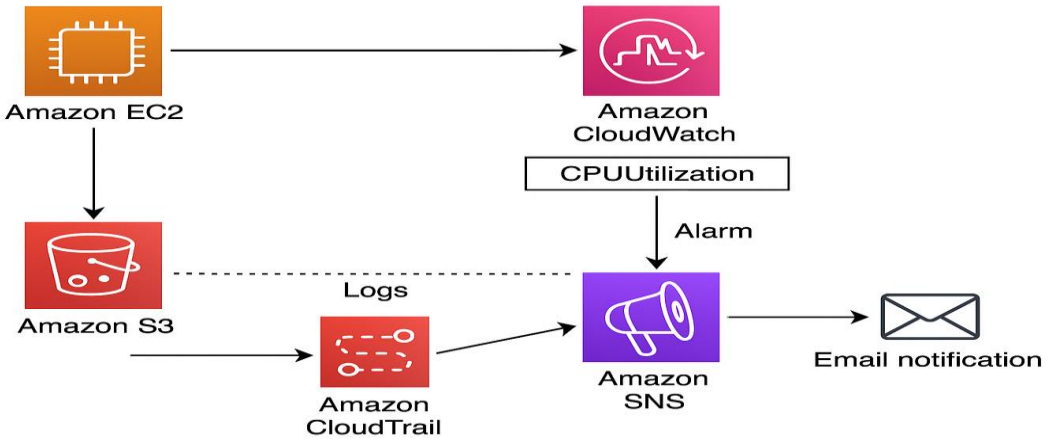
Mise en place d'un système d'alerte CPU avec AWS EC2, S3, CloudWatch, CloudTrail et SNS

Objectif

Créer un environnement AWS en appliquant les bonnes pratiques de sécurisé, observabilité et de traçabilité basé sur une instance EC2 avec journalisation et alertes, tout en respectant les contraintes du compte AWS Free Tier.

Architecture du système



Compétences

- Appliquer le principe du moindre privilège avec IAM.
- Suivre les activités utilisateur et API avec AWS CloudTrail.
- Superviser les performances EC2 avec CloudWatch Metrics et Logs.
- Centraliser le stockage des logs dans un compartiment S3.
- Créer une alerte CloudWatch déclenchant une notification SNS.
- Protéger l'accès SSH via des groupes de sécurité restrictifs.

Services AWS Utilisés

- **AWS EC2** : Hébergement d'une instance Web Amazon Linux 2 (t2.micro - Free Tier).
- **AWS S3** : Stockage des logs CloudTrail de manière centralisée
- **AWS IAM** : Gestion des accès et permissions.
- **AWS CloudTrail** : Suivi et audit des appels API AWS.
- **AWS CloudWatch** : Métriques, journaux et alarmes.
- **AWS SNS** : Envoi d'alertes par e-mail.
- **AWS Security Group** : Contrôle des accès à l'instance EC2.

Étape 1 Création de l'instance EC2

1. Amazon Linux 2023
2. Type : **t2.micro** (Free Tier)
3. Groupe de sécurité :

a. Port 22 : autoriser le trafic **SSH** depuis **N'importe où**
b. Port 80 : autoriser le trafic **HTTP** depuis l'**Internet**

4. Dans **Détails avancés** > **Données utilisateurs** colle le script ci-dessus pour l'installation et configuration de l'agent CloudWatch, puis clique sur **Lancer l'instance**.

```
#!/bin/bash

# Mise à jour du système

yum update -y

# Installation de l'agent CloudWatch

yum install -y amazon-cloudwatch-agent

# Création du fichier de configuration CloudWatch agent

cat <<EOF > /opt/aws/amazon-cloudwatch-agent/bin/config.json

{

  "agent": {

    "metrics_collection_interval": 60,

    "logfile": "/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log",

    "run_as_user": "root"

  },

  "metrics": {

    "append_dimensions": {

      "InstanceId": "\${aws:InstanceId}"

    },

    "metrics_collected": {

      "cpu": {

        "measurement": [

          "cpu_usage_idle",

          "cpu_usage_user",

          "cpu_usage_system"

        ],

        "metrics_collection_interval": 60,

        "totalcpu": true

      },

      "mem": {

        "measurement": [

          "mem_used_percent"
```

```
      ],
      "metrics_collection_interval": 60
    }
  }
 },
 "logs": {
  "logs_collected": {
    "files": {
      "collect_list": [
        {
          "file_path": "/var/log/messages",
          "log_group_name": "/ec2/messages",
          "log_stream_name": "{instance_id}"
        }
      ]
    }
  }
 }
}
EOF
# Lancer l'agent CloudWatch avec la configuration
/opt/aws/amazon-cloudwatch-agent/bin/amazon-cloudwatch-agent-ctl \
 -a fetch-config \
 -m ec2 \
 -c file:/opt/aws/amazon-cloudwatch-agent/bin/config.json \
 -s
```

EC2 > Instances

EC2
Tableau de bord
Vue globale EC2
Événements
Instances
Instances
Types d'instances
Modèles de lancement

Instances Informations
Date de la dernière mise à jour Il y a less than a minute
Se connecter | État de l'instance | Actions | Lancer des instances
Rechercher Instance par attribut ou identification (case-sensitive) | Tous les é...
Name | ID d'instance | État de l'insta... | Type d'insta... | Contrôle des statu | Statut d'alarme | Zone de dispon... | DNS IPv4 pul

Aucune instance
Vous n'avez aucune instance dans cette région
Lancer des instances

EC2 > Instances > Lancer une instance

EC2
Tableau de bord
Vue globale EC2
Événements
Instances
Instances
Types d'instances
Modèles de lancement

Lancer une instance Informations

Amazon EC2 vous permet de créer des machines virtuelles, ou des instances, qui s'exécutent sur le Cloud AWS. Démarrez rapidement en suivant les étapes simples indiquées ci-dessous.

Nom et balises Informations

Nom

Agent CloudWatch

Ajouter des balises supplémentaires

Images d'applications et de systèmes d'exploitation (Amazon Machine Image) Informations

Une AMI est un modèle contenant la configuration logicielle (système d'exploitation, serveur d'applications et applications) requise pour lancer votre instance. Parcourez ou recherchez des AMI si vous ne trouvez pas ce que vous recherchez ci-dessous.

Effectuer une recherche dans notre catalogue complet, qui comprend des milliers d'images d'applications et de systèmes d'exploitation

Récentes | Démarrage rapide

Amazon Linux | macOS | Ubuntu | Windows | Red Hat | SUSE Linux | Debian

Explorer plus d'AMI
Y compris les AMI d'AWS, de Marketplace et de la communauté

Amazon Machine Image (AMI)

AMI Amazon Linux 2023 — Éligible à l'offre gratuite
ami-07b0c09aab6e66ee9 (64 bits (x86), uefi-preferred) / ami-05d2ed97ce7162747 (64 bits (Arm), uefi)
Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs

Description

Amazon Linux 2023 est un système d'exploitation moderne basé sur Linux, à usage général et offrant cinq ans de support garanti. Optimisé pour AWS, il est conçu afin de fournir un environnement d'exécution sécurisé, stable et à hautes performances pour le développement et l'exécution de vos applications cloud.

Amazon Linux 2023 AMI 2023.7.20250428.1 x86_64 HVM kernel-6.1

Architecture	Mode de démarrage	ID AMI	Date de publication	Nom d'utilisateur
64 bits (x86)	uefi-preferred	ami-07b0c09aab6e66ee9	2025-04-30	ec2-user

Fournisseur vérifié

Type d'instance Informations | Obtenez des conseils

Type d'instance

t2.micro — Éligible à l'offre gratuite
Famille: t2 1 vCPU 1 Gio Mémoire Génération actuelle: true
À la demande Linux base tarification: 0.0116 USD par heure À la demande SUSE base tarification: 0.0116 USD par heure
À la demande Windows base tarification: 0.0162 USD par heure
À la demande RHEL base tarification: 0.026 USD par heure À la demande Ubuntu Pro base tarification: 0.0134 USD par heure

Toutes les générations

Comparer les types d'instance

Des frais supplémentaires s'appliquent pour les AMI avec un logiciel préinstallé

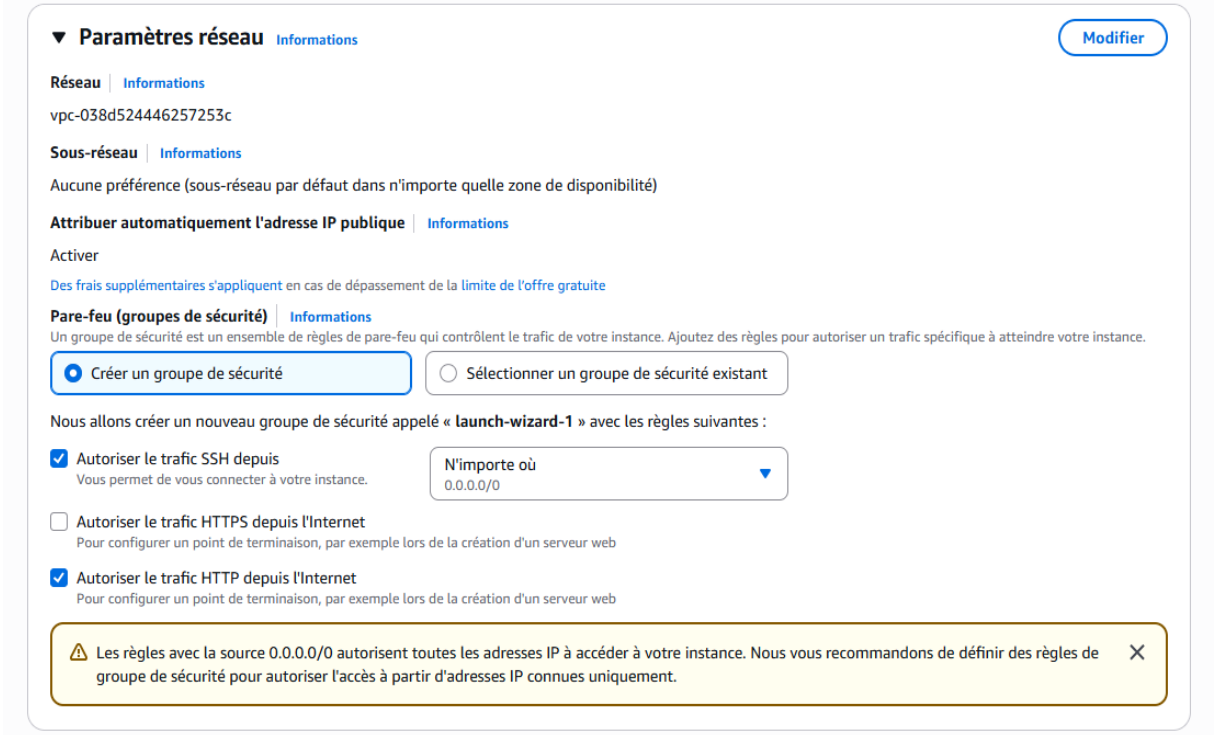
Paire de clés (connexion) Informations

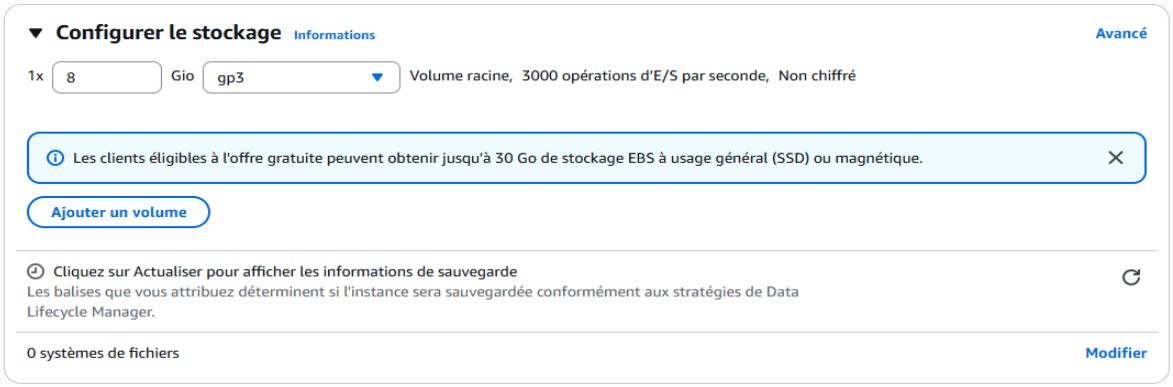
Vous pouvez utiliser une paire de clés pour vous connecter en toute sécurité à votre instance. Assurez-vous d'avoir accès à la paire de clés sélectionnée avant de lancer l'instance.

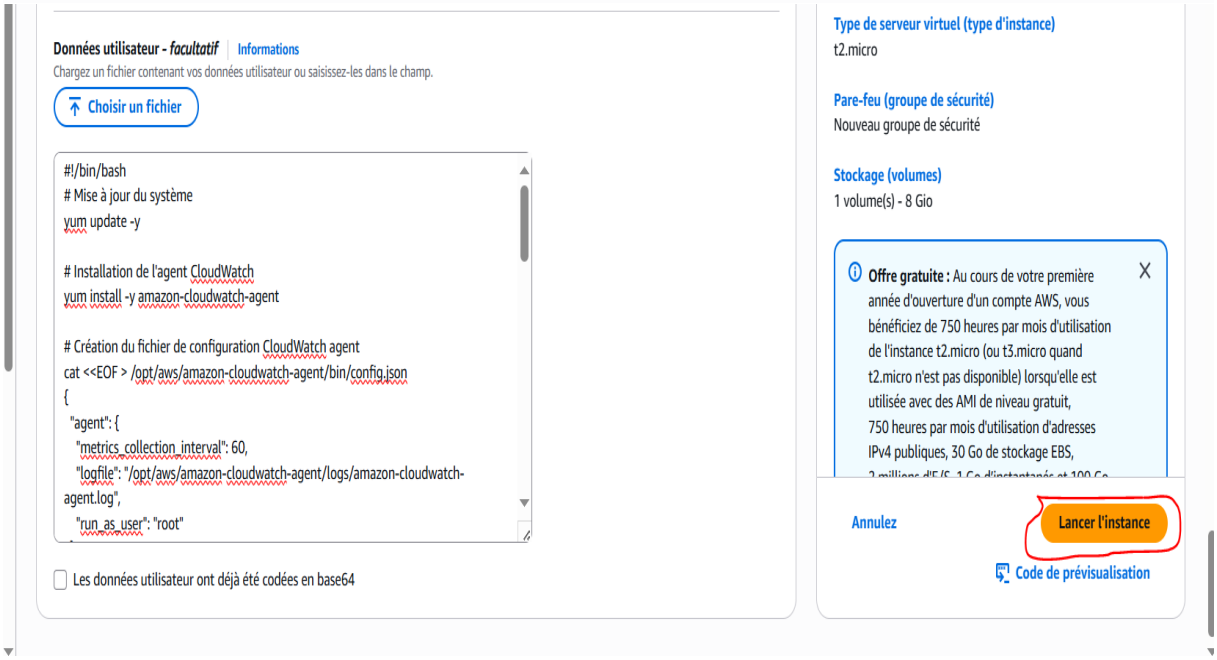
Nom de la paire de clés - *obligatoire*

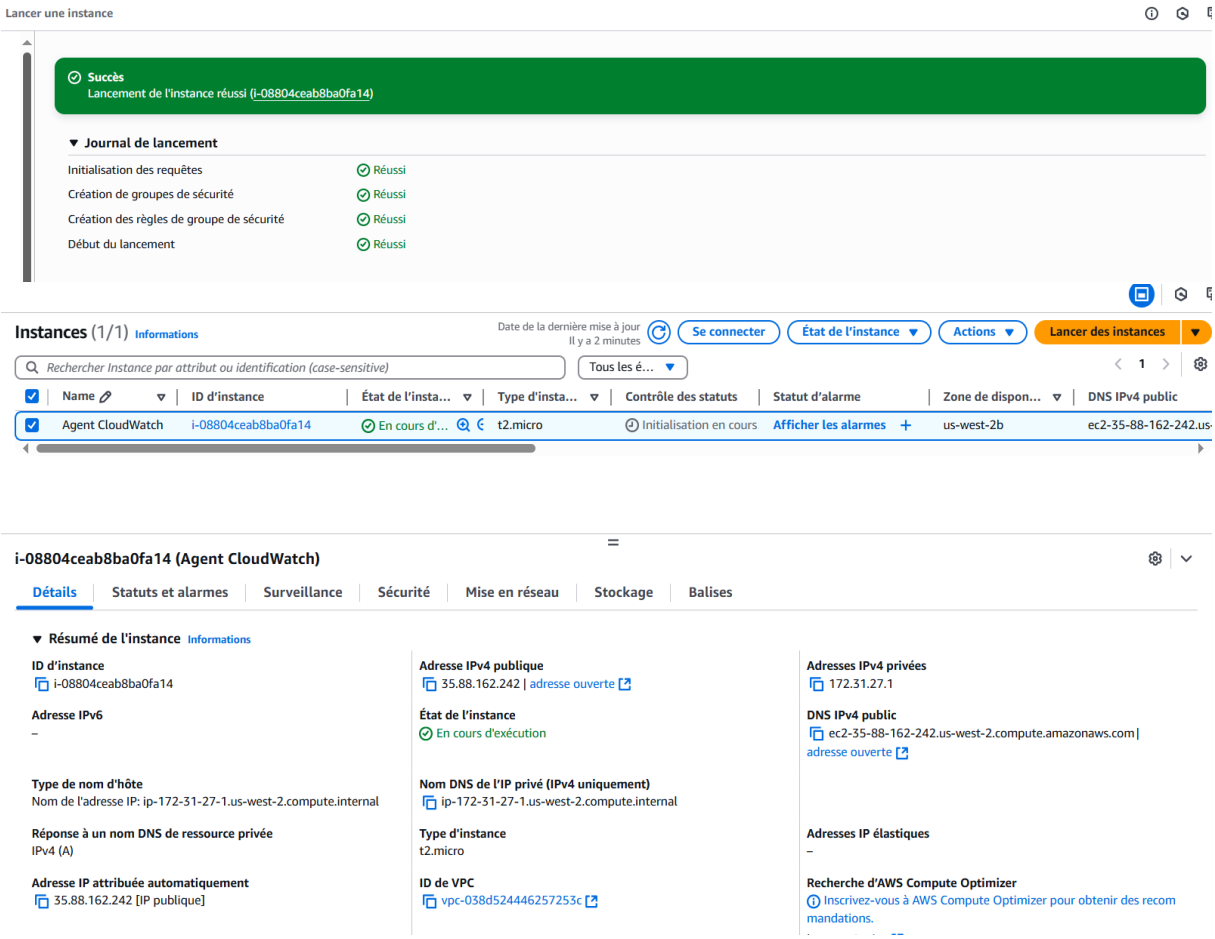
Continuer sans paire de clés (déconseillé) — Valeur par défaut

Créer une paire de clés


Paramètres réseau Informations
Modifier
Réseau Informations
vpc-038d524446257253c
Sous-réseau Informations
Aucune préférence (sous-réseau par défaut dans n'importe quelle zone de disponibilité)
Attribuer automatiquement l'adresse IP publique Informations
Activer
Des frais supplémentaires s'appliquent en cas de dépassement de la limite de l'offre gratuite
Pare-feu (groupes de sécurité) Informations
Un groupe de sécurité est un ensemble de règles de pare-feu qui contrôlent le trafic de votre instance. Ajoutez des règles pour autoriser un trafic spécifique à atteindre votre instance.
Créer un groupe de sécurité
Sélectionner un groupe de sécurité existant
Nous allons créer un nouveau groupe de sécurité appelé « launch-wizard-1 » avec les règles suivantes :
Autoriser le trafic SSH depuis
Vous permet de vous connecter à votre instance.
N'importe où
0.0.0.0/0
Autoriser le trafic HTTPS depuis l'Internet
Pour configurer un point de terminaison, par exemple lors de la création d'un serveur web
Autoriser le trafic HTTP depuis l'Internet
Pour configurer un point de terminaison, par exemple lors de la création d'un serveur web
Les règles avec la source 0.0.0.0/0 autorisent toutes les adresses IP à accéder à votre instance. Nous vous recommandons de définir des règles de groupe de sécurité pour autoriser l'accès à partir d'adresses IP connues uniquement.

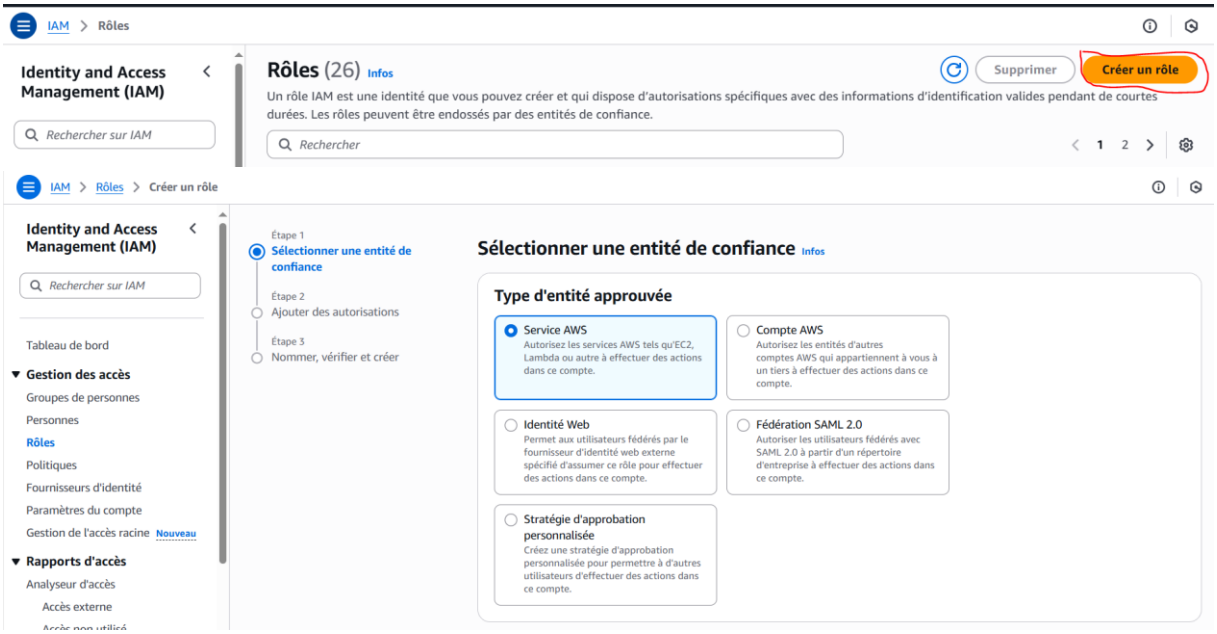

Configurer le stockage Informations
Avancé
1x 8 Gio gp3 Volume racine, 3000 opérations d'E/S par seconde, Non chiffré
Les clients éligibles à l'offre gratuite peuvent obtenir jusqu'à 30 Go de stockage EBS à usage général (SSD) ou magnétique.
Ajouter un volume
Cliquez sur Actualiser pour afficher les informations de sauvegarde
Les balises que vous attribuez déterminent si l'instance sera sauvegardée conformément aux stratégies de Data Lifecycle Manager.
0 systèmes de fichiers
Modifier

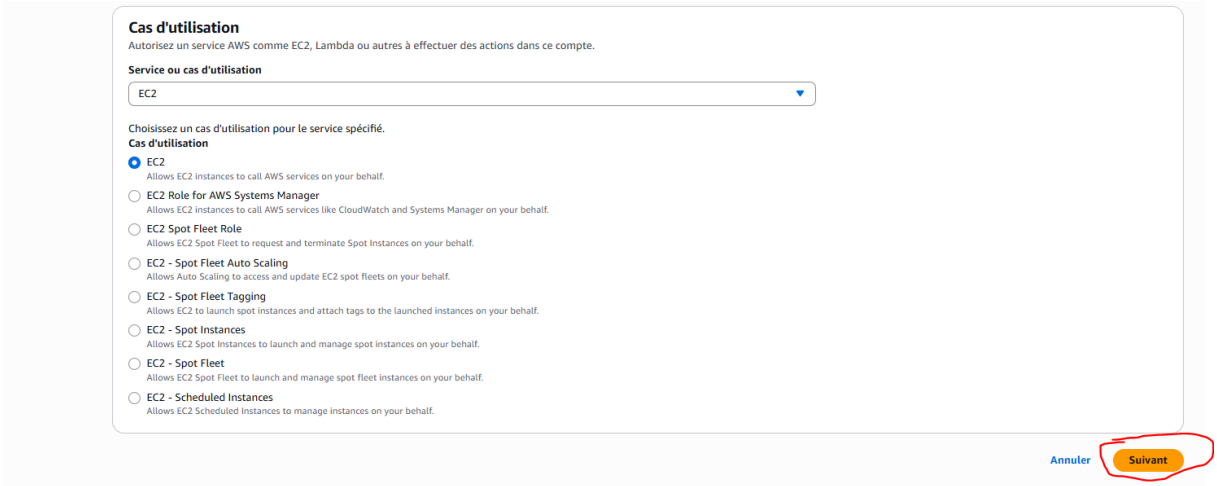

Données utilisateur - facultatif Informations
Chargez un fichier contenant vos données utilisateur ou saisissez-les dans le champ.
Choisir un fichier
#!/bin/bash
Mise à jour du système
yum update -y
Installation de l'agent CloudWatch
yum install -y amazon-cloudwatch-agent
Création du fichier de configuration CloudWatch agent
cat <<EOF > /opt/aws/amazon-cloudwatch-agent/bin/config.json
{
"agent": {
"metrics_collection_interval": 60,
"logfile": "/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log",
"run_as_user": "root"
Les données utilisateur ont déjà été codées en base64
Type de serveur virtuel (type d'instance)
t2.micro
Pare-feu (groupe de sécurité)
Nouveau groupe de sécurité
Stockage (volumes)
1 volume(s) - 8 Gio
Offre gratuite : Au cours de votre première année d'ouverture d'un compte AWS, vous bénéficiez de 750 heures par mois d'utilisation de l'instance t2.micro (ou t3.micro quand t2.micro n'est pas disponible) lorsqu'elle est utilisée avec des AMI de niveau gratuit, 750 heures par mois d'utilisation d'adresses IPv4 publiques, 30 Go de stockage EBS,
Annulez
Lancer l'instance
Code de prévisualisation

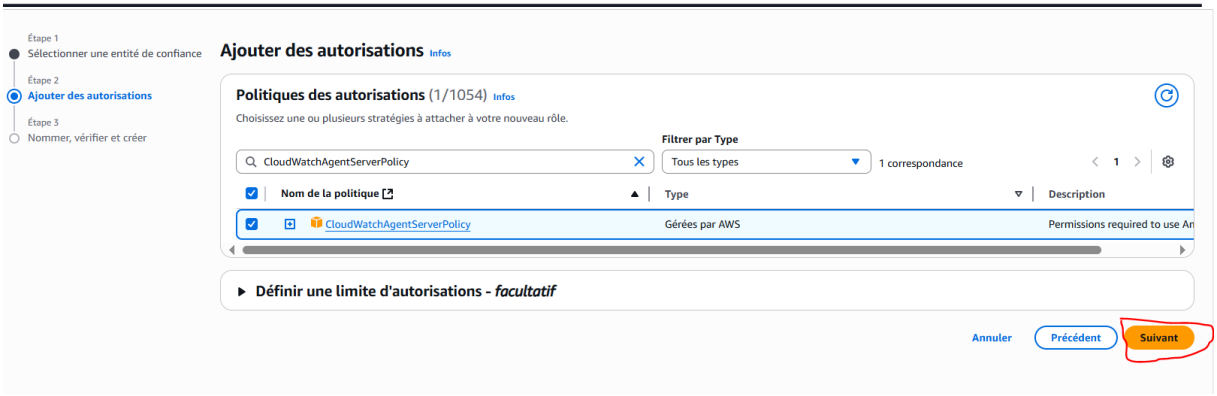


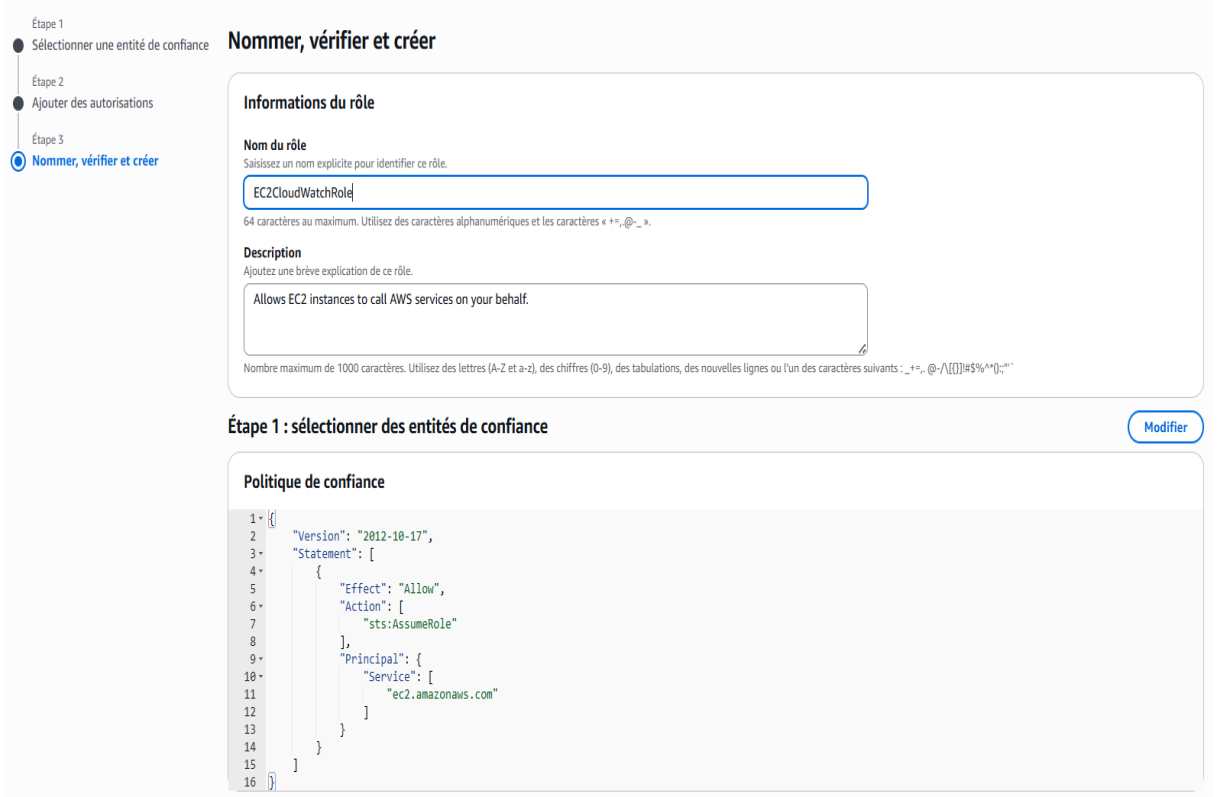
Étape 2 Créer un rôle IAM pour EC2

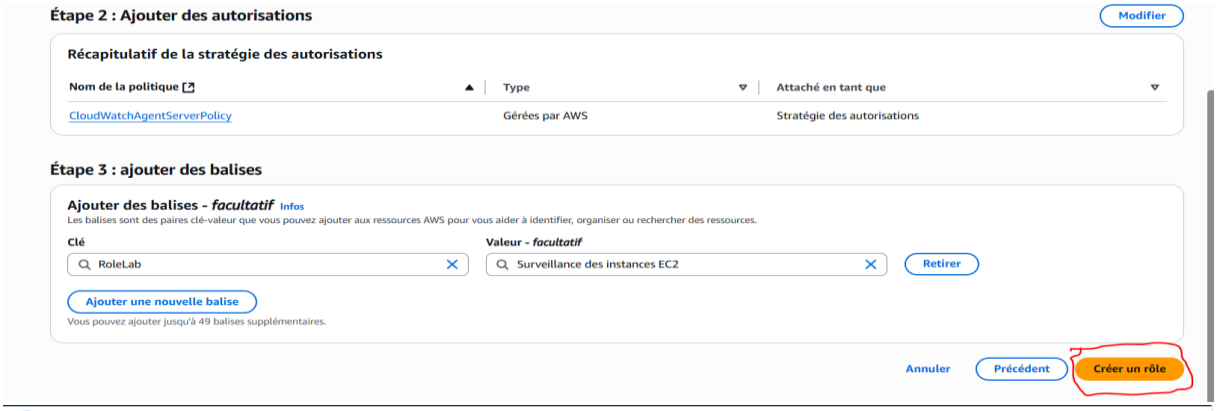
1. Nom : EC2CloudWatchRole
2. Politique attachée : CloudWatchAgentServerPolicy
3. Attacher le rôle à ton instance EC2

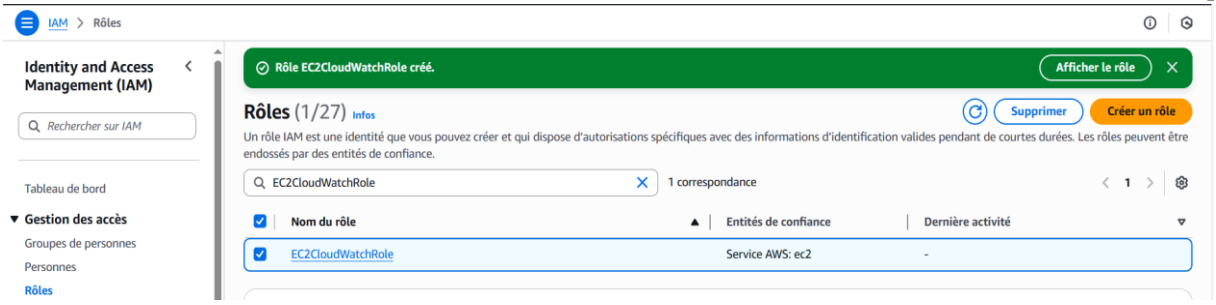


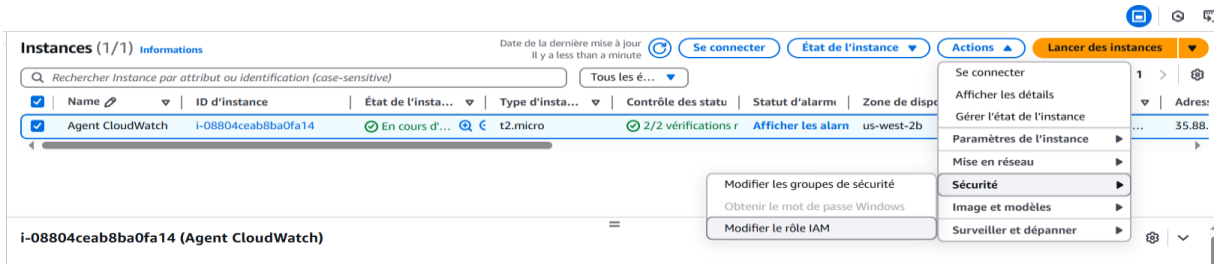

Cas d'utilisation
Autorisez un service AWS comme EC2, Lambda ou autres à effectuer des actions dans ce compte.
Service ou cas d'utilisation
EC2
Choisissez un cas d'utilisation pour le service spécifié.
Cas d'utilisation
EC2
Allows EC2 instances to call AWS services on your behalf.
EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.
EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.
EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.
EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.
EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.
EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.
EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.
Annuler
Suivant


Étape 1
Sélectionner une entité de confiance
Étape 2
Ajouter des autorisations
Étape 3
Nommer, vérifier et créer
Ajouter des autorisations Infos
Politiques des autorisations (1/1054) Infos
Choisissez une ou plusieurs stratégies à attacher à votre nouveau rôle.
Filtrer par Type
CloudWatchAgentServerPolicy
Tous les types
1 correspondance
Nom de la politique
Type
Description
CloudWatchAgentServerPolicy
Gérées par AWS
Permissions required to use An
Définir une limite d'autorisations - facultatif
Annuler
Précédent
Suivant

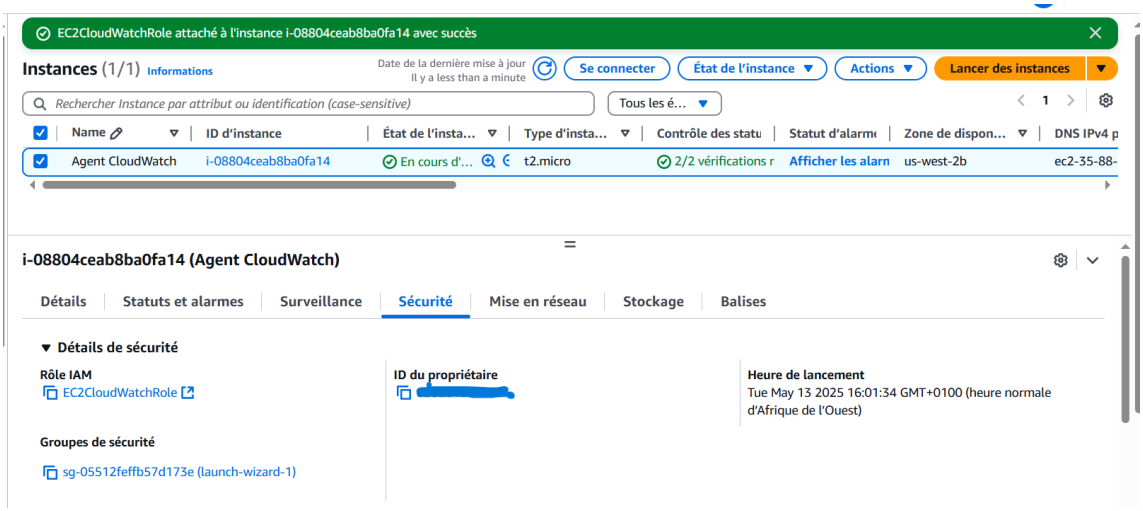

Étape 1
Sélectionner une entité de confiance
Étape 2
Ajouter des autorisations
Étape 3
Nommer, vérifier et créer
Nommer, vérifier et créer
Informations du rôle
Nom du rôle
Saisissez un nom explicite pour identifier ce rôle.
EC2CloudWatchRole
64 caractères au maximum. Utilisez des caractères alphanumériques et les caractères « +=,.@-_ ».
Description
Ajoutez une brève explication de ce rôle.
Allows EC2 instances to call AWS services on your behalf.
Nombre maximum de 1000 caractères. Utilisez des lettres (A-Z et a-z), des chiffres (0-9), des tabulations, des nouvelles lignes ou l'un des caractères suivants : _+=,.@-/\[{}]!#$%^*();:"'`
Étape 1 : sélectionner des entités de confiance
Modifier
Politique de confiance
{
"Version": "2012-10-17",
"Statement": [
{
"Effect": "Allow",
"Action": [
"sts:AssumeRole"
],
"Principal": {
"Service": [
"ec2.amazonaws.com"
]
}
}
]
}


Étape 2 : Ajouter des autorisations
Modifier
Récapitulatif de la stratégie des autorisations
Nom de la politique
Type
Attaché en tant que
CloudWatchAgentServerPolicy
Gérées par AWS
Stratégie des autorisations
Étape 3 : ajouter des balises
Ajouter des balises - facultatif Infos
Les balises sont des paires clé-valeur que vous pouvez ajouter aux ressources AWS pour vous aider à identifier, organiser ou rechercher des ressources.
Clé
Valeur - facultatif
RoleLab
Surveillance des instances EC2
Retirer
Ajouter une nouvelle balise
Vous pouvez ajouter jusqu'à 49 balises supplémentaires.
Annuler
Précédent
Créer un rôle


IAM > Rôles
Identity and Access Management (IAM)
Rôle EC2CloudWatchRole créé.
Afficher le rôle
Rôles (1/27) Infos
Supprimer
Créer un rôle
Un rôle IAM est une identité que vous pouvez créer et qui dispose d'autorisations spécifiques avec des informations d'identification valides pendant de courtes durées. Les rôles peuvent être endossés par des entités de confiance.
EC2CloudWatchRole
1 correspondance
Tableau de bord
Gestion des accès
Groupes de personnes
Personnes
Rôles
Nom du rôle
Entités de confiance
Dernière activité
EC2CloudWatchRole
Service AWS: ec2

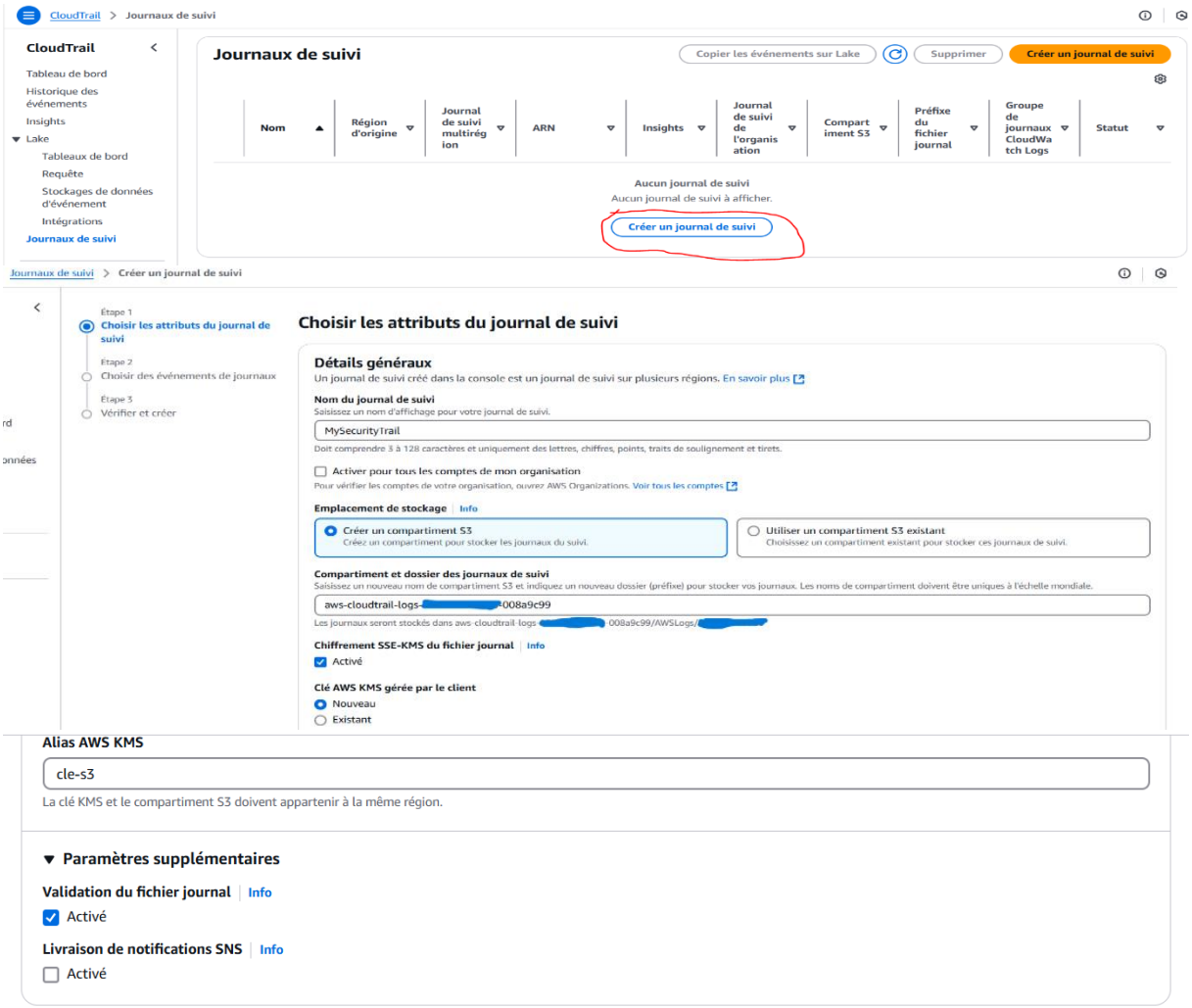

Instances (1/1) Informations
Se connecter
État de l'instance
Actions
Lancer des instances
Name
ID d'instance
Agent CloudWatch
i-08804ceab8ba0fa14
t2.micro
us-west-2b
Se connecter
Afficher les détails
Gérer l'état de l'instance
Paramètres de l'instance
Mise en réseau
Sécurité
Image et modèles
Surveiller et dépanner
Modifier les groupes de sécurité
Obtenir le mot de passe Windows
Modifier le rôle IAM
i-08804ceab8ba0fa14 (Agent CloudWatch)

i-08804ceab8ba0fa14 > Modifier le rôle IAM
Modifier le rôle IAM Informations
Attachez un rôle IAM à votre instance.
ID d'instance
i-08804ceab8ba0fa14 (Agent CloudWatch)
Rôle IAM
Sélectionner un rôle IAM à attacher à votre instance ou créer un rôle si vous n'en avez pas encore créé. Le rôle que vous sélectionnez remplace tous les rôles actuellement attachés à votre instance.
EC2CloudWatchRole
Créer un nouveau rôle IAM
Annulez
Mettre à jour le rôle IAM


EC2CloudWatchRole attaché à l'instance i-08804ceab8ba0fa14 avec succès
Instances (1/1) Informations
Se connecter
État de l'instance
Actions
Lancer des instances
Name
ID d'instance
Agent CloudWatch
i-08804ceab8ba0fa14
t2.micro
us-west-2b
i-08804ceab8ba0fa14 (Agent CloudWatch)
Détails
Statuts et alarmes
Surveillance
Sécurité
Mise en réseau
Stockage
Balises
Détails de sécurité
Rôle IAM
EC2CloudWatchRole
ID du propriétaire
Heure de lancement
Tue May 13 2025 16:01:34 GMT+0100 (heure normale d'Afrique de l'Ouest)
Groupes de sécurité
sg-05512feffb57d173e (launch-wizard-1)

Étape 3 Création de journal CloudTrail

1. Nom du journal : **MySecurityTrail**
2. Type : trail unique régional
3. Créer un bucket S3 pour stocker les logs CloudTrail :
    - Emplacement de stockage : **Créer un compartiment S3**
4. Activer CloudWatch Logs :
    - CloudWatch Logs : **Activé**
    - Groupe de journaux : **Nouveau**
    - Rôle IAM : **Nouveau**
    - Nom du rôle IAM : **RoleCloudTrailForLogsCloudWatch**
5. Evénements de journaux :
    - Evénements : **Evénements de gestion**
    - Activité d'API : **Lecture** et **écriture**
6. Vérifier que les journaux sont bien collectés et stockés dans le bucket S3
7. Vérifier que le groupe de journaux a été créer



CloudWatch Logs - *facultatif*

Configurez CloudWatch Logs pour surveiller vos journaux de suivi et être averti en cas d'activité spécifique. Des frais standards CloudWatch et CloudWatch Logs seront facturés. En savoir plus

CloudWatch Logs Infos

☑ Activé

Groupe de journaux Infos

◉ Nouveau
○ Existant

Nom du groupe de journaux

aws-cloudtrail-logs-[redacted]-3cdd8820

Doit comprendre entre 1 et 512 caractères et uniquement des lettres, chiffres, tirets, traits de soulignement, barres obliques et points.

Rôle IAM Infos

AWS CloudTrail utilise ce rôle pour envoyer des événements CloudTrail à votre groupe de journaux CloudWatch Logs.

◉ Nouveau
○ Existant

Nom du rôle

RoleCloudTrailForLogsCloudWatch

▸ **Document relatif à la stratégie**

Balises - *facultatif* Info

Vous pouvez ajouter une ou plusieurs balises afin de faciliter la gestion et l'organisation de vos ressources, y compris les journaux de suivi.

Clé	Valeur - *facultatif*	
key	surveillance des alertes	Supprimer

Ajouter une balise

Vous pouvez encore ajouter 49 balises.

Annuler **Suivant**

CloudTrail > Journaux de suivi > Créer un journal de suivi

Étape 1
Choisir les attributs du journal de suivi

Étape 2
Choisir des événements de journaux

Étape 3
Vérifier et créer

Choisir des événements de journaux

Événements Info

Enregistrez l'activité d'API des ressources individuelles ou de toutes les ressources actuelles et futures dans le compte AWS. Des frais supplémentaires seront facturés

Type d'événement

Choisissez le type d'événements que vous souhaitez journaliser.

☑ Événements de gestion
Capturez les opérations de gestion effectuées sur vos ressources AWS.

☐ Événements de données
Journalisez les opérations de ressource effectuées sur ou au sein d'une ressource.

☐ Événements Insights
Identifiez les activités inhabituelles, les erreurs ou le comportement des utilisateurs dans votre compte.

☐ Événements d'activité réseau
Les événements d'activité réseau fournissent des informations sur les opérations concernant les ressources effectuées sur une ressource au sein d'un point de terminaison du cloud privé virtuel.

Événements de gestion Info

Les événements de gestion affichent des informations sur les opérations de gestion effectuées sur les ressources de votre compte AWS.

ⓘ Aucuns frais supplémentaires ne s'appliquent aux événements de gestion des journaux sur ce journal de suivi, car il s'agit de votre première copie des événements de gestion.

Activité d'API

Choisissez les activités que vous souhaitez journaliser.

☑ Lecture ☑ Écrire

☐ Exclure les événements AWS KMS

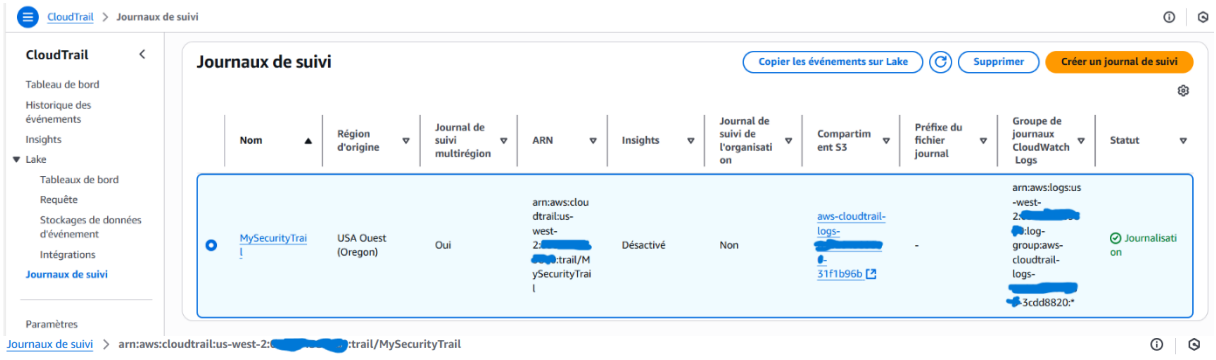
☐ Exclure les événements API de données Amazon RDS

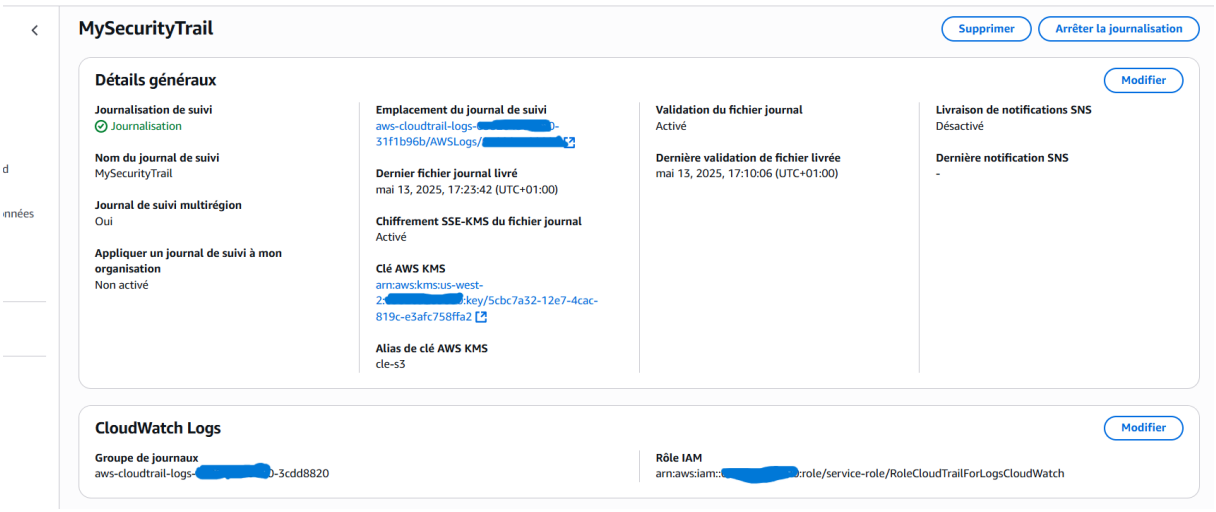
Annuler Précédent **Suivant**

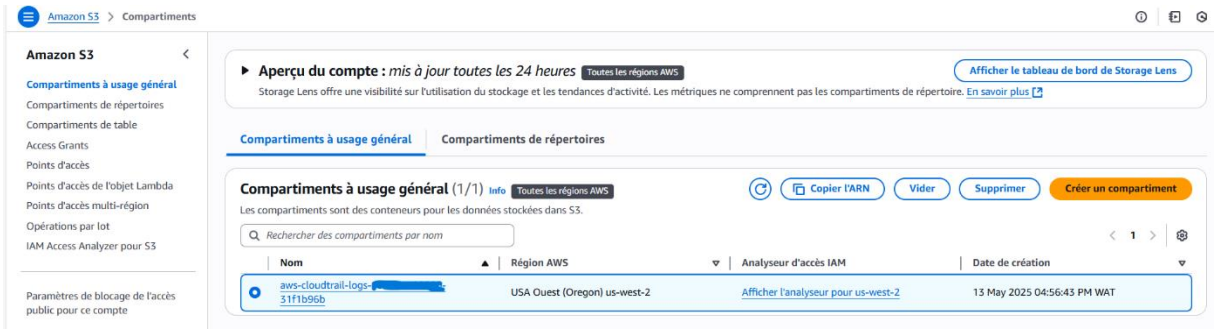
Événements d'activité réseau

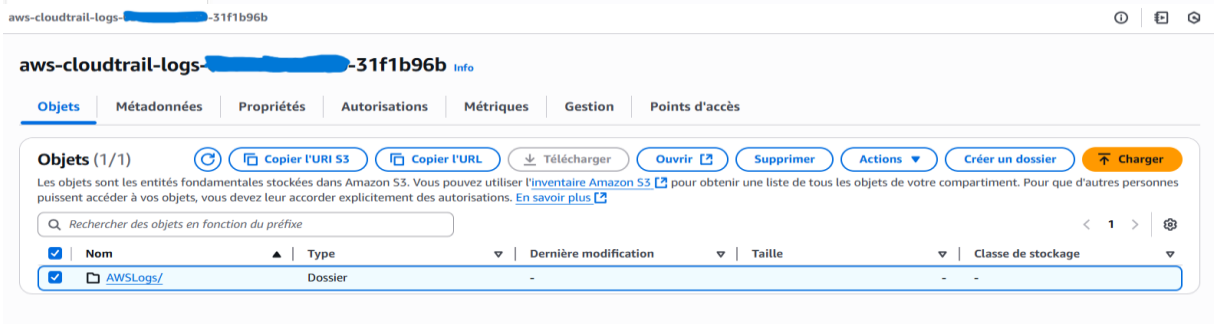
La collecte des événements d'activité réseau n'est pas configurée pour ce journal de suivi

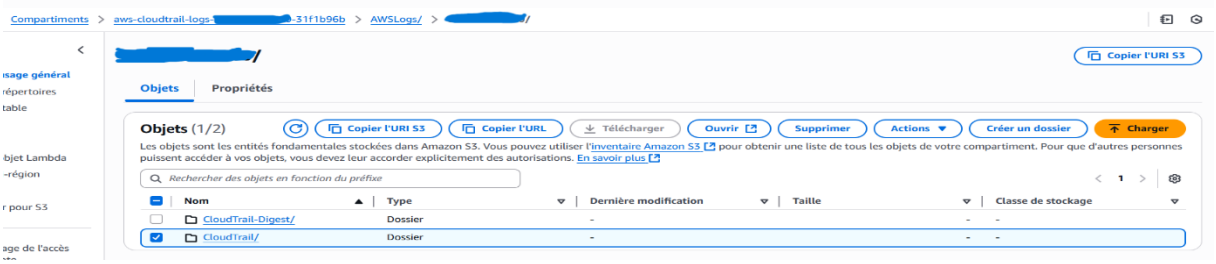
Annuler Précédent **Créer un journal de suivi**

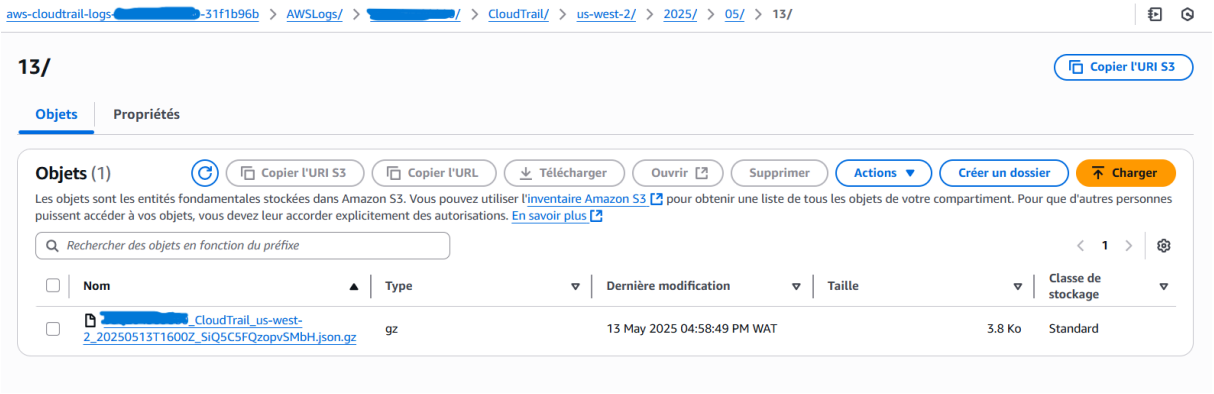

CloudTrail > Journaux de suivi
CloudTrail
Tableau de bord
Historique des événements
Insights
Lake
Tableaux de bord
Requête
Stockages de données d'événement
Intégrations
Journaux de suivi
Paramètres
Journaux de suivi
Copier les événements sur Lake
Supprimer
Créer un journal de suivi
Nom
Région d'origine
Journal de suivi multirégion
ARN
Insights
Journal de suivi de l'organisation
Compartiment S3
Préfixe du fichier journal
Groupe de journaux CloudWatch Logs
Statut
MySecurityTrail
USA Ouest (Oregon)
Oui
Désactivé
Non
Journalisation

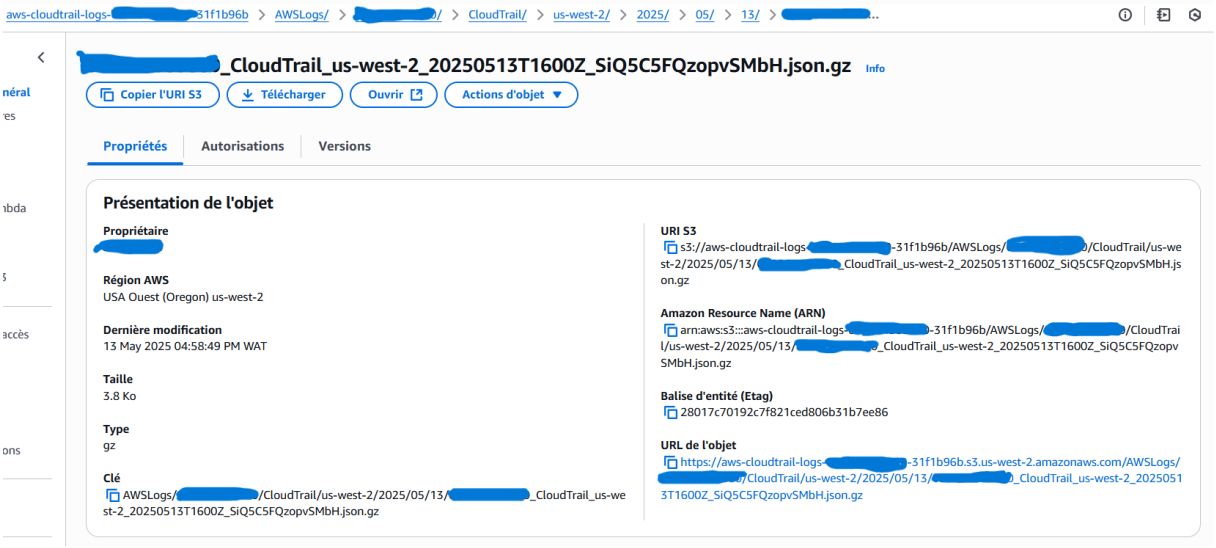

Journaux de suivi > arn:aws:cloudtrail:us-west-2:[redacted]:trail/MySecurityTrail
MySecurityTrail
Supprimer
Arrêter la journalisation
Détails généraux
Modifier
Journalisation de suivi
Journalisation
Nom du journal de suivi
MySecurityTrail
Journal de suivi multirégion
Oui
Appliquer un journal de suivi à mon organisation
Non activé
Emplacement du journal de suivi
Dernier fichier journal livré
mai 13, 2025, 17:23:42 (UTC+01:00)
Chiffrement SSE-KMS du fichier journal
Activé
Clé AWS KMS
Alias de clé AWS KMS
cle-s3
Validation du fichier journal
Activé
Dernière validation de fichier livrée
mai 13, 2025, 17:10:06 (UTC+01:00)
Livraison de notifications SNS
Désactivé
Dernière notification SNS
CloudWatch Logs
Groupe de journaux
Rôle IAM

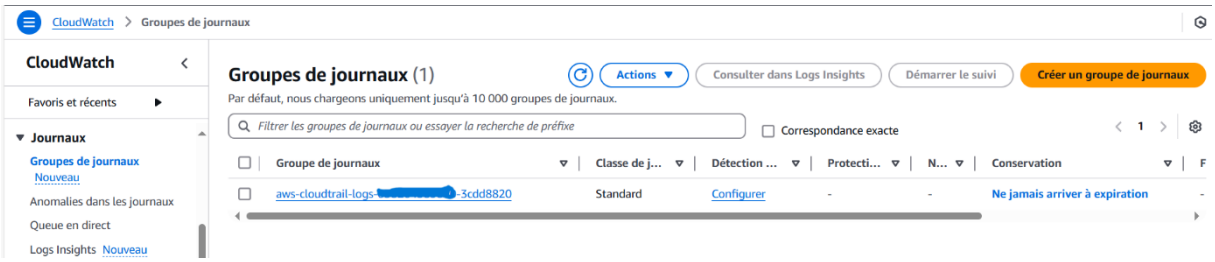

Amazon S3 > Compartiments
Amazon S3
Compartiments à usage général
Compartiments de répertoires
Compartiments de table
Access Grants
Points d'accès
Points d'accès de l'objet Lambda
Points d'accès multi-région
Opérations par lot
IAM Access Analyzer pour S3
Paramètres de blocage de l'accès public pour ce compte
Aperçu du compte : mis à jour toutes les 24 heures
Toutes les régions AWS
Afficher le tableau de bord de Storage Lens
Storage Lens offre une visibilité sur l'utilisation du stockage et les tendances d'activité. Les métriques ne comprennent pas les compartiments de répertoire. En savoir plus
Compartiments à usage général
Compartiments de répertoires
Compartiments à usage général (1/1)
Copier l'ARN
Vider
Supprimer
Créer un compartiment
Les compartiments sont des conteneurs pour les données stockées dans S3.
Rechercher des compartiments par nom
Nom
Région AWS
Analyseur d'accès IAM
Date de création
USA Ouest (Oregon) us-west-2
Afficher l'analyseur pour us-west-2
13 May 2025 04:56:43 PM WAT


aws-cloudtrail-logs-[redacted]-31f1b96b
Objets
Métadonnées
Propriétés
Autorisations
Métriques
Gestion
Points d'accès
Objets (1/1)
Copier l'URI S3
Copier l'URL
Télécharger
Ouvrir
Supprimer
Actions
Créer un dossier
Charger
Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l'inventaire Amazon S3 pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. En savoir plus
Rechercher des objets en fonction du préfixe
Nom
Type
Dernière modification
Taille
Classe de stockage
AWSLogs/
Dossier


Compartiments > aws-cloudtrail-logs-[redacted]-31f1b96b > AWSLogs/ > [redacted]/
Copier l'URI S3
Objets
Propriétés
Objets (1/2)
Copier l'URI S3
Copier l'URL
Télécharger
Ouvrir
Supprimer
Actions
Créer un dossier
Charger
Les objets sont les entités fondamentales stockées dans Amazon S3. Vous pouvez utiliser l'inventaire Amazon S3 pour obtenir une liste de tous les objets de votre compartiment. Pour que d'autres personnes puissent accéder à vos objets, vous devez leur accorder explicitement des autorisations. En savoir plus
Rechercher des objets en fonction du préfixe
Nom
Type
Dernière modification
Taille
Classe de stockage
CloudTrail-Digest/
Dossier
CloudTrail/
Dossier

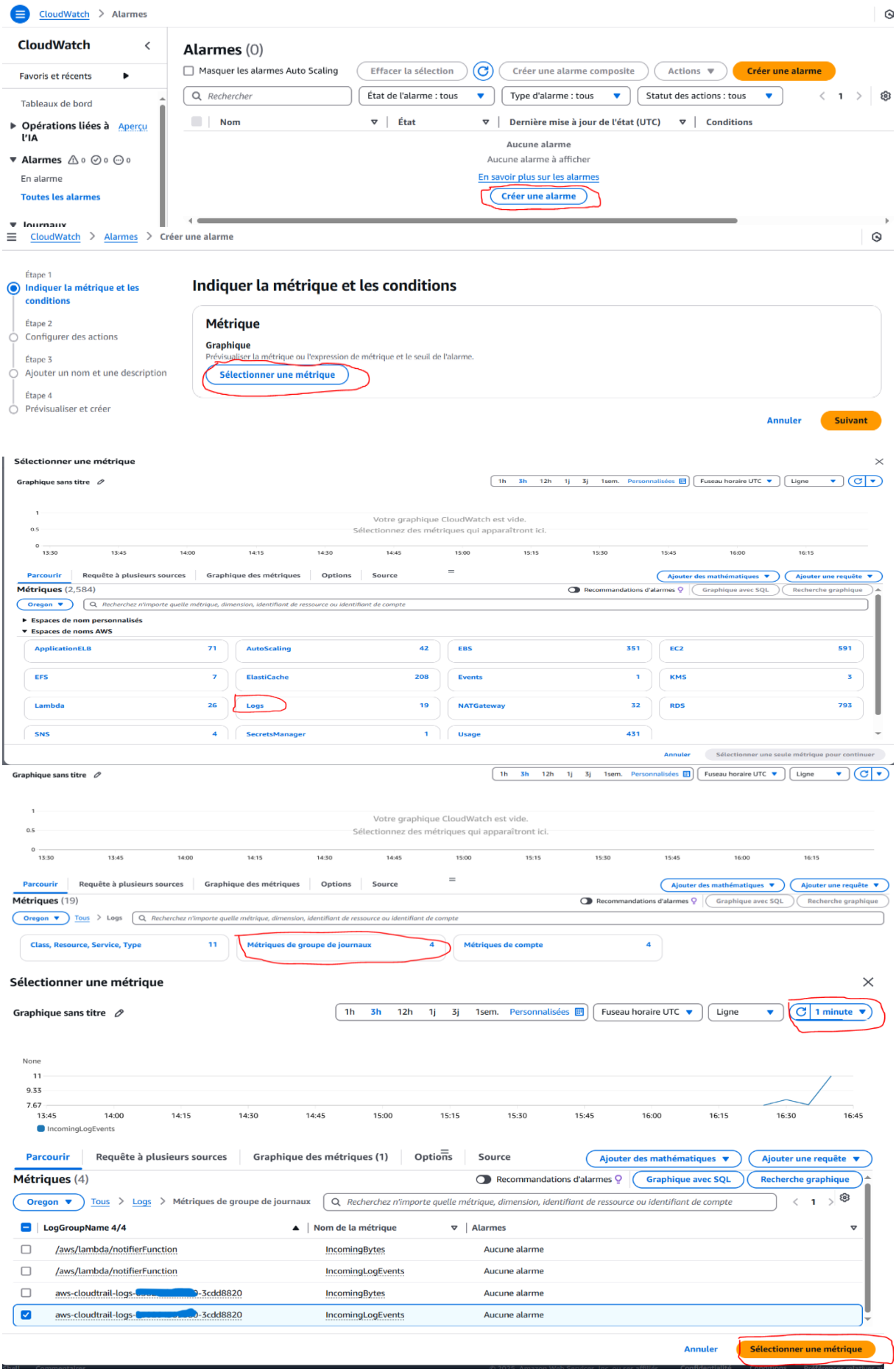






Étape 4 Créer une alarme CloudWatch

1. Va dans **CloudWatch > Alarmes > Créer une alarme** :
    - Nom : **CPUUtilizationAlarm**
    - Nom de la métrique : **IncomingLogEvents**
    - Statistique : **Moyenne**
    - Période : **1 min**
    - Type de seuil : Statique
    - Seuil : CPU > **10%**
    - Déclencheur d'état d'alarme : **En alarme**
2. Créer un **topic SNS** + abonnement email
3. Lier l'alarme CloudWatch à ce topic
4. Vérifier que le topic SNS et l'alarme CloudWatch ont été créer.


CloudWatch > Alarmes
CloudWatch
Favoris et récents
Tableaux de bord
Opérations liées à l'IA
Aperçu
Alarmes
En alarme
Toutes les alarmes
Journaux
Alarmes (0)
Masquer les alarmes Auto Scaling
Effacer la sélection
Créer une alarme composite
Actions
Créer une alarme
Rechercher
État de l'alarme : tous
Type d'alarme : tous
Statut des actions : tous
Nom
État
Dernière mise à jour de l'état (UTC)
Conditions
Aucune alarme
Aucune alarme à afficher
En savoir plus sur les alarmes
Créer une alarme
CloudWatch > Alarmes > Créer une alarme
Étape 1
Indiquer la métrique et les conditions
Étape 2
Configurer des actions
Étape 3
Ajouter un nom et une description
Étape 4
Prévisualiser et créer
Indiquer la métrique et les conditions
Métrique
Graphique
Prévisualiser la métrique ou l'expression de métrique et le seuil de l'alarme.
Sélectionner une métrique
Annuler
Suivant
Sélectionner une métrique
Graphique sans titre
Votre graphique CloudWatch est vide.
Sélectionnez des métriques qui apparaîtront ici.
Parcourir
Requête à plusieurs sources
Graphique des métriques
Options
Source
Métriques (2,584)
Recommandations d'alarmes
Graphique avec SQL
Recherche graphique
Oregon
Espaces de nom personnalisés
Espaces de noms AWS
ApplicationELB 71
AutoScaling 42
EBS 351
EC2 591
EFS 7
ElastiCache 208
Events 1
KMS 3
Lambda 26
Logs 19
NATGateway 32
RDS 793
SNS 4
SecretsManager 1
Usage 431
Annuler
Sélectionner une seule métrique pour continuer
Métriques (19)
Tous > Logs
Class, Resource, Service, Type 11
Métriques de groupe de journaux 4
Métriques de compte 4
Sélectionner une métrique
Graphique sans titre
1h 3h 12h 1j 3j 1sem. Personnalisées
Fuseau horaire UTC
Ligne
1 minute
None
IncomingLogEvents
Parcourir
Requête à plusieurs sources
Graphique des métriques (1)
Options
Source
Métriques (4)
Oregon
Tous > Logs > Métriques de groupe de journaux
LogGroupName 4/4
Nom de la métrique
Alarmes
/aws/lambda/notifierFunction IncomingBytes Aucune alarme
/aws/lambda/notifierFunction IncomingLogEvents Aucune alarme
aws-cloudtrail-logs-[redacted]-3cdd8820 IncomingBytes Aucune alarme
aws-cloudtrail-logs-[redacted]-3cdd8820 IncomingLogEvents Aucune alarme
Annuler
Sélectionner une métrique

CloudWatch > Alarmes > Créer une alarme

Étape 1
Indiquer la métrique et les conditions
Étape 2
Configurer des actions
Étape 3
Ajouter un nom et une description
Étape 4
Prévisualiser et créer

Indiquer la métrique et les conditions

Métrique

Modifier

Graphique
Cette alarme se déclenche lorsque la ligne bleue passe au-dessus de de la ligne rouge pour 1 points de données dans 1 minute.

Espace de nom
AWS/Logs

Nom de la métrique
IncomingLogEvents

LogGroupName
aws-cloudtrail-logs[redacted]-3cdd8820

Statistique
Moyenne

Période
1 minute

Conditions

Type de seuil

- Statique — Utiliser une valeur comme seuil
- Détection des anomalies — Utilisez une bande comme seuil

Chaque fois que IncomingLogEvents est...
Définissez la condition d'alarme.

- Supérieur — > seuil
- Supérieur/égal — >= seuil
- Inférieur/égal — <= seuil
- Inférieur — < seuil

à...
Définissez la valeur de seuil.
10
Doit être un nombre

▸ **Configuration supplémentaire**

Annuler | Passer à Prévisualiser et créer | Suivant

Déclencheur d'état d'alarme
Définissez l'état d'alarme qui déclenchera cette action.

Supprimer

- En alarme — La métrique ou l'expression de métrique dépasse le seuil défini.
- OK — La métrique ou l'expression de métrique respecte le seuil défini.
- Données insuffisantes — L'alarme vient d'être déclenchée ou les données sont insuffisantes.

Envoyer une notification à la prochaine rubrique SNS
Définissez la rubrique SNS (Simple Notification Service) qui recevra la notification.

- Sélectionner une rubrique SNS existante
- Créer une rubrique
- Utiliser l'ARN de rubrique pour notifier d'autres comptes

Créer une nouvelle rubrique...
Le nom de rubrique doit être unique.
Default_CloudWatch_Alarms_Topic
Les noms de rubrique SNS peuvent uniquement contenir des caractères alphanumériques, des tirets (-) et traits de soulignement (_).

Points de terminaison d'adresse e-mail qui recevront la notification...
Ajoutez une liste d'adresses e-mail séparées par une virgule. Chaque adresse sera ajoutée sous la forme d'un abonnement à la rubrique ci-dessus.
stanbant94@gmail.com
utilisateur1@exemple.com, utilisateur2@exemple.com

Créer une rubrique
Ajouter une notification

Déclencheur d'état d'alarme
Définissez l'état d'alarme qui déclenchera cette action.

Supprimer

- En alarme — La métrique ou l'expression de métrique dépasse le seuil défini.
- OK — La métrique ou l'expression de métrique respecte le seuil défini.
- Données insuffisantes — L'alarme vient d'être déclenchée ou les données sont insuffisantes.

Envoyer une notification à la prochaine rubrique SNS
Définissez la rubrique SNS (Simple Notification Service) qui recevra la notification.

- Sélectionner une rubrique SNS existante
- Créer une rubrique
- Utiliser l'ARN de rubrique pour notifier d'autres comptes

Envoyer une notification à...

Default_CloudWatch_Alarms_Topic

Seuls les rubriques appartenant à ce compte sont répertoriées ici. Toutes les personnes et applications abonnées à la rubrique sélectionnée recevront des notifications.

Adresse e-mail (points de terminaison)
stanbant94@gmail.com - Afficher dans la console SNS

Ajouter une notification

Gmail — Rechercher dans les messages

Nouveau message
Boîte de réception 5
Messages suivis
En attente

1-50 sur 946

Principale | Promotions | Réseaux sociaux 1 nouveau (LinkedIn - France Stanislas, vos ...) | Notifications

AWS Notifications	**AWS Notification - Subscription Confirmation** - You have chosen to subscribe to the topic: arn:aws:sns:us-west-2:058264389880:Default_CloudWatch_Alarms...	17:56
Oracle Training and.	**Special Edition: Join the Raise Your Game skills challenge now** - Oracle Training and Certification Dear France Stanislas, Join the Raise Your Game skills chall...	17:39

Gmail — Rechercher dans les messages

Nouveau message
Boîte de réception 4
Messages suivis
En attente
Messages envoyés
Brouillons
Plus
Libellés

1 sur 946

AWS Notification - Subscription Confirmation (Notification AWS - Confirmation d'abonnement) Boîte de réception ×

AWS Notifications <no-reply@sns.amazonaws.com> 17:56 (il y a 2 minutes)
À moi

anglais → français
Afficher l'original

Vous avez choisi de vous abonner au sujet :
arn:aws:sns:us-west-2:[redacted]:Default_CloudWatch_Alarms_Topic

Pour confirmer cet abonnement, cliquez ou visitez le lien ci-dessous (si cela était une erreur, aucune action n'est nécessaire) :
Confirmer l'abonnement

Veuillez ne pas répondre directement à cet e-mail. Si vous souhaitez ne plus recevoir de demandes de confirmation d'abonnement aux réseaux sociaux, veuillez envoyer un e-mail à sns-opt-out.

sns.us-west-2.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-west-2:058264389880:Default_CloudWatch_Alarms_Topic&Token=2...

1 1 nouvelle notifica... | Inscrivez-vous | Kod... | Microsoft Certified:... | NGINX Virtual Mach... | Les 32 meilleures q... | Installer Samba 4 -... | Discord | #papotag...

aws

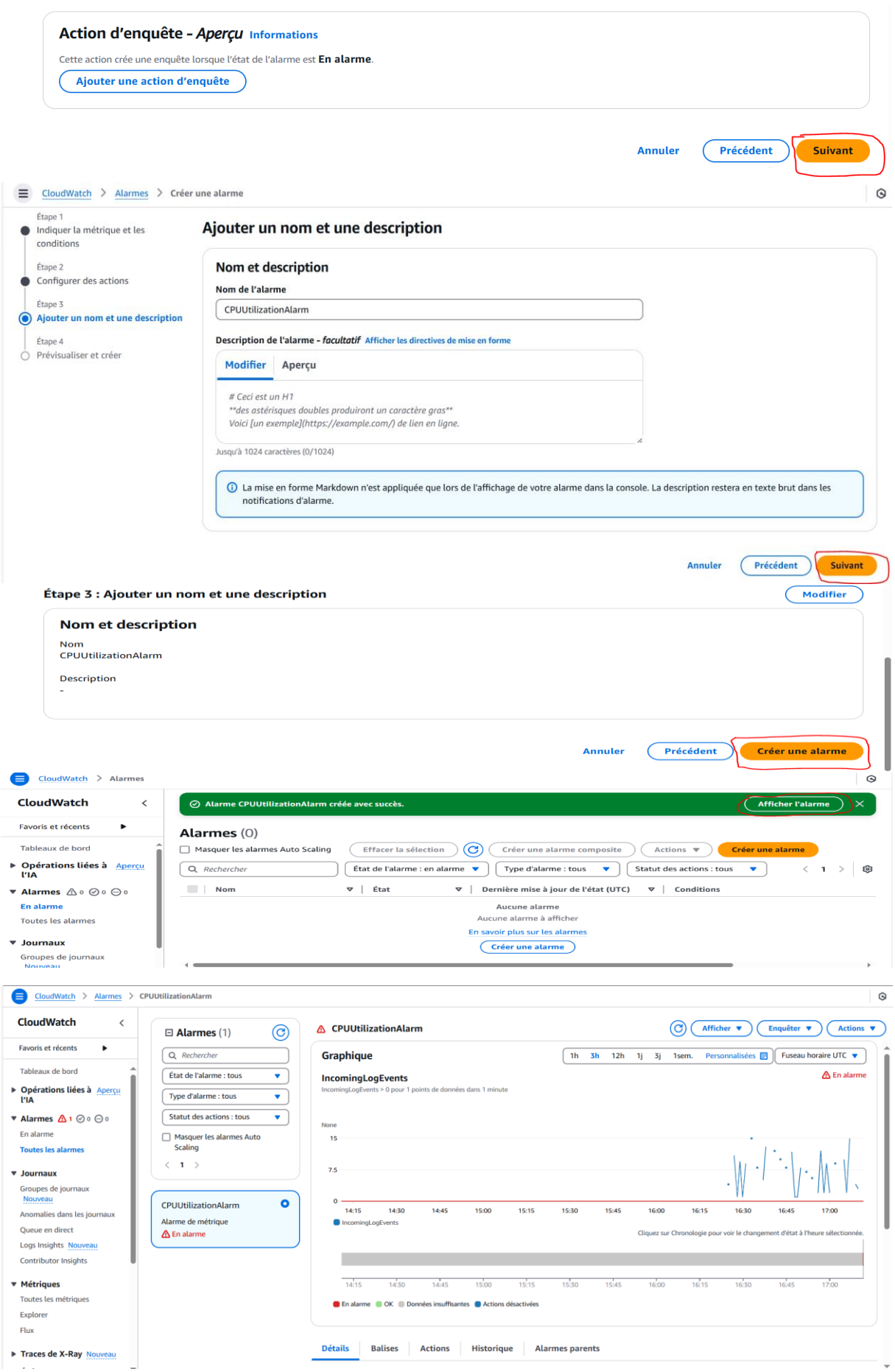
Service de notification simple

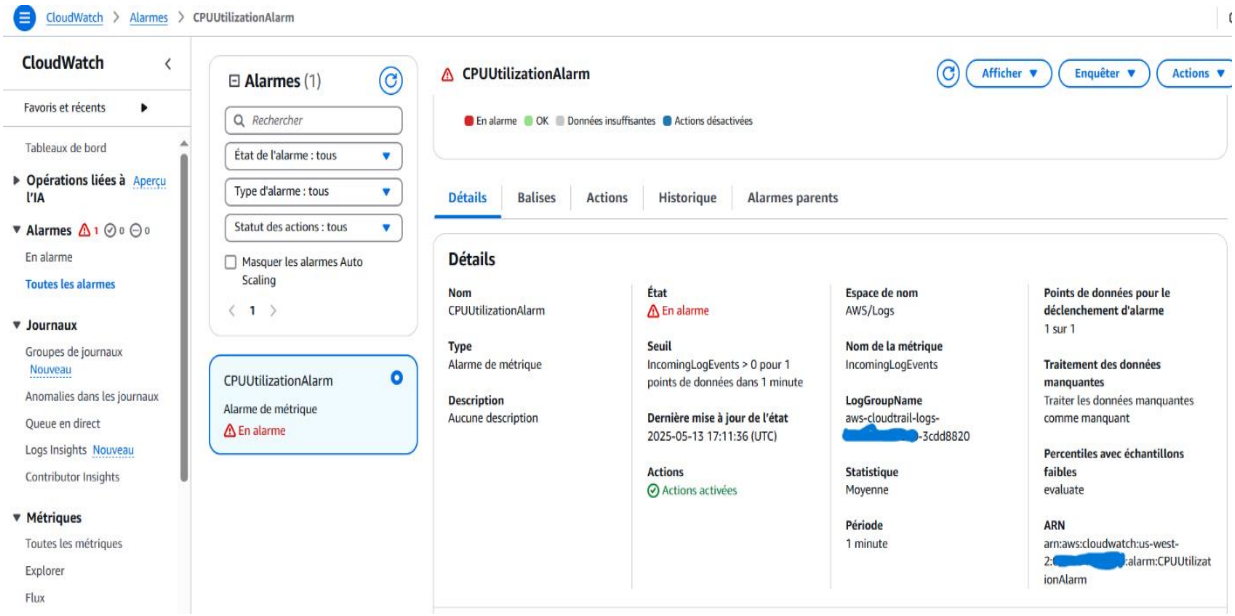
Abonnement confirmé !

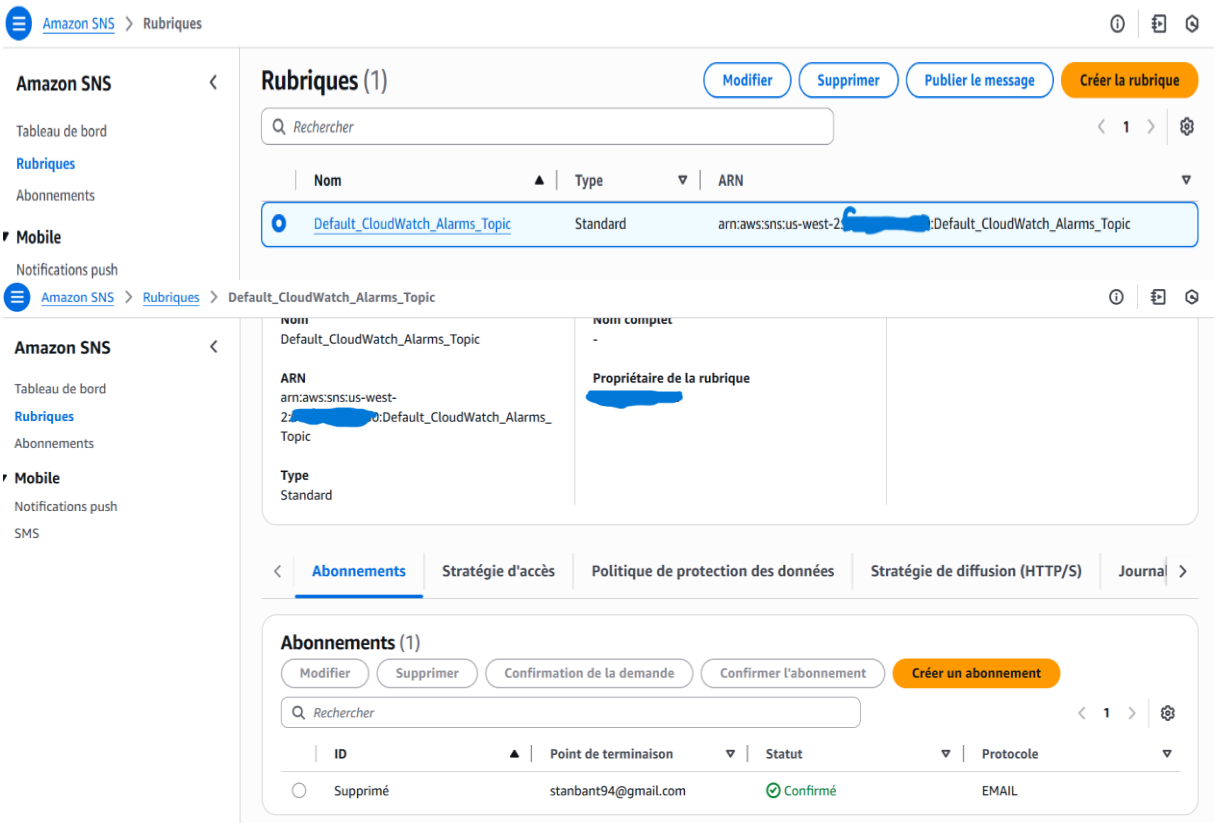
Vous êtes inscrit avec succès.

L'identifiant de votre abonnement est :
`arn:aws:sns:us-west-2:[redacted]:Default_CloudWatch_Alarms_Topic:0cbbeeac-f2f3-4701-8181-39862b61318d`

Si ce n'était pas votre intention de vous abonner, cliquez ici pour vous désabonner .


Action d'enquête - Aperçu Informations
Cette action crée une enquête lorsque l'état de l'alarme est En alarme.
Ajouter une action d'enquête
Annuler
Précédent
Suivant
CloudWatch > Alarmes > Créer une alarme
Étape 1
Indiquer la métrique et les conditions
Étape 2
Configurer des actions
Étape 3
Ajouter un nom et une description
Étape 4
Prévisualiser et créer
Ajouter un nom et une description
Nom et description
Nom de l'alarme
CPUUtilizationAlarm
Description de l'alarme - facultatif Afficher les directives de mise en forme
Modifier
Aperçu
Ceci est un H1
des astérisques doubles produiront un caractère gras
Voici [un exemple](https://example.com/) de lien en ligne.
Jusqu'à 1024 caractères (0/1024)
La mise en forme Markdown n'est appliquée que lors de l'affichage de votre alarme dans la console. La description restera en texte brut dans les notifications d'alarme.
Annuler
Précédent
Suivant
Étape 3 : Ajouter un nom et une description
Modifier
Nom et description
Nom
CPUUtilizationAlarm
Description
-
Annuler
Précédent
Créer une alarme
CloudWatch > Alarmes
CloudWatch
Alarme CPUUtilizationAlarm créée avec succès.
Afficher l'alarme
Favoris et récents
Tableaux de bord
Opérations liées à l'IA
Aperçu
Alarmes
En alarme
Toutes les alarmes
Journaux
Groupes de journaux
Alarmes (0)
Masquer les alarmes Auto Scaling
Effacer la sélection
Créer une alarme composite
Actions
Créer une alarme
Rechercher
État de l'alarme : en alarme
Type d'alarme : tous
Statut des actions : tous
Nom
État
Dernière mise à jour de l'état (UTC)
Conditions
Aucune alarme
Aucune alarme à afficher
En savoir plus sur les alarmes
Créer une alarme
CloudWatch > Alarmes > CPUUtilizationAlarm
CloudWatch
Alarmes (1)
CPUUtilizationAlarm
Alarme de métrique
En alarme
CPUUtilizationAlarm
Afficher
Enquêter
Actions
Graphique
1h 3h 12h 1j 3j 1sem. Personnalisées
Fuseau horaire UTC
IncomingLogEvents
IncomingLogEvents > 0 pour 1 points de données dans 1 minute
En alarme
Cliquez sur Chronologie pour voir le changement d'état à l'heure sélectionnée.
En alarme OK Données insuffisantes Actions désactivées
Détails
Balises
Actions
Historique
Alarmes parents
Métriques
Toutes les métriques
Explorer
Flux
Traces de X-Ray Nouveau





Étape 5 Test et validation

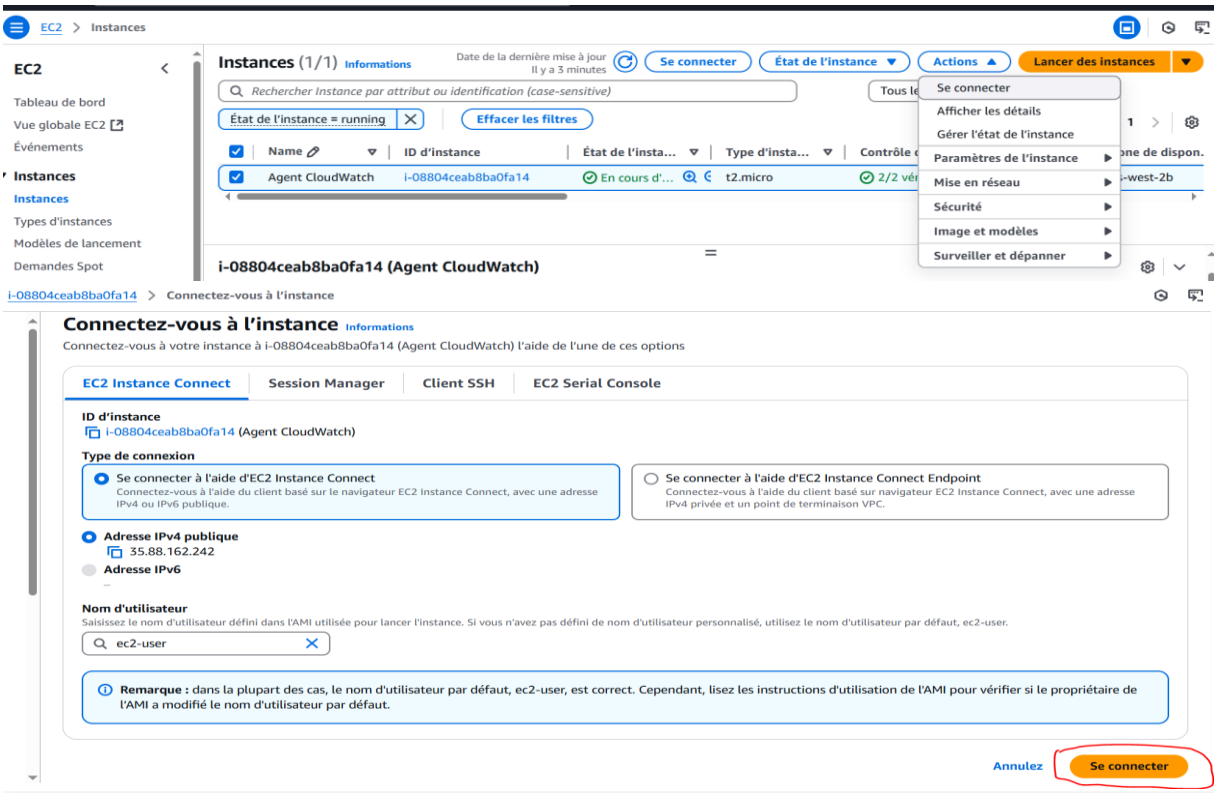
1. Connecte-toi à ton instance EC2
2. Installe et lance l'outil de charge stress en exécutant les commandes suivantes :

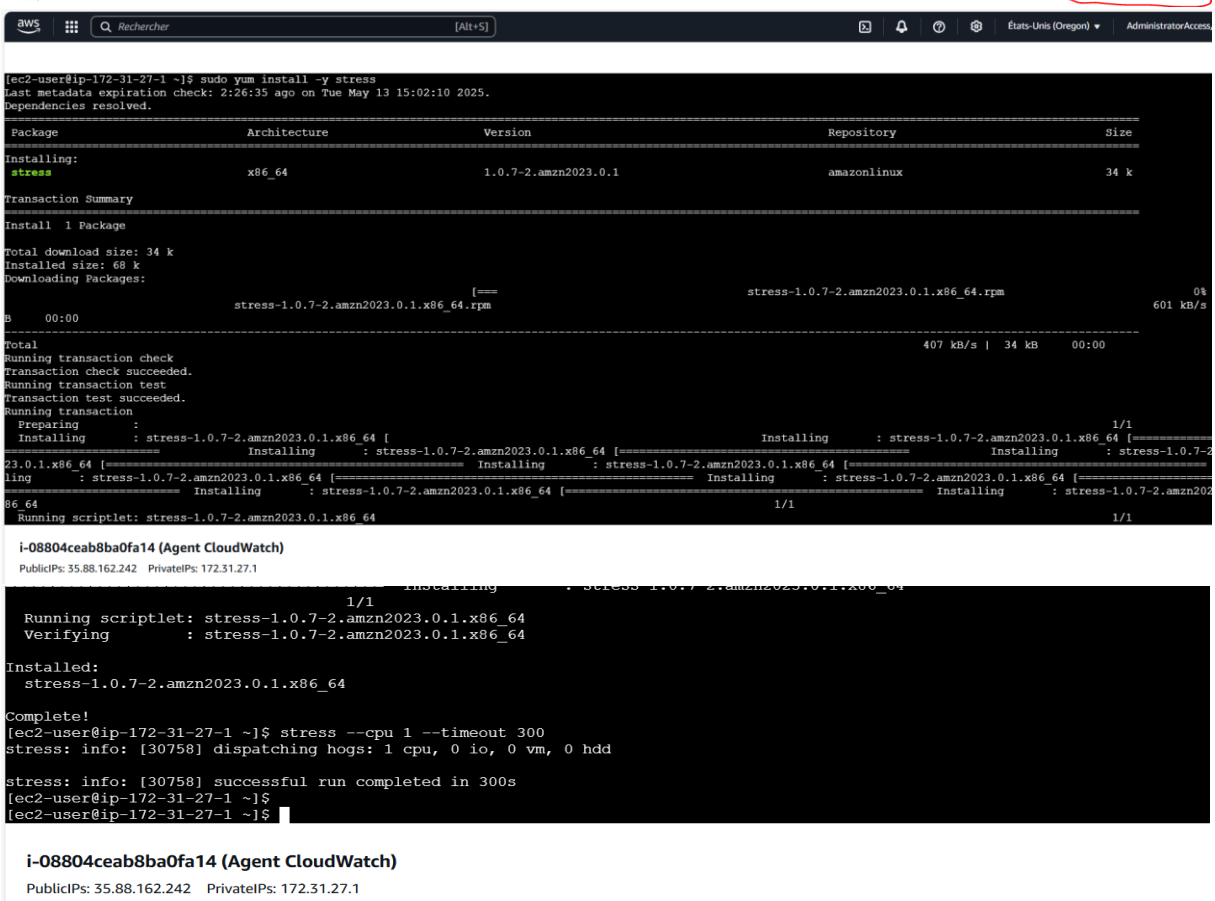
```
sudo yum install -y stress
stress --cpu 1 --timeout 300
```

3. Vérifie le déclenchement de l'alarme et la réception de l'e-mail :

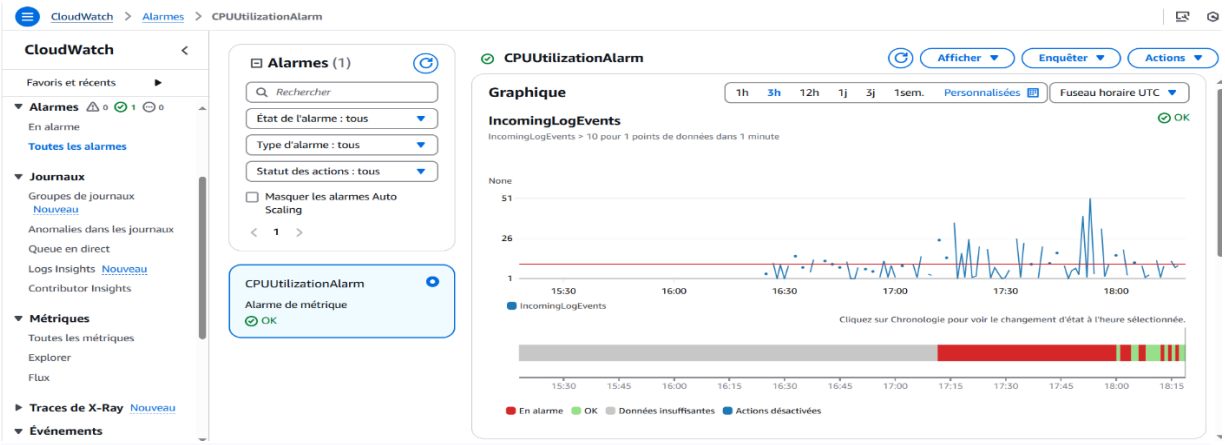
- Ton alarme devrait passer brièvement à l'état ALARM, puis retourner à OK
- Tu dois recevoir une **notification SNS** par mail

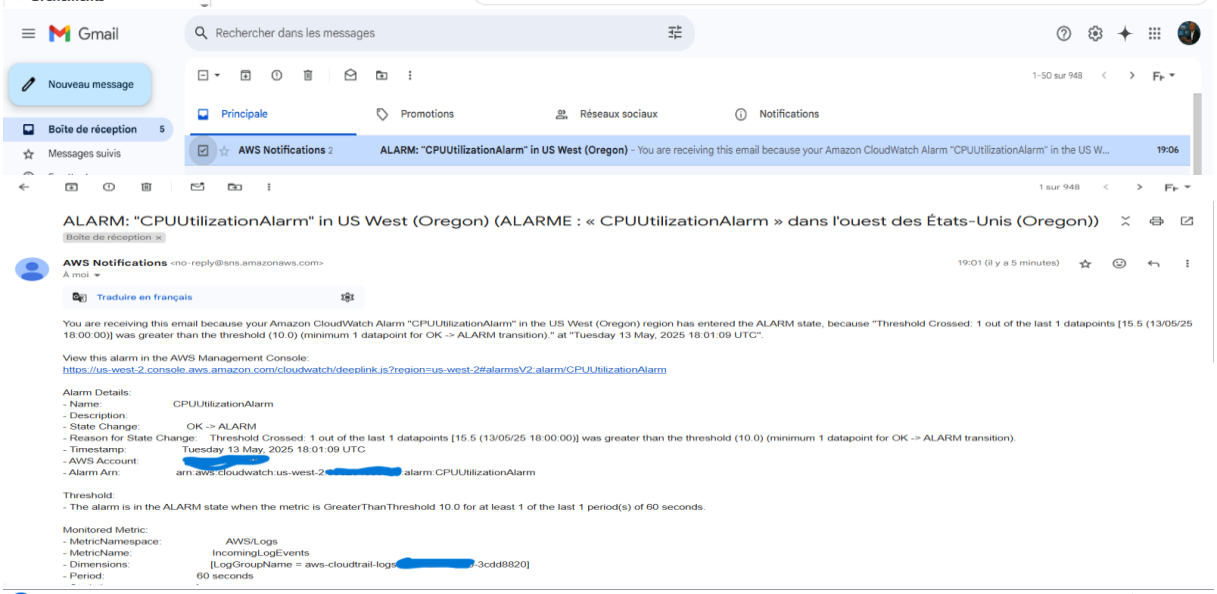
4. Vérifie le stockage des fichiers journaux dans ton bucket S3

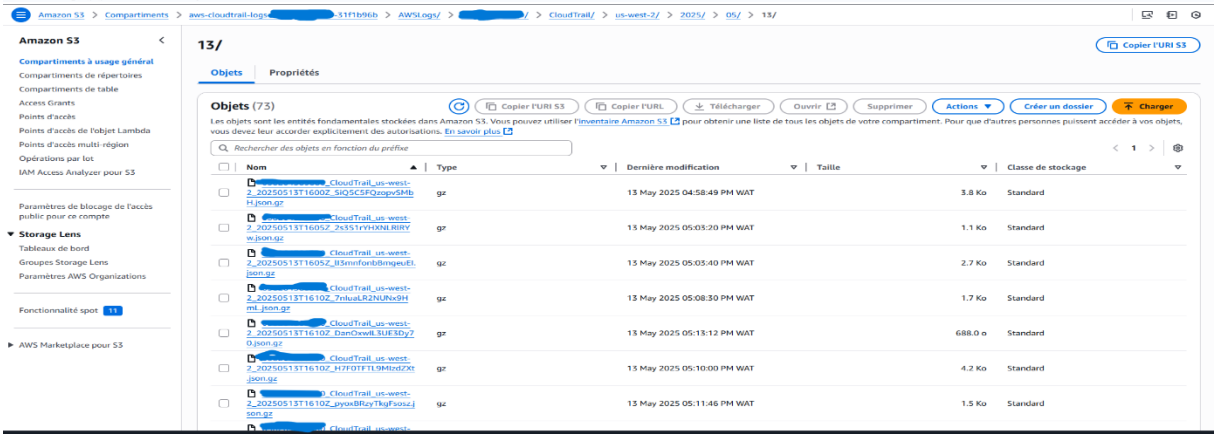




Tableaux de bord
Opérations liées à l'IA
Aperçu
Alarmes
En alarme
Toutes les alarmes
Journaux
Groupes de journaux
Nouveau
Anomalies dans les journaux
Queue en direct
Logs Insights
Nouveau
Contributor Insights
Métriques
Rechercher
État de l'alarme : en alarme
Type d'alarme : tous
Statut des actions : tous
Masquer les alarmes Auto Scaling
CPUUtilizationAlarm
Alarme de métrique
En alarme
None
36
18
0
15:00
15:30
16:00
16:30
17:00
17:30
IncomingLogEvents
Cliquez sur Chronologie pour voir le changement d'état à l'heure sélectionnée.
En alarme
OK
Données insuffisantes
Actions désactivées


CloudWatch > Alarmes > CPUUtilizationAlarm
CloudWatch
Favoris et récents
Alarmes
En alarme
Toutes les alarmes
Journaux
Groupes de journaux
Nouveau
Anomalies dans les journaux
Queue en direct
Logs Insights
Nouveau
Contributor Insights
Métriques
Toutes les métriques
Explorer
Flux
Traces de X-Ray
Nouveau
Événements
Alarmes (1)
Rechercher
État de l'alarme : tous
Type d'alarme : tous
Statut des actions : tous
Masquer les alarmes Auto Scaling
CPUUtilizationAlarm
Alarme de métrique
OK
CPUUtilizationAlarm
Afficher
Enquêter
Actions
Graphique
1h
3h
12h
1j
3j
1sem.
Personnalisées
Fuseau horaire UTC
IncomingLogEvents
IncomingLogEvents > 10 pour 1 points de données dans 1 minute
OK
None
51
26
1
15:30
16:00
16:30
17:00
17:30
18:00
IncomingLogEvents
Cliquez sur Chronologie pour voir le changement d'état à l'heure sélectionnée.
En alarme
OK
Données insuffisantes
Actions désactivées


Gmail
Rechercher dans les messages
Nouveau message
Boîte de réception
Messages suivis
Principale
Promotions
Réseaux sociaux
Notifications
AWS Notifications
ALARM: "CPUUtilizationAlarm" in US West (Oregon) - You are receiving this email because your Amazon CloudWatch Alarm "CPUUtilizationAlarm" in the US W...
19:06
ALARM: "CPUUtilizationAlarm" in US West (Oregon) (ALARME : « CPUUtilizationAlarm » dans l'ouest des États-Unis (Oregon))
AWS Notifications <no-reply@sns.amazonaws.com>
Traduire en français
You are receiving this email because your Amazon CloudWatch Alarm "CPUUtilizationAlarm" in the US West (Oregon) region has entered the ALARM state, because "Threshold Crossed: 1 out of the last 1 datapoints [15.5 (13/05/25 18:00:00)] was greater than the threshold (10.0) (minimum 1 datapoint for OK -> ALARM transition)." at "Tuesday 13 May, 2025 18:01:09 UTC".
View this alarm in the AWS Management Console:
https://us-west-2.console.aws.amazon.com/cloudwatch/deeplink.js?region=us-west-2#alarmsV2:alarm/CPUUtilizationAlarm
Alarm Details:
- Name: CPUUtilizationAlarm
- Description:
- State Change: OK -> ALARM
- Reason for State Change: Threshold Crossed: 1 out of the last 1 datapoints [15.5 (13/05/25 18:00:00)] was greater than the threshold (10.0) (minimum 1 datapoint for OK -> ALARM transition).
- Timestamp: Tuesday 13 May, 2025 18:01:09 UTC
- AWS Account:
- Alarm Arn: arn:aws:cloudwatch:us-west-2 alarm:CPUUtilizationAlarm
Threshold:
- The alarm is in the ALARM state when the metric is GreaterThanThreshold 10.0 for at least 1 of the last 1 period(s) of 60 seconds.
Monitored Metric:
- MetricNamespace: AWS/Logs
- MetricName: IncomingLogEvents
- Period: 60 seconds


Amazon S3
Compartiments à usage général
Compartiments de répertoires
Compartiments de table
Storage Lens
13/
Objets
Propriétés
Objets (73)
Copier l'URI S3
Copier l'URL
Télécharger
Ouvrir
Supprimer
Actions
Créer un dossier
Charger
Nom
Type
Dernière modification
Taille
Classe de stockage