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.

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.

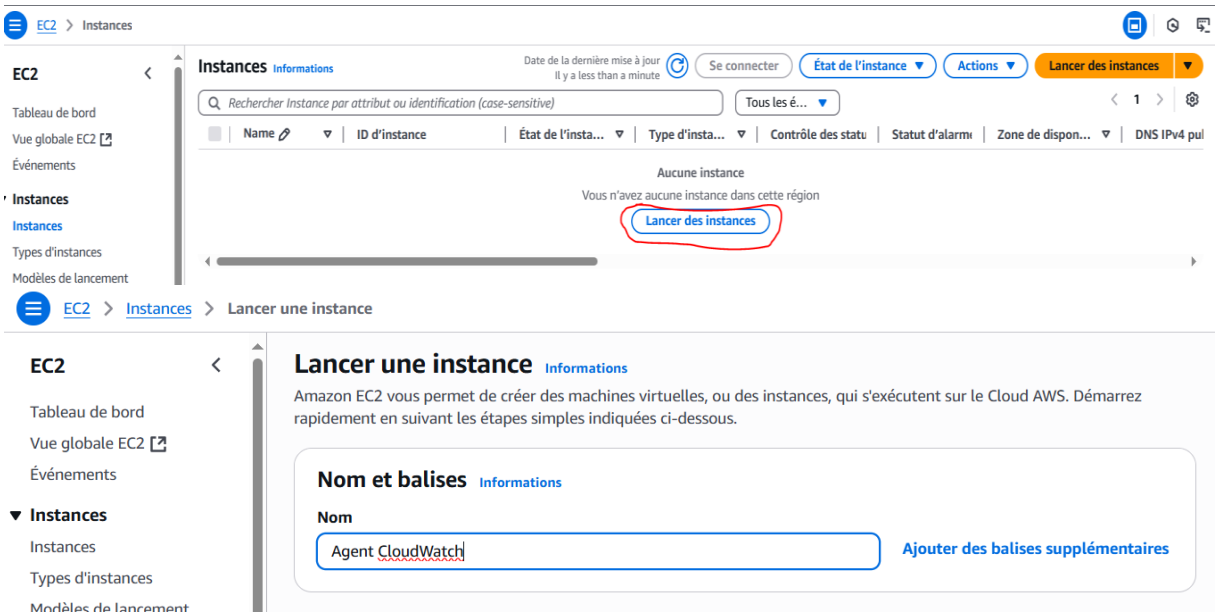
Étape 1 Création de l'instance EC2

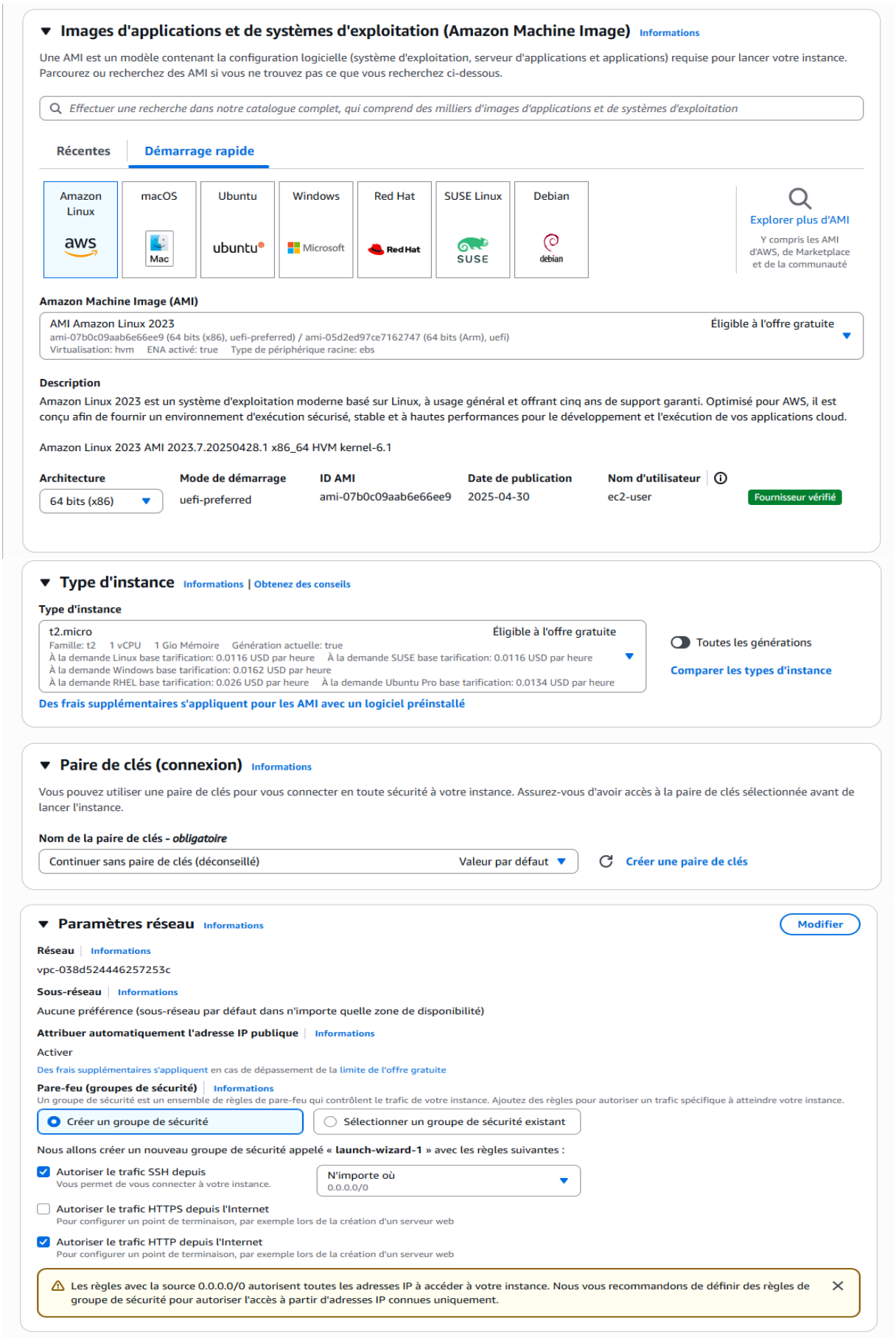
1. Amazon Linux 2023
2. Type : **t2.micro** (Free Tier)
3. Groupe de sécurité :
    a. Port 22 : autoriser le trafic **SSH** depuis **N'importe où**
    b. Port 80 : autoriser le trafic **HTTP** depuis l'**Internet**
4. Dans **Détails avancés** > **Données utilisateurs** colle le script ci-dessus pour l'installation et configuration de l'agent CloudWatch, puis clique sur **Lancer l'instance**.

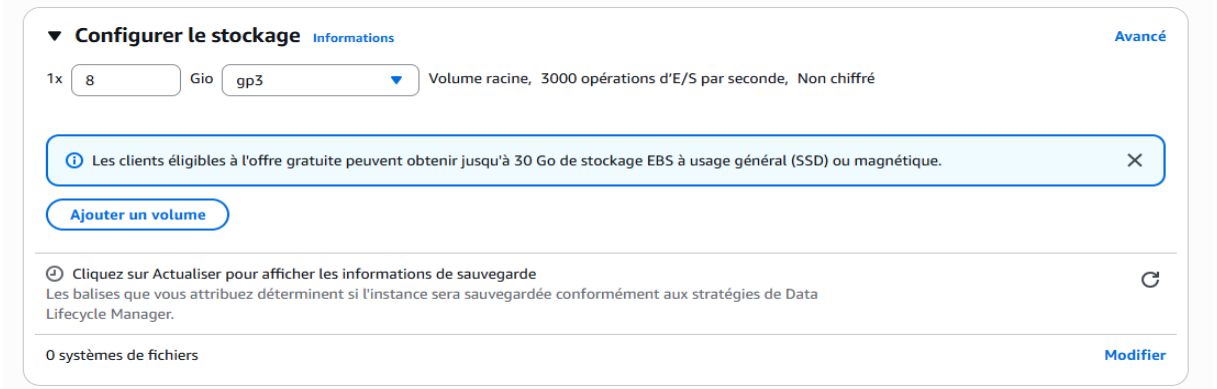
```
#!/bin/bash

# Mise à jour du système

yum update -y
```

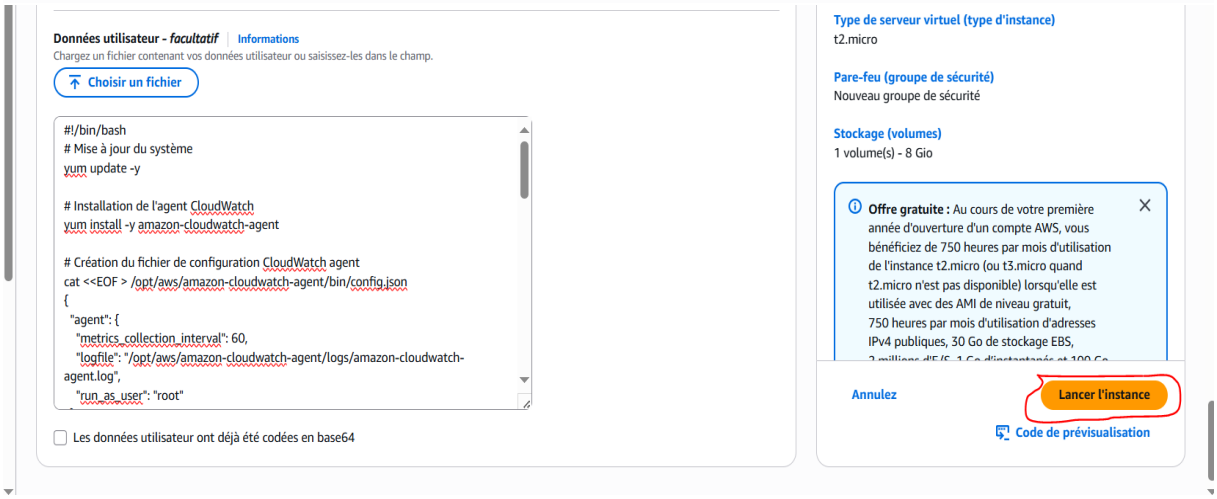
```
# Installation de l'agent CloudWatch
yum install -y amazon-cloudwatch-agent
# Création du fichier de configuration CloudWatch agent
cat <<EOF > /opt/aws/amazon-cloudwatch-agent/bin/config.json
{
  "agent": {
    "metrics_collection_interval": 60,
    "logfile": "/opt/aws/amazon-cloudwatch-agent/logs/amazon-cloudwatch-agent.log",
    "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
```

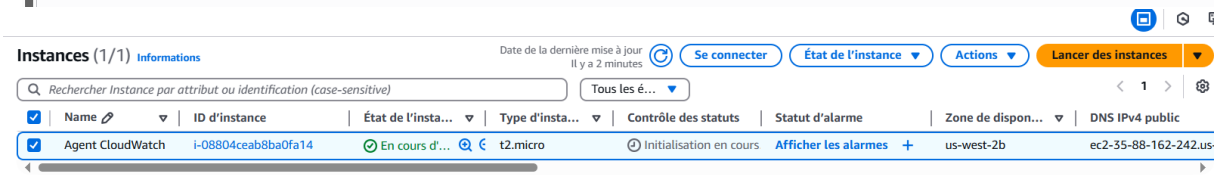


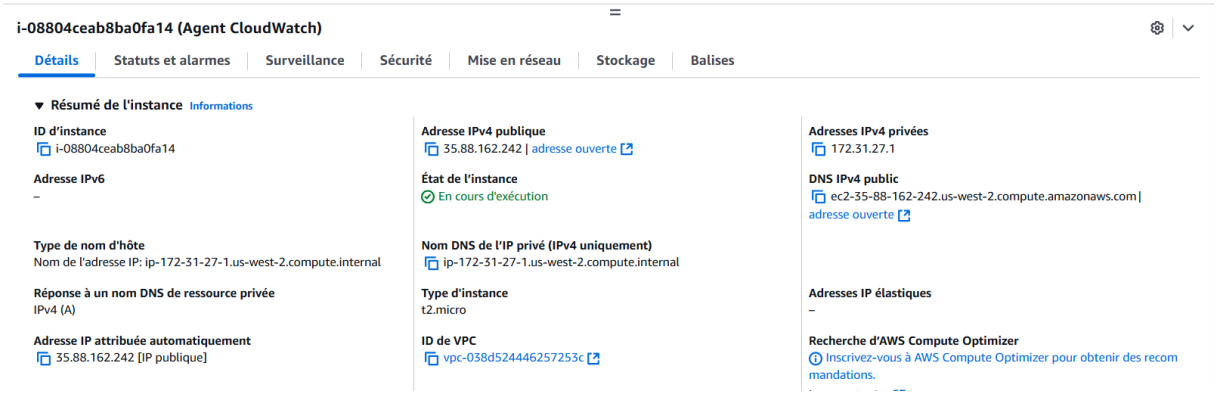

Images d'applications et de systèmes d'exploitation (Amazon Machine Image) Informations
Une AMI est un modèle contenant la configuration logicielle (système d'exploitation, serveur d'applications et applications) requise pour lancer votre instance. Parcourez ou recherchez des AMI si vous ne trouvez pas 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
ami-07b0c09aab6e66ee9 (64 bits (x86), uefi-preferred) / ami-05d2ed97ce7162747 (64 bits (Arm), uefi)
Virtualisation: hvm ENA activé: true Type de périphérique racine: ebs
Éligible à l'offre gratuite
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
64 bits (x86)
Mode de démarrage
uefi-preferred
ID AMI
ami-07b0c09aab6e66ee9
Date de publication
2025-04-30
Nom d'utilisateur
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

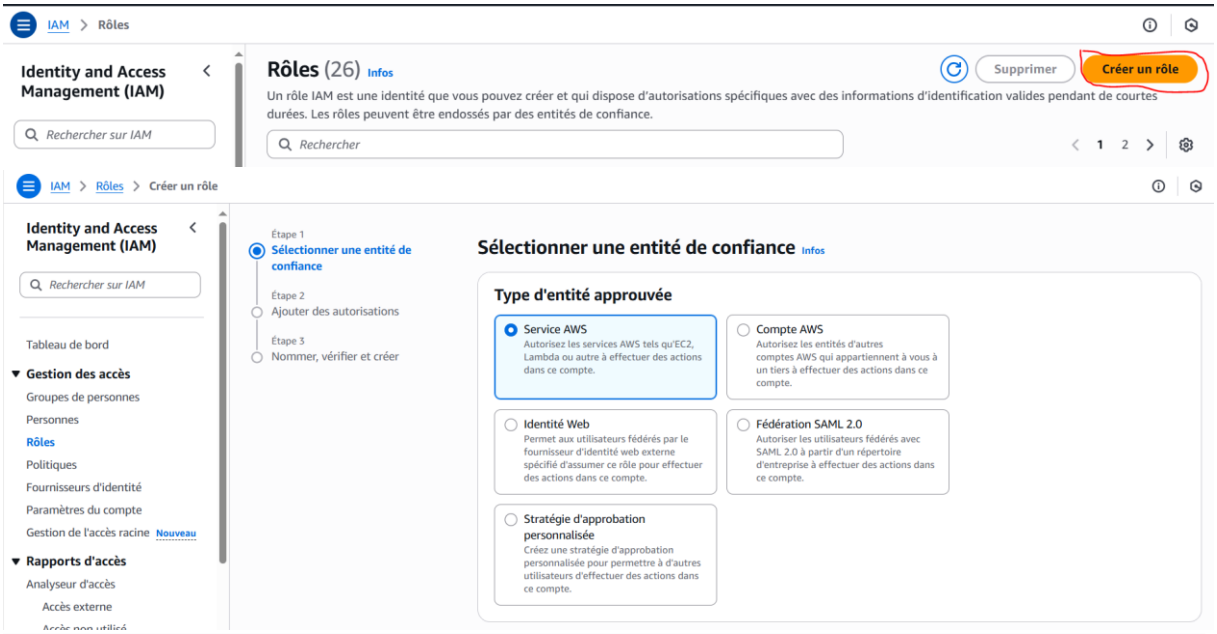
Lancer une instance
Succès
Lancement de l'instance réussi (i-08804ceab8ba0fa14)
Journal de lancement
Initialisation des requêtes Réussi
Création de groupes de sécurité Réussi
Création des règles de groupe de sécurité Réussi
Début du lancement Réussi

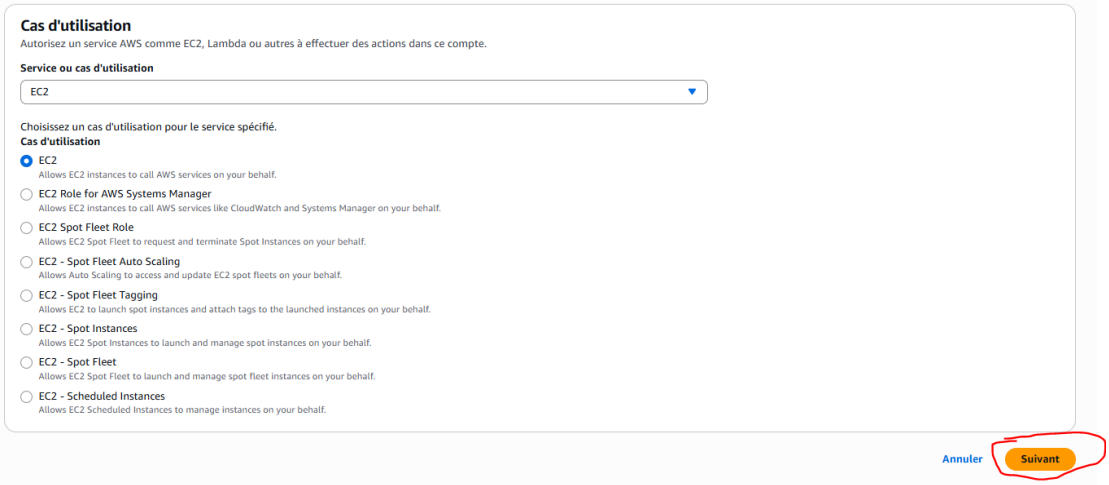

Instances (1/1) Informations
Date de la dernière mise à jour Il y a 2 minutes
Se connecter
État de l'instance
Actions
Lancer des instances
Rechercher Instance par attribut ou identification (case-sensitive)
Tous les é...
Name
ID d'instance
État de l'insta...
Type d'insta...
Contrôle des statuts
Statut d'alarme
Zone de dispon...
DNS IPv4 public
Agent CloudWatch
i-08804ceab8ba0fa14
En cours d'...
t2.micro
Initialisation en cours
Afficher les alarmes
us-west-2b
ec2-35-88-162-242.us-

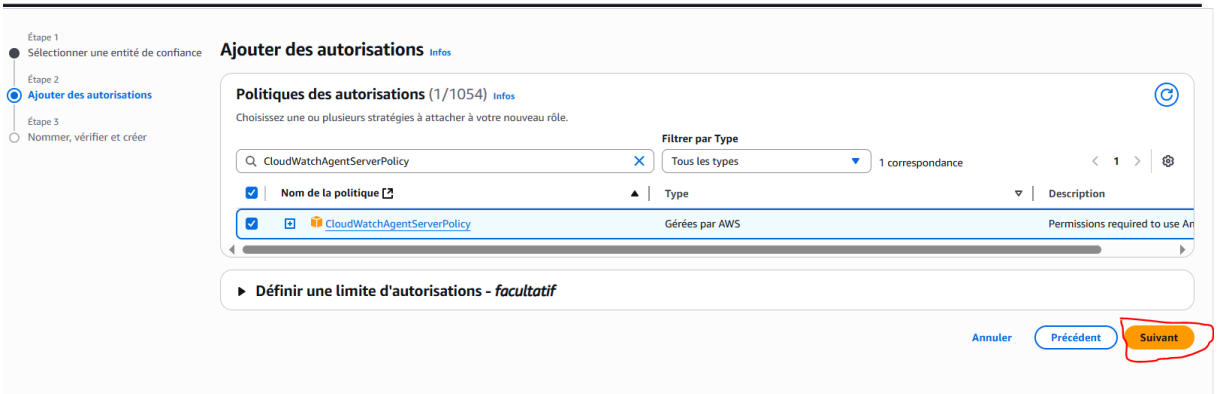

i-08804ceab8ba0fa14 (Agent CloudWatch)
Détails
Statuts et alarmes
Surveillance
Sécurité
Mise en réseau
Stockage
Balises
Résumé de l'instance Informations
ID d'instance
i-08804ceab8ba0fa14
Adresse IPv6
–
Type de nom d'hôte
Nom de l'adresse IP: ip-172-31-27-1.us-west-2.compute.internal
Réponse à un nom DNS de ressource privée
IPv4 (A)
Adresse IP attribuée automatiquement
35.88.162.242 [IP publique]
Adresse IPv4 publique
35.88.162.242 | adresse ouverte
État de l'instance
En cours d'exécution
Nom DNS de l'IP privé (IPv4 uniquement)
ip-172-31-27-1.us-west-2.compute.internal
Type d'instance
t2.micro
ID de VPC
vpc-038d524446257253c
Adresses IPv4 privées
172.31.27.1
DNS IPv4 public
ec2-35-88-162-242.us-west-2.compute.amazonaws.com | adresse ouverte
Adresses IP élastiques
–
Recherche d'AWS Compute Optimizer
Inscrivez-vous à AWS Compute Optimizer pour obtenir des recommandations.

Étape 2 Créer un rôle IAM pour EC2

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







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

```
1  {
2      "Version": "2012-10-17",
3      "Statement": [
4          {
5              "Effect": "Allow",
6              "Action": [
7                  "sts:AssumeRole"
8              ],
9              "Principal": {
10                 "Service": [
11                     "ec2.amazonaws.com"
12                 ]
13             }
14         }
15     ]
16 }
```

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)
Rechercher sur IAM
Tableau de bord
Gestion des accès
Groupes de personnes
Personnes
Rôles

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

Nom du rôle	Entités de confiance	Dernière activité
EC2CloudWatchRole	Service AWS: ec2	-

Instances (1/1) 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'alarm	Zone de dispo	Adres
Agent CloudWatch	i-08804ceab8ba0fa14	En cours d'...	t2.micro	2/2 vérifications r	Afficher les alarm	us-west-2b	35.88.

Actions :
- 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

Sécurité :
- 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

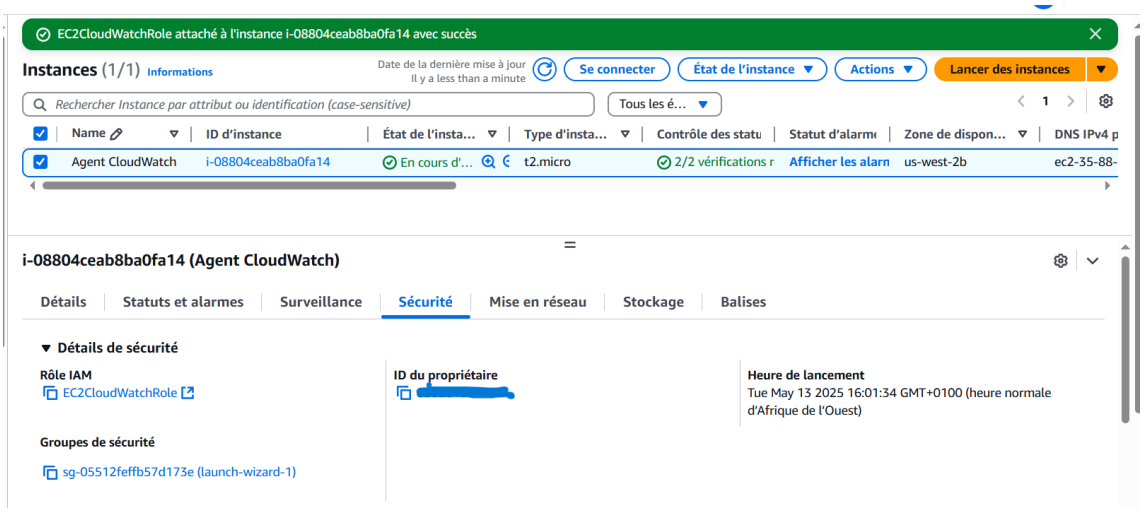
Modifier le rôle IAM Informations

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



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

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

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

Aucun journal de suivi
Aucun journal de suivi à afficher.
Créer un journal de suivi

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 les attributs du journal de suivi

Détails généraux
Un journal de suivi créé dans la console est un journal de suivi sur plusieurs régions. En savoir plus

Nom du journal de suivi
Saisissez un nom d'affichage pour votre journal de suivi.
MySecurityTrail
Doit comprendre 3 à 128 caractères et uniquement des lettres, chiffres, points, traits de soulignement et tirets.

☐ Activer pour tous les comptes de mon organisation
Pour vérifier les comptes de votre organisation, ouvrez AWS Organizations. Voir tous les comptes

Emplacement de stockage | Info
- (•) Créer un compartiment S3 — Créez un compartiment pour stocker les journaux du suivi.
- ( ) Utiliser un compartiment S3 existant — Choisissez un compartiment existant pour stocker ces journaux de suivi.

Compartiment et dossier des journaux de suivi
Saisissez un nouveau nom de compartiment S3 et indiquez un nouveau dossier (préfixe) pour stocker vos journaux. Les noms de compartiment doivent être uniques à l'échelle mondiale.
aws-cloudtrail-logs-[redacted]008a9c99
Les journaux seront stockés dans aws-cloudtrail-logs-[redacted]008a9c99/AWSLogs/[redacted]

Chiffrement SSE-KMS du fichier journal | Info
☑ Activé

Clé AWS KMS gérée par le client
- (•) Nouveau
- ( ) Existant

Alias AWS KMS
cle-s3
La clé KMS et le compartiment S3 doivent appartenir à la même région.

▼ Paramètres supplémentaires

Validation du fichier journal | Info
☑ Activé

Livraison de notifications SNS | Info
☐ Activé

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.

- [x] 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.

- [x] Lecture
- [x] 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	arn:aws:cloudtrail:us-west-2:[redacted]:trail/MySecurityTrail	Désactivé	Non	aws-cloudtrail-logs-[redacted]-31f1b96b	-	arn:aws:logs:us-west-2:[redacted]:log-group:aws-cloudtrail-logs-[redacted]-3cdd8820:*	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
aws-cloudtrail-logs-[redacted]-31f1b96b/AWSLogs/[redacted]

Dernier fichier journal livré
mai 13, 2025, 17:23:42 (UTC+01:00)

Chiffrement SSE-KMS du fichier journal
Activé

Clé AWS KMS
arn:aws:kms:us-west-2:[redacted]:key/5cbc7a32-12e7-4cac-819c-e3afc758ffa2

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

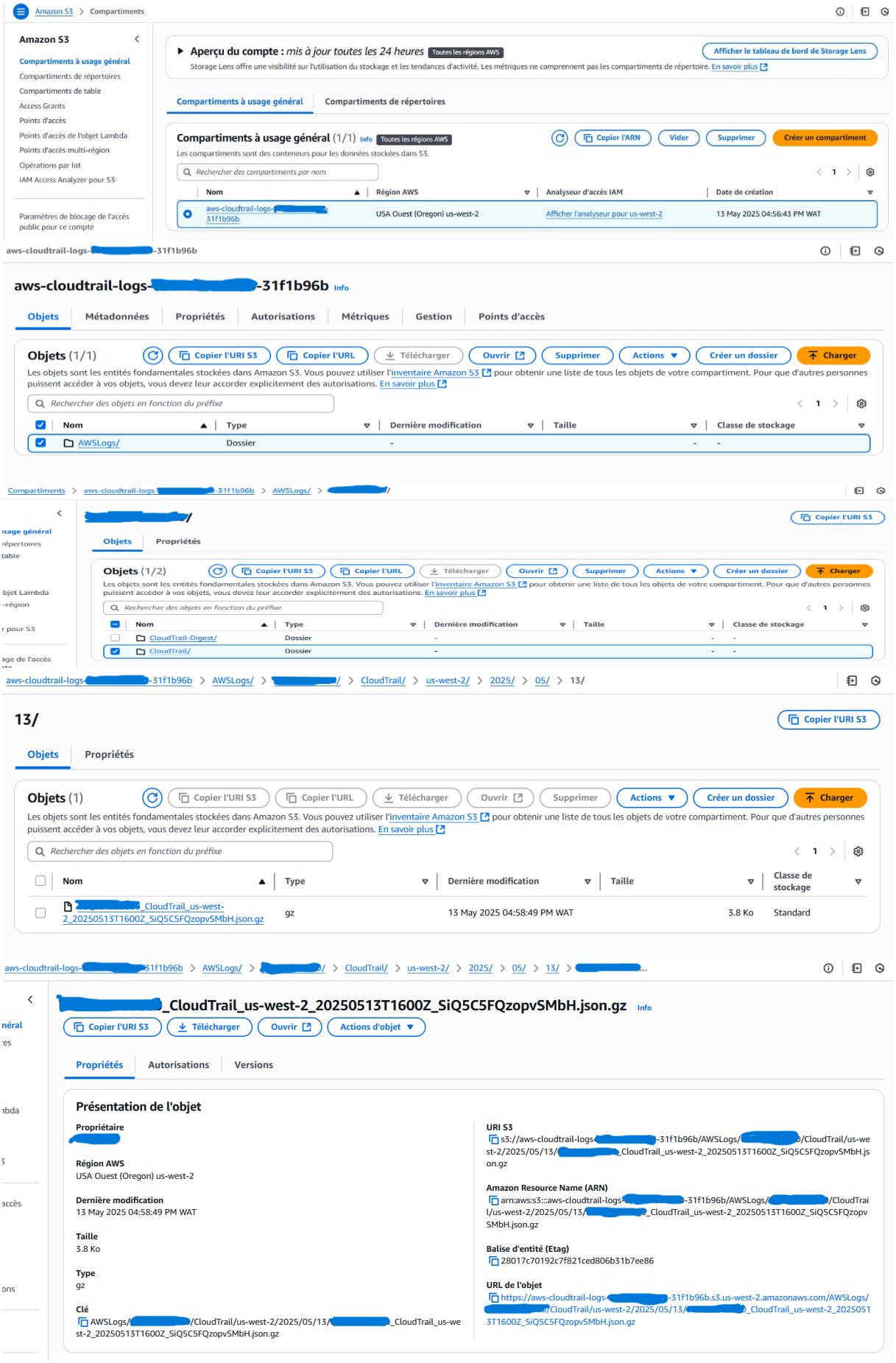
Dernière notification SNS
-

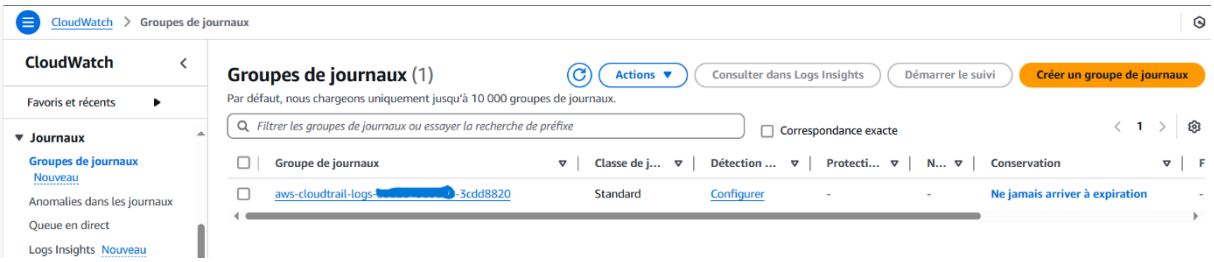
CloudWatch Logs

Modifier

Groupe de journaux
aws-cloudtrail-logs-[redacted]-3cdd8820

Rôle IAM
arn:aws:iam::[redacted]:role/service-role/RoleCloudTrailForLogsCloudWatch


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) Info
Toutes les régions AWS
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
aws-cloudtrail-logs-[redacted]-31f1b96b
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
aws-cloudtrail-logs-[redacted]-31f1b96b Info
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]/
[redacted]/
Objets (1/2)
CloudTrail-Digest/
CloudTrail/
aws-cloudtrail-logs-[redacted]-31f1b96b > AWSLogs/ > [redacted]/ > CloudTrail/ > us-west-2/ > 2025/ > 05/ > 13/
13/
Objets (1)
[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz
gz
13 May 2025 04:58:49 PM WAT
3.8 Ko
Standard
aws-cloudtrail-logs-[redacted]-31f1b96b > AWSLogs/ > [redacted]/ > CloudTrail/ > us-west-2/ > 2025/ > 05/ > 13/ > [redacted]
[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz Info
Télécharger
Actions d'objet
Propriétés
Autorisations
Versions
Présentation de l'objet
Propriétaire
[redacted]
Région AWS
USA Ouest (Oregon) us-west-2
Dernière modification
13 May 2025 04:58:49 PM WAT
Taille
3.8 Ko
Type
gz
Clé
AWSLogs/[redacted]/CloudTrail/us-west-2/2025/05/13/[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz
URI S3
s3://aws-cloudtrail-logs-[redacted]-31f1b96b/AWSLogs/[redacted]/CloudTrail/us-west-2/2025/05/13/[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz
Amazon Resource Name (ARN)
arn:aws:s3:::aws-cloudtrail-logs-[redacted]-31f1b96b/AWSLogs/[redacted]/CloudTrail/us-west-2/2025/05/13/[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz
Balise d'entité (Etag)
28017c70192c7f821ced806b31b7ee86
URL de l'objet
https://aws-cloudtrail-logs-[redacted]-31f1b96b.s3.us-west-2.amazonaws.com/AWSLogs/[redacted]/CloudTrail/us-west-2/2025/05/13/[redacted]_CloudTrail_us-west-2_20250513T1600Z_SiQ5C5FQzopvSMbH.json.gz



Étape 4 Créer une alarme CloudWatch

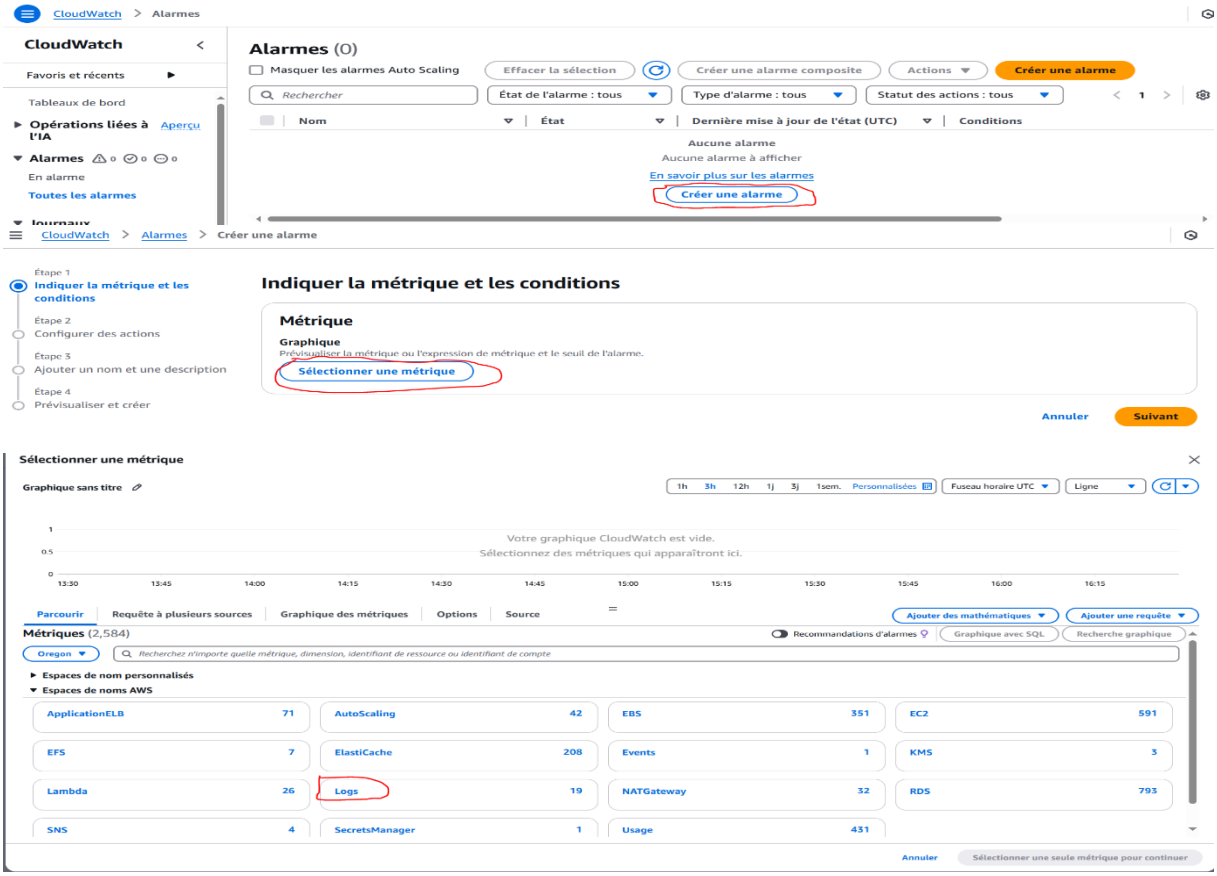
1. Va dans **CloudWatch > Alarmes > Créer une alarme** :

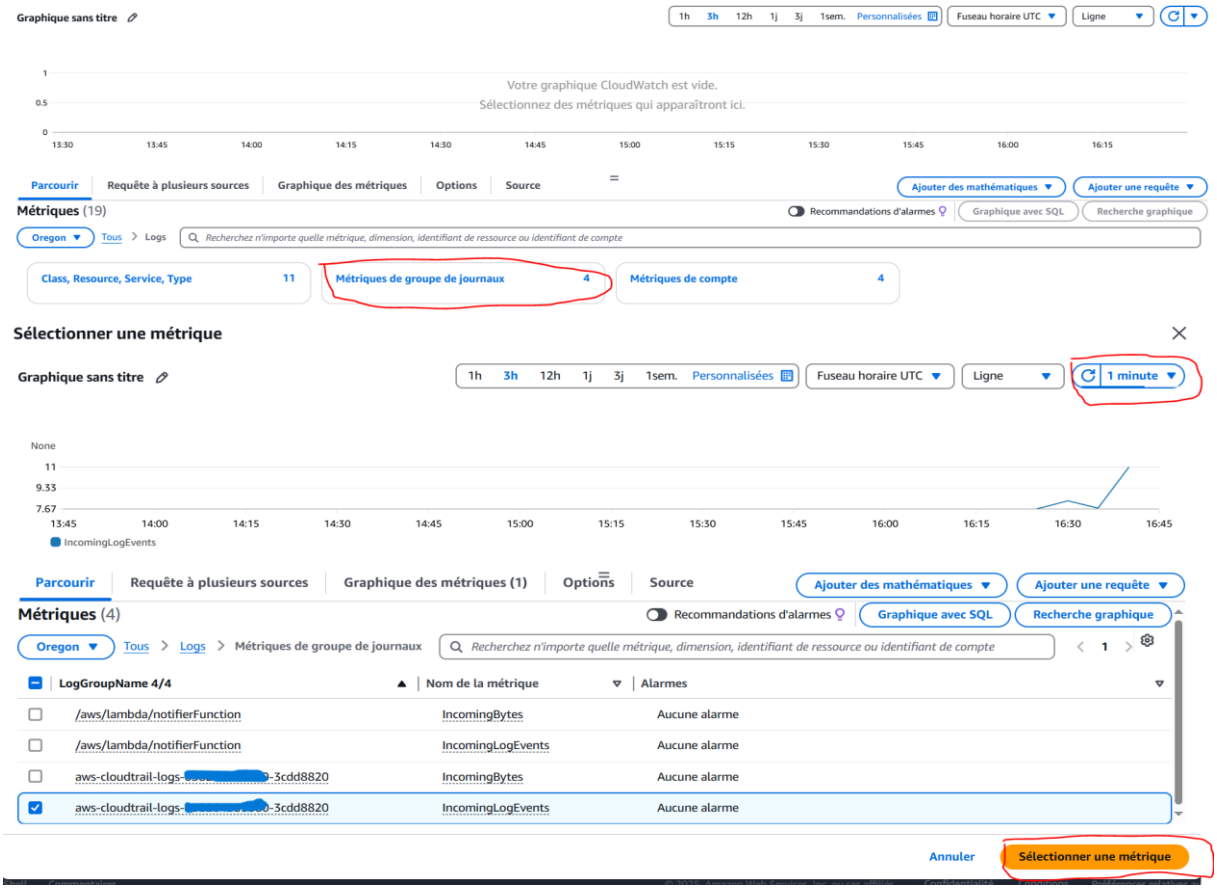
    - Nom : **CPUUtilizationAlarm**
    - Nom de la métrique : **IncomingLogEvents**
    - Statistique : **Moyenne**
    - Période : **1 min**
    - Type de seuil : Statique
    - Seuil : CPU > **10%**
    - Déclencheur d'état d'alarme : **En alarme**

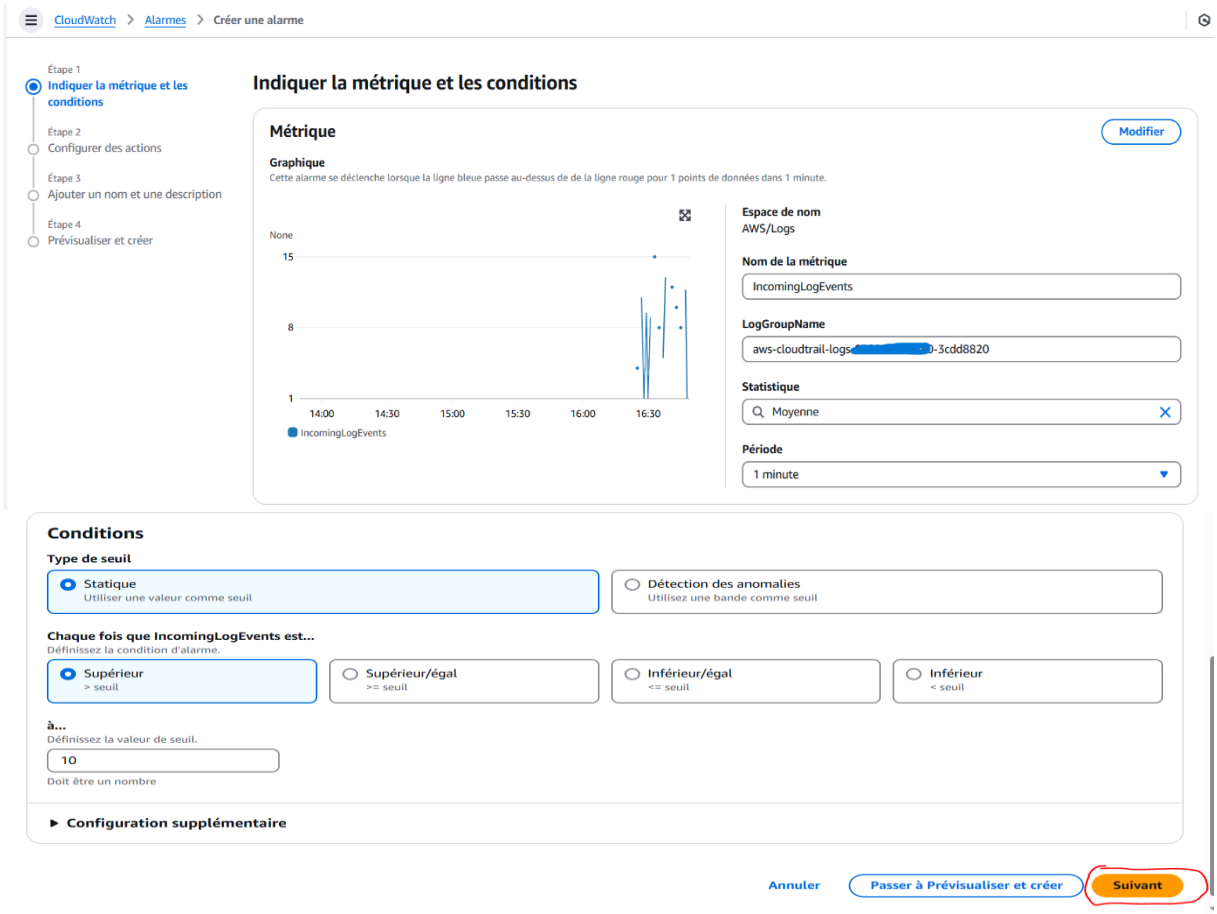
2. Créer un **topic SNS** + abonnement email

3. Lier l'alarme CloudWatch à ce topic

4. Vérifier que le topic SNS et l'alarme CloudWatch ont été créer.




Graphique sans titre
1h 3h 12h 1j 3j 1sem. Personnalisées
Fuseau horaire UTC
Ligne
Votre graphique CloudWatch est vide.
Sélectionnez des métriques qui apparaîtront ici.
Parcourir
Requête à plusieurs sources
Graphique des métriques
Options
Source
Ajouter des mathématiques
Ajouter une requête
Métriques (19)
Recommandations d'alarmes
Graphique avec SQL
Recherche graphique
Oregon
Tous > Logs
Recherchez n'importe quelle métrique, dimension, identifiant de ressource ou identifiant de compte
Class, Resource, Service, Type 11
Métriques de groupe de journaux 4
Métriques de compte 4
Sélectionner une métrique
Graphique sans titre
1 minute
IncomingLogEvents
Métriques (4)
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.
IncomingLogEvents
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
Principale — Promotions — Réseaux sociaux 1 nouveau — Notifications
1–50 sur 946
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

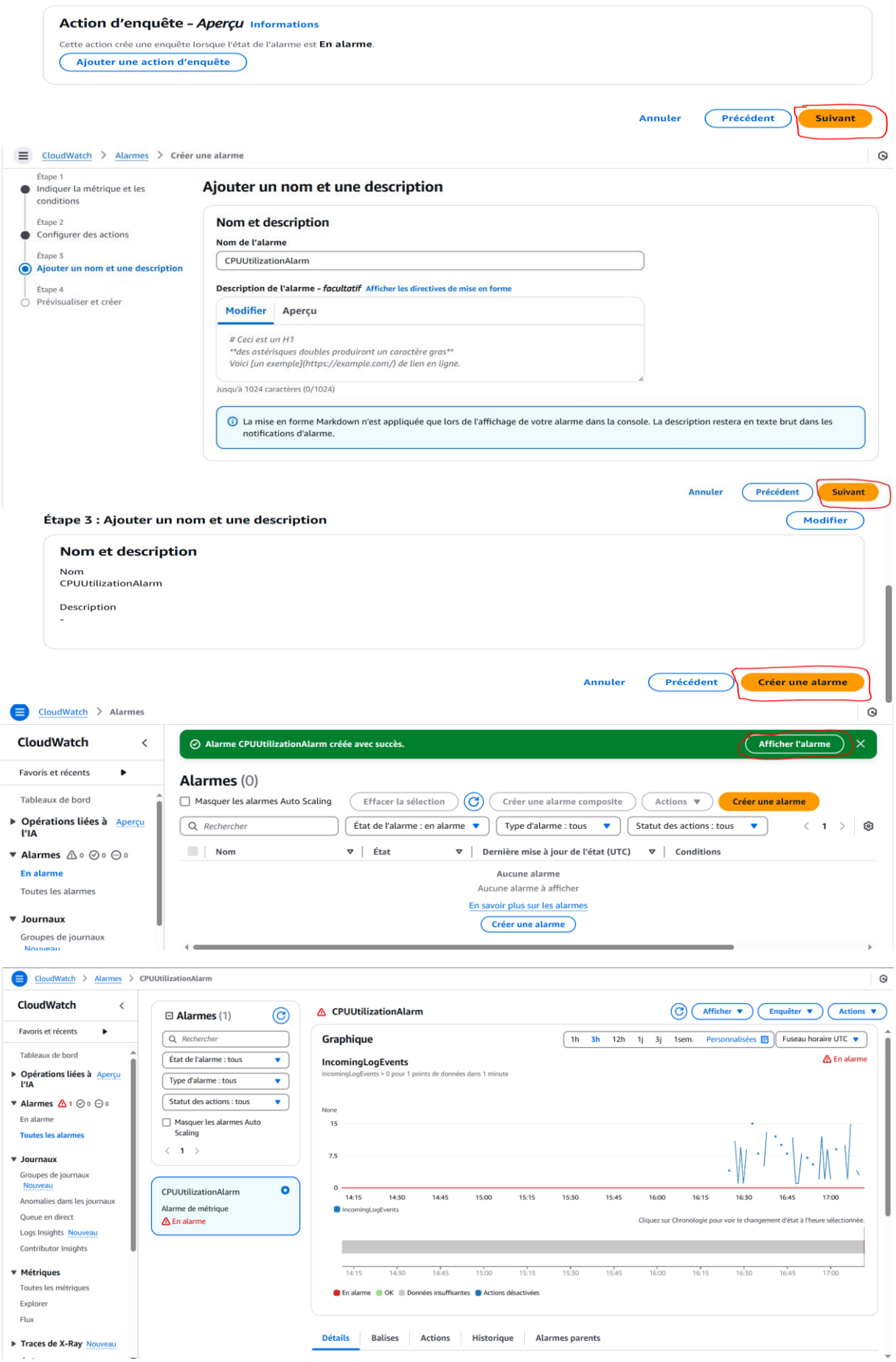
Pour confirmer cet abonnement, cliquez ou visitez le lien ci-dessous (si cela était une erreur, aucune action n'est nécessaire) :
Confirmer l'abonnement

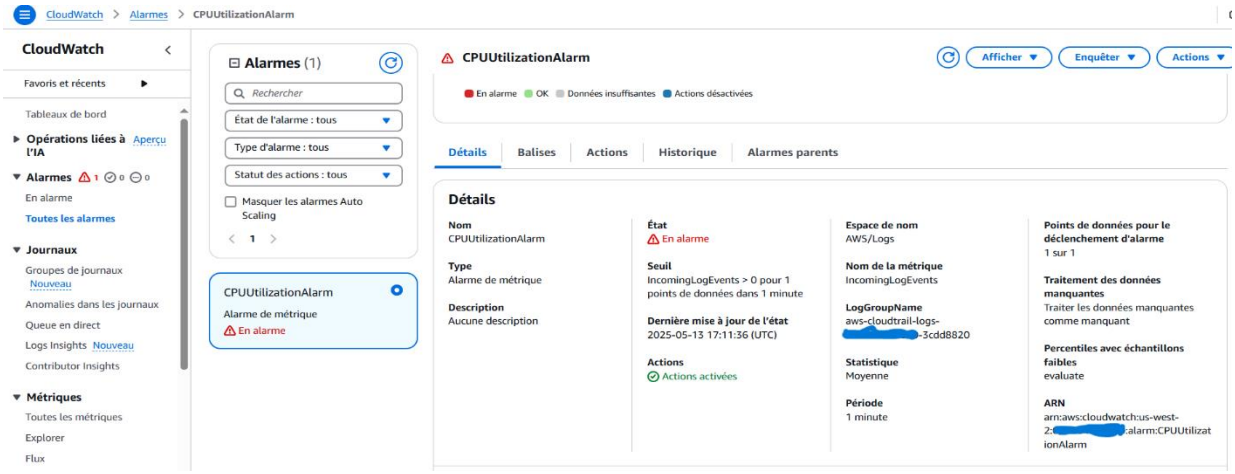
Veuillez ne pas répondre directement à cet e-mail. Si vous souhaitez ne plus recevoir de demandes de confirmation d'abonnement aux réseaux sociaux, veuillez envoyer un e-mail à sns-opt-out.

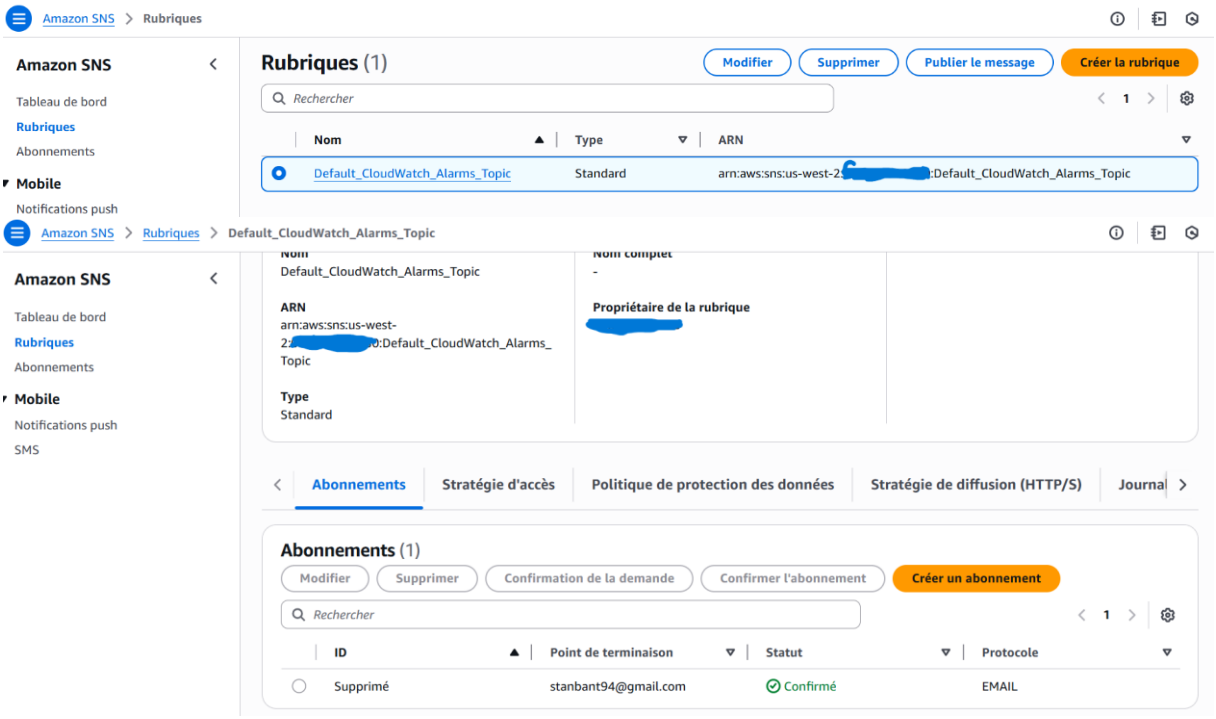
sns.us-west-2.amazonaws.com/confirmation.html?TopicArn=arn:aws:sns:us-west-2:058264389880:Default_CloudWatch_Alarms_Topic&Token=2...
1 1 nouvelle notifica... | Inscrivez-vous | Kod... | Microsoft Certified:... | NGINX Virtual Mach... | Les 32 meilleures q... | Installer Samba 4 -... | Discord | #papotag...

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
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
Cliquez sur Chronologie pour voir le changement d'état à l'heure sélectionnée.
Métriques
Traces de X-Ray
Détails
Balises
Actions
Historique
Alarmes parents



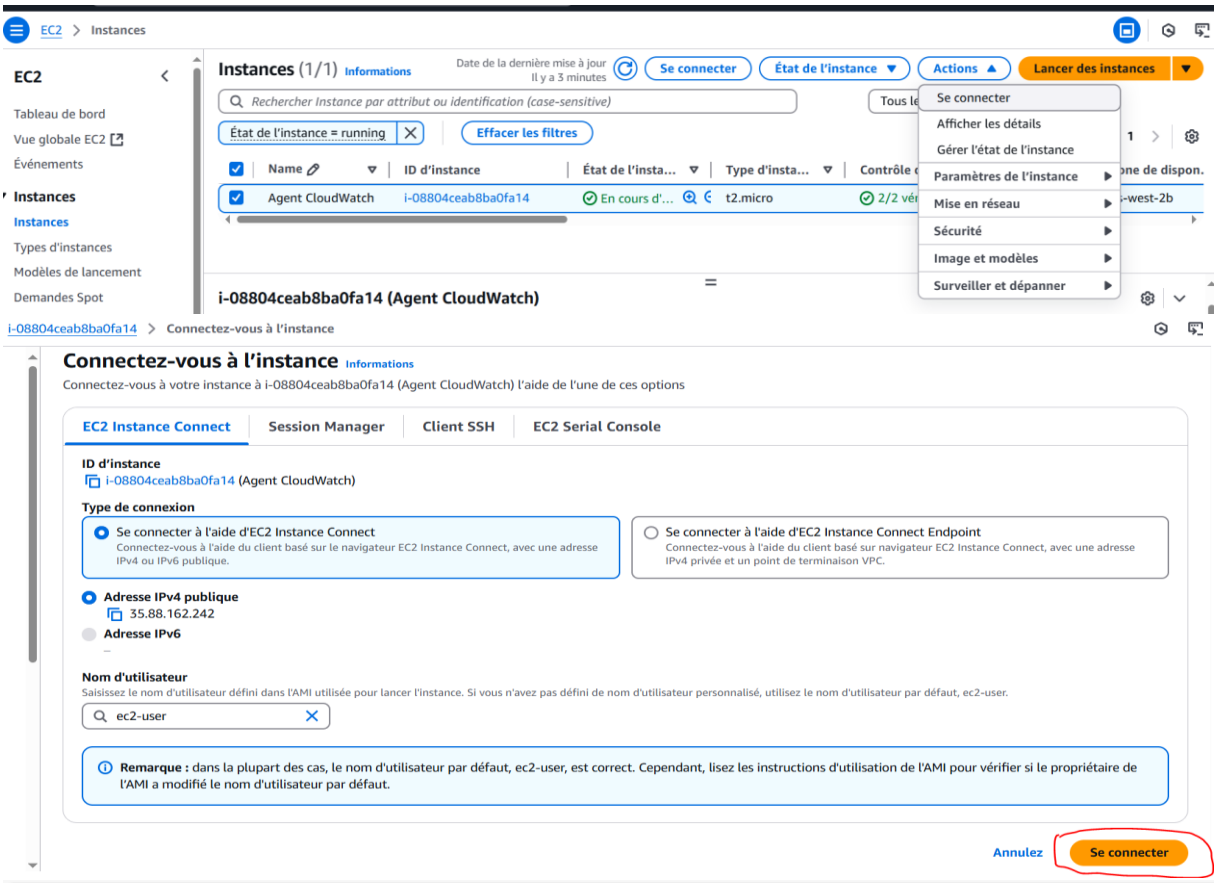


Étape 5 Test et validation

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
```

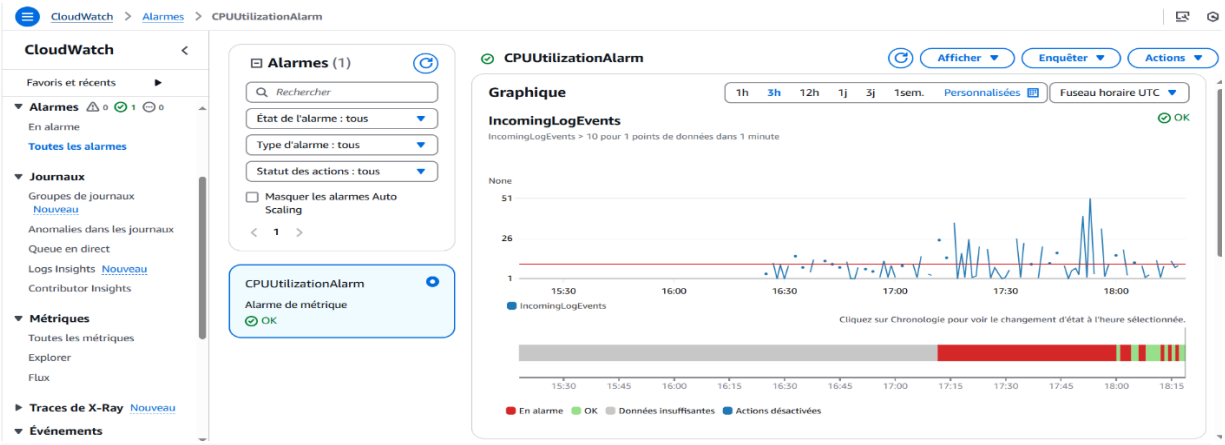
3. Vérifie le déclenchement de l'alarme et la réception de l'e-mail :
   - Ton alarme devrait passer brièvement à l'état ALARM, puis retourner à OK
   - Tu dois recevoir une **notification SNS** par mail
4. Vérifie le stockage des fichiers journaux dans ton bucket S3

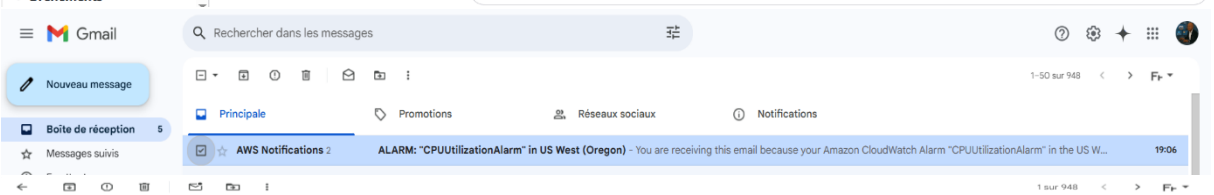

EC2 > Instances
EC2
Tableau de bord
Vue globale EC2
Événements
Instances
Instances
Types d'instances
Modèles de lancement
Demandes Spot
Instances (1/1) Informations
Date de la dernière mise à jour
Il y a 3 minutes
Se connecter
État de l'instance
Actions
Lancer des instances
Rechercher Instance par attribut ou identification (case-sensitive)
État de l'instance = running
Effacer les filtres
Name
ID d'instance
État de l'insta...
Type d'insta...
Agent CloudWatch
i-08804ceab8ba0fa14
En cours d'...
t2.micro
2/2 vér
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
i-08804ceab8ba0fa14 (Agent CloudWatch)
i-08804ceab8ba0fa14 > Connectez-vous à l'instance
Connectez-vous à l'instance Informations
Connectez-vous à votre instance à i-08804ceab8ba0fa14 (Agent CloudWatch) l'aide de l'une de ces options
EC2 Instance Connect
Session Manager
Client SSH
EC2 Serial Console
ID d'instance
i-08804ceab8ba0fa14 (Agent CloudWatch)
Type de connexion
Se connecter à l'aide d'EC2 Instance Connect
Connectez-vous à l'aide du client basé sur le navigateur EC2 Instance Connect, avec une adresse IPv4 ou IPv6 publique.
Se connecter à l'aide d'EC2 Instance Connect Endpoint
Connectez-vous à l'aide du client basé sur navigateur EC2 Instance Connect, avec une adresse IPv4 privée et un point de terminaison VPC.
Adresse IPv4 publique
35.88.162.242
Adresse IPv6
Nom d'utilisateur
Saisissez le nom d'utilisateur défini dans l'AMI utilisée pour lancer l'instance. Si vous n'avez pas défini de nom d'utilisateur personnalisé, utilisez le nom d'utilisateur par défaut, ec2-user.
ec2-user
Remarque : dans la plupart des cas, le nom d'utilisateur par défaut, ec2-user, est correct. Cependant, lisez les instructions d'utilisation de l'AMI pour vérifier si le propriétaire de l'AMI a modifié le nom d'utilisateur par défaut.
Annulez
Se connecter

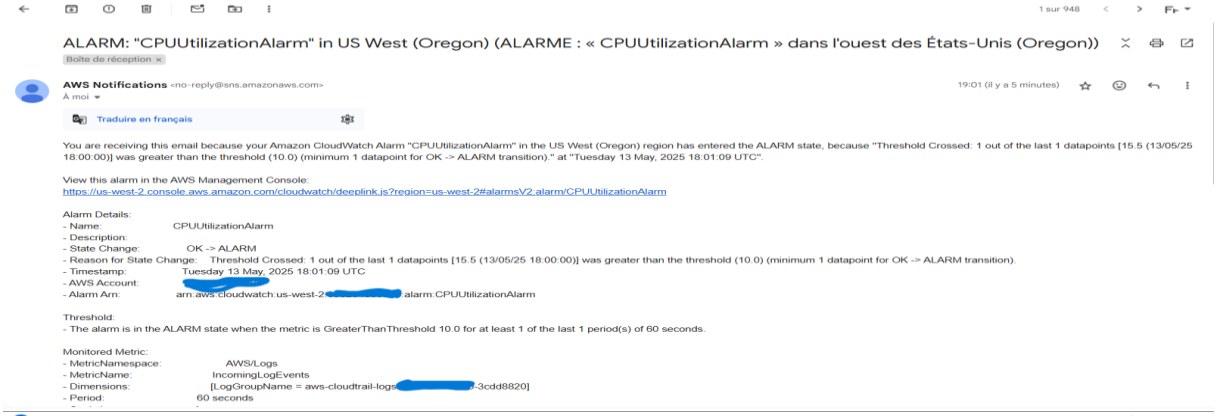
aws
Rechercher
[Alt+S]
États-Unis (Oregon)
AdministratorAccess
[ec2-user@ip-172-31-27-1 ~]$ sudo yum install -y stress
Last metadata expiration check: 2:26:35 ago on Tue May 13 15:02:10 2025.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
stress x86_64 1.0.7-2.amzn2023.0.1 amazonlinux 34 k
Transaction Summary
Install 1 Package
Total download size: 34 k
Installed size: 68 k
Downloading Packages:
stress-1.0.7-2.amzn2023.0.1.x86_64.rpm
Total
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing :
Installing : stress-1.0.7-2.amzn2023.0.1.x86_64
Running scriptlet: stress-1.0.7-2.amzn2023.0.1.x86_64
i-08804ceab8ba0fa14 (Agent CloudWatch)
PublicIPs: 35.88.162.242 PrivateIPs: 172.31.27.1

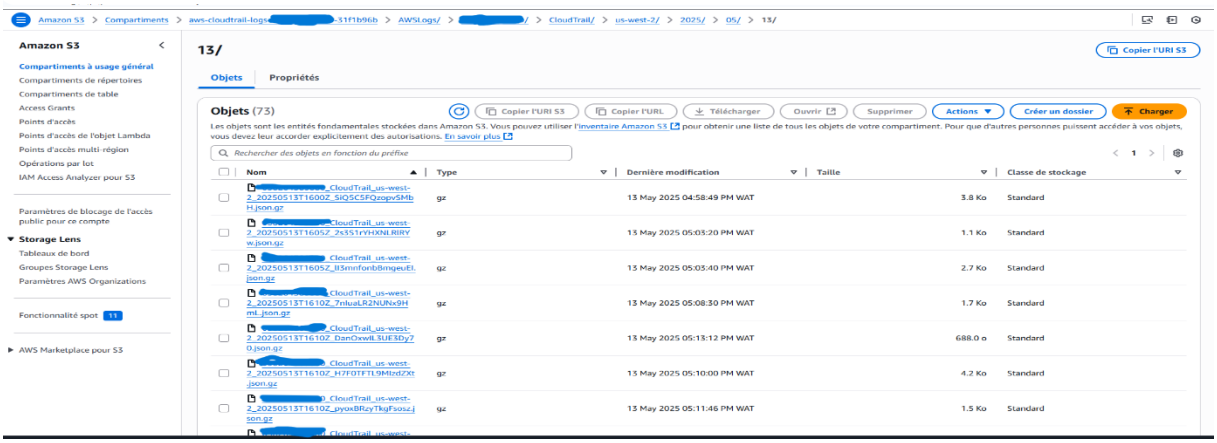
Running scriptlet: stress-1.0.7-2.amzn2023.0.1.x86_64
Verifying : stress-1.0.7-2.amzn2023.0.1.x86_64
Installed:
stress-1.0.7-2.amzn2023.0.1.x86_64
Complete!
[ec2-user@ip-172-31-27-1 ~]$ stress --cpu 1 --timeout 300
stress: info: [30758] dispatching hogs: 1 cpu, 0 io, 0 vm, 0 hdd
stress: info: [30758] successful run completed in 300s
[ec2-user@ip-172-31-27-1 ~]$
[ec2-user@ip-172-31-27-1 ~]$
i-08804ceab8ba0fa14 (Agent CloudWatch)
PublicIPs: 35.88.162.242 PrivateIPs: 172.31.27.1

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
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
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))
Boîte de réception
AWS Notifications <no-reply@sns.amazonaws.com>
19:01 (il y a 5 minutes)
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
- Dimensions: [LogGroupName = aws-cloudtrail-logs -3cdd8820]
- Period: 60 seconds


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
Storage Lens
Tableaux de bord
Groupes Storage Lens
Paramètres AWS Organizations
AWS Marketplace pour S3
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