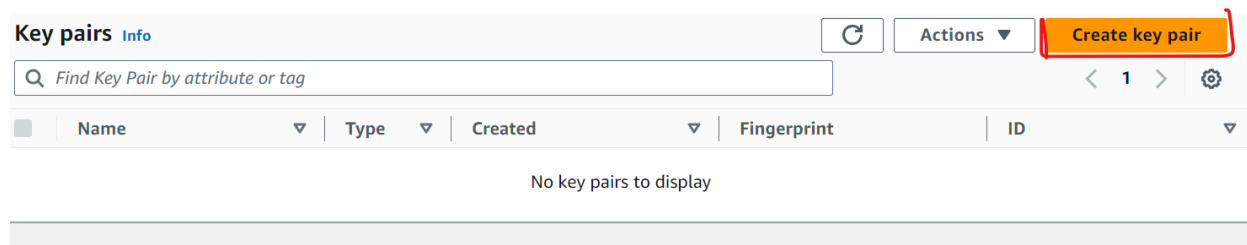
Sécurisation d'une application avec de multiple services AWS



Coûts: offre free tier

Réalisation¹

- Accédez à la console EC2 en recherchant et en sélectionnant EC2 dans la barre de recherche supérieure, ou en la sélectionnant dans la liste des sites récemment visités.
- Dans le menu de navigation de gauche, sous Réseau et sécurité, cliquez sur Paires de clés.



¹ AWS Cloud Engineer BootCamp by EazyTraining

- Dans le coin supérieur droit, cliquez sur Créer une paire de clés.
- Sous Nom, entrez sur **MyKeyPair**.
- Laissez les autres paramètres par défaut et cliquez sur Créer une paire de clés.

Create key pair

Key pair name

Key pairs allow you to connect to your instance securely.

MyKey

The name can include up to 255 ASCII characters. It can't include leading or trailing spaces.

Key pair type

☒ RSA
RSA encrypted private and public key pair

☐ ED25519
ED25519 encrypted private and public key pair

Private key file format

☒ .pem
For use with OpenSSH

☐ .ppk
For use with PuTTY

Cancel

Create key pair

- Dans la barre de recherche en haut, recherchez et sélectionnez VPC.

Last updated less than a minute ago

Actions

Create VPC

Create default VPC

Create flow log

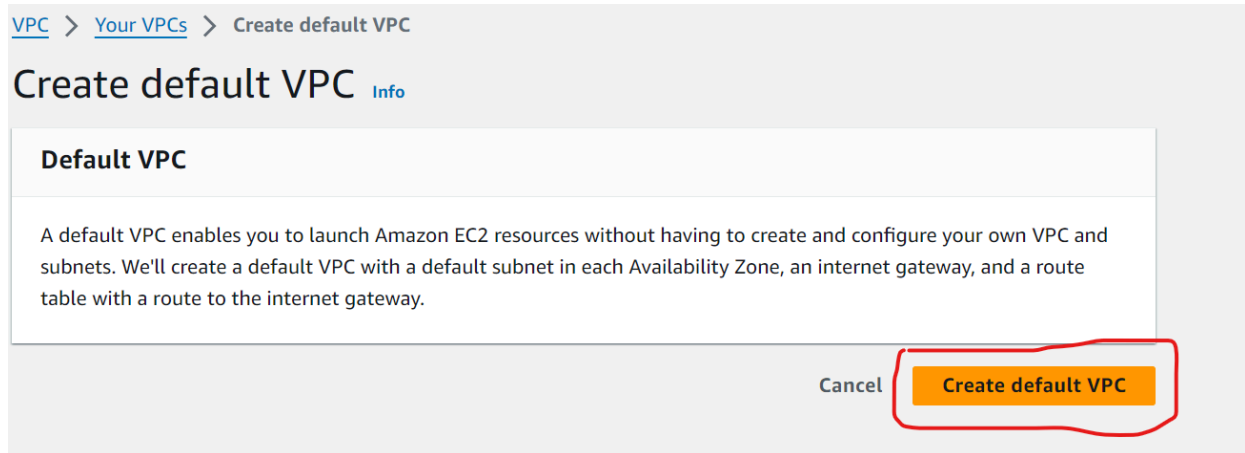
Edit VPC settings

Edit CIDRs

Manage middlebox routes

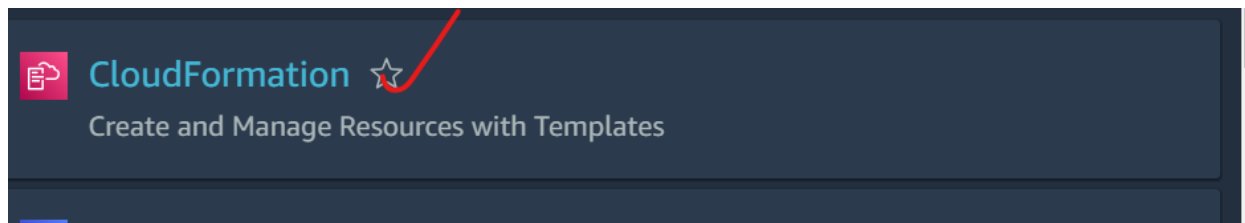
VPC ID	State
vpc-01084b270e74e9eb5	Available

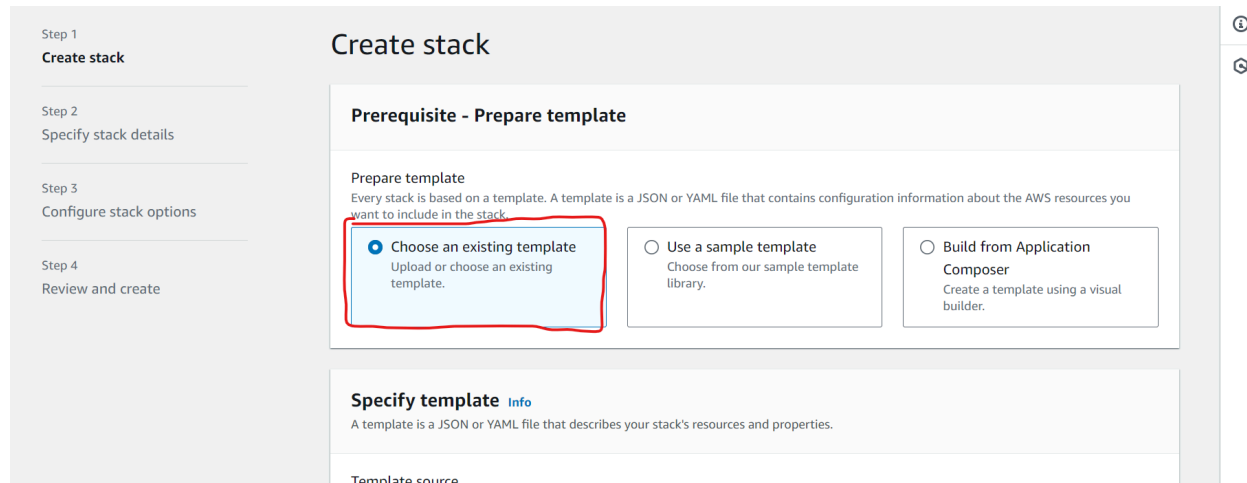
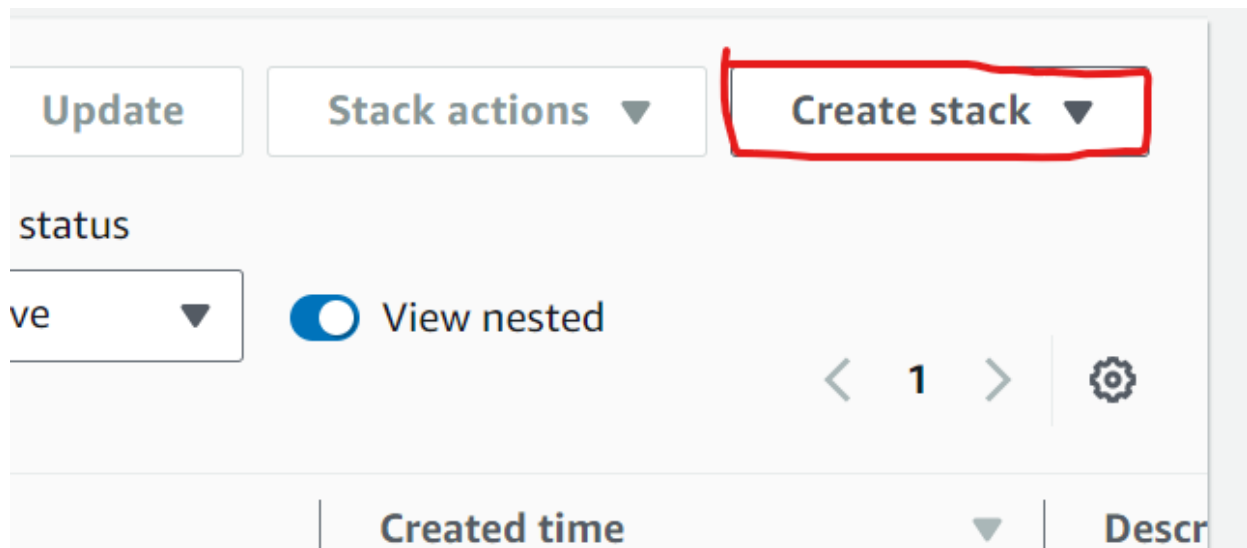
- Sous ressources par région, cliquez sur VPC.
- Dans le coin supérieur droit, cliquez sur le menu déroulant Actions et sélectionnez Créer un VPC par défaut.
- Cliquez sur Créer un VPC par défaut.



1. Déployer une application à l'aide d'un modèle CloudFormation

- Dans la console CloudFormation, sélectionnez Créer une pile.





- Téléchargez le modèle fourni.

Specify template [Info](#)

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

☐ Amazon S3 URL

Provide an Amazon S3 URL to your template.

☒ Upload a template file

Upload your template directly to the console.

☐ Sync from Git - *new*

Sync a template from your Git repository.

Upload a template file

 Choose file

WordPress.json

JSON or YAML formatted file

S3 URL: <https://s3.us-east-1.amazonaws.com/cf-templates-1wfc4uykqucx6-us-east-1/2024-08-08T182609.842Zxx8-WordPress.json>

[View in Application Composer](#)

- Cliquez sur l'icône pour créer une pile.
- Entrez les paramètres.
- Cliquez sur Suivant.
- Cliquez sur Suivant.
- Cliquez sur Submit (pour créer la pile).
- Créer des secrets dans Secrets Manager

[CloudFormation](#) > [Stacks](#) > Create stack

Step 1

[Create stack](#)

Step 2

Specify stack details

Step 3

Configure stack options

Step 4

Review and create

Specify stack details

Provide a stack name

Stack name

my-stack

Stack name must be 1 to 128 characters, start with a letter, and only contain alphanumeric characters. Character count: 8/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

DBAllocatedStorage

The size of the database (Gb)

5

DBClass

Database instance class

db.t3.small

DBName

The WordPress database name

wordpressdb

DBPassword

The WordPress database admin account password

.....

DBUser

The WordPress database admin account username

.....

InstanceType

WebServer EC2 instance type

instance type

WebServer EC2 instance type

t3.micro

KeyName

Name of an existing EC2 KeyPair to enable SSH access to the instances

MyKeyPair

MultiAZDatabase

Create a Multi-AZ MySQL Amazon RDS database instance

false

SSHLocation

The IP address range that can be used to SSH to the EC2 instances

0.0.0.0/0

Subnets

The list of SubnetIds in your Virtual Private Cloud (VPC)

Select List<AWS::EC2::Subnet::Id>

subnet-0bc572b5b4764c56c

subnet-03fc2157315dfa099

subnet-0b99596c7d9b805b9

VpcId

VpcId of your existing Virtual Private Cloud (VPC)

vpc-0b64f94d2bc0ab4c0

WebServerCapacity

The initial number of WebServer instances

1

Cancel

Previous

Next

CloudFormation > Stacks > Create stack

Step 1

[Create stack](#)

Step 2

[Specify stack details](#)

Step 3

Configure stack options

Step 4

Review and create

Configure stack options

Tags - optional

Tags (key-value pairs) are used to apply metadata to AWS resources, which can help in organizing, identifying, and categorizing those resources. You can add up to 50 unique tags for each stack.

No tags associated with the stack.

Add new tag

You can add 50 more tag(s)

Permissions - optional

Specify an existing AWS Identity and Access Management (IAM) service role that CloudFormation can assume.

CloudFormation > Stacks > Create stack

Step 1

[Create stack](#)

Step 2

[Specify stack details](#)

Step 3

[Configure stack options](#)

Step 4

Review and create

Review and create

Step 1: Specify template

Edit

Prerequisite - Prepare template

Template

-

Template

Template URL

<https://s3.us-east-1.amazonaws.com/cf-templates-1wfc4uykqucx6-us-east-1/template-1723142691540.json>

Quick-create link

Use quick-create links to get stacks up and running quickly from the AWS CloudFormation console with the same basic configuration as this stack. Copy the URL on the link to share. [Learn more](#)

Open quick-create link

Create change set

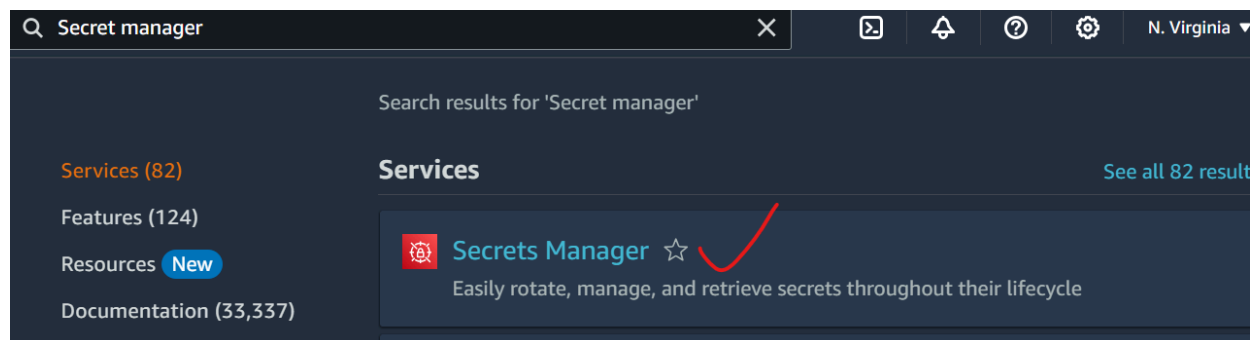
Cancel

Previous

Submit

2. Dans la console Secrets Manager, cliquez sur Store a new secret.

- Saisissez le nom d'utilisateur et le mot de passe du secret.
- Sélectionnez la base de données, puis cliquez sur Suivant.
- Donnez un nom au secret, puis cliquez sur Suivant.
- Cliquez sur Suivant, puis sur Stocker.



Security, Identity, & Compliance

AWS Secrets Manager

Easily rotate, manage,
and retrieve secrets

Get started

You can store database credentials or
any other type of secret.

Store a new secret

[AWS Secrets Manager](#) > [Secrets](#) > Store a new secret

Step 1

Choose secret type

Step 2

Configure secret

Step 3 - optional

Configure rotation

Step 4

Review

Choose secret type

Secret type [Info](#)

☒ Credentials for Amazon RDS database

☐ Credentials for Amazon DocumentDB database

☐ Credentials for Amazon Redshift data warehouse

☐ Credentials for other database

☐ Other type of secret
API key, OAuth token, other.

Credentials [Info](#)

User name

Credentials [Info](#)

User name

Password

☐ Show password

Encryption key [Info](#)

You can encrypt using the KMS key that Secrets Manager creates or a customer managed KMS key that you create.



[Add new key](#)

Database [Info](#)

Search instances

< 1 >

	DB insta... ▾	DB engine ▾	Status ▾	Creation date (UTC) ▾
	my-stack-d...	mysql	backing-up	August 8, 2024 at 19:06:14

Cancel

Next

Configure secret

Secret name and description [Info](#)

Secret name

A descriptive name that helps you find your secret later.

labsecret

Secret name must contain only alphanumeric characters and the characters /_+=.@-

Description - *optional*

labsecret

Maximum 250 characters.

Resource permissions - optional [Info](#)

[Edit permissions](#)

Add or edit a resource policy to access secrets across AWS accounts.

► Replicate secret - optional

Create read-only replicas of your secret in other Regions. Replica secrets incur a charge.

Cancel

Previous

Next

Configure rotation - *optional*

Configure automatic rotation [Info](#)

Configure AWS Secrets Manager to rotate this secret automatically.

☒ Automatic rotation

Rotation schedule [Info](#)

☒ Schedule expression builder

☐ Schedule expression

Time unit

Days ▼

Days

1

☒ Create a rotation function

☐ Use a rotation function from your account

Lambda rotation function

Secrets Manager adds the prefix 'SecretsManager' to your function name.

SecretsManager `mysql-rotation-lambda`

Function name is required. Rotation function name including prefix must be maximum 64 alphanumeric characters, hyphens, and underscores.

Rotation strategy [Info](#)

☒ Single user

The user must have permission to update their password.

☐ Alternating users

This strategy clones the initial user and stores both sets of credentials in one secret. One set of credentials is always valid. You must provide admin credentials in a separate secret.

Cancel

Previous

Next

Store a new secret

Review

Secret type

Secret type

Amazon RDS database

Encryption key

aws/secretsmanager

Secret configuration

```
2 // If you need more information about configurations or implementing the sample
3 // code, visit the AWS docs:
4 // https://docs.aws.amazon.com/sdk-for-java/latest/developer-guide/home.html
5
6 // Make sure to import the following packages in your code
7 // import software.amazon.awssdk.regions.Region;
8 // import software.amazon.awssdk.services.secretsmanager.SecretsManagerClient;
9 // import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueRequest;
10 // import software.amazon.awssdk.services.secretsmanager.model.GetSecretValueResponse;
11
12 public static void getSecret() {
13
14     String secretName = "labsecret";
```

Java Line 1, Column 1  Errors: 0  Warnings: 0 

 [Download AWS SDK for Java](#)

Cancel

Previous

Store

- Retournez à l'onglet du navigateur CloudFormation.
- Sur la gauche, assurez-vous que my-stack est sélectionné, puis dans le coin supérieur droit, cliquez sur Update.

my-stack

Delete

Update

Stack actions ▼

Create



Stack info

Events

Resources

Outputs

Parameters

Events (29)

Detect root cause

Search events

- Sous Prérequis - Préparer le modèle > Préparer le modèle, assurez-vous que Editer le modèle dans le concepteur est sélectionné.

Prerequisite - Prepare template

Prepare template

Every stack is based on a template. A template is a JSON or YAML file that contains configuration information about the AWS resources you want to include in the stack.

☐ Use existing template
Proceed with the template you are already using for this stack.

☐ Replace existing template
Replace your existing template with a new template.

☒ Edit in Application Composer
Edit your template in a visual builder.

Edit template in Application Composer

Use Application Composer to visually edit your stacks on a simple, drag-and-drop interface. Application Composer automatically updates and validates the template.

If your template references external files, it cannot be opened in Application Composer. [Learn more](#)

Edit in Application Composer

Canvas Template YAML JSON

Valid Update template

```
593
718 : {
817 },
818     "/g\" wp-config.php\n",
819     "sed -i \"s/'username_here'/'\", \"{{resolve:secretsmanager:labsecret:SecretString:u
820
821     "/g\" wp-config.php\n",
822     "sed -i \"s/'password_here'/'\", \"{{resolve:secretsmanager:labsecret:SecretString:pa
823
824     "/g\" wp-config.php\n",
825     "sed -i \"s/'localhost'/'\",
826     {
827         "Fn::GetAtt": [
828             "DBInstance",
```

Continue to CloudFormation

i We're putting the template in this existing bucket: cf-templates-1lof6k1qgp5l-us-west-1.
For more information, see [Using Application Composer in CloudFormation console mode](#).

► Use a different bucket

Cancel Confirm and continue to CloudFormation

Ensuite cliquer sur next et next et enfin submit

Change set preview

Changes (2)

< 1 >

Action	Logical ID	Physical ID	Resource type	Replacement
Modify	DBInstance	my-stack-dbinstance-u...	AWS::RDS::DBInstance	True
Modify	LaunchConfig	my-stack-LaunchConfi...	AWS::AutoScaling::Lau...	False

View change set

Cancel

Previous


Submit

3. Dans la console WAF, cliquez sur Create web ACL (Créer une liste de contrôle d'accès Web).

- Saisissez un nom pour l'ACL Web.


Search results for 'WAF'

Services [See all 10 results ►](#)



WAF & Shield ☆

Protects Against DDoS Attacks and Malicious Web Traffic



AWS Firewall Manager ☆

Central management of firewall rules

Security, Identity, and Compliance

AWS WAF

Protect your web applications from common web exploits

AWS WAF is a web application firewall service that lets you monitor web requests

Get started with AWS WAF

Set up protection for your Amazon CloudFront distributions, Application Load Balancers, and/or Amazon API Gateway stages in just under 5 minutes.

Create web ACL

Describe web ACL and associate it to AWS resources [Info](#)

Web ACL details

Resource type

Choose the type of resource to associate with this web ACL. Changing this setting will reset the page.

- ☐ Amazon CloudFront distributions
- ☒ Regional resources (Application Load Balancers, Amazon API Gateway REST APIs, AWS AppSync GraphQL APIs, Amazon Cognito user pools and AWS Verified Access Instances)

Region

Choose the AWS Region to create this web ACL in. Changing this setting will reset the page.

US West (N. California)

Name

My-Web-ACL

Description - optional

My-Web-ACL

The description can have 1-256 characters.

CloudWatch metric name

My-Web-ACL

The name must have 1-128 characters. Valid characters: A-Z, a-z, 0-9, - (hyphen), and _ (underscore).

- Cliquez sur Next (Suivant).
- Sélectionnez Add Rules (Ajouter des règles), puis Add AWS Managed Rules (Ajouter des règles gérées par AWS).

S Services Search [Alt+S] Global alphoncine @ aws-bootcamp-ea

AWS WAF > Web ACLs > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0) Edit Delete Add rules ▲

If a request matches a rule, take the corresponding action. The rules are prioritized in order.

Add managed rule groups ←

Add my own rules and rule groups

Name	Capacity
No rules.	
You don't have any rules added.	

Add AWS resources

Resource type

Select the resource type and then select the resource you want to associate with this web ACL.

☒ Application Load Balancer

☐ Amazon API Gateway REST API

☐ AWS AppSync GraphQL API

☐ Amazon Cognito user pool

☐ AWS Verified Access

Select the resources you want to associate with the web ACL.

Find AWS resources to associate < 1 > ⚙

Name
<input checked="" type="checkbox"/> my-sta-Appli-3nnUAXBRAqPW

Cancel Add

Associated AWS resources - optional (1/1)

Remove Add AWS resources

Find associated AWS resources < 1 > ⚙

Name	Resource type	Region
<input checked="" type="checkbox"/> my-sta-Appli-3nnUAXBRAqPW	Application Load Balancer	US West (N. California)

Cancel Next

- Cliquez sur Ajouter des règles.

Services Search [Alt+S] Global alphonsine @ aws-bootcamp-ea

AWS WAF > Web ACLs > Create web ACL

Step 1
[Describe web ACL and associate it to AWS resources](#)

Step 2
Add rules and rule groups

Step 3
Set rule priority

Step 4
Configure metrics

Step 5

Add rules and rule groups [Info](#)

A rule defines attack patterns to look for in web requests and the action to take when a request matches the patterns. Rule groups are reusable collections of rules. You can use managed rule groups offered by AWS and AWS Marketplace sellers. You can also write your own rules and use your own rule groups.

Rules (0)

If a request matches a rule, take the corresponding action. The rules are prioritized in order.

☐ Name Capacity

No rules.
You don't have any rules added.

Edit Delete Add rules ▲

Add managed rule groups ←

Add my own rules and rule groups

- Cliquez sur les boutons radio **Core rule set**, **SQL database** et **Known bad input**.

Add managed rule groups [Info](#)

Managed rule groups are created and maintained for you by AWS and AWS Marketplace sellers. Any fees that a managed rule group provider charges for using a managed rule group are in addition to the standard service charges for AWS WAF. [AWS WAF Pricing](#)

► **AWS managed rule groups**

Core rule set	700	<input checked="" type="radio"/> Add to web ACL Edit
Known bad inputs	200	<input checked="" type="radio"/> Add to web ACL Edit

► **ThreatSTOP managed rule groups**

Cancel [Add rules](#)

Rules (3)
Edit
Delete
Add rules ▼

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

<input type="checkbox"/>	Name	Capacity	Action
<input type="checkbox"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions
<input type="checkbox"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions

Web ACL capacity units (WCUs) used by your web ACL

The WCUs used by the web ACL will be less than or equal to the sum of the capacities for all of the rules in the web ACL.

The total WCUs for a web ACL can't exceed 5000. Using over 1500 WCUs affects your costs. [AWS WAF Pricing](#)

1100/5000 WCUs

Rules (3)
Move up
Move down

If a request matches a rule, take the corresponding action. The rules are prioritized in order they appear.

	Name	Capacity	Action
<input type="radio"/>	AWS-AWSManagedRulesCommonRuleSet	700	Use rule actions
<input checked="" type="radio"/>	AWS-AWSManagedRulesSQLiRuleSet	200	Use rule actions
<input type="radio"/>	AWS-AWSManagedRulesKnownBadInputsRuleSet	200	Use rule actions

Cancel
Previous
Next

- Cliquez sur Suivant jusqu'à ce que vous puissiez cliquer sur Créer une ACL Web.

Rules	CloudWatch metric name
<input checked="" type="checkbox"/> AWS-AWSManagedRulesCommonRuleSet	<input type="text" value="AWS-AWSManagedRulesCommonRuleSet"/>
<input checked="" type="checkbox"/> AWS-AWSManagedRulesSQLiRuleSet	<input type="text" value="AWS-AWSManagedRulesSQLiRuleSet"/>
<input checked="" type="checkbox"/> AWS-AWSManagedRulesKnownBadInputsRuleSet	<input type="text" value="AWS-AWSManagedRulesKnownBadInputsRuleSet"/>

Request sampling options

If you disable request sampling, you can't view requests that match your web ACL rules.

Options

☒ Enable sampled requests

☐ Disable sampled requests

☐ Enable sampled requests with exclusions

CancelPreviousNext

Review and create web ACL [Info](#)

Step 1: Describe web ACL and associate it to AWS resources

Edit step 1

Web ACL details

Name	Scope
My-Web-ACL	REGIONAL
Description	Region
My-Web-ACL	us-west-1
CloudWatch metric name	
My-Web-ACL	

Amazon CloudWatch metrics (3)

Rules	CloudWatch metric name
AWS-AWSManagedRulesCommonRuleSet	AWS-AWSManagedRulesCommonRuleSet
AWS-AWSManagedRulesSQLiRuleSet	AWS-AWSManagedRulesSQLiRuleSet
AWS-AWSManagedRulesKnownBadInputsRuleSet	AWS-AWSManagedRulesKnownBadInputsRuleSet

Sampled requests

Sampled requests

Enabled

Sampled requests for web ACL default actions

Enabled

Cancel

Previous

Create web ACL

Web ACLs [Info](#)

Web ACLs (1)

Web ACLs that you have defined in the selected region.

US West (N. California) ▼ Copy ARN Delete Create

Name	Description	ID
My-Web-ACL	My-Web-ACL	8acab84e-8af9-43ab-8261-

4. Dans la console IAM, sélectionnez Rôles, puis Créez un rôle.

IAM

Search results for 'IAM'

Services (11)

Features (24)

Resources New

Documentation (59,388)

Knowledge Articles (471)

Services

IAM

Manage access to AWS resources

IAM Identity Center

Dashboard

▼ Access management

User groups

Users

Roles 

Policies

Identity providers

Account settings

▼ Access reports



Delete

Create role

ations. Roles can be assumed by entities that you



< 1 >



trusted entities

Last activ

IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity [Info](#)

Trusted entity type

- ☒ **AWS service**
Allow AWS services like EC2, Lambda, or others to perform actions in this account.
- ☐ **AWS account**
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.
- ☐ **Web identity**
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.
- ☐ **SAML 2.0 federation**
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.
- ☐ **Custom trust policy**
Create a custom trust policy to enable others to perform actions in this account.

- Sélectionnez EC2, puis cliquez sur Suivant.

Use case

Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case

EC2

Choose a use case for the specified service.

Use case

- ☒ EC2

Cancel **Next**

- Attachez une politique : **AmazonSSMManagedInstanceCore**.


Add permissions [Info](#)

Permissions policies (1/951) [Info](#)

Choose one or more policies to attach to your new role.

Filter by Type

All types 1 match

<input checked="" type="checkbox"/>	Policy name ↗	Type	Description
<input checked="" type="checkbox"/>	 AmazonSSMManagedIns...	AWS managed	The policy for Amazon EC2 Role to ena...

► Set permissions boundary - *optional*

Cancel

Previous

Next

- Cliquez sur Suivant, nommez le rôle, puis cliquez sur Créer un rôle.

Name, review, and create

Role details

Role name

Enter a meaningful name to identify this role.

LabInstanceRole

Maximum 64 characters. Use alphanumeric and '+=, @-/_' characters.

Description

Add a short explanation for this role.

LabInstanceRole

Maximum 1000 characters. Use letters (A-Z and a-z), numbers (0-9), tabs, new lines, or any of the following characters: _+=, @-/_\[\]!#\$%^*()~;

Step 3: Add tags

Add tags - optional [Info](#)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

No tags associated with the resource.

Add new tag

You can add up to 50 more tags.

Cancel

Previous

Create role

- Allez sur la console de Ec2, sélectionner le serveur et aller sur action, ensuite security

Instances (1/1) [Info](#)

Find Instance by attribute or tag (case-sensitive)

Instance state = running X Clear filters

<input checked="" type="checkbox"/>	Name	Instance ID	Instance state	Instance type	State
<input checked="" type="checkbox"/>	1	i-0841437f39ad3bc86	Running	t3.micro	2

i-0841437f39ad3bc86

- Connect
- View details
- Manage instance state
- Instance settings
- Networking
- Security 3
- Image and templates
- Monitor and troubleshoot

Change security groups

Get Windows password

Modify IAM role 4

Modify IAM role [Info](#)

Attach an IAM role to your instance.

Instance ID

i-0841437f39ad3bc86

IAM role

Select an IAM role to attach to your instance or create a new role if you haven't created any. The role you select replaces any roles that are currently attached to your instance.

LabInstanceRole ✓

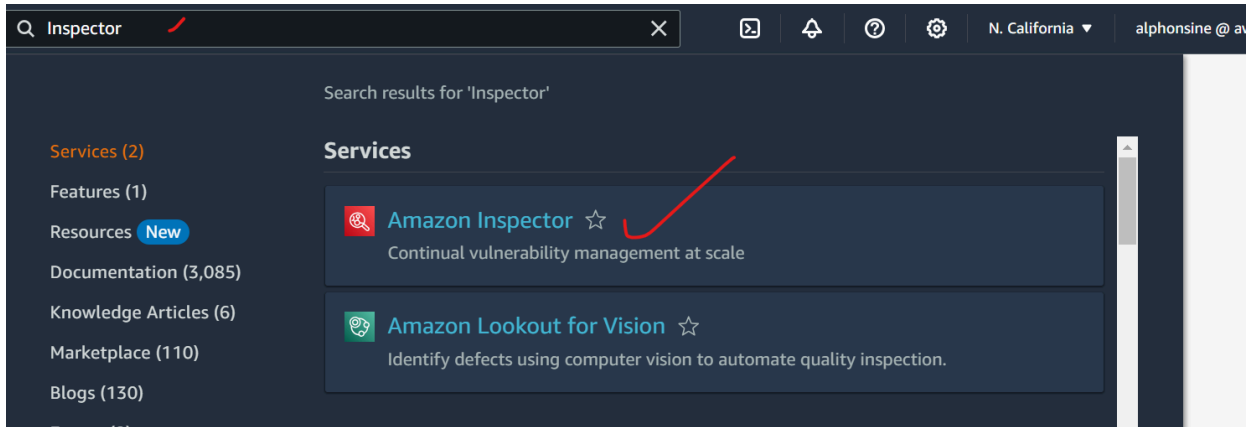
Refresh

Create new IAM role

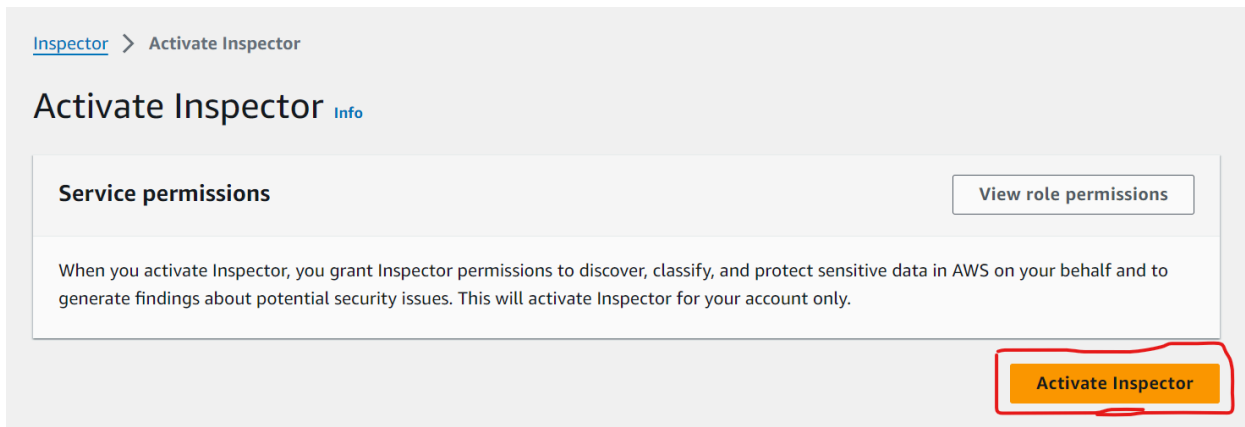
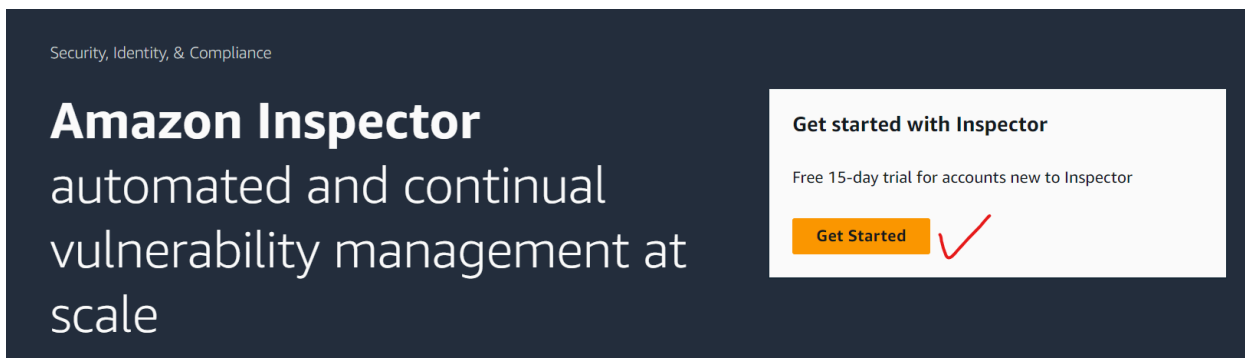
Cancel

Update IAM role

5. Dans la console de l'inspecteur, cliquez sur Démarrer.



- Cliquez sur Enable Inspector (Activer l'inspecteur).



- Dans la console Security Hub, sélectionnez Enable AWS Config.

Q Security hub X

Search results for 'Security hub'

Services (37) See all 37 results ▶

Features (48)

Resources **New**

Documentation (32,784)

Knowledge Articles (87)




Marketplace (367)

Blogs (3,912)

Events (161)

Tutorials (10)

Services

-  **Security Hub** ☆
AWS Security Hub is AWS's security and compliance center
-  **Security Lake** ☆
Automatically centralize all your security data with a few clicks
-  **AWS Resilience Hub** ☆
AWS Resilience Hub provides a central place to define, validate, and track the resilien...

- Sélectionnez Enable Security Hub.

Security, Identity, & Compliance

AWS Security Hub

Manage and improve your security posture

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

Get started with Security Hub

- Try out Security Hub for free with a 30-day trial
- Run automated security checks across your AWS environment
- Prioritize and remediate security issues
- Consolidate security findings from AWS and partner products in a standard format across all of your accounts

Go to Security Hub

30-day free trial

Management Tools

AWS Config

Record and evaluate configurations of your AWS resources

AWS Config provides a detailed view of the resources associated with your AWS account, including how they are configured, how they are related to one another, and how the configurations and their relationships have changed over time.

Set up AWS Config

A summarized view of AWS and non-AWS resources and the compliance status of the rules and the resources in each AWS Region.

Get started **1-click setup**


Security standards

Enabling AWS Security Hub grants it permissions to conduct security checks. [Service Linked Roles \(SLRs\)](#) with the following services are used to conduct security checks: Amazon CloudWatch, Amazon SNS, AWS Config, and AWS CloudTrail.

- ☒ Enable AWS Foundational Security Best Practices v1.0.0
- ☐ Enable AWS Resource Tagging Standard v1.0.0
- ☒ Enable CIS AWS Foundations Benchmark v1.2.0
- ☐ Enable CIS AWS Foundations Benchmark v1.4.0
- ☐ Enable CIS AWS Foundations Benchmark v3.0.0
- ☐ Enable NIST Special Publication 800-53 Revision 5
- ☐ Enable PCI DSS v3.2.1

AWS Integrations

Enabling Security Hub grants it permissions to import findings from AWS services that you have enabled.

[Learn more](#) 

Cancel Enable Security Hub

NB: Nettoyer toutes les ressources à la fin sinon vous risquez d'être facturé.