



AWS Concepts et procédures de détection et de réponse aux incidents

# AWS Guide de l'utilisateur sur la détection et la réponse aux incidents



Version July 3, 2024

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

# AWSGuide de l'utilisateur sur la détection et la réponse aux incidents: AWSConcepts et procédures de détection et de réponse aux incidents

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Les marques et la présentation commerciale d'Amazon ne peuvent être utilisées en relation avec un produit ou un service qui n'est pas d'Amazon, d'une manière susceptible de créer une confusion parmi les clients, ou d'une manière qui dénigre ou discrédite Amazon. Toutes les autres marques commerciales qui ne sont pas la propriété d'Amazon appartiennent à leurs propriétaires respectifs, qui peuvent ou non être affiliés ou connectés à Amazon, ou sponsorisés par Amazon.

# Table of Contents

Qu'est-ce qu'AWS Incident Detection and Response ? .....	1
Termes du produit .....	2
Disponibilité .....	2
RACI .....	3
Architecture .....	6
Commencez avec la détection et la réponse aux incidents .....	7
Intégrez une charge de travail .....	7
Intégration de la charge de travail .....	8
Ingestion d'alarmes .....	8
Abonnement au compte .....	8
Découverte de la charge .....	11
Configuration de l'alarme .....	11
Créez des CloudWatch alarmes adaptées à votre activité .....	14
Utiliser AWS CloudFormation modèles pour créer des CloudWatch alarmes .....	17
Exemples de cas d'utilisation pour les CloudWatch alarmes .....	20
Intégrez les alertes à la détection et à la réponse aux AWS incidents .....	23
Accès aux provisions .....	23
Intégrez avec CloudWatch .....	24
Intégrez les alarmes APMs grâce à l'intégration EventBridge .....	24
Exemple : intégration des notifications de Datadog et Splunk .....	26
Intégrez les alarmes APMs sans intégration directe avec Amazon EventBridge .....	36
Développez des runbooks .....	36
Testez les charges de travail intégrées .....	43
CloudWatch alarmes .....	44
APM Alarmes tierces .....	45
Principaux résultats .....	45
Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes .....	45
Questionnaire d'intégration de la charge de travail - Questions générales .....	45
Questionnaire d'intégration de la charge de travail - Questions d'architecture .....	46
Questionnaire d'intégration de la charge de travail - AWS Questions relatives aux événements de service .....	49
Questionnaire relatif à l'ingestion .....	49
Matrice d'alarme .....	51
Demander des modifications à une charge de travail .....	55

---

Décharger une charge de travail .....	57
Surveillance et observabilité .....	59
Mettre en œuvre l'observabilité .....	60
Gestion des incidents .....	61
Fournir un accès aux équipes chargées des applications .....	63
Gestion des incidents pour les événements de service .....	64
Demande de réponse à un incident .....	66
AWS Application de support dans Slack .....	70
Notifications d'incidents déclenchées par une alarme dans Slack .....	71
Demandes de réponse aux incidents dans Slack .....	71
Génération de rapports .....	72
Sécurité et résilience .....	73
Accès à vos comptes .....	74
Vos données d'alarme .....	74
Historique de la documentation .....	75
AWS Glossaire .....	80
.....	lxxi

# Qu'est-ce qu'AWS Incident Detection and Response ?

AWS Incident Detection and Response offre aux clients éligibles du support aux AWS entreprises éligibles un engagement proactif en cas d'incident afin de réduire les risques de défaillance et d'accélérer le rétablissement des charges de travail critiques après une interruption. La détection et la réponse aux incidents facilitent votre collaboration AWS pour développer des runbooks et des plans de réponse personnalisés en fonction de chaque charge de travail intégrée. Une équipe d'ingénieurs de gestion des incidents (IME) surveille vos charges de travail intégrées 24 heures sur 24, 7 jours sur 7 et vous met en contact avec un pont d'appels dans les 5 minutes suivant une alarme critique.

La détection et la réponse aux incidents offrent les fonctionnalités clés suivantes :

- **Observabilité améliorée** : des AWS experts fournissent des conseils pour vous aider à définir et à corréliser les métriques et les alarmes entre les couches d'application et d'infrastructure de votre charge de travail afin de détecter les perturbations à un stade précoce.
- **Temps de réponse de 5 minutes** : les IME surveillent vos charges de travail intégrées 24 heures sur 24, 7 jours sur 7 pour détecter les incidents critiques. Les IME répondent dans les 5 minutes suivant le déclenchement d'une alarme ou en réponse à un dossier de Support critique que vous soumettez à la section Détection et réponse aux incidents.
- **Résolution plus rapide** : les IME utilisent des runbooks prédéfinis et personnalisés développés pour vos charges de travail afin de répondre dans les 5 minutes, de créer un dossier de support en votre nom et de gérer les incidents liés à votre charge de travail. Les IME permettent de gérer les incidents de manière centralisée et vous permettent de rester en contact avec les bons AWS experts jusqu'à ce que l'incident soit résolu.
- **Gestion des incidents liés aux AWS événements** : Parce que nous comprenons le contexte de votre charge de travail critique (par exemple, les comptes, les services et les instances), nous pouvons détecter et vous informer de manière proactive d'un impact potentiel sur votre charge de travail lors d'un événement de AWS service. Sur demande, les IME vous contactent lors des événements AWS de service et fournissent des mises à jour sur les événements. Bien que la détection et la réponse aux incidents ne puissent pas vous donner la priorité en matière de restauration lors d'un événement de service, Incident Detection and Response fournit des conseils de support pour vous aider à mettre en œuvre votre plan d'atténuation.
- **Risque de défaillance réduit** : après résolution, les IME vous fournissent un examen post-incident (sur demande). De plus, des AWS experts travaillent avec vous pour appliquer les leçons apprises

afin d'améliorer le plan de réponse aux incidents et les livrets d'exécution. Vous pouvez également tirer parti AWS Resilience Hub du suivi continu de la résilience de vos charges de travail.

## Termes relatifs aux produits de détection et de réponse aux incidents

- AWS Incident Detection and Response est disponible pour les comptes de support aux entreprises directs et revendus par des partenaires.
- AWS Incident Detection and Response n'est pas disponible pour les comptes bénéficiant du service Partner Led Support.
- Vous devez maintenir le Support AWS d'entreprise à tout moment pendant la durée de votre service de détection et de réponse aux incidents. Pour plus d'informations, consultez la section [Support aux entreprises](#). La résiliation du support aux entreprises entraîne la suppression simultanée du service AWS Incident Detection and Response.
- Toutes les charges de travail sur AWS Incident Detection and Response doivent de passer par le processus d'intégration des charges de travail.
- La durée minimale pour souscrire un compte à AWS Incident Detection and Response est de quatre-vingt-dix (90) jours. Toute demande d'annulation doit être soumise trente (30) jours avant la date d'entrée en vigueur prévue de l'annulation.
- AWS traite vos informations comme décrit dans l'[avis AWS de confidentialité](#).

### Note

Pour les questions relatives à la détection et à la réponse aux incidents relatives à la facturation, voir [Obtenir de l'aide en matière AWS de facturation](#).

## Disponibilité de la détection des incidents et de la réponse

AWS Incident Detection and Response est actuellement disponible en anglais pour les comptes de support aux entreprises hébergés dans l'un des établissements suivants Régions AWS :

Nom	Région AWS
us-east-1	USA Est (Virginie)
us-east-2	USA Est (Ohio)
us-west-1	USA Ouest (Californie du Nord)
us-west-2	USA Ouest (Oregon)
ca-central-1	Canada (Centre)
sa-east-1	Amérique du Sud (São Paulo)
eu-central-1	Europe (Francfort)
eu-west-1	Europe (Irlande)
eu-west-2	Europe (Londres)
eu-west-3	Europe (Paris)
eu-north-1	Europe (Stockholm)
ap-south-1	Asie-Pacifique (Mumbai)
ap-northeast-1	Asie-Pacifique (Tokyo)
ap-northeast-2	Asie-Pacifique (Séoul)
ap-southeast-1	Asie-Pacifique (Singapour)
ap-southeast-2	Asie-Pacifique (Sydney)

## Détection et réponse aux incidents AWS RACI

Le tableau suivant indique les responsables, responsables, consultés et informés d'AWS en matière de détection et de réponse aux incidents (RACI).

Activité	Client	Détection et réponse aux incidents
Collecte de données		
Présentation du client et de la charge de travail	C	R
Architecture	R	A
Opérations	R	A
Déterminer les CloudWatch alarmes à configurer	R	A
Définir le plan de réponse aux incidents	R	A
Remplir le questionnaire d'intégration	R	A
Examen du niveau de préparation des opérations		
Réaliser un examen bien architectural (WAR) de la charge de travail	C	R
Valider la réponse aux incidents	C	R
Valider la matrice d'alarme	C	R
Identifier les principaux AWS services utilisés par la charge de travail	A	R
Configuration du compte		
Créer un rôle IAM dans le compte client	R	I
Installer une EventBridge règle gérée à l'aide du rôle créé	I	R
CloudWatch Alarmes de test	R	A
Vérifiez que les alarmes des clients déclenchent la détection et la réponse aux incidents	I	R

Activité	Client	Détection et réponse aux incidents
Actualiser les alarmes	R	C
Mettre à jour les runbooks	C	R
Gestion des incidents		
Notifier de manière proactive les incidents détectés par Incident Detection and Response	I	R
Fournir une réponse aux incidents	I	R
Assurer la résolution des incidents/la restauration de l'infrastructure	R	C
Révision après l'incident		
Demander un examen après un incident	R	I
Fournir un examen après l'incident	I	R

# Architecture de détection et de réponse aux incidents AWS

AWS Incident Detection and Response s'intègre à votre environnement existant, comme le montre le graphique suivant. L'architecture inclut les services suivants :

- Amazon EventBridge : Amazon EventBridge est le seul point d'intégration entre vos charges de travail et AWS Incident Detection and Response. Les alarmes sont ingérées depuis vos outils de surveillance, tels qu'Amazon CloudWatch, via Amazon EventBridge en utilisant des règles prédéfinies gérées par AWS. Pour permettre à Incident Detection and Response de créer et de gérer la EventBridge règle, vous installez un rôle lié à un service. Pour en savoir plus sur ces services, consultez [Qu'est-ce qu'Amazon EventBridge](#) et [EventBridge les règles d'Amazon, Qu'est-ce qu'Amazon CloudWatch](#) et [Utilisation des rôles liés à un service](#) ? AWS Health
- AWS Health: AWS Health fournit une visibilité continue sur les performances de vos ressources et sur la disponibilité de vos comptes Services AWS et de vos comptes. La détection et la réponse aux incidents Services AWS sont utilisées AWS Health pour suivre les événements liés à l'utilisation de vos charges de travail et pour vous avertir lorsqu'une alerte a été reçue concernant votre charge de travail. Pour en savoir plus AWS Health, consultez la section [Qu'est-ce que AWS Health](#).
- AWS Systems Manager: Systems Manager fournit une interface utilisateur unifiée pour l'automatisation et la gestion des tâches sur l'ensemble de vos AWS ressources. AWS Incident Detection and Response héberge les informations relatives à vos charges de travail, notamment les diagrammes d'architecture des charges de travail, les détails des alarmes et les manuels de gestion des incidents correspondants dans AWS Systems Manager des documents (pour plus de détails, voir [AWS Systems Manager Documents](#)). Pour en savoir plus AWS Systems Manager, consultez la section [Qu'est-ce que AWS Systems Manager](#).
- Vos runbooks spécifiques : un runbook de gestion des incidents définit les actions effectuées par AWS Incident Detection and Response lors de la gestion des incidents. Vos runbooks spécifiques indiquent à AWS Incident Detection and Response qui contacter, comment les contacter et quelles informations partager.

# Commencez avec la détection et la réponse aux AWS incidents

Vous pouvez sélectionner des charges de travail spécifiques pour la surveillance et la gestion des incidents critiques à l'aide de la détection et de la réponse aux AWS incidents. Une charge de travail est un ensemble de ressources et de code qui fonctionnent ensemble pour apporter une valeur commerciale. Une charge de travail peut être l'ensemble des ressources et du code qui constituent votre portail de paiement bancaire ou un système de gestion de la relation client (CRM). Vous pouvez héberger une charge de travail en un seul AWS compte ou multiple AWS comptes.

Par exemple, vous pouvez avoir une application monolithique hébergée sur un seul compte (par exemple, l'application Employee Performance dans la figure 1). Il se peut également qu'une application (par exemple, Storefront Webapp sur la figure 1) soit divisée en microservices répartis sur différents comptes. Une charge de travail peut partager des ressources, telles qu'une base de données, avec d'autres applications ou charges de travail, comme le montre la figure 1.

## Note

Pour apporter des modifications à vos runbooks, aux informations de charge de travail ou aux alarmes surveillées sur AWS Incident Detection and Response, créez un [Demander des modifications à une charge de travail intégrée](#).

## Intégration

AWS travaille avec vous pour intégrer votre charge de travail et vos alarmes à la détection et à la réponse aux AWS incidents. Vous fournissez des informations clés à AWS dans le [Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes](#). Il est recommandé d'enregistrer également vos charges de travail. AppRegistry Pour plus d'informations, consultez le [guide de AppRegistry l'utilisateur](#).

Le schéma suivant montre le flux d'intégration de la charge de travail et d'ingestion des alarmes dans Incident Detection and Response :

## Intégration de la charge de travail

Lors de l'intégration de la charge de travail, AWS travaille avec vous pour comprendre votre charge de travail et savoir comment vous aider en cas d'incident et AWS Événements de service. Vous fournissez des informations clés sur votre charge de travail qui contribuent à atténuer les impacts.

Principaux résultats :

- Informations générales sur la charge de travail
- Détails de l'architecture, y compris les schémas
- Informations sur le Runbook
- Incidents déclenchés par le client
- AWS Événements liés au service

## Ingestion d'alarmes

AWS travaille avec vous pour intégrer vos alarmes. AWS Incident Detection and Response peut intégrer les alarmes provenant d'Amazon CloudWatch et d'outils tiers de surveillance des performances des applications (APM) via Amazon EventBridge. L'intégration des alarmes permet une détection proactive des incidents et un engagement automatique. Pour plus d'informations, consultez [Ingérer des APMs alarmes directement intégrées à Amazon EventBridge](#).

Principaux résultats :

- Matrice d'alarme

Le tableau suivant répertorie les étapes requises pour intégrer une charge de travail à la détection et à la réponse aux AWS incidents. Ce tableau présente des exemples de durée de chaque tâche. Les dates réelles de chaque tâche sont définies en fonction de la disponibilité de votre équipe et du calendrier.

## Abonnement au compte

Pour abonner une charge de travail à AWS Incident Detection and Response, créez un nouveau dossier de support pour chaque charge de travail. Lorsque vous créez le dossier de support, tenez compte des points suivants :

- Pour intégrer une charge de travail intégrée dans un seul AWS compte, créez le dossier d'assistance soit depuis le compte de la charge de travail, soit depuis votre compte payeur.
- Pour intégrer une charge de travail qui couvre plusieurs AWS comptes, créez le dossier d'assistance depuis votre compte payeur. Dans le corps du dossier d'assistance, listez tous les comptes IDs à intégrer.

### Important

Si vous créez un dossier d'assistance pour abonner une charge de travail à Incident Detection and Response à partir du mauvais compte, vous risquez de rencontrer des retards et des demandes d'informations supplémentaires avant de pouvoir souscrire à vos charges de travail.

## Pour abonner une charge de travail

1. Accédez au [AWS Support Centrez](#), puis sélectionnez Créer un dossier comme indiqué dans l'exemple suivant. Vous ne pouvez souscrire des charges de travail qu'à partir de comptes inscrits au Support aux entreprises.
2. Complétez le formulaire de demande d'assistance :
  - Sélectionnez Support technique.
  - Pour Service, choisissez Incident Detection and Response.
  - Dans Catégorie, choisissez Onboard New Workload.
  - Dans le champ Sévérité, sélectionnez Directives générales.
3. Entrez un objet pour cette modification. Par exemple :  
[À bord] Détection et réponse aux AWS incidents - *workload\_name*
4. Entrez une description pour cette modification. Par exemple, saisissez « Cette demande vise à intégrer une charge de travail à la détection et à la réponse aux AWS incidents ». Assurez-vous d'inclure les informations suivantes dans votre demande :
  - Nom de la charge de travail : nom de votre charge de travail.
  - Identifiant (s) de compte :ID1,ID2,ID3, et ainsi de suite. Il s'agit des comptes que vous souhaitez intégrer à AWS Incident Detection and Response.

- Date de début de l'abonnement : date à laquelle vous souhaitez démarrer l'abonnement à la détection et à la réponse aux AWS incidents.
5. Dans la section Contacts supplémentaires - facultatif, entrez l'e-mail dans l'ID auquel vous souhaitez recevoir de la correspondance concernant cette demande.

Voici un exemple de la section Contacts supplémentaires - facultative :

 Important

Le fait de ne pas ajouter d'e-mail IDs dans la section Contacts supplémentaires - facultatif peut retarder le processus d'intégration de la détection et de la réponse aux AWS incidents.

6. Sélectionnez Envoyer.

Après avoir soumis la demande, vous pouvez ajouter des e-mails supplémentaires provenant de votre organisation. Pour ajouter des e-mails, répondez au dossier, puis ajoutez l'e-mail ID dans la section Contacts supplémentaires - facultatif.

Voici un exemple de la section Contacts supplémentaires - facultative :

Après avoir créé un dossier d'assistance pour la demande d'abonnement, préparez les deux documents suivants pour poursuivre le processus d'intégration de la charge de travail :

- AWS schéma d'architecture de charge de travail.
- [Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes](#): Complétez toutes les informations du questionnaire relatives à la charge de travail que vous êtes en train d'intégrer. Si vous devez intégrer plusieurs charges de travail, créez un nouveau questionnaire d'intégration pour chaque charge de travail. Si vous avez des questions concernant le remplissage du questionnaire d'intégration, contactez votre responsable de compte technique (TAM).

**Note**

NOTJOIGNEZ ces deux documents au dossier à l'aide de l'option Joindre des fichiers. AWSL'équipe de détection et de réponse aux incidents répondra au cas par un lien Amazon Simple Storage Service Uploader vous permettant de télécharger les documents.

Pour plus d'informations sur la façon de créer un dossier avec AWS Incident Detection and Response pour demander des modifications à une charge de travail intégrée existante, voir. [Demander des modifications à une charge de travail intégrée](#) Pour plus d'informations sur la manière de déléguer une charge de travail, consultez [Décharger une charge de travail](#).

## Découverte de la charge

AWS travaille avec vous pour comprendre le plus possible le contexte de votre charge de travail. AWS Incident Detection and Response utilise ces informations pour créer des runbooks destinés à vous aider lors d'incidents et AWS Événements de service. Les informations requises sont saisies dans le [Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes](#). Il est recommandé d'enregistrer vos charges de travail sur AppRegistry. Pour plus d'informations, consultez le [guide de AppRegistry l'utilisateur](#).

Principaux résultats :

- Informations sur la charge de travail, telles que la description de la charge de travail, les diagrammes d'architecture, les coordonnées et les détails de l'escalade.
- Détails de la façon dont la charge de travail emploie AWS services dans chacun AWS Région.
- Informations spécifiques sur la manière dont AWS vous soutient lors d'un événement de service.
- Alarmes utilisées par votre équipe pour détecter un impact critique sur la charge de travail.

## Configuration de l'alarme

AWS travaille avec vous pour définir des métriques et des alarmes afin de fournir une visibilité sur les performances de vos applications et sur leurs sous-jacents AWS infrastructure. Nous demandons que les alarmes respectent les critères suivants lors de la définition et de la configuration des seuils :

- Les alarmes ne passent à l'état « Alarme » que lorsqu'elles ont un impact critique sur la charge de travail surveillée (perte de revenus ou dégradation de l'expérience client réduisant considérablement les performances) nécessitant une attention immédiate de la part de l'opérateur.
- Les alarmes doivent également impliquer les résolveurs que vous avez spécifiés pour la charge de travail en même temps ou avant que l'équipe de gestion des incidents ne soit engagée. Les ingénieurs de gestion des incidents doivent collaborer avec les résolveurs que vous avez spécifiés dans le cadre du processus d'atténuation, et non agir en tant qu'intervenants de première ligne pour ensuite vous contacter.
- Les seuils d'alarme doivent être fixés à un seuil et à une durée appropriés afin qu'une enquête soit menée chaque fois qu'une alarme se déclenche. Si une alarme passe de l'état « Alarme » à l'état « OK », l'impact est suffisant pour justifier la réponse et l'attention de l'opérateur.

#### Types d'alarmes :

- Des alarmes qui indiquent le niveau d'impact sur l'entreprise et transmettent des informations pertinentes pour une détection simple des défauts.
- CloudWatch Canaris d'Amazon. Pour plus d'informations, consultez [Canaries and X-Ray tracing](#) et [X-Ray](#).
- Alarme agrégée (surveillance des dépendances)

Exemple d'alarme, le tout utilisant le système CloudWatch de surveillance

Nom de la métrique/ Seuil d'alarme	ID d'alarme ARN ou de ressource	Si cette alarme se déclenche	Si vous êtes engagé, soumettez un dossier de Support Premium pour ces services
APIerreurs/  Nombre d'erreurs >= 10 pour 10 points de données	arn:aws:cloudwatch:us-west-2:000000000000:Alarm:E2 - Erreurs MPmimLambda	Ticket coupé à l'équipe de l'administrateur de la base de données (DBA)	Lambda, passerelle API
ServiceUnavailable (Code d'état HTTP 503)  Nombre d'erreurs >=3 pour 10 points de données (clients différents) dans une fenêtre de 5 minutes	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode503	Ticket réduit pour l'équipe de service	Lambda, passerelle API
ThrottlingException (Code d'état HTTP 400)	arn:aws:cloudwatch:us-west-2:xxxxx:alarm:httperrorcode400	Ticket réduit pour l'équipe	EC2, Amazon Aurora

Nom de la métrique/ Seuil d'alarme	ID d'alarme ARN ou de ressource	Si cette alarme se déclenche	Si vous êtes engagé, soumettez un dossier de Support Premium pour ces services
Nombre d'erreurs $\geq 3$ pour 10 points de données (clients différents) dans une fenêtre de 5 minutes		de service	

Pour en savoir plus, consultez [Surveillance et observabilité de la détection et de la réponse aux incidents AWS](#).

Principaux résultats :

- Définition et configuration des alarmes sur vos charges de travail.
- Compléter les détails de l'alarme sur le questionnaire d'intégration.

## Créez des CloudWatch alarmes adaptées aux besoins de votre entreprise en matière de détection et de réponse aux incidents

Lorsque vous créez des CloudWatch alarmes Amazon, vous pouvez suivre plusieurs étapes pour vous assurer que vos alarmes répondent le mieux aux besoins de votre entreprise.

### Passez en revue vos CloudWatch alarmes proposées

Passez en revue les alarmes que vous proposez pour vous assurer qu'elles ne passent à l'état « Alarme » que lorsqu'elles ont un impact critique sur la charge de travail surveillée (perte de revenus

ou dégradation de l'expérience client entraînant une réduction significative des performances). Par exemple, considérez-vous que cette alarme est suffisamment critique pour que vous deviez réagir immédiatement si elle passe à l'état « Alarme » ?

Voici des indicateurs suggérés susceptibles d'avoir un impact commercial critique, par exemple en influant sur l'expérience de vos utilisateurs finaux avec une application :

- CloudFront: pour plus d'informations, consultez la section [Affichage CloudFront et indicateurs des fonctions Edge](#).
- Équilibreurs de charge d'application : il est recommandé de créer les alarmes suivantes pour les équilibreurs de charge d'application, si possible :
  - HTTPCode\_ELB\_5xx\_Count
  - HTTPCode\_TARGET\_5XX\_Count

Les alarmes précédentes vous permettent de surveiller les réponses des cibles situées derrière l'Application Load Balancer ou derrière d'autres ressources. Cela permet d'identifier plus facilement la source des erreurs 5XX. Pour plus d'informations, consultez [CloudWatch les métriques de votre Application Load Balancer](#).

- Amazon API Gateway : si vous l'utilisez WebSocket API dans Elastic Beanstalk, pensez à utiliser les métriques suivantes :
  - Taux d'erreurs d'intégration (filtré à 5XX erreurs)
  - Latence d'intégration
  - Erreurs d'exécution

Pour plus d'informations, consultez la section [Surveillance de WebSocket API l'exécution à l'aide de CloudWatch métriques](#).

- Amazon Route 53 : surveillez la EndPointUnhealthyENICountmétrique. Cette métrique correspond au nombre d'interfaces réseau élastiques en état de restauration automatique. Cet état indique les tentatives du résolveur pour récupérer une ou plusieurs interfaces réseau Amazon Virtual Private Cloud associées au point de terminaison (spécifié par EndpointId). Au cours du processus de restauration, le terminal fonctionne avec une capacité limitée. Le point de terminaison ne peut pas traiter DNS les requêtes tant qu'il n'est pas complètement rétabli. Pour plus d'informations, consultez la section [Surveillance des points de terminaison du résolveur Route 53 avec Amazon CloudWatch](#)

## Validez vos configurations d'alarme

Après avoir confirmé que les alarmes que vous proposez répondent aux besoins de votre entreprise, validez la configuration et l'historique des alarmes :

- Validez le seuil pour que la métrique passe à l'état « Alarme » par rapport à la tendance graphique de la métrique.
- Validez la période utilisée pour interroger les points de données. L'interrogation des points de données à 60 secondes permet de détecter rapidement les incidents.
- Validez la DatapointToAlarmconfiguration. Dans la plupart des cas, il est recommandé de définir ce paramètre sur 3 ou 5 sur 5. En cas d'incident, l'alarme se déclenche au bout de 3 minutes lorsqu'elle est définie comme [métrique de 60 secondes avec 3 sur 3 DatapointToAlarm] ou 5 minutes si elle est définie comme [métrique de 60 secondes avec 5 sur 5 DatapointToAlarm]. Utilisez cette combinaison pour éliminer les alarmes bruyantes.

### Note

Les recommandations précédentes peuvent varier en fonction de la manière dont vous utilisez un service. Chaque AWS service fonctionne différemment au sein d'une charge de travail. De plus, le même service peut fonctionner différemment lorsqu'il est utilisé à plusieurs endroits. Vous devez être sûr de comprendre comment votre charge de travail utilise les ressources qui alimentent l'alarme, ainsi que les effets en amont et en aval.

## Validez la façon dont vos alarmes gèrent les données manquantes

Certaines sources de mesures n'envoient pas de données CloudWatch à intervalles réguliers. Pour ces indicateurs, il est recommandé de traiter les données manquantes comme notBreaching. Pour plus d'informations, voir [Configuration de la manière dont les CloudWatch alarmes traitent les données manquantes](#) et [Éviter les transitions prématurées vers l'état d'alarme](#).

Par exemple, si une métrique surveille un taux d'erreur et qu'il n'y a aucune erreur, elle ne rapporte aucun point de données (zéro). Si vous configurez l'alarme pour traiter les données manquantes comme manquantes, un seul point de données en violation suivi de deux points de données nuls fait passer la métrique à l'état « Alarme » (pour 3 points de données sur 3). Cela est dû au fait que la configuration de données manquante évalue le dernier point de données connu au cours de la période d'évaluation.

Dans les cas où les métriques surveillent un taux d'erreur, en l'absence de dégradation du service, vous pouvez partir du principe que l'absence de données est une bonne chose. Il est recommandé de traiter les données manquantes de manière à ce que les données manquantes soient considérées comme « OK » et que la métrique ne passe pas à l'état « Alarme » sur un seul point de données.

## Consultez l'historique de chaque alarme

Si l'historique d'une alarme indique qu'elle passe fréquemment à l'état « Alarme » puis se rétablit rapidement, l'alarme peut devenir un problème pour vous. Assurez-vous de régler l'alarme pour éviter le bruit ou les fausses alarmes.

## Valider les métriques pour les ressources sous-jacentes

Assurez-vous que vos indicateurs portent sur des ressources sous-jacentes valides et utilisent les bonnes statistiques. Si une alarme est configurée pour vérifier les noms de ressources non valides, elle risque de ne pas être en mesure de suivre les données sous-jacentes. Cela peut faire passer l'alarme à l'état « Alarme ».

## Création d'alarmes composites

Si vous fournissez aux opérations de détection et de réponse aux incidents un grand nombre d'alarmes à intégrer, il se peut que l'on vous demande de créer des alarmes composites. Les alarmes composites réduisent le nombre total d'alarmes à intégrer.

## Utiliser AWS CloudFormation modèles pour créer des CloudWatch alarmes dans Incident Detection and Response

Pour accélérer l'intégration à la détection et à la réponse aux AWS incidents et pour réduire les efforts nécessaires à la création d'alarmes, AWS vous fournit AWS CloudFormation modèles. Ces modèles incluent des paramètres d'alarme optimisés pour les services couramment intégrés, tels que Application Load Balancer, Network Load Balancer et Amazon CloudFront.

Créez des CloudWatch alarmes à l'aide CloudFormation de modèles

1. Téléchargez un modèle à l'aide des liens fournis :

NameSpace	Métriques	ComparisonOperator (Seuil)	Période	DatapointsToAlarm	TreatingData	Statistique	Lien vers le modèle
Application : Elastic Load Balancer	$(m1+m2)/(m1+m2+m3+m4) * 100$ m1= <code>_TARGET_XX_Count</code> m2= <code>_TARGET_XX_Count</code> m3= <code>_TARGET_XX_Count</code> m4= <code>_TARGET_XX_Count</code> <code>HTTPCodeHTTPCodeHTTPCodeHTTPCode</code>	LessThanThreshold(95)	60	3 sur 3	manquant	Somme	<a href="#">Modèle</a>
Amazon CloudFront	TotalErrorRate	GreaterThanThreshold(5)	60	3 sur 3	notBreaching	Moyenne	<a href="#">Modèle</a>
Application : Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 sur 3	notBreaching	Maximum	<a href="#">Modèle</a>

NameSpace	Métriques	ComparisonOperator (Seuil)	Période	DatapointsToAlarm	TreatingData	Statistique	Lien vers le modèle
Network Elastic Load Balancer	UnHealthyHostCount	GreaterThanOrEqualToThreshold(2)	60	3 sur 3	notBreaching	Maximum	<a href="#">Modèle</a>

2. Vérifiez le JSON fichier téléchargé pour vous assurer qu'il est conforme aux processus de fonctionnement et de sécurité de votre organisation.
3. Créez une CloudFormation pile :

 Note

Les étapes suivantes utilisent le processus de création de CloudFormation pile standard. Pour connaître les étapes détaillées, consultez [la section Création d'une pile sur la AWS CloudFormation console](#).

- a. Ouvrez le fichier AWS CloudFormation console sur <https://console.aws.amazon.com/cloudformation>.
- b. Sélectionnez Créer la pile.
- c. Choisissez Le modèle est prêt, puis téléchargez le fichier modèle depuis votre dossier local.

Voici un exemple de l'écran Create stack.

- d. Choisissez Suivant.
- e. Entrez les informations obligatoires suivantes :
  - AlarmNameConfig et AlarmDescriptionConfig: Entrez le nom et la description de votre alarme.
  - ThresholdConfig: Révissez la valeur du seuil pour répondre aux exigences de votre application.

- DistributionIDConfig : Assurez-vous que l'ID de distribution pointe vers les bonnes ressources du compte que vous créez AWS CloudFormation empiler.
- f. Choisissez Suivant.
  - g. Vérifiez les valeurs par défaut dans les DatapointsToAlarmConfigchamps PeriodConfigEvaluationPeriodConfig, et. Il est recommandé d'utiliser les valeurs par défaut pour ces champs. Vous pouvez apporter des modifications, si nécessaire, pour répondre aux exigences de votre application.
  - h. Entrez éventuellement des balises et des informations de SNS notification selon les besoins. Il est recommandé d'activer la protection de terminaison pour empêcher la suppression accidentelle de l'alarme. Pour activer la protection contre le licenciement, sélectionnez le bouton radio Activé, comme indiqué dans l'exemple suivant :
  - i. Choisissez Suivant.
  - j. Vérifiez les paramètres de votre pile, puis choisissez Create stack.
  - k. Après avoir créé la pile, l'alarme apparaît dans la liste Amazon CloudWatch Alarm, comme illustré dans l'exemple suivant :
4. Après avoir créé toutes vos alarmes dans le bon compte et AWS Région, informez votre responsable de compte technique (TAM). L'équipe de détection et de réponse aux AWS incidents examine l'état de vos nouvelles alarmes, puis poursuit votre intégration.

## Exemple de cas d'utilisation d' CloudWatch alarmes dans le cadre de la détection et de la réponse aux incidents

Consultez les cas d'utilisation suivants pour découvrir comment vous pouvez utiliser les CloudWatch alarmes Amazon dans le cadre de la détection et de la réponse aux incidents.

### Exemple de cas d'utilisation A : Application Load Balancer

Créez l' CloudWatch alarme suivante qui signale un impact potentiel sur la charge de travail. Vous pouvez créer une métrique mathématique qui émet une alarme lorsque les connexions réussies tombent en dessous d'un certain seuil. Pour les CloudWatch métriques disponibles, consultez les [CloudWatch métriques de votre Application Load Balancer](#)

Métrique :

$\text{HTTPCode\_Target\_3XX\_Count}; \text{HTTPCode\_Target\_4XX\_Count}; \text{HTTPCode\_Target\_5XX\_Count} .$   
 $(m1+m2)/(m1+m2+m3+m4)*100$  m1 = HTTP Code 2xx || m2 = HTTP Code 3xx || m3 =  
HTTP Code 4xx || m4 = HTTP Code 5xx

NameSpace: AWS/Demande ELB

ComparisonOperator(Seuil) : inférieur à x (x = seuil du client).

Période : 60 secondes

DatapointsToAlarm: 3 sur 3

Traitement des données manquantes : considérez les données manquantes comme des [violations](#).

Statistique : somme

Le schéma suivant montre le flux pour le cas d'utilisation A :

## Exemple de cas d'utilisation B : Amazon API Gateway

Créez l' CloudWatch alarme suivante qui signale un impact potentiel sur la charge de travail. Vous pouvez créer une métrique composite qui émet une alarme en cas de latence élevée ou d'un nombre moyen élevé d'erreurs 4XX dans la passerelle. API Pour les statistiques disponibles, consultez les [dimensions et statistiques d'Amazon API Gateway](#)

Métrique : `compositeAlarmAPI Gateway (ALARM(error4XXMetricApiGatewayAlarm)) OR (AALARM(latencyMetricApiGatewayAlarm))`

NameSpace: AWS/APIPasserelle

ComparisonOperator(Seuil) : supérieur aux seuils (x ou y du client)

Période : 60 secondes

DatapointsToAlarm: 1 sur 1

Traitement des données manquantes : considérez les données manquantes comme s'il ne s'[agissait pas d'une violation](#).

Statistique :

Le schéma suivant montre le flux pour le cas d'utilisation B :

## Exemple de cas d'utilisation C : Amazon Route 53

Vous pouvez surveiller vos ressources en créant des bilans de santé Route 53 qui permettent de collecter et CloudWatch de traiter les données brutes pour en faire des indicateurs lisibles en temps quasi réel. Vous pouvez créer l' CloudWatch alarme suivante pour signaler un impact potentiel sur la charge de travail. Vous pouvez utiliser les CloudWatch métriques pour créer une alarme qui se déclenche lorsqu'elle dépasse le seuil établi. Pour les CloudWatch métriques disponibles, consultez les [CloudWatch métriques relatives aux bilans de santé de Route 53](#)

Métrique : R53-HC-Success

NameSpace: AWS/Route 53

Seuil HealthCheckStatus : HealthCheckStatus < x pour 3 points de données en 3 minutes (étant le seuil de x pour le client)

Durée : 1 minute

DatapointsToAlarm: 3 sur 3

Traitement des données manquantes : considérez les données manquantes comme des [violations](#).

Statistique : minimum

Le schéma suivant montre le flux pour le cas d'utilisation C :

## Exemple de cas d'utilisation D : surveillance d'une charge de travail avec une application personnalisée

Il est essentiel que vous preniez le temps de définir un bilan de santé approprié dans ce scénario. Si vous vérifiez uniquement que le port d'une application est ouvert, cela signifie que vous n'avez pas vérifié que l'application fonctionne. De plus, appeler la page d'accueil d'une application n'est pas nécessairement la bonne méthode pour déterminer si l'application fonctionne. Par exemple, si une application dépend d'une base de données AND Amazon Simple Storage Service, le bilan de santé doit valider tous les éléments. Pour ce faire, vous pouvez créer une page Web de surveillance, telle que /monitor. La page Web de surveillance appelle la base de données pour s'assurer qu'elle peut se connecter et obtenir des données. De plus, la page Web de surveillance appelle Amazon S3. Ensuite, vous pointez le contrôle de santé de l'équilibreur de charge vers la page /monitor.

Le schéma suivant montre le flux pour le cas d'utilisation D :

## Intégrez les alertes à la détection et à la réponse aux AWS incidents

AWS Incident Detection and Response prend en charge l'ingestion d'alarmes via [Amazon EventBridge](#). Cette section explique comment intégrer la détection et la réponse aux AWS incidents à différents outils de surveillance des performances des applications (APM), notamment Amazon CloudWatch, APMs avec une intégration directe avec Amazon EventBridge (par exemple, DataDog et New Relic), et APMs sans intégration directe avec Amazon EventBridge. Pour une liste complète des intégrations directes APMs à Amazon EventBridge, consultez la section [EventBridgeIntégrations Amazon](#).

### Rubriques

- [Fournir un accès pour l'ingestion des alertes à la détection et à la réponse aux incidents](#)
- [Intégrez la détection et la réponse aux incidents à Amazon CloudWatch](#)
- [Intégrez les alarmes directement intégrées à Amazon APMs EventBridge](#)
- [Exemple : intégrer les notifications de Datadog et Splunk](#)
- [Utilisez des webhooks pour ingérer des alarmes APMs sans intégration directe avec Amazon EventBridge](#)

## Fournir un accès pour l'ingestion des alertes à la détection et à la réponse aux incidents

Pour permettre à AWS Incident Detection and Response d'intégrer les alarmes de votre compte, installez le rôle `AWSServiceRoleForHealth_EventProcessor` lié au service (). SLR AWS suppose que SLR pour créer une règle EventBridge gérée par Amazon. La règle gérée envoie des notifications depuis vos comptes à AWS Incident Detection and Response. Pour plus d'informations à ce sujet SLR, y compris les AWS politiques gérées, voir [Utilisation de rôles liés à un service](#) dans le AWS Health Guide de l'utilisateur.

Vous pouvez installer ce rôle lié à un service dans votre compte en suivant les instructions de la section [Créer un rôle lié à un service](#) dans AWS Identity and Access Management Guide de

l'utilisateur. Vous pouvez également utiliser la commande d'interface de ligne de commande AWS (AWSCLI) suivante :

```
aws iam create-service-linked-role --aws-service-name event-processor.health.amazonaws.com
```

### Principaux résultats

- Installation réussie du rôle lié au service dans votre compte.

### Informations connexes

Pour plus d'informations, consultez les rubriques suivantes :

- [Utilisation de rôles liés à un service pour Health AWS](#)
- [Création d'un rôle lié à un service](#)
- [AWSPolitique gérée : AWSHealth\\_EventProcessorServiceRolePolicy](#)

## Intégrez la détection et la réponse aux incidents à Amazon CloudWatch

AWSIncident Detection and Response utilise le rôle lié au service (SLR) que vous avez activé lors de l'attribution des accès pour créer une règle gérée par Amazon EventBridge dans votre AWS compte nommé `AWSHealthEventProcessor-DO-NOT-DELETE`. Incident Detection and Response utilise cette règle pour ingérer les CloudWatch alarmes Amazon depuis vos comptes. Aucune étape supplémentaire n'est requise pour ingérer les alarmes depuis CloudWatch.

## Ingérez les alarmes directement intégrées à Amazon APMs EventBridge

L'illustration suivante montre le processus d'envoi de notifications à AWS Incident Detection and Response à partir d'outils de surveillance des performances des applications (APM) directement intégrés à Amazon EventBridge, tels que Datadog et Splunk. Pour une liste complète de ceux APMs qui sont directement intégrés EventBridge, consultez [Amazon EventBridge Integrations](#)

Suivez les étapes ci-dessous pour configurer l'intégration avec AWS Incident Detection and Response. Avant d'effectuer ces étapes, vérifiez que AWS le rôle lié au service (SLR) `AWSServiceRoleForHealth_EventProcessor` est [installé](#) dans vos comptes.

## Configurer l'intégration avec la détection et la réponse aux AWS incidents

Vous devez suivre les étapes suivantes pour chaque AWS compte et AWS Région. Les alertes doivent provenir du AWS compte et AWS Région dans laquelle se trouvent les ressources de l'application.

1. Configurez chacune de vos sources d'événements APMs en tant que EventBridge partenaires Amazon (par exemple, `aws.partner/my_apm/integrationName`). Pour obtenir des instructions sur la configuration de votre compte APM en tant que source d'événements, consultez la section [Réception d'événements d'un partenaire SaaS avec Amazon EventBridge](#). Cela crée un bus d'événements partenaires sur votre compte.
2. Effectuez l'une des actions suivantes :
  - (Méthode recommandée) Créez un bus d' EventBridge événements personnalisé. AWS Incident Detection and Response installe un bus de règles gérées (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) via le `AWSServiceRoleForHealth_EventProcessorSLR`. La source de la règle est le bus d'événements personnalisé. La destination de la règle est la détection et la réponse aux AWS incidents. La règle correspond au schéma d'ingestion d'APM événements tiers.
  - (Méthode alternative) Utilisez le bus d'événements par défaut au lieu d'un bus d'événements personnalisé. Le bus d'événements par défaut nécessite la règle gérée pour envoyer des APM alertes à AWS Incident Detection and Response.
3. Créez un [AWS Lambda](#) fonction (par exemple, `My_APM-AWSIncidentDetectionResponse-LambdaFunction`) pour transformer les événements du bus d'événements de votre partenaire. Les événements transformés correspondent à la règle gérée `AWSHealthEventProcessorEventSource-DO-NOT-DELETE`.
  - a. Les événements transformés incluent un identifiant unique de détection et de réponse aux AWS incidents, et définissent la source et le type de détail de l'événement selon les valeurs requises. Le modèle correspond à la règle gérée.
  - b. Définissez la cible de la fonction Lambda sur le bus d'événements personnalisé créé à l'étape 2 (méthode recommandée) ou sur votre bus d'événements par défaut.
4. Créez une EventBridge règle et définissez les modèles d'événements correspondant à la liste des événements que vous souhaitez transmettre à la détection et à la réponse aux AWS incidents. La source de la règle est le bus d'événements partenaire que vous définissez à l'étape 1 (par exemple, `integrationName aws.partner/my_apm/`). La cible de la règle est la fonction Lambda que vous définissez à l'étape 3 (par exemple, `My_APM-`

`AWSIncidentDetectionResponse-LambdaFunction`). Pour obtenir des instructions sur la définition de votre EventBridge règle, consultez les [EventBridge règles d'Amazon](#).

Pour des exemples expliquant comment configurer l'intégration d'un bus d'événements partenaire à utiliser avec la détection et la réponse aux AWS incidents, voir [Exemple : intégrer les notifications de Datadog et Splunk](#).

## Exemple : intégrer les notifications de Datadog et Splunk

Cet exemple fournit des étapes détaillées pour intégrer les notifications de Datadog et Splunk à la détection et à la réponse aux AWS incidents.

1. Configurez votre AWS compte en APM tant que source EventBridge d'événements sur Amazon.
2. Créez un bus d'événements personnalisé.
3. Créez un AWS Lambda fonction de transformation.
4. Créez votre EventBridge règle personnalisée.

### Étape 1 : configurer votre compte APM en tant que source d'événements sur Amazon EventBridge

Configurez chacune d'entre elles APMs comme source d'événements sur Amazon EventBridge dans votre AWS compte. Pour obtenir des instructions sur la configuration de votre outil APM en tant que source d'événements, consultez les [instructions de configuration de la source d'événements pour votre outil chez les EventBridge partenaires Amazon](#).

En le configurant APM comme source d'événements, vous pouvez ingérer les notifications de votre part APM vers un bus d'événements de votre AWS compte. Après la configuration, AWS Incident Detection and Response peut démarrer le processus de gestion des incidents lorsque le bus d'événements reçoit un événement. Ce processus ajoute Amazon EventBridge comme destination dans votre APM.

### Étape 2 : Création d'un bus d'événements personnalisé

Il est recommandé d'utiliser un bus événementiel personnalisé. AWS La détection et la réponse aux incidents utilisent le bus d'événements personnalisé pour ingérer les événements transformés. Un AWS Lambda La fonction transforme l'événement du bus d'événements du partenaire et l'envoie au

bus d'événements personnalisé. AWSIncident Detection and Response installe une règle gérée pour ingérer les événements provenant du bus d'événements personnalisé.

Vous pouvez utiliser le bus d'événements par défaut au lieu d'un bus d'événements personnalisé. AWSIncident Detection and Response modifie la règle gérée afin qu'elle soit ingérée à partir du bus d'événements par défaut au lieu d'une règle personnalisée.

Créez un bus événementiel personnalisé dans votre AWS compte :

1. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>
2. Choisissez Bus, Event Bus.
3. Sous Bus d'événements personnalisé, choisissez Create.
4. Entrez un nom pour le bus de votre événement sous Nom. Le format recommandé est APMName- AWSIncidentDetectionResponse - EventBus.

Par exemple, utilisez l'une des options suivantes si vous utilisez Datadog ou Splunk :

- Datadog : Datadog - - AWSIncidentDetectionResponse EventBus
- Splunk : Splunk- - AWSIncidentDetectionResponse EventBus

### Étape 3 : Création d'un AWS Lambda fonction de transformation

La fonction Lambda transforme les événements entre le bus d'événements partenaire de l'étape 1 et le bus d'événements personnalisé (ou par défaut) de l'étape 2. La transformation de la fonction Lambda correspond à la règle gérée de détection et de réponse aux AWS incidents.

Créez un AWS Lambda fonctionne dans votre AWS compte

1. Ouvrez la [page Fonctions](#) sur le AWS Lambda console.
2. Sélectionnez Create function (Créer une fonction).
3. Choisissez l'onglet Auteur à partir de zéro.
4. Pour Nom de la fonction, entrez un nom en utilisant le formatAPMName - AWSIncidentDetectionResponse - LambdaFunction.

Voici des exemples pour Datadog et Splunk :

- Datadog : Datadog - - AWSIncidentDetectionResponse LambdaFunction
- Splunk : Splunk- - AWSIncidentDetectionResponse LambdaFunction

5. Pour Runtime, entrez Python 3.10.
6. Conservez les valeurs par défaut pour les autres champs. Sélectionnez Create function (Créer une fonction).
7. Sur la page d'édition du code, remplacez le contenu de la fonction Lambda par défaut par la fonction des exemples de code suivants.

Notez les commentaires commençant par # dans les exemples de code suivants. Ces commentaires indiquent les valeurs à modifier.

Modèle de code de transformation Datadog :

```
import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
# use your default event bus which is called 'default'.
# Example 'Datadog-AWSIncidentDetectionResponse-EventBus'
EventBusName = "Datadog-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifiant"] value to
    # the name of your alert that is coming from your APM. Each APM is different and
    # each unique alert will have a different name.
    # Replace the dictionary path, event["detail"]["meta"]["monitor"]["name"], with
    # the path to your alert name based on your APM payload.
    # This example is for finding the alert name for Datadog.
    event["detail"]["incident-detection-response-identifiant"] = event["detail"]
    ["meta"]["monitor"]["name"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
        Entries=[
            {
                'Detail': json.dumps(event["detail"], indent=2),
                'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
                DetailType value is required.
```

```

        'Source': 'GenericAPMEvent', # Do not modify. This Source value is
required.
        'EventBusName': EventBusName # Do not modify. This variable is set
at the top of this code as a global variable. Change the variable value for your
eventbus name at the top of this code.
    }
]
)
print(response['Entries'])

```

### Modèle de code de transformation Splunk :

```

import logging
import json
import boto3

logger = logging.getLogger()
logger.setLevel(logging.INFO)

# Change the EventBusName to the custom event bus name you created previously or
use your default event bus which is called 'default'.
# Example Splunk-AWSIncidentDetectionResponse-EventBus
EventBusName = "Splunk-AWSIncidentDetectionResponse-EventBus"

def lambda_handler(event, context):
    # Set the event["detail"]["incident-detection-response-identifier"] value to
the name of your alert that is coming from your APM. Each APM is different and
each unique alert will have a different name.
    # replace the dictionary path event["detail"]["ruleName"] with the path to your
alert name based on your APM payload.
    # This example is for finding the alert name in Splunk.
    event["detail"]["incident-detection-response-identifier"] = event["detail"]
["ruleName"]
    logger.info(f"We got: {json.dumps(event, indent=2)}")

    client = boto3.client('events')
    response = client.put_events(
        Entries=[
            {
                'Detail': json.dumps(event["detail"], indent=2),
                'DetailType': 'ams.monitoring/generic-apm', # Do not modify. This
DetailType value is required.

```

```
'Source': 'GenericAPMEvent', # Do not modify. This Source value is
required.
    'EventBusName': EventBusName # Do not modify. This variable is set
at the top of this code as a global variable. Change the variable value for your
eventbus name at the top of this code.
    }
]
)
print(response['Entries'])
```

8. Choisissez Deploy (Déployer).
9. Ajoutez une PutEventsautorisation au rôle d'exécution Lambda pour le bus d'événements auquel vous envoyez les données transformées :
  - a. Ouvrez la [page Fonctions](#) sur le AWS Lambda console.
  - b. Sélectionnez la fonction, puis choisissez Autorisations dans l'onglet Configuration.
  - c. Sous Rôle d'exécution, sélectionnez le nom du rôle pour ouvrir le rôle d'exécution dans AWS Identity and Access Management console.
  - d. Sous Politiques d'autorisations, sélectionnez le nom de la politique existante pour ouvrir la politique.
  - e. Sous Autorisations définies dans cette politique, choisissez Modifier.
  - f. Sur la page de l'éditeur de politiques, sélectionnez Ajouter une nouvelle déclaration :
  - g. L'éditeur de politiques ajoute une nouvelle déclaration vide similaire à la suivante
  - h. Remplacez la nouvelle instruction générée automatiquement par la suivante :

```
{
  "Sid": "AWSIncidentDetectionResponseEventBus0",
  "Effect": "Allow",
  "Action": "events:PutEvents",
  "Resource": "arn:aws:events:{region}:{accountId}:event-bus/{custom-eventbus-
name}"
}
```

- i. La ressource est celle ARN du bus d'événements personnalisé que vous avez créé [Étape 2 : Création d'un bus d'événements personnalisé](#) ou celle ARN de votre bus d'événements par défaut si vous utilisez le bus d'événements par défaut dans votre code Lambda.

10. Vérifiez et confirmez que les autorisations requises sont ajoutées au rôle.
11. Choisissez Définir cette nouvelle version comme version par défaut, puis cliquez sur Enregistrer les modifications.

Quelles sont les exigences d'une transformation de charge utile ?

Les paires JSON clé:valeur suivantes sont requises dans les événements du bus d'événements ingérés par AWS Incident Detection and Response.

```
{
  "detail-type": "ams.monitoring/generic-apm",
  "source": "GenericAPMEvent"
  "detail" : {
    "incident-detection-response-identifiant": "Your alarm name from your APM",
  }
}
```

Les exemples suivants montrent un événement provenant d'un bus d'événements partenaire avant et après sa transformation.

```
{
  "version": "0",
  "id": "a6150a80-601d-be41-1a1f-2c5527a99199",
  "detail-type": "Datadog Alert Notification",
  "source": "aws.partner/datadog.com/Datadog-aaa111bbbc",
  "account": "123456789012",
  "time": "2023-10-25T14:42:25Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "alert_type": "error",
    "event_type": "query_alert_monitor",
    "meta": {
      "monitor": {
        "id": 222222,
        "org_id": 3333333333,
        "type": "query alert",
        "name": "UnHealthyHostCount",
        "message": "@awseventbridge-Datadog-aaa111bbbc",

```

```
    "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
\u003c\u003d 1",
    "created_at": 1686884769000,
    "modified": 1698244915000,
    "options": {
      "thresholds": {
        "critical": 1.0
      }
    },
  },
  "result": {
    "result_id": 7281010972796602670,
    "result_ts": 1698244878,
    "evaluation_ts": 1698244868,
    "scheduled_ts": 1698244938,
    "metadata": {
      "monitor_id": 222222,
      "metric": "aws.applicationelb.un_healthy_host_count"
    }
  },
  "transition": {
    "trans_name": "Triggered",
    "trans_type": "alert"
  },
  "states": {
    "source_state": "OK",
    "dest_state": "Alert"
  },
  "duration": 0
},
"priority": "normal",
"source_type_name": "Monitor Alert",
"tags": [
  "aws_account:123456789012",
  "monitor"
]
}
```

Notez qu'avant que l'événement ne soit transformé, cela detail-type indique APM que l'alerte provient d'un partenaire APM et que la incident-detection-response-identifier clé n'est pas présente.

La fonction Lambda transforme l'événement ci-dessus et le place dans le bus d'événements personnalisé ou par défaut cible. La charge utile transformée inclut désormais les paires clé:valeur requises.

```
{
  "version": "0",
  "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
  "detail-type": "aws.monitoring/generic-apm",
  "source": "GenericAPMEvent",
  "account": "123456789012",
  "time": "2023-10-25T14:42:25Z",
  "region": "us-east-1",
  "resources": [],
  "detail": {
    "incident-detection-response-identifiant": "UnHealthyHostCount",
    "alert_type": "error",
    "event_type": "query_alert_monitor",
    "meta": {
      "monitor": {
        "id": 222222,
        "org_id": 3333333333,
        "type": "query alert",
        "name": "UnHealthyHostCount",
        "message": "@awseventbridge-Datadog-aaa111bbbc",
        "query":
"max(last_5m):avg:aws.applicationelb.un_healthy_host_count{aws_account:123456789012}
\u003c\u003d 1",
        "created_at": 1686884769000,
        "modified": 1698244915000,
        "options": {
          "thresholds": {
            "critical": 1.0
          }
        },
      },
    },
    "result": {
      "result_id": 7281010972796602670,
      "result_ts": 1698244878,
      "evaluation_ts": 1698244868,
      "scheduled_ts": 1698244938,
      "metadata": {
        "monitor_id": 222222,
        "metric": "aws.applicationelb.un_healthy_host_count"
      }
    }
  }
}
```

```
    }
  },
  "transition": {
    "trans_name": "Triggered",
    "trans_type": "alert"
  },
  "states": {
    "source_state": "OK",
    "dest_state": "Alert"
  },
  "duration": 0
},
"priority": "normal",
"source_type_name": "Monitor Alert",
"tags": [
  "aws_account:123456789012",
  "monitor"
]
}
```

Notez que `detail-type` c'est maintenant `aws.monitoring/generic-apm`, la source est maintenant `GenericAPMEvent`, et en détail, il y a une nouvelle paire clé:valeur `incident-detection-response-identifier`

Dans l'exemple précédent, la `incident-detection-response-identifier` valeur est extraite du nom de l'alerte situé sous le chemin `$.detail.meta.monitor.name`. APM Les chemins des noms d'alertes sont différents APM les uns des autres. La fonction Lambda doit être modifiée pour prendre le nom de l'alarme à partir du JSON chemin d'événement partenaire correct et l'utiliser comme valeur `incident-detection-response-identifier`

Chaque nom unique défini sur le `incident-detection-response-identifier` est fourni à l'équipe de détection et de réponse aux AWS incidents lors de l'intégration. Les événements dont le nom est inconnu `incident-detection-response-identifier` ne sont pas traités.

#### Étape 4 : créer une EventBridge règle Amazon personnalisée

Le bus d'événements partenaire créé à l'étape 1 nécessite une EventBridge règle que vous créez. La règle envoie les événements souhaités depuis le bus d'événements partenaire vers la fonction Lambda créée à l'étape 3.

Pour obtenir des instructions sur la définition de votre EventBridge règle, consultez les [EventBridge règles d'Amazon](#).

1. Ouvrez la EventBridge console Amazon à l'adresse <https://console.aws.amazon.com/events/>
2. Choisissez Rules, puis sélectionnez le bus d'événements partenaire associé à votre APM. Voici des exemples de bus dédiés aux événements organisés par des partenaires :
  - Datadog : `aws.partner/datadog.com/eventbus-name`
  - Splunk : `aws.partner/signalfx.com/ RandomString`
3. Choisissez Créer une règle pour créer une nouvelle EventBridge règle.
4. Pour le nom de la règle, entrez un nom au format suivant `APMName-AWS Incident Detection and Response-EventBridgeRule`, puis choisissez Next. Voici des exemples de noms :
  - Datadog : `Datadog- - AWSIncidentDetectionResponse EventBridgeRule`
  - Splunk : `Splunk- - AWSIncidentDetectionResponse EventBridgeRule`
5. Dans Source de l'événement, sélectionnez AWS des événements ou des événements EventBridge partenaires.
6. Conservez les valeurs par défaut pour l'événement Sample et la méthode de création.
7. Pour Modèle d'événement, choisissez ce qui suit :
  - a. Source de l'événement : EventBridge partenaires.
  - b. Partenaire : Sélectionnez votre APM partenaire.
  - c. Type d'événement : Tous les événements.

Voici des exemples de modèles d'événements :

Exemple de modèle d'événement Datadog

Exemple de modèle d'événement Splunk

8. Pour Targets, choisissez ce qui suit :
  - a. Types de cibles : AWS web
  - b. Sélectionnez une cible : Choisissez la fonction Lambda.

- c. Fonction : nom de la fonction Lambda que vous avez créée à l'étape 2.
9. Choisissez Suivant, puis Enregistrer la règle.

## Utilisez des webhooks pour ingérer des alarmes APMs sans intégration directe avec Amazon EventBridge

AWS Incident Detection and Response prend en charge l'utilisation de webhooks pour l'ingestion d'alarmes provenant de tiers APMs qui ne sont pas directement intégrés à Amazon EventBridge.

Pour une liste des intégrations directes APMs avec Amazon EventBridge, consultez la section [EventBridge Intégrations Amazon](#).

Suivez les étapes ci-dessous pour configurer l'intégration avec AWS Incident Detection and Response. Avant d'effectuer ces étapes, vérifiez que la règle AWS gérée, `AWSHealthEventProcessorEventSource-DO-NOT-DELETE`, est installée dans vos comptes

Ingérez des événements à l'aide de webhooks

1. Définissez une Amazon API Gateway pour accepter la charge utile de votre APM.
2. Définissez un AWS Lambda fonction d'autorisation à l'aide d'un jeton d'authentification, comme indiqué dans l'illustration précédente.
3. Définissez une deuxième fonction Lambda pour transformer et ajouter l'identifiant de détection et de réponse aux AWS incidents à votre charge utile. Vous pouvez également utiliser cette fonction pour filtrer les événements que vous souhaitez envoyer à AWS Incident Detection and Response.
4. Configurez votre APM appareil pour envoyer des notifications aux URL personnes générées par la API passerelle.

## Développez des runbooks pour la détection et la réponse aux AWS incidents

Vous pouvez télécharger un exemple de runbook de détection et de réponse aux incidents : [aws-idr-runbook-example.zip](#).

Incident Detection and Response utilise les informations recueillies à partir de votre questionnaire d'intégration pour développer des runbooks et des plans de réponse pour la gestion des incidents affectant vos charges de travail. Runbooks documente les étapes suivies par les gestionnaires d'incidents lorsqu'ils répondent à un incident. Un plan de réponse est mappé à au moins une de vos charges de travail. L'équipe de gestion des incidents crée ces modèles à partir des informations que vous avez fournies lors de la découverte de la charge de travail, décrite précédemment. Les plans d'intervention sont AWS Systems Manager (SSM) modèles de documents utilisés pour déclencher des incidents. Pour en savoir plus sur SSM les documents, voir [AWS Systems Manager Documents](#), pour en savoir plus sur Incident Manager, voir [Qu'est-ce que AWS Systems Manager Incident Manager?](#)

Principaux résultats :

- Finalisation de la définition de votre charge de travail sur la détection et la réponse aux AWS incidents.
- Achèvement des alarmes, des runbooks et de la définition du plan de réponse sur la détection et la réponse aux AWS incidents.

Vous pouvez également télécharger un exemple de manuel de détection et de réponse aux AWS incidents : [aws-idr-runbook-example.zip](#).

Exemple de runbook :

#### **Runbook template for AWS Incident Detection and Response**

# Description

This document is intended for [CustomerName] [WorkloadName].

[Insert short description of what the workload is intended for].

## Step: Priority

\*\*Priority actions\*\*

1. When a case is created with Incident Detection and Response, lock the case to yourself, verify the Customer Stakeholders in the Case from \*Engagement Plans - Initial Engagement\*.
2. Send the first correspondence on the support case to the customer as below. If there is no support case or if it is not possible to use the support case then backup communication details are listed in the steps that follow.

...

Hello,

```
This is <<Engineer's name>> from AWS Incident Detection and Response. An alarm has triggered for your workload <<application name>>. I am currently investigating and will update you in a few minutes after I have finished initial investigation.
```

```
Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>
```

```
...
```

```
**Compliance and regulatory requirements for the workload**
```

```
<<e.g. The workload deals with patient health records which must be kept secured and confidential. Information not to be shared with any third parties.>>
```

```
**Actions required from Incident Detection and Response in complying**
```

```
<<e.g Incident Management Engineers must not shared data with third parties.>>
```

```
## Step: Information
```

```
**Review of common information**
```

```
* This section provides a space for defining common information which may be needed through the life of the incident.
```

```
* The target user of this information is the Incident Management Engineer and Operations Engineer.
```

```
* The following steps may reference this information to complete an action (for example, execute the "Initial Engagement" plan).
```

```
---
```

```
**Engagement plans**
```

```
Describe the engagement plans applicable to this runbook. This section contains only contact details. Engagement plans will be referenced in the step by step
```

```
**Communication Plans**.
```

```
* **Initial engagement**
```

```
AWS Incident Detection and Response Team will add customer stakeholder addresses below to the Support Case. AWS Stakeholders are for additional stakeholders that may need to be made aware of any issues.
```

```
When updating customer stakeholders details in this plan also update the Backup Mailto links.
```

```
* ***Customer Stakeholders***: customeremail1; customeremail2; etc
```

```
* ***AWS Stakeholders***: aws-idr-oncall@amazon.com; tam-team-email; etc.
```

```
* ***One Time Only Contacts***: [These are email contacts that are included on only the first communication. Remove these contacts after the first communication has gone
```

out. These could be customer paging email addresses such as pager-duty that must not be paged for every correspondence]

- \* **Backup Mailto Impact Template**: <Insert Impact Template Mailto Link here>
  - \* Use the backup Mailto when communication over cases is not possible.
- \* **Backup Mailto No Impact Template**: <Insert No Impact Mailto Link here>
  - \* Use the backup Mailto when communication over cases is not possible.

#### \* **Engagement Escalation**

AWS Incident Detection and Response will reach out to the following contacts when the contacts from the **Initial engagement** plan do not respond to incidents.

For each Escalation Contact indicate if they must be added to the support case, phoned or both.

- \* **First Escalation Contact**: [escalationEmailAddress#1] / [PhoneNumber] - Wait XX Minutes before escalating to this contact.
  - \* [add Contact to Case / phone] this contact.
- \* **Second Escalation Contact**: [escalationEmailAddress#2] / [PhoneNumber] - Wait XX Minutes before escalating to this contact.
  - \* [add Contact to Case / phone] this contact.
- \* Etc;

---

#### \* **Communication plans**

Describe how Incident Management Engineer communicates with designated stakeholders outside the incident call and communication channels.

##### \* **Impact Communication plan**

This plan is initiated when Incident Detection and Response have determined from step **Triage** that an alert indicates potential impact to a customer.

Incident Detection and Response will request the customer to join the predetermined bridge (Chime Bridge/Customer Provided Bridge / Customer Static Bridge) as indicated in **Engagement plans - Incident call setup**.

All backup email templates for use when cases can't be used are in **Engagement plans - Initial engagement**.

- \* 1 - Before sending the impact notification, verify then remove and/or add customer contacts from the Support Case CC based on the contacts listed in the **Initial engagement** Engagement plan.
- \* 2 - Send the engagement notification to the customer based the following Template:

(choose one and remove the rest)

**Impact Template - Chime Bridge**

...

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert state change reason>

Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>

Please join the Chime Bridge below so we can start the steps outlined in your Runbook:

<insert Chime Meeting ID>

<insert Link to Chime Bridge>

International dial-in numbers: <https://chime.aws/dialinnumbers/>

...

\*\*\*Impact Template - Customer Provided Bridge\*\*\*

...

The following alarm has engaged AWS Incident Detection and Response:

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert state change reason>

Alarm Start Time - <Example: 1 January 2023 3:30 PM UTC>

Please respond with your internal bridge details so we can join and start the steps outlined in your Runbook.

...

\*\*\*Impact Template - Customer Static Bridge\*\*\*

...

The following alarm has engaged AWS Incident Detection and Response to an Incident bridge:

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert state change reason>

Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>

Please join the Bridge below so we can start the steps outlined in your Runbook:

Conference Number: <insert conference number>

Conference URL : <insert bridgeURL>

...

- \* 3 - Set the Case to Pending Customer Action
- \* 4 - Follow **Engagement Escalation** plan as mentioned above.
- \* 5 - If the customer does not respond within 30 minutes, disengage and continue to monitor until the alarm recovers.

\* **No Impact Communication plan**

This plan is initiated when an alarm recovers before Incident Detection and Response have completed initial **Triage**.

- \* 1 - Before sending the no impact notification, verify then remove and/or add customer contacts from the Support Case CC based on the contacts listed in the **Engagement plans - Initial engagement** Engagement plan.

\* 2 - Send a no engagement notification to the customer based on the below template:

\*\*\*No Impact Template\*\*\*

```\n

AWS Incident Detection and Response received an alarm that has recovered for your workload.

Alarm Identifier - <insert CloudWatch Alarm ARN or APM Response Identifier>

Alarm State Change Reason - <insert state change reason>

Alarm Start Time - <Example: 1 January 2023, 3:30 PM UTC>

Alarm End Time - <Example: 1 January 2023, 3:35 PM UTC>

This may indicate a brief customer impact that is currently not ongoing.

If there is an ongoing impact to your workload, please let us know and we will engage to assist.

```\n

\* 3 - Put the case in to Pending Customer Action.

\* 4 - If the customer does not respond within 30 minutes Resolve the case.

\* \*\*Updates\*\*

If AWS Incident Detection and Response is expected to provide regular updates to customer stakeholders, list those stakeholders here. Updates must be sent via the same support case.

Remove this section if not needed.

\* Update Cadence: Every XX minutes

\* External Update Stakeholders: customeremailaddress1; customeremailaddress2; etc

\* Internal Update Stakeholders: awsemailaddress1; awsemailaddress2; etc

---\n

\*\*Application architecture overview\*\*

This section provides an overview of the application/workload architecture for Incident Management Engineer and Operations Engineer awareness.

\* \*\*AWS Accounts and Regions with key services\*\* - list of AWS accounts with regions supporting this application. Assists Engineers in assessing underlying infrastructure supporting the application.

\* 123456789012

\* US-EAST-1 - brief desc as appropriate

\* EC2 - brief desc as appropriate

\* DynamoDB - brief desc as appropriate

\* etc.

\* US-WEST-1 - brief desc as appropriate

\* etc.

\* another-account-etc.

\* **Resource identification** - describe how engineers determine resource association with application

- \* Resource groups: etc.
- \* Tag key/value: AppId=123456

\* **CloudWatch Dashboards** - list dashboards relevant to key metrics and services

- \* 123456789012
  - \* us-east-1
    - \* some-dashboard-name
    - \* etc.
  - \* some-other-dashboard-name-in-current-acct

## ## Step: Triage

**Evaluate incident and impact**

This section provides instructions for triaging of the incident to determine correct impact, description, and overall correct runbook being executed.

\* **Evaluation of initial incident information**

- \* 1 - Review Incident Alarm, noting time of first detected impact as well as the alarm start time.
- \* 2 - Identify which service(s) in the customer application is seeing impact.
- \* 3 - Review AWS Service Health for services listed under **AWS Accounts and Regions with key services**.
- \* 4 - Review any customer provided dashboards listed under **CloudWatch Dashboards**

---

\* **Impact**

Impact is determined when either the customer's metrics do not recover, appear to be trending worse or if there is indication of AWS Service Impact.

- \* 1 - Start **Communication plans - Impact Communication plan**
- \* 2 - Start **Engagement plans - Engagement Escalation** if no response is received from the **Initial Engagement** contacts.
- \* 3 - Start **Communication plans - Updates** if specified in **Communication plans**

\* **No Impact**

No Impact is determined when the customer's alarm recovers before Triage is complete and there are no indications of AWS service impact or sustained impact on the customer's CloudWatch Dashboards.

- \* 1 - Start **Communication plans - No Impact Communication plan**

## ## Step: Investigate

**Investigation**

This section describes performing investigation of known and unknown symptoms.

#### **\*\*Known issue\*\***

- \* **List all known issues with the application and their standard actions here\***

#### **\*\*Unknown issues\*\***

- \* Investigate with the customer and AWS Premium Support.
- \* Escalate internally as required.

### **## Step: Mitigation**

#### **\*\*Collaborate\*\***

- \* Communicate any changes or important information from the **\*\*Investigate\*\*** step to the members of the incident call.

#### **\*\*Implement mitigation\*\***

- \* **List customer failover plans / Disaster Recovery plans / etc here for implementing mitigation.**

### **## Step: Recovery**

#### **\*\*Monitor customer impact\*\***

- \* Review metrics to confirm recovery.
- \* Ensure recovery is across all Availability Zones / Regions / Services
- \* Get confirmation from the customer that impact is over and the application has recovered.

#### **\*\*Identify action items\*\***

- \* Record key decisions and actions taken, including temporary mitigation that might have been implemented.
- \* Ensure outstanding action items have assigned owners.
- \* Close out any Communication plans that were opened during the incident with a final confirmation of recovery notification.

## Testez les charges de travail intégrées

### Note

Le AWS Identity and Access Management l'utilisateur ou le rôle que vous utilisez pour tester les alarmes doit disposer d'une `cloudwatch:SetAlarmState` autorisation.

La dernière étape du processus d'intégration consiste à organiser une journée de jeu adaptée à votre nouvelle charge de travail. Une fois l'enregistrement des alarmes terminé, AWS Incident Detection and Response confirme la date et l'heure que vous avez choisies pour commencer votre journée de jeu.

Votre journée de jeu a deux objectifs principaux :

- **Validation fonctionnelle** : confirme que AWS Incident Detection and Response peut correctement recevoir vos événements d'alarme. De plus, la validation fonctionnelle confirme que vos événements d'alarme déclenchent les runbooks appropriés et toute autre action souhaitée, telle que la création automatique d'un dossier si vous l'avez sélectionnée lors de l'ingestion de l'alarme.
- **Simulation** : La journée de jeu est une simulation de bout en bout de ce qui pourrait se passer lors d'un incident réel. AWS La détection et la réponse aux incidents suivent les étapes que vous avez prescrites pour vous donner un aperçu de la manière dont un véritable incident peut se dérouler. La journée de jeu est l'occasion pour vous de poser des questions ou d'affiner les instructions afin d'améliorer l'engagement.

Pendant le test d'alarme, AWS Incident Detection and Response travaille avec vous pour résoudre les problèmes identifiés.

## CloudWatch alarmes

AWS Incident Detection and Response teste vos CloudWatch alarmes Amazon en surveillant le changement d'état de votre alarme. Pour ce faire, passez manuellement l'alarme à l'état Alarme à l'aide du AWS Command Line Interface. Vous pouvez également accéder au AWS CLI from AWS CloudShell. AWS Incident Detection and Response vous fournit une liste des AWS CLI commandes que vous pouvez utiliser pendant les tests.

Exemple AWS CLI commande pour définir un état d'alarme :

```
aws cloudwatch set-alarm-state --alarm-name "ExampleAlarm" --state-value ALARM --state-reason "Testing AWS Incident Detection and Response" --region us-east-1
```

Pour en savoir plus sur la modification manuelle de l'état des CloudWatch alarmes, consultez [SetAlarmState](#).

Pour en savoir plus sur les autorisations requises pour les CloudWatch API opérations, consultez la [référence CloudWatch des autorisations Amazon](#).

## APMAlarmes tierces

Les charges de travail qui utilisent un outil tiers de surveillance des performances des applications (APM) DataDog, tel que Splunk ou Dynatrace NewRelic, nécessitent des instructions différentes pour simuler une alarme. Au début du GameDay, AWS Incident Detection and Response vous demande de modifier temporairement vos seuils d'alarme ou de modifier les opérateurs de comparaison pour forcer l'alarme à passer au ALARMstatut. Ce statut déclenche une charge utile pour la détection et la réponse aux AWS incidents.

### Principaux résultats

Principaux résultats :

- L'ingestion de l'alarme est réussie et la configuration de votre alarme est correcte.
- Les alarmes sont créées et reçues avec succès par AWS Incident Detection and Response.
- Un dossier d'assistance est créé pour votre engagement et les contacts que vous avez prescrits sont informés.
- AWSIncident Detection and Response peut communiquer avec vous par les moyens de conférence que vous avez prescrits.
- Toutes les alarmes et demandes d'assistance générées dans le cadre du Gameday sont résolues.
- Un e-mail de lancement est envoyé pour confirmer que votre charge de travail est désormais surveillée par AWS Incident Detection and Response.

## Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes

Téléchargez le [questionnaire d'intégration de Workload](#).

Téléchargez le [questionnaire d'ingestion d'Alarm](#).

### Questionnaire d'intégration de la charge de travail - Questions générales

Questions générales

| Question            | Exemple de réponse |
|---------------------|--------------------|
| Nom de l'entreprise | Amazon Inc.        |

| Question  | Exemple de réponse  |
|---|---|
| Nom de cette charge de travail (inclure les abréviations éventuelles)   | Opérations de vente au détail sur Amazon (ARO)  |
| L'utilisateur final principal et le fonctionnement de cette charge de travail.  | Cette charge de travail est une application de commerce électronique qui permet aux utilisateurs finaux d'acheter divers articles. Cette charge de travail est la principale source de revenus pour notre entreprise. |
| Exigences réglementaires et/ou de conformité applicables à cette charge de travail et à toute action requise auprès de AWS après un incident. | La charge de travail concerne les dossiers médicaux des patients, qui doivent être sécurisés et confidentiels.  |

## Questionnaire d'intégration de la charge de travail - Questions d'architecture

### Questions d'architecture

| Question   | Exemple de réponse                                 |
|--|--|
| Une liste de AWS balises de ressources utilisées pour définir les ressources faisant partie de cette charge de travail. AWS utilise ces balises pour identifier les ressources de cette charge de travail afin d'accélérer le support en cas d'incident. | appName: Optimax<br><br>environnement : Production |

 **Note**

Les balises sont sensibles à la casse. Si vous fournissez plusieurs balises, toutes les ressources utilisées par cette charge de travail doivent avoir les mêmes balises.

| Question   | Exemple de réponse  |
|--|---|
| <p>Une liste de AWS Services utilisés par cette charge de travail et AWS Compte et régions dans lesquels ils se trouvent.</p> <div data-bbox="115 422 792 642"><p> Note</p><p>Créez une nouvelle ligne pour chaque service.</p></div>     | <p>Route 53 : achemine le trafic Internet vers leALB.</p> <p>Compte : 123456789101</p> <p>Région : États-Unis- EAST -1, États-Unis- WEST -2</p>   |
| <p>Une liste de AWS Services utilisés par cette charge de travail et AWS Compte et régions dans lesquels ils se trouvent.</p> <div data-bbox="115 852 792 1073"><p> Note</p><p>Créez une nouvelle ligne pour chaque service.</p></div>    | <p>ALB: Achemine le trafic entrant vers un groupe cible de ECS conteneurs.</p> <p>Compte : 123456789101</p> <p>Région : N/A</p>   |
| <p>Une liste de AWS Services utilisés par cette charge de travail et AWS Compte et régions dans lesquels ils se trouvent.</p> <div data-bbox="115 1283 792 1503"><p> Note</p><p>Créez une nouvelle ligne pour chaque service.</p></div> | <p>ECS: infrastructure informatique pour le parc logique métier principal. Responsable du traitement des demandes des utilisateurs entrantes et de l'envoi de requêtes à la couche de persistance.</p> <p>Compte : 123456789101</p> <p>Région : US- EAST -1</p> |

| Question   | Exemple de réponse  |
|--|---|
| <p>Une liste de AWS Services utilisés par cette charge de travail et AWS Compte et régions dans lesquels ils se trouvent.</p> <div data-bbox="115 420 792 638"><p> <b>Note</b></p><p>Créez une nouvelle ligne pour chaque service.</p></div>  | <p>RDS: Le cluster Amazon Aurora stocke les données utilisateur accessibles par la couche de logique ECS métier.</p> <p>Compte : 123456789101</p> <p>Région : US- EAST -1</p> |
| <p>Une liste de AWS Services utilisés par cette charge de travail et AWS Compte et régions dans lesquels ils se trouvent.</p> <div data-bbox="115 848 792 1066"><p> <b>Note</b></p><p>Créez une nouvelle ligne pour chaque service.</p></div> | <p>S3 : Stocke les actifs statiques du site Web.</p> <p>Compte : 123456789101</p> <p>Région : N/A</p>   |
| <p>Détaillez tous les composants en amont/en aval qui ne sont pas intégrés et qui pourraient affecter cette charge de travail en cas de panne.</p>   | <p>Microservice d'authentification : empêchera les utilisateurs de charger leurs dossiers médicaux car ils ne seront pas authentifiés.</p>                                    |
| <p>Y en a-t-il sur site ou non AWS composants pour cette charge de travail ? Dans l'affirmative, quels sont-ils et quelles sont les fonctions exécutées ?</p>  | <p>Tout le trafic Internet entrant/sortant de AWS est acheminé via notre service proxy sur site.</p>  |
| <p>Fournissez les détails de tout plan de basculement ou de reprise après sinistre manuel ou automatisé au niveau de la zone de disponibilité et de la région.</p>   | <p>Mode veille à chaud. Basculement automatique vers WEST US-2 en cas de baisse prolongée du taux de réussite.</p>  |

## Questionnaire d'intégration de la charge de travail - AWS Questions relatives aux événements de service

### AWS Questions relatives aux événements de service

| Question  | Exemple de réponse  |
|---|---|
| Fournissez les coordonnées (nom/e-mail/téléphone) de l'équipe interne de gestion des incidents majeurs ou des crises informatiques de votre entreprise.   | Équipe de gestion des incidents majeurs<br><br>mim@example.com<br><br>+61 2 3456 7890       |
| Fournissez des détails sur tout pont statique de gestion des incidents/crises établi par votre entreprise. Si vous utilisez des ponts non statiques, spécifiez votre application préférée et AWS demandera ces informations lors d'un incident. | Amazon Chime<br><br><a href="https://chime.aws/1234567890">https://chime.aws/1234567890</a> |

 **Note**

Si aucun n'est fourni, alors AWS vous contactera lors d'un incident et vous fournira un pont Chime que vous pourrez rejoindre.

## Questionnaire relatif à l'ingestion

### Questions relatives au Runbook

| Question   | Exemple de réponse  |
|--|---|
| AWS mobilisera les contacts liés à la charge de travail par le AWS Support Affaire. Qui est le contact principal lorsqu'une alarme se déclenche pour cette charge de travail ? | Équipe de candidature<br><br>app@example.com<br><br>+61 2 3456 7890 |

| Question   | Exemple de réponse  |
|--|---|
| <p>Spécifiez votre application de conférence préférée et AWS demandera ces informations lors d'un incident.</p> <div data-bbox="115 401 792 764" style="border: 1px solid #add8e6; border-radius: 10px; padding: 10px;"><p> <b>Note</b></p><p>Si aucune application de conférence préférée n'est fournie, alors AWS vous contactera lors d'un incident et vous fournira un pont Chime que vous pourrez rejoindre.</p></div> |   |
| <p>Si le contact principal n'est pas disponible lors d'un incident, veuillez indiquer les contacts d'escalade et le calendrier dans l'ordre de communication préféré.</p>  | <ol style="list-style-type: none"><li>1. Au bout de 10 minutes, en l'absence de réponse de la part du contact principal, contactez :<br/><br/>John Smith - Superviseur des applications<br/><br/>john.smith@example.com<br/><br/>+61 2 3456 7890</li><li>2. Après 10 minutes, si John Smith ne répond pas, contactez :<br/><br/>Jane Smith - Directrice des opérations<br/><br/>jane.smith@example.com<br/><br/>+61 2 3456 7890</li></ol> |
| <p>AWS communique les mises à jour par le biais du dossier de support à intervalles réguliers tout au long de l'incident. D'autres contacts devraient-ils recevoir ces mises à jour ?</p>  | <p>john.smith@example.com, jane.smith@example.com</p>   |

# Matrice d'alarme

## Matrice d'alarme

Fournissez les informations suivantes pour identifier l'ensemble d'alarmes qui déclencheront la détection et la réponse aux AWS incidents afin de créer des incidents au nom de votre charge de travail. Une fois que les ingénieurs de AWS Incident Detection and Response auront examiné vos alarmes, des étapes d'intégration supplémentaires seront effectuées.

AWS Critères d'alerte critique relatifs à la détection des incidents et à la réponse :

- AWS Les alarmes de détection et de réponse aux incidents ne doivent passer à l'état « alarme » qu'en cas d'impact commercial significatif sur la charge de travail surveillée (perte de revenus/ dégradation de l'expérience client) nécessitant une attention immédiate de la part de l'opérateur.
- AWS Les alarmes de détection et de réponse aux incidents doivent également impliquer vos résolveurs pour la charge de travail en même temps ou avant l'engagement. AWS Les gestionnaires d'incidents collaborent avec vos résolveurs dans le cadre du processus d'atténuation et ne jouent pas le rôle d'intervenants de première ligne qui vous contactent ensuite.
- AWS Les seuils d'alarme de détection et de réponse aux incidents doivent être fixés à un seuil et à une durée appropriés afin qu'une enquête soit menée chaque fois qu'une alarme se déclenche. Si une alarme passe de l'état « Alarme » à l'état « OK », l'impact est suffisant pour justifier la réponse et l'attention de l'opérateur.

AWS Politique de détection des incidents et de réponse en cas de violation des critères :

Ces critères ne peuvent être évalués qu'au fur et à case-by-case mesure que les événements se produisent. L'équipe de gestion des incidents travaille avec vos responsables de comptes techniques (TAMs) pour ajuster les alarmes et, dans de rares cas, désactiver la surveillance s'il est soupçonné que les alarmes des clients ne répondent pas à ces critères et fait appel à l'équipe de gestion des incidents de manière inutilement régulière.

### Important

Indiquez les adresses e-mail de distribution d'un groupe lorsque vous fournissez des adresses de contact, afin de pouvoir contrôler les ajouts et les suppressions de destinataires sans mettre à jour le runbook.

Indiquez le numéro de téléphone de votre équipe d'ingénierie de fiabilité du site (SRE) si vous souhaitez que l'équipe de détection et de réponse aux AWS incidents l'appelle après avoir envoyé un e-mail d'engagement initial.

Table Alarm Matrix

| Nom de la métriqueARN//Seuil  | Description   | Remarques  | Actions demandées  |
|---|---|--|--|
| <p>Volume de charge de travail/<br/><i>CW Alarm ARN /</i><br/>CallCount &lt; 100 000 pour 5 points de données en 5 minutes, traiter les données manquantes comme manquantes</p> | <p>Cette métrique représente le nombre de demandes entrantes destinées à la charge de travail, mesuré au niveau de l'Application Load Balancer.</p> <p>Cette alarme est importante car des baisses importantes du nombre de demandes entrantes peuvent indiquer des problèmes de connectivité réseau en amont ou des problèmes liés à notre DNS implémentation empêchant les utilisateurs d'accéder à la charge de travail.</p> | <p>L'alarme est passée à l'état « Alarme » 10 fois la semaine dernière. Cette alarme présente un risque de faux positifs. Une révision des seuils est prévue.</p> <p>Des problèmes ? Non ou Oui (si Non, laissez le champ vide) : cette alarme se déclenche fréquemment lors de l'exécution d'une tâche par lots donnée.</p> <p>Résolveurs : ingénieurs de fiabilité des sites</p> | <p>Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à <a href="mailto:SRE@xyz.com">SRE@xyz.com</a></p> <p>Créez un dossier AWS de Support Premium pour nos services ELB et Route 53.</p> <p>Si IMMEDIATE une action est nécessaire : cochez la case Mémoire EC2 libre/ espace disque et informez le <i>XYZ</i></p> <p>Faites équipe par e-mail pour redémarrer l'instance ou pour vider le journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)</p> |

| Nom de la métriqueARN//Seuil   | Description   | Remarques   | Actions demandées  |
|--|---|---|--|
| <p>Latence des demandes de charge de travail/</p> <p><i>CW Alarm ARN /</i></p> <p>p90 Latence &gt; 100 ms pour 5 points de données en 5 minutes, traiter les données manquantes comme manquantes</p> | <p>Cette métrique représente la latence p90 pour les HTTP demandes à traiter par la charge de travail.</p> <p>Cette alarme représente la latence (mesure importante de l'expérience client pour le site Web).</p> | <p>L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière.</p> <p>Des problèmes ? Non ou Oui (si Non, laissez le champ vide) : cette alarme se déclenche fréquemment lors de l'exécution d'une tâche par lots donnée.</p> <p>Résolveurs : ingénieurs de fiabilité des sites</p> | <p>Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à <a href="mailto:SRE@xyz.com">SRE@xyz.com</a></p> <p>Créez un dossier AWS de Support Premium pour nos ECW services. RDS</p> <p>Si IMMEDIATE une action est nécessaire : cochez la case Mémoire EC2 libre/ espace disque et informez le <i>XYZ</i></p> <p>Faites équipe par e-mail pour redémarrer l'instance ou pour vider le journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)</p> |

| Nom de la métriqueARN//Seuil   | Description  | Remarques   | Actions demandées  |
|--|--|---|--|
| <p>Disponibilité des demandes de charge de travail/</p> <p><i>CW Alarm ARN /</i></p> <p>Disponibilité &lt; 95 % pour 5 points de données en 5 minutes, considérez les données manquantes comme manquantes.</p> | <p>Cette métrique représente la disponibilité des HTTP demandes à traiter par la charge de travail. (nombre de HTTP 200/nombre de demandes) par période.</p> <p>Cette alarme indique la disponibilité de la charge de travail.</p> | <p>L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière.</p> <p>Des problèmes ? Non ou Oui (si Non, laissez le champ vide) : cette alarme se déclenche fréquemment lors de l'exécution d'une tâche par lots donnée.</p> <p>Résolveurs : ingénieurs de fiabilité des sites</p> | <p>Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à <a href="mailto:SRE@xyz.com">SRE@xyz.com</a></p> <p>Créez un dossier AWS de Support Premium pour nos services ELB et Route 53.</p> <p>Si IMMEDIATE une action est nécessaire : cochez la case Mémoire EC2 libre/ espace disque et informez le <i>XYZ</i></p> <p>Faites équipe par e-mail pour redémarrer l'instance ou pour vider le journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)</p> |

Exemple d'alarme New Relic

| Nom de la métriqueARN//Seuil   | Description   | Remarques   | Actions demandées  |
|--|---|---|--|
| <p>Test d'intégration de bout en bout/<br/><i>CW Alarm ARN /</i></p> <p>Taux d'échec de 3 % pour les métriques d'une minute sur une durée de 3 minutes, traiter les données manquantes comme manquantes</p> <p>Identifiant de charge de travail : flux de travail de test de bout en bout, AWS région : US- EAST -1, ID de AWS compte : 012345678910</p> | <p>Cette métrique teste si une demande peut traverser chaque couche de la charge de travail. Si ce test échoue, cela représente un échec critique du traitement des transactions commerciales.</p> <p>Cette alarme indique la capacité de traiter les transactions commerciales correspondant à la charge de travail.</p> | <p>L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière.</p> <p>Des problèmes ? Non ou Oui (si Non, laissez le champ vide) : cette alarme se déclenche fréquemment lors de l'exécution d'une tâche par lots donnée.</p> <p>Résolveurs : ingénieurs de fiabilité des sites</p> | <p>Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à <a href="mailto:SRE@xyz.com">SRE@xyz.com</a></p> <p>Créez un dossier de AWS support Premium pour nos ECS services et ceux de DynamoDB.</p> <p>Si IMMEDIATE une action est nécessaire : cochez la case Mémoire EC2 libre/ espace disque et informez le <i>XYZ</i></p> <p>Faites équipe par e-mail pour redémarrer l'instance ou pour vider le journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)</p> |

## Demander des modifications à une charge de travail intégrée

Pour demander des modifications à une charge de travail intégrée, procédez comme suit pour créer un dossier d'assistance avec AWS Incident Detection and Response.

1. Accédez au [AWS Support Centrez](#), puis sélectionnez Créer un dossier, comme indiqué dans l'exemple suivant :
2. Choisissez Technique.
3. Pour Service, choisissez Incident Detection and Response.
4. Pour Catégorie, choisissez Demande de modification de charge de travail.
5. Dans le champ Severity, sélectionnez General Guidance.
6. Entrez un objet pour cette modification. Par exemple :

AWS Détection et réponse aux incidents - *workload\_name*

7. Entrez une description pour cette modification. Par exemple, saisissez « Cette demande concerne des modifications apportées à une charge de travail existante intégrée à AWS Incident Detection and Response ». Assurez-vous d'inclure les informations suivantes dans votre demande :
  - Nom de la charge de travail : nom de votre charge de travail.
  - Identifiant (s) de compte :ID1,ID2,ID3, et ainsi de suite.
  - Détails de la modification : Entrez les détails de la modification demandée.
8. Dans la section Contacts supplémentaires - facultatif, saisissez l'e-mail dans IDs lequel vous souhaitez recevoir de la correspondance concernant cette modification.

Voici un exemple de la section Contacts supplémentaires - facultative.

 Important

L'échec de l'ajout d'e-mail IDs dans la section Contacts supplémentaires - facultatif peut retarder le processus de modification.

9. Sélectionnez Envoyer.

Après avoir soumis la demande de modification, vous pouvez ajouter des e-mails supplémentaires provenant de votre organisation. Pour ajouter des e-mails, choisissez Répondre dans les détails du dossier, comme illustré dans l'exemple suivant :

Ajoutez ensuite l'e-mail IDs dans la section Contacts supplémentaires - facultatif.

Voici un exemple de page de réponse indiquant où vous pouvez saisir des e-mails supplémentaires.

## Décharger une charge de travail

Pour décharger une charge de travail de la fonction AWS Incident Detection and Response, créez un nouveau dossier de support pour chaque charge de travail. Lorsque vous créez le dossier de support, tenez compte des points suivants :

- Pour décharger une charge de travail qui se trouve dans un seul AWS compte, créez le dossier d'assistance soit depuis le compte de la charge de travail, soit depuis votre compte payeur.
- Pour décharger une charge de travail qui couvre plusieurs AWS comptes, puis créez le dossier d'assistance à partir de votre compte payeur. Dans le corps du dossier d'assistance, listez tous les comptes IDs à supprimer.

### Important

Si vous créez un dossier d'assistance pour décharger une charge de travail du mauvais compte, vous risquez de rencontrer des retards et des demandes d'informations supplémentaires avant que vos charges de travail ne puissent être déchargées.

### Demande de déchargement d'une charge de travail

1. Accédez au [AWS Support Centrez](#), puis sélectionnez Créer un dossier.
2. Choisissez Technique.
3. Pour Service, choisissez Incident Detection and Response.
4. Dans Catégorie, choisissez Workload Offboarding.
5. Dans le champ Severity, sélectionnez General Guidance.
6. Entrez un objet pour cette modification. Par exemple :

[Offboard] Détection et réponse aux AWS incidents - *workload\_name*

7. Entrez une description pour cette modification. Par exemple, saisissez « Cette demande concerne le transfert d'une charge de travail existante intégrée dans AWS Incident Detection and Response ». Assurez-vous d'inclure les informations suivantes dans votre demande :
  - Nom de la charge de travail : nom de votre charge de travail.
  - Identifiant (s) de compte : ID1, ID2, ID3, et ainsi de suite.
  - Motif du désenclavement : indiquez le motif du déchargement de la charge de travail.
8. Dans la section Contacts supplémentaires - facultatif, entrez l'e-mail dans IDs lequel vous souhaitez recevoir de la correspondance concernant cette demande de désenclavement.
9. Sélectionnez Envoyer.

# Surveillance et observabilité de la détection et de la réponse aux incidents AWS

AWS Incident Detection and Response vous fournit des conseils d'experts sur la définition de l'observabilité dans l'ensemble de vos charges de travail, de la couche applicative à l'infrastructure sous-jacente. La surveillance vous indique que quelque chose ne va pas. L'observabilité utilise la collecte de données pour vous dire ce qui ne va pas et pourquoi cela s'est produit.

Le système de détection et de réponse aux incidents surveille vos AWS charges de travail pour détecter les défaillances et les dégradations de performances en tirant parti de AWS services natifs tels qu'Amazon CloudWatch et Amazon EventBridge pour détecter les événements susceptibles d'avoir un impact sur votre charge de travail. La surveillance vous avertit en cas de défaillances imminentes, en cours, en cours, en cours ou potentielles, ou en cas de dégradation des performances. Lorsque vous intégrez votre compte à Incident Detection and Response, vous sélectionnez les alarmes de votre compte qui doivent être surveillées par le système de surveillance de la détection et de la réponse aux incidents et vous associez ces alarmes à une application et à un runbook utilisés lors de la gestion des incidents.

Incident Detection and Response utilise Amazon CloudWatch et d'autres Services AWS entreprises pour créer votre solution d'observabilité. AWS Incident Detection and Response vous aide à améliorer l'observabilité de deux manières :

- **Mesures des résultats commerciaux** : l'observabilité sur AWS Incident Detection and Response commence par la définition des indicateurs clés qui surveillent les résultats de vos charges de travail ou de l'expérience de l'utilisateur final. AWS des experts travaillent avec vous pour comprendre les objectifs de votre charge de travail, les principaux résultats ou facteurs susceptibles d'avoir un impact sur l'expérience utilisateur, et pour définir les mesures et les alertes qui capturent toute dégradation de ces indicateurs clés. Par exemple, un indicateur commercial clé pour une application d'appel mobile est le taux de réussite de la configuration des appels (surveille le taux de réussite des tentatives d'appel des utilisateurs), et un indicateur clé pour un site Web est la vitesse de page. L'engagement en cas d'incident est déclenché en fonction des indicateurs des résultats commerciaux.
- **Mesures au niveau de l'infrastructure** : à ce stade, nous identifions le sous-jacent Services AWS et l'infrastructure supportant votre application, puis nous définissons des métriques et des alarmes pour suivre les performances de ces services d'infrastructure. Il peut s'agir de mesures telles que celles relatives `ApplicationLoadBalancerErrorCount` aux instances d'Application Load

Balancer. Cela commence une fois que la charge de travail a été intégrée et que la surveillance a été configurée.

## Implémentation de l'observabilité sur AWS Incident Detection and Response

L'observabilité étant un processus continu qui peut ne pas être réalisé en un seul exercice ou en un seul laps de temps, AWS Incident Detection and Response met en œuvre l'observabilité en deux phases :

- Phase d'intégration : L'observabilité lors de l'intégration vise à détecter les cas où les résultats commerciaux de votre application sont altérés. À cette fin, l'observabilité pendant la phase d'intégration est axée sur la définition des principaux indicateurs de résultats commerciaux au niveau de la couche application afin AWS de signaler les perturbations de vos charges de travail. Cette méthode AWS peut répondre rapidement à ces perturbations et vous aider à vous rétablir.
- Phase post-intégration : AWS Incident Detection and Response propose un certain nombre de services proactifs pour l'observabilité, notamment la définition de métriques au niveau de l'infrastructure, le réglage des métriques et la configuration de traces et de journaux en fonction du niveau de maturité du client. La mise en œuvre de ces services peut s'étendre sur plusieurs mois et impliquer plusieurs équipes. AWS Incident Detection and Response fournit des conseils sur la configuration de l'observabilité et les clients sont tenus de mettre en œuvre les modifications requises dans leur environnement de charge de travail. Pour obtenir de l'aide concernant la mise en œuvre pratique des fonctionnalités d'observabilité, adressez-vous à vos responsables de comptes techniques (TAM).

# Gestion des AWS incidents avec détection et réponse aux incidents

AWS Incident Detection and Response vous propose une surveillance proactive et une gestion des incidents 24 h/24, 7 j/7, assurées par une équipe désignée de responsables des incidents.

1. **Génération d'alarmes** : les alarmes déclenchées sur vos charges de travail sont transmises via Amazon EventBridge à AWS Incident Detection and Response. AWS Incident Detection and Response ouvre automatiquement le runbook associé à votre alarme et en informe le responsable des incidents. Si un incident critique survient sur votre charge de travail et n'est pas détecté par les alarmes surveillées par AWS Incident Detection and Response, vous pouvez créer un dossier d'assistance pour demander une réponse aux incidents. Pour plus d'informations sur la demande de réponse à un incident, consultez [Demande de réponse à un incident](#).
2. **AWS Engagement du responsable des incidents** : le responsable des incidents répond à l'alarme et vous contacte lors d'une conférence téléphonique ou comme indiqué dans le runbook. Le responsable des incidents vérifie l'état de santé des Services AWS pour déterminer si l'alarme est liée à des problèmes liés à Services AWS utilisé par la charge de travail et donne des conseils sur l'état des services sous-jacents. Si nécessaire, le responsable des incidents crée ensuite un dossier en votre nom et engage le droit AWS des experts pour vous aider.

Parce que la détection et la réponse aux AWS incidents surveillent Services AWS spécifiquement pour vos applications, la détection et la réponse aux AWS incidents peuvent déterminer que l'incident est lié à un Service AWS problème avant même qu'un Service AWS l'événement est déclaré. Dans ce scénario, le responsable des incidents vous conseille sur l'état du Service AWS, déclenche le AWS Flux de gestion des incidents liés aux événements de service et suivi de la résolution auprès de l'équipe de service. Les informations fournies vous donnent la possibilité de mettre en œuvre vos plans de reprise ou vos solutions de contournement à un stade précoce afin d'atténuer l'impact de la AWS Événement de service. Pour de plus amples informations, veuillez consulter [Gestion des incidents pour les événements de service](#).

3. **Résolution des incidents** : le responsable des incidents coordonne l'incident selon les critères requis AWS fait équipe et veille à ce que vous restiez engagé avec les bonnes AWS experts jusqu'à ce que l'incident soit atténué ou résolu.
4. **Examen post-incident (si demandé)** : Après un AWS incident, Incident Detection and Response peut effectuer un examen post-incident à votre demande et générer un rapport post-incident. Le

rapport publié après l'incident inclut une description du problème, de son impact, des équipes impliquées et des solutions ou mesures prises pour atténuer ou résoudre l'incident. Le rapport post-incident peut contenir des informations qui peuvent être utilisées pour réduire le risque de récurrence d'un incident ou pour améliorer la gestion d'un futur incident similaire. Le rapport publié après l'incident n'est pas une analyse des causes premières (RCA). Vous pouvez demander un complément RCA au rapport post-incident. Un exemple de rapport post-incident est fourni dans la section suivante.

### Important

Le modèle de rapport suivant n'est qu'un exemple.

#### **Post \*\* Incident \*\* Report \*\* Template**

**Post Incident Report** - 0000000123

**Customer:** Example Customer

**AWS Support case ID(s):** 0000000000

**Customer internal case ID (if provided):** 1234567890

**Incident start:** 2023-02-04T03:25:00 UTC

**Incident resolved:** 2023-02-04T04:27:00 UTC

**Total Incident time:** 1:02:00 s

**Source Alarm ARN:** arn:aws:cloudwatch:us-east-1:000000000000:alarm:alarm-prod-workload-impaired-useast1-P95

#### **Problem Statement:**

Outlines impact to end users and operational infrastructure impact.

Starting at 2023-02-04T03:25:00 UTC, the customer experienced a large scale outage of their workload that lasted one hour and two minutes and spanning across all Availability Zones where the application is deployed. During impact, end users were unable to connect to the workload's Application Load Balancers (ALBs) which service inbound communications to the application.

#### **Incident Summary:**

Summary of the incident in chronological order and steps taken by AWS Incident Managers to direct the incident to a path to mitigation.

At 2023-02-04T03:25:00 UTC, the workload impairments alarm triggered a critical incident for the workload. AWS Incident Detection and Response Managers responded to the alarm, checking AWS service health and steps outlined in the workload's runbook.

At 2023-02-04T03:28:00 UTC, \*\* per the runbook, the alarm had not recovered and the Incident Management team sent the engagement email to the customer's Site Reliability

Team (SRE) team, created a troubleshooting bridge, and an AWS Support support case on behalf of the customer.

At 2023-02-04T03:32:00 UTC, \*\* the customer's SRE team, and AWS Support Engineering joined the bridge. The Incident Manager confirmed there was no on-going AWS impact to services the workload depends on. The investigation shifted to the specific resources in the customer account.

At 2023-02-04T03:45:00 UTC, the Cloud Support Engineer discovered a sudden increase in traffic volume was causing a drop in connections. The customer confirmed this ALB was a newly provisioned to handle an increase in workload traffic for an on-going promotional event.

At 2023-02-04T03:56:00 UTC, the customer instituted back off and retry logic. The Incident Manager worked with the Cloud Support Engineer to raise an escalation a higher support level to quickly scale the ALB per the runbook.

At 2023-02-04T04:05:00 UTC, ALB support team initiates scaling activities. The back-off/retry logic yields mild recovery but timeouts are still being seen for some clients.

By 2023-02-04T04:15:00 UTC, scaling activities complete and metrics/alarms return to pre-incident levels. Connection timeouts subside.

At 2023-02-04T04:27:00 UTC, per the runbook the call was spun down, after 10 minutes of recovery monitoring. Full mitigation is agreed upon between AWS and the customer.

**Mitigation:**

Describes what was done to mitigate the issue. NOTE: this is not an Root Cause Analysis (RCA).

Back-off and retries yielded mild recovery. Full mitigation happened after escalation to ALB support team (per runbook) to scale the newly provisioned ALB.

**Follow up action items (if any):**

Action items to be reviewed with your Technical Account Manager (TAM), if required. Review alarm thresholds to engage AWS Incident Detection and Response closer to the time of impact.

Work with AWS Support and TAM team to ensure newly created ALBs are pre-scaled to accommodate expected spikes in workload traffic.

## Fournir un accès aux équipes chargées des applications

AWS Incident Detection and Response communique avec vous via AWS Support cas survenus au cours du cycle de vie d'un incident. Pour correspondre avec les responsables des incidents, vos équipes doivent avoir accès au AWS Support Centre.

Pour plus d'informations sur le provisionnement de l'accès, voir [Gérer l'accès à AWS Support Centre](#) dans le AWS Support Guide de l'utilisateur.

# Gestion des incidents pour les événements de service

AWS La fonction de détection et de réponse aux incidents vous informe d'un événement de service en cours dans votre AWS Région, que votre charge de travail soit affectée ou non. Au cours d'une AWS événement de service, AWS Incident Detection and Response crée un AWS Support, rejoint votre passerelle de conférence téléphonique pour recevoir des commentaires sur l'impact et le sentiment, et fournit des conseils pour invoquer vos plans de relance pendant l'événement. Vous recevez également une notification via AWS Health contenant les détails de l'événement. Les clients qui ne sont pas concernés par le AWS événement de service propre (par exemple, opération dans un autre AWS Région, n'utilisez pas le AWS service altéré, etc.) continuent d'être pris en charge par l'engagement standard. Pour plus d'informations sur AWS Health, voir [Qu'est-ce que AWS Health?](#).

Publier un rapport d'incident pour les événements de service (si demandé) : si un événement de service est à l'origine d'un incident, vous pouvez demander à AWS Incident Detection and Response de procéder à un examen après l'incident et de générer un rapport post-incident. Le rapport post-incident relatif aux événements de service inclut les éléments suivants :

- Description du problème
- L'impact de l'incident
- Informations partagées sur le AWS Health tableau de bord
- Les équipes impliquées lors de l'incident
- Solutions de contournement et mesures prises pour atténuer ou résoudre l'incident

Le rapport post-incident relatif aux événements de service peut contenir des informations qui peuvent être utilisées pour réduire le risque de récurrence d'un incident ou pour améliorer la gestion d'un futur incident similaire. Le rapport publié après l'incident pour les événements de service n'est pas une analyse des causes premières (RCA). Vous pouvez demander un complément RCA au rapport post-incident pour les événements de service.

Voici un exemple de rapport post-incident relatif à un événement de service :

## Note

Le modèle de rapport suivant n'est qu'un exemple.

**Post Incident Report - LSE000123****Customer:** Example Customer**AWS Support Case ID(s):** 0000000000**Incident Start: Example:** 1 January 2024, 3:30 PM UTC**Incident Resolved: Example:** 1 January 2024, 3:30 PM UTC**Incident Duration:** 1:02:00**Service(s) Impacted:** Lists the impacted services such as EC2, ALB**Region(s):** Lists the impacted AWS Regions, such as US-EAST-1**Alarm Identifiers:** Lists any customer alarms that triggered during the Service Level Event**Problem Statement:**

Outlines impact to end users and operational infrastructure impact during the Service Level Event.

Starting at 2023-02-04T03:25:00 UTC, the customer experienced a service outage...

**Impact Summary for Service Level Event:**

(This section is limited to approved messaging available on the AWS Health Dashboard)

Outline approved customer messaging as provided on the AWS Health Dashboard.

Between 1:14 PM and 4:33 PM UTC, we experienced increased error rates for the Amazon SNS Publish, Subscribe, Unsubscribe, Create Topic, and Delete Topic APIs in the EU-WEST-1 Region. The issue has been resolved and the service is operating normally.

**Incident Summary:**

Summary of the incident in chronological order and steps taken by AWS Incident Managers during the Service Level Event to direct the incident to a path to mitigation.

At 2024-01-04T01:25:00 UTC, the workload alarm triggered a critical incident...

At 2024-01-04T01:27:00 UTC, customer was notified via case 0000000000 about the triggered alarm

At 2024-01-04T01:30:00 UTC, IDR team identified an ongoing service event which was related to the customer triggered alarm

At 2024-01-04T01:32:00 UTC, IDR team sent an impact case correspondence requesting for the incident bridge details

At 2024-01-04T01:32:00 UTC, customer provided the incident bridge details

At 2024-01-04T01:32:00 UTC, IDR team joined the incident bridge and provided information about the ongoing service outage

By 2024-01-04T02:35:00 UTC, customer failed over to the secondary region (EU-WEST-1) to mitigate impact...

At 2024-01-04T03:27:00 UTC, customer confirmed recovery, the call was spun down...

**Mitigation:**

Describes what was done to mitigate the issue. NOTE: this is not an Root Cause Analysis (RCA).

Back-off and retries yielded mild recovery. Full mitigation happened ...

**Follow up action items (if any):**

Action items to be reviewed with your Technical Account Manager (TAM), if required.

Review alarm thresholds to engage AWS Incident Detection and Response closer ...

Work with AWS Support and TAM team to ensure ...

## Demande de réponse à un incident

Si un incident critique survient sur votre charge de travail et n'est pas détecté par les alarmes surveillées par AWS Incident Detection and Response, vous pouvez créer un dossier d'assistance pour demander une réponse aux incidents. Vous pouvez demander une réponse aux incidents pour toute charge de travail abonnée à AWS Incident Detection and Response, y compris les charges de travail en cours d'intégration.

Pour demander une réponse à un incident ayant un impact actif sur votre charge de travail, créez un AWS Support Affaire. Une fois le dossier d'assistance déposé, AWS Incident Detection and Response vous contactera sur une passerelle de conférence avec le AWS experts nécessaires pour accélérer le rétablissement de votre charge de travail.

Demandez une réponse à un incident à l'aide du AWS Support Center Console

1. Ouvrez le fichier [AWS Support Center Console](#), puis choisissez Create case.
2. Choisissez Technique.
3. Pour Service, choisissez Incident Detection and Response.
4. Dans Catégorie, choisissez Incident actif.
5. Pour Severity, choisissez Business-critical system down.
6. Entrez un sujet pour cet incident. Par exemple :

AWSDétection et réponse aux incidents - Incident actif - workload\_name

7. Entrez la description du problème pour cet incident. Ajoutez les informations suivantes :
  - Informations techniques :

Service (s) concerné (s) :

Ressource (s) affectée (s) :

Région (s) affectée (s) :

Nom de la charge de travail :

- Informations commerciales :

Description de l'impact sur l'entreprise :

[Facultatif] Détails du pont client :

8. Dans la section Contacts supplémentaires, entrez les adresses e-mail auxquelles vous souhaitez recevoir des correspondances concernant cet incident.

L'illustration suivante montre l'écran de la console avec le champ Contacts supplémentaires surligné.

9. Sélectionnez Envoyer.

Après avoir soumis une demande de réponse aux incidents, vous pouvez ajouter des adresses e-mail supplémentaires provenant de votre organisation. Pour ajouter des adresses supplémentaires, répondez au dossier, puis ajoutez les adresses e-mail dans la section Contacts supplémentaires.

L'illustration suivante montre l'écran des détails du dossier avec le bouton Répondre surligné.

L'illustration suivante montre le dossier Répondre avec le champ Contacts supplémentaires et le bouton Soumettre surlignés.

- 10 AWS Incident Detection and Response accuse réception de votre dossier dans les cinq minutes et vous contacte sur une passerelle de conférence avec les personnes appropriées AWS experts.

Demandez une réponse à un incident à l'aide du AWS Support API

Support : les dossiers de support peuvent être créés par programmation à l'aide du [AWS Support API](#).

## Demandez une réponse à un incident à l'aide du AWS Support App in Slack

1. Ouvrez le canal Slack que vous avez configuré AWS Support App in Slack dans.
2. Entrez la commande suivante :

```
/awssupport create
```

3. Entrez un sujet pour cet incident. Par exemple, entrez AWS Incident Detection and Response - Active Incident - workload\_name.
4. Entrez la description du problème pour cet incident. Ajoutez les informations suivantes :

Informations techniques :

Service (s) concerné (s) :

Ressource (s) affectée (s) :

Région (s) affectée (s) :

Nom de la charge de travail :

Informations commerciales :

Description de l'impact sur l'entreprise :

[Facultatif] Détails du pont client :

5. Choisissez Suivant.
6. Dans Type de problème, choisissez Support technique.
7. Pour Service, choisissez Incident Detection and Response.
8. Dans Catégorie, choisissez Incident actif.
9. Pour Severity, choisissez Business-critical system down.
10. Pour la méthode de contact, choisissez les notifications par e-mail et Slack.

 Note

AWS La fonction de détection et de réponse aux incidents ne prend pas en charge le chat en direct dans Slack. Si vous sélectionnez cette option, vous constaterez un retard dans les réponses à votre demande de réponse aux incidents.

11. Vous pouvez configurer des contacts supplémentaires auxquels vous souhaitez recevoir des copies des courriers électroniques concernant cet incident.
12. Choisissez Examiner.
13. Un nouveau message qui n'est visible que par vous apparaît dans la chaîne Slack. Vérifiez les détails du dossier, puis choisissez Créer un dossier.
14. Votre numéro de dossier est fourni dans un nouveau message du AWS Support App in Slack.
15. Incident Detection and Response accuse réception de votre dossier dans les cinq minutes et vous contacte sur une passerelle de conférence avec les personnes appropriées AWS experts.
16. La correspondance provenant de Incident Detection and Response est mise à jour dans le fil de discussion du dossier.

# AWS Application de support dans Slack

AWS Les clients peuvent utiliser le [AWS Support App in Slack](#) pour gérer leur AWS Support cas dans Slack.

AWS Les clients de la détection et de la réponse aux incidents peuvent utiliser le AWS Support App in Slack pour recevoir des notifications concernant de nouveaux [incidents déclenchés par une alarme](#) sur leur charge de travail, ou pour créer une [demande de réponse aux incidents](#).

Pour configurer le AWS Support App in Slack, suivez les instructions fournies dans le [AWS Support Guide de l'utilisateur](#).

## Important

- Lorsque vous mettez à jour ou créez un dossier de Support avec AWS Détection et réponse aux incidents par le biais du AWS Support App in Slack, vous devez choisir la méthode de contact par e-mail et notifications Slack.

AWS Incident Detection and Response prend en charge uniquement la correspondance par e-mail concernant les dossiers de support. Le chat en direct n'est pas pris en charge.

- Pour être sûr de recevoir des notifications dans Slack pour tous les incidents déclenchés par une alarme sur votre charge de travail, vous devez configurer le AWS Support App in Slack pour tous les comptes de votre charge de travail intégrés à AWS Détection et réponse aux incidents. Support : les dossiers de support sont créés dans le compte d'origine de l'alarme de charge de travail.
- Plusieurs dossiers de support très sévères peuvent être ouverts en votre nom lors d'un incident pour engager AWS Support résolveurs. Vous recevez des notifications dans Slack pour tous les dossiers d'assistance ouverts lors d'un incident qui correspondent à votre [configuration de notification pour le canal Slack](#).
- Les notifications que vous recevez par le biais du AWS Support App in Slack ne remplacent pas les contacts initiaux et d'escalade de votre charge de travail qui sont contactés par e-mail ou par téléphone par AWS Détection des incidents et réponse lors d'un incident.

# Notifications d'incidents déclenchées par une alarme dans Slack

Lorsque l'application AWS Support de Slack est configurée sur votre chaîne Slack, vous êtes averti des incidents déclenchés par des alarmes sur votre AWS charge de travail surveillée par la détection et la réponse aux incidents.

L'exemple suivant montre comment les notifications relatives aux incidents déclenchés par une alarme apparaissent dans Slack.

## Exemple de notification

Lorsque l'incident déclenché par votre alarme est reconnu par AWS Incident Detection and Response, une notification similaire à celle ci-dessous est générée dans Slack :

Pour consulter l'intégralité de la correspondance ajoutée par AWS Incident Detection and Response, choisissez [Voir les détails](#).

D'autres mises à jour relatives à la détection et à la réponse aux AWS incidents apparaissent dans le fil de discussion de l'affaire.

Choisissez [Voir les détails](#) pour afficher l'intégralité de la correspondance ajoutée par AWS Incident Detection and Response.

## Demandes de réponse aux incidents dans Slack

Pour savoir comment créer une demande de réponse aux incidents via l'application AWS Support de Slack, consultez la section [Demandes de réponse aux incidents](#).

# Rapports de détection et de réponse aux incidents AWS

Incident Detection and Response fournit des données opérationnelles et de performance pour vous aider à comprendre comment le service est configuré, l'historique de vos incidents et les performances du service de détection et de réponse aux incidents.

## Données de configuration

- Tous les comptes sont intégrés
- Noms de toutes les applications
- Les alarmes, les runbooks et les profils de support associés à chaque application

## Données relatives aux incidents

- Les dates, le nombre et la durée des incidents pour chaque application
- Les dates, le nombre et la durée des incidents associés à une alarme spécifique
- Rapport postérieur à l'incident

## Données de performance

- Performances liées aux objectifs de niveau de service (SLO)

Contactez votre responsable de compte technique pour obtenir les données opérationnelles et de performance dont vous pourriez avoir besoin.

# Sécurité et résilience de la détection et de la réponse aux incidents

Le [modèle de responsabilité partagée](#) d'AWS s'applique à la protection des données dans AWS Support. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur cette infrastructure relève de votre responsabilité. Ce contenu inclut la configuration de la sécurité et les tâches de gestion pour le Services AWS produit que vous utilisez.

Pour plus d'informations sur la confidentialité des données, consultez les [FAQ sur la confidentialité des données](#).

Pour plus d'informations sur la protection des données en Europe, consultez le [modèle de responsabilité AWS partagée et le billet de blog sur le RGPD](#) sur le blog sur la AWS sécurité.

Pour des raisons de protection des données, nous vous recommandons de protéger les informations d'identification des AWS comptes et de configurer des comptes utilisateur individuels avec AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez les certificats SSL/TLS (Secure Sockets Layer/Transport Layer Security) pour communiquer avec les ressources. AWS Nous recommandons TLS 1.2 ou version ultérieure. Pour plus d'informations, voir [Qu'est-ce qu'un certificat SSL/TLS ?](#).
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations, veuillez consulter [AWS CloudTrail](#).
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut au sein AWS des services. Pour plus d'informations, consultez la section [Services et outils AWS cryptographiques](#).
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données personnelles stockées dans Amazon S3. Pour plus d'informations sur Amazon Macie, consultez Amazon [Macie](#).
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS.

Pour plus d'informations sur les points de terminaison FIPS disponibles, consultez la [norme fédérale de traitement de l'information \(FIPS\) 140-2](#).

Nous vous recommandons vivement de ne jamais placer d'informations confidentielles ou sensibles, telles que des adresses électroniques de vos clients, dans des balises ou des champs de forme libre tels qu'un champ Nom. Cela inclut lorsque vous travaillez avec AWS Support ou d'autres utilisateurs de la Services AWS console, de l'API, de la AWS CLI ou AWS des SDK. Toutes les données que vous saisissez dans des identifications ou des champs de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

## Accès à vos comptes via AWS Incident Detection and Response

AWS Identity and Access Management (IAM) est un service Web qui vous permet de contrôler en toute sécurité l'accès aux AWS ressources. Vous pouvez utiliser IAM pour contrôler les personnes qui s'authentifient (sont connectées) et sont autorisées (disposent d'autorisations) à utiliser des ressources.

## AWS Incident Detection and Response et vos données d'alarme

Par défaut, Incident Detection and Response reçoit le nom de la ressource Amazon (ARN) et l'état de chaque CloudWatch alarme de votre compte, puis lance le processus de détection et de réponse aux incidents lorsque votre alarme intégrée passe à l'état ALARM. Si vous souhaitez personnaliser les informations que la détection et la réponse aux incidents reçoivent concernant les alarmes provenant de votre compte, contactez votre responsable technique de compte.

# Historique du document

Le tableau suivant décrit les modifications importantes apportées à la documentation depuis la dernière version du IDR guide.

- Dernière mise à jour de la documentation : 12 juin 2024

| Modification   | Description  | Date              |
|--|--|-------------------|
| Ajout d'une nouvelle page AWS Support App in Slack                               | Ajout d'une nouvelle page pour AWS Support App in Slack  | 10 septembre 2024 |
| Gestion des incidents actualisée avec détection et réponse aux AWS incidents     | Gestion des incidents mise à jour avec détection et réponse aux AWS incidents pour ajouter une nouvelle section intitulée « Demander une réponse aux incidents à l'aide du AWS Support App in Slack ».   |                   |
| Abonnement au compte mis à jour  | La section d'abonnement au compte a été mise à jour pour inclure des informations sur l'endroit où ouvrir un dossier d'assistance lorsque vous demandez à créer un compte.<br><br>Section mise à jour : <a href="#">Abonnement au compte</a>                                     | 12 juin 2024      |
| Le rapport post-incident pour les événements de service est désormais disponible | Mise à jour de la section Gestion des incidents pour les événements de service afin d'inclure des informations sur le rapport post-incident relatif aux événements de service.<br><br>Section mise à jour : <a href="#">Gestion des incidents pour les événements de service</a> | 8 mai 2024        |
| Ajout d'une nouvelle section : Décharger une charge de travail                   | Ajout de la section Décharger une charge de travail dans Getting started pour inclure des informations sur le déchargement des charges de travail  | 28 mars 2024      |

| Modification  | Description  | Date            |
|---|--|-----------------|
|   | Pour plus d'informations, voir <a href="#">Décharger une charge</a> de travail.  |                 |
| Abonnement au compte mis à jour                                       | Mise à jour de la section d'abonnement au compte pour inclure des informations sur les charges de travail liées au désenclavement<br><br>Pour plus d'informations, voir <a href="#">Abonnement au compte</a>   | 28 mars 2024    |
| Tests mis à jour  | La section Tests a été mise à jour pour inclure des informations sur les tests effectués les jours de jeu, comme dernière étape du processus d'intégration.<br><br>Section mise à jour : <a href="#">Testez les charges de travail intégrées</a>   | 29 février 2024 |
| Mise à jour de ce qu'est la détection et la réponse aux AWS incidents | Mise à jour de la section Qu'est-ce que la détection et la réponse aux AWS incidents ?<br><br>Section mise à jour : <a href="#">Qu'est-ce qu'AWS Incident Detection and Response ?</a>   | 19 février 2024 |
| Section du questionnaire mise à jour                                  | Mise à jour du questionnaire d'intégration de la charge de travail et ajout du questionnaire d'ingestion des alarmes. La section a été renommée, passant du questionnaire d'intégration aux questionnaires d'intégration de la charge de travail et d'ingestion des alarmes.<br><br>Section mise à jour : <a href="#">Questionnaires d'intégration des charges de travail et d'ingestion d'alarmes</a> | 2 février 2024  |

| Modification   | Description   | Date             |
|--|---|------------------|
| Mis à jour AWS Informations sur le service, l'événement et l'intégration | <p>Plusieurs sections ont été mises à jour avec de nouvelles informations pour l'intégration.</p> <p>Sections mises à jour :</p> <ul style="list-style-type: none"><li>• <a href="#">Gestion des incidents pour les événements de service</a></li><li>• <a href="#">Découverte de la charge</a></li><li>• <a href="#">Intégration</a></li><li>• <a href="#">Abonnement au compte</a></li></ul> <p>Nouvelles sections</p> <ul style="list-style-type: none"><li>• <a href="#">Fournir un accès aux équipes chargées des applications</a></li></ul> | 31 janvier 2024  |
| Ajout d'une section d'informations connexes                              | <p>Ajout d'une section d'informations connexes dans le provisionnement des accès.</p> <p>Section mise à jour : <a href="#">Fournir un accès pour l'ingestion des alertes à la détection et à la réponse aux incidents</a></p>   | 17 janvier 2024  |
| Exemples d'étapes mis à jour   | <p>Mise à jour de la procédure pour les étapes 2, 3 et 4 dans Exemple : intégration des notifications de Datadog et Splunk.</p> <p>Section mise à jour : <a href="#">Exemple : intégrer les notifications de Datadog et Splunk</a></p>  | 21 décembre 2023 |

| Modification                                 | Description  | Date              |
|--|--|-------------------|
| Graphisme et texte d'introduction mis à jour | <p>Graphique mis à jour dans les alarmes Ingest à partir APMs d'une intégration directe avec Amazon EventBridge.</p> <p>Section mise à jour : <a href="#">Développez des runbooks pour la détection et la réponse aux AWS incidents</a></p>  | 21 décembre 2023  |
| Modèle de runbook mis à jour                 | <p>Le modèle de manuel a été mis à jour dans Développement de livres d'exécution pour la détection et la AWS réponse aux incidents.</p> <p>Section mise à jour : <a href="#">Développez des runbooks pour la détection et la réponse aux AWS incidents</a></p>   | 4 décembre 2023   |
| Configurations d'alarme actualisées          | <p>Configurations d'alarme mises à jour avec des informations détaillées sur la configuration des CloudWatch alarmes.</p> <p>Nouvelle section : <a href="#">Créez des CloudWatch alarmes adaptées aux besoins de votre entreprise en matière de détection et de réponse aux incidents</a></p> <p>Nouvelle section : <a href="#">Utiliser AWS CloudFormation modèles pour créer des CloudWatch alarmes dans Incident Detection and Response</a></p> <p>Nouvelle section : <a href="#">Exemple de cas d'utilisation d' CloudWatch alarmes dans le cadre de la détection et de la réponse aux incidents</a></p> | 28 septembre 2023 |

| Modification                          | Description   | Date              |
|---------------------------------------|---|-------------------|
| Mise à jour : mise en route           | Mise à jour de Getting Started avec des informations sur les demandes de modification de la charge de travail<br><br>Nouvelle section : <a href="#">Demander des modifications à une charge de travail intégrée</a><br><br>Section mise à jour : <a href="#">Abonnement au compte</a> | 05 septembre 2023 |
| Nouvelle section dans Getting Started | Ajout <a href="#">Intégrez les alertes à la détection et à la réponse aux AWS incidents</a> d'alertes d'ingestion dans la détection et la réponse aux AWS incidents.  | 30 juin 2023      |
| Document original                     | AWS Détection et réponse aux incidents publiés pour la première fois  | 15 mars 2023      |

# AWS Glossaire

Pour la AWS terminologie la plus récente, consultez le [AWS glossaire](#) dans la Glossaire AWS référence.

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.