Concepts et procédures de détection et de réponse aux incidents AWS

Guide de l'utilisateur d'AWS pour la détection et la réponse aux incidents

Version May 12, 2026

Guide de l'utilisateur d'AWS pour la détection et la réponse aux incidents: Concepts et procédures de détection et de réponse aux incidents AWS

Table of Contents

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.

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 corréler 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 ingénieurs de gestion des incidents vous contactent de manière proactive dans les 5 minutes suivant une alarme, concernant vos charges de travail ou en réponse à un cas critique que vous soumettez.
- Résolution plus rapide : les IME utilisent des runbooks prédéfinis et personnalisés développés pour vos charges de travail, créent un dossier de support en votre nom et gèrent 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.
- 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 manuels d'exécution. Vous pouvez également tirer parti AWS Resilience Hub du suivi continu de la résilience de vos charges de travail.

Rubriques

Conditions d'utilisation relatives à la détection et à la réponse aux incidents

La liste suivante décrit les principales exigences et limites relatives à l'utilisation d'AWS Incident Detection and Response. Il est important que vous compreniez ces informations avant d'utiliser le service, car elles couvrent des aspects tels que les exigences du plan de support, le processus d'intégration et la durée minimale d'abonnement.

- AWS Incident Detection and Response est disponible pour les comptes de support direct et Partner-resold d'entreprise.
- 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. Toutes les demandes d'annulation doivent être soumises 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.

Architecture de détection et de réponse aux incidents

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 des informations sur vos charges de travail, notamment les détails de l'architecture des charges de travail, les détails des alarmes et les runbooks 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.

Rôles et responsabilités en matière de détection et de réponse aux incidents

Le tableau RACI (Responsible, Accountable, Consulted, and Informed) d'AWS relatif à la détection et à la réponse aux incidents décrit les rôles et les responsabilités des différentes activités liées à la détection et à la réponse aux incidents. Ce tableau permet de définir l'implication du client et de l'équipe de détection et de réponse aux incidents d'AWS pour des tâches telles que la collecte de

données, l'examen de l'état de préparation des opérations, la configuration du compte, la gestion des incidents et l'examen post-incident.

Activité	Client	Détection et réponse aux incidents
Collecte de données		
Présentation du client et de la charge de travail	Consulté	Responsable
Architecture	Responsable	Responsable
Opérations	Responsable	Responsable
Déterminer les CloudWatch alarmes à configurer	Responsable	Responsable
Définir le plan de réponse aux incidents	Responsable	Responsable
Examen du niveau de préparation des opérations		
Réaliser un examen bien architectural (WAR) de la charge de travail	Consulté	Responsable
Valider la réponse aux incidents	Consulté	Responsable
Valider la matrice d'alarme	Consulté	Responsable
Identifier les principaux AWS services utilisés par la charge de travail	Responsable	Responsable

Activité	Client	Détection et réponse aux incidents
Configuration du compte		
Créer un rôle IAM dans le compte client	Responsable	Informé
Installer une EventBridge règle gérée à l'aide du rôle créé	Informé	Responsable
CloudWatch Alarmes de test	Responsable	Responsable
Vérifiez que les alarmes des clients déclenchent la détection et la réponse aux incidents	Informé	Responsable
Actualiser les alarmes	Responsable	Consulté
Mettre à jour les runbooks	Consulté	Responsable
Gestion des incidents		
Notifier de manière proactive les incidents détectés par Incident Detection and Response	Informé	Responsable
Fournir une réponse aux incidents	Informé	Responsable
Assurer la résolution des incidents/la restauration de l'infrastructure	Responsable	Consulté
Post-incident examen		

Activité	Client	Détection et réponse aux incidents
Demander un examen après un incident	Responsable	Informé
Fournir un examen après l'incident	Informé	Responsable

Disponibilité des régions pour la détection et la réponse aux incidents

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

Région AWS	Nom
Région USA Est (Virginie du Nord)	us-east-1
Région USA Est (Ohio)	us-east-2
Région US West (N. California)	us-west-1
Région USA Ouest (Oregon)	us-west-2
Région Canada (Centre)	ca-central-1
Région Canada Ouest (Calgary)	ca-west-1
Région Amérique du Sud (São Paulo)	sa-east-1
Région Europe (Francfort)	eu-central-1

Région AWS	Nom
Région Europe (Irlande)	eu-west-1
Région Europe (Londres)	eu-west-2
Région Europe (Paris)	eu-west-3
Région Europe (Stockholm)	eu-north-1
Région Europe (Zurich)	eu-central-2
Europe (Milan) Region	eu-south-1
Région Europe (Espagne)	eu-south-2
Asie-Pacifique (Mumbai)	ap-south-1
Asie-Pacifique (Tokyo)	ap-northeast-1
Asie-Pacifique (Séoul)	ap-northeast-2
Asie-Pacifique (Singapour)	ap-southeast-1
Asie-Pacifique (Sydney)	ap-southeast-2
Asie-Pacifique (Hong Kong)	ap-east-1
Asie-Pacifique (Osaka)	ap-northeast-3
Asie-Pacifique (Hyderabad)	ap-south-2
Asie-Pacifique (Jakarta)	ap-southeast-3
Asie-Pacifique (Melbourne)	ap-southeast-4
Asie-Pacifique (Malaisie)	ap-southeast-5
Afrique (Le Cap)	af-south-1
Israël (Tel Aviv)	il-central-1

Région AWS	Nom
Moyen-Orient (EAU)	me-central-1
Moyen-Orient (Bahreïn)	me-south-1
AWS GovCloud (US-East)	us-gov-east-1
AWS GovCloud (US-West)	us-gov-west-1

Commencez avec la détection et la réponse aux incidents

Les charges de travail et les alarmes sont au cœur de la détection et de la réponse aux incidents d'AWS. AWS travaille en étroite collaboration avec vous pour définir et surveiller les charges de travail spécifiques qui sont essentielles pour votre entreprise. AWS vous aide à configurer des alarmes qui signalent à votre équipe des problèmes de performance importants ou de l'impact sur les clients. Des alarmes correctement configurées sont essentielles pour une surveillance proactive et une réponse rapide aux incidents dans le cadre de la détection et de la réponse aux incidents.

À propos des charges de travail dans Incident Detection and Response

Vous pouvez sélectionner des charges de travail spécifiques pour la surveillance et la gestion des incidents critiques à l'aide d'AWS Incident Detection and Response. Une charge de travail est un ensemble de ressources et de code qui fonctionnent ensemble pour apporter de la 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 unique Compte AWS ou multiple Comptes AWS.

Par exemple, vous pouvez avoir une application monolithique hébergée sur un seul compte (par exemple, Employee Performance App dans le schéma suivant). Il se peut également qu'une application (par exemple, Storefront Webapp dans le schéma) 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 le schéma suivant.

Pour commencer à intégrer les charges de travail, consultezIntégrez les charges de travail à la détection et à la réponse aux incidents.

À propos des alarmes dans Incident Detection and Response

Les alarmes sont un élément clé de la détection et de la réponse aux incidents. Les alarmes fournissent une visibilité sur les performances de vos applications et de AWS l'infrastructure sous-jacente. AWS travaille avec vous pour définir les mesures appropriées et les seuils d'alarme qui ne se déclenchent qu'en cas d'impact critique sur vos charges de travail surveillées. L'objectif est que les alarmes engagent les résolveurs que vous avez spécifiés, qui collaborent ensuite avec l'équipe de gestion des incidents pour atténuer rapidement les problèmes. Configurez vos alarmes pour

qu'elles n'entrent en état d'alarme qu'en cas de dégradation significative des performances ou de l'expérience client nécessitant une attention immédiate. Parmi les principaux types d'alarmes, citons celles qui indiquent l'impact commercial, CloudWatch les canaries Amazon et les alarmes agrégées qui surveillent les dépendances.

Pour commencer avec l'ingestion d'alarmes, voirIngestion d'alarmes.

Intégrez les charges de travail à la détection et à la réponse aux incidents

AWS Incident Detection and Response permet de surveiller et de gérer les incidents critiques pour les charges de travail que vous avez sélectionnées. Une charge de travail est un ensemble de ressources travaillant ensemble pour apporter de la valeur commerciale, comme un portail de paiement ou un système de gestion de la relation client (CRM). Vous pouvez héberger ces charges de travail sur un seul compte Compte AWS ou les répartir sur plusieurs comptes, en fonction de votre architecture.

Table des matières

Intégration à la détection et à la réponse aux incidents avec la CLI IDR

L'interface de ligne de commande client (IDR CLI) AWS Incident Detection and Response est un outil d'interface de ligne de commande qui rationalise l'intégration à AWS Incident Detection and Response.

La CLI IDR s'exécute AWS CloudShell pour exécuter les fonctions suivantes :

- Collectez les informations d'intégration
- Collectez AWS des données sur les ressources via l'API Resource Groups Tagging
- Gérez les AWS Support dossiers
- Créez de nouvelles CloudWatch alarmes Amazon ou ingérez vos alarmes existantes
- Déployez et testez l'infrastructure AWS CloudFormation pour permettre à des outils tiers d'envoyer des alertes à la détection et à la réponse aux incidents.

La CLI IDR peut fonctionner en mode interactif pour vous guider tout au long des étapes d'intégration, ou en mode hors ligne pour les cas groupés ou DevOps d'utilisation.

Pour plus d'informations sur l'utilisation de la CLI IDR, notamment sur l'installation, les conditions requises et des exemples de bout en bout, consultez la section CLI pour AWS Incident Detection and Response.

Support linguistique pour la CLI IDR

AWS Incident Detection and Response est disponible en anglais, japonais, mandarin et coréen. Si vous avez besoin d'assistance en japonais, mandarin ou coréen, contactez AWS le AWS Support dossier créé par la CLI IDR ou contactez votre responsable de compte technique (TAM).

Options alternatives pour l'intégration des charges de travail

Si vous ne pouvez pas utiliser la CLI IDR pour l'intégration, consultez votre responsable de compte technique (TAM) pour d'autres options. Pour de plus amples informations, consultez Questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans Incident Detection and Response (chemin d'exception).

Ingestion d'alarmes

L'interface de ligne de commande client (IDR CLI) AWS Incident Detection and Response peut créer de nouvelles CloudWatch alarmes Amazon ou ingérer vos alarmes existantes et peut déployer et tester une infrastructure afin de permettre AWS CloudFormation à des outils tiers d'envoyer des alertes à AWS Incident Detection and Response.

AWS Incident Detection and Response peut intégrer les alarmes d'Amazon CloudWatch et d'outils tiers de surveillance des performances des applications (APM) via Amazon : EventBridge

- Ingestion d'alarmes CloudWatch
- Ingestion des alarmes de surveillance des performances des applications tierces

Étapes pour l'ingestion d'une alarme

Les étapes suivantes doivent être effectuées pour l'ingestion d'une alarme :

- Définition de l'alarme

- Ingestion des alarmes à l'aide de la CLI IDR
- Révision des alarmes et commentaires
- Fournir un accès pour l'ingestion des alarmes à la détection et à la réponse aux incidents
- Test des alarmes (Gameday)
- Les alarmes sont activées pour une surveillance active par AWS Incident Detection and Response une fois les étapes précédentes terminées.

Options alternatives pour l'ingestion des alarmes

Si vous ne pouvez pas utiliser la CLI IDR pour l'ingestion d'alarmes, consultez votre responsable de compte technique (TAM) pour d'autres options. Pour de plus amples informations, consultez Questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans Incident Detection and Response (chemin d'exception).

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

> **Note**
>
> Si vous n'avez pas créé le rôle lié au service (SLR) lors de l'intégration de la CLI IDR, suivez les étapes ci-dessous pour octroyer manuellement l'accès.

Pour permettre à AWS Incident Detection and Response d'intégrer les alarmes de votre compte, créez le `AWSServiceRoleForHealth_EventProcessor` SLR. AWS suppose que le SLR crée une EventBridge règle gérée dans votre compte. La EventBridge règle gérée envoie des notifications depuis votre compte à AWS Incident Detection and Response. Pour plus d'informations sur ce SLR, y compris la politique AWS gérée associée, consultez la section Utilisation des rôles liés à un service dans le Guide de l'utilisateur.

Vous pouvez créer ce rôle lié à un service dans votre compte en suivant les instructions de la section Créer un rôle lié à un service dans le Guide de l'utilisateur.Gestion des identités et des accès AWS Vous pouvez également utiliser la commande suivante AWS Command Line Interface (AWS CLI) :

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

Principaux résultats

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

> **Note**
>
> Le rôle lié au service - AWSServiceRoleForHealth _ EventProcessor doit être créé dans chaque compte que vous utiliserez pour envoyer des alarmes à AWS Incident Detection and Response.

Informations connexes

Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation des rôles liés à un service pour
- Création d'un rôle lié à un service
- AWS politique gérée : AWS Health_EventProcessorServiceRolePolicy

Définition de l'alarme

Lorsque vous intégrez vos alarmes à AWS Incident Detection and Response, vous êtes chargé de définir les métriques et les configurations d'alarme qui fournissent une visibilité sur les performances de vos applications. Dans le cadre de ce processus, vous devez également identifier les équipes de votre organisation chargées de répondre à ces alarmes.

Lors de la préparation des alarmes, nous recommandons les meilleures pratiques suivantes :

- Les alarmes ne passent à l'état « Alarme » que lorsqu'elles ont un impact critique continu sur votre charge de travail surveillée nécessitant une attention immédiate de la part de votre équipe et AWS. Les alarmes qui se déclenchent et ne se rétablissent pas automatiquement obligent vos équipes à rejoindre une passerelle d'incidents avec AWS Incident Detection and Response.
- Assurez-vous que les informations de contact que vous fournissez permettent à AWS Incident Detection and Response d'impliquer de manière fiable les équipes appropriées au sein de votre organisation pour résoudre un incident 24/7.

Principaux résultats

- Une liste d'alarmes et de coordonnées, que vous fournissez à AWS Incident Detection and Response à l'aide de la CLI IDR.

Pour plus d'informations sur la définition et l'ingestion des CloudWatch alarmes Amazon, consultezIngestion d'alarmes CloudWatch.

Pour plus d'informations sur l'ingestion des alarmes de surveillance des performances des applications tierces, consultezIngestion des alarmes de surveillance des performances des applications tierces.

Ingestion d'alarmes CloudWatch

AWS Incident Detection and Response peut intégrer les CloudWatch alarmes Amazon afin de fournir une surveillance proactive de vos charges de travail critiques. En ingérant vos CloudWatch alarmes Amazon à des fins de surveillance, AWS Incident Detection and Response peut :

- Détecte automatiquement lorsque vos alarmes passent à l'état « Alarme ».
- Mobilisez vos équipes pour répondre aux incidents et les résoudre de manière collaborative.

Pour garantir l'efficacité des alarmes que vous intégrez, AWS Incident Detection and Response recommande les meilleures pratiques suivantes :

- Configurez les alarmes à l'aide d'expressions mathématiques métriques pour les supprimer pendant les périodes de maintenance régulière ou d'exécution de tâches par lots afin d'éviter les déclenchements d'alarmes faussement positifs.
- Définissez le traitement des données manquantes sur les alarmes en fonction de la fréquence de livraison prévue des points de données. Par exemple, les métriques de surveillance des alarmes qui génèrent un flux continu de points de données doivent traiter les données manquantes comme des « violations » (mauvaises), car des points de données manquants peuvent indiquer un problème lié à la ressource sous-jacente surveillée. Inversement, les métriques de surveillance des alarmes qui signalent rarement des points de données, par exemple les métriques de surveillance des alarmes qui n'enregistrent les points de données qu'en cas de défaillance ou d'erreur, doivent considérer les données manquantes comme (bonnes). NotBreaching
- Définissez des alarmes qui passent à l'état « Alarme » en cas d'impact critique et continu sur votre charge de travail. Par exemple, configurez les alarmes pour qu'elles se déclenchent après le délai prévu pour remplacer automatiquement les ressources défectueuses, plutôt que lors de la détection initiale de ressources défectueuses.

- Identifiez et créez des alarmes pour des métriques personnalisées qui représentent directement l'expérience client adaptée à votre charge de travail.

Pour obtenir la liste des CloudWatch alarmes Amazon les plus courantes recommandées Services AWS, consultez les meilleures pratiques en matière de détection des incidents et de réponse aux alarmes sur AWS Re:post.

Ingestion des alarmes de surveillance des performances des applications tierces

AWS Incident Detection and Response prend en charge l'ingestion d'alarmes à partir d'outils tiers de surveillance des performances des applications (APM) via Amazon EventBridge. Cette intégration apporte de la flexibilité en ingérant des alertes APM, ce qui permet d'acheminer les événements APM via différents vers Services AWS un bus d' EventBridge événements Amazon de votre compte.

Exemples de parcours d'intégration :

- Source (APM) → AWS Service (exemple : Amazon API Gateway ou Amazon SNS) → Fonction Transform Lambda → Bus d' EventBridge événements Amazon personnalisé → Détection et réponse aux incidents AWS
- Source (APM) → Partenaire Amazon EventBridge Event Bus → Fonction Transform Lambda → Bus d'événements EventBridge Amazon personnalisé → Détection et réponse aux incidents AWS

AWS Incident Detection and Response installe une règle gérée sur le bus d'événements personnalisé afin d'ingérer les alertes qui lui sont envoyées par Transform Lambda Functions. Il est important de noter que pour les EventBridge intégrations Amazon SaaS, le bus d'événements du partenaire n'est pas le bus d'événements sur lequel une règle gérée est installée. Pour une liste complète des APM intégrant des partenaires à Amazon EventBridge, consultez la section Intégrations Amazon EventBridge .

Exemple d'intégration à l'aide d'un bus d'événements partenaire ou d'autres sources de bus d' AWS événements

Le schéma suivant montre un exemple d'intégration à l'aide d'un bus d'événements partenaire ou d'autres sources de bus d' AWS événements.

Pour une liste complète des APM intégrant des partenaires à Amazon EventBridge, consultez la section Intégrations Amazon EventBridge .

Exemple d'intégration à l'aide d'Amazon API Gateway

Le schéma suivant montre un exemple d'intégration à l'aide d'une API Gateway.

Exemple d'intégration à l'aide d'Amazon Simple Notification Service

Le schéma suivant montre un exemple d'intégration à l'aide d'un Amazon SNS.

Pour simplifier le processus d'intégration, AWS Incident Detection and Response fournit des CloudFormation modèles pour les types d'intégration les plus couramment utilisés. Ces modèles automatisent la configuration des AWS ressources et des rôles IAM nécessaires.

CloudFormation Vous trouverez des modèles et des instructions pour créer manuellement différents types d'intégration dans la documentation d'intégration correspondante ci-dessous :

- Ingérez les alarmes des APM grâce à l'intégration directe EventBridge
- Ingérez les alarmes des APM sans intégration directe avec EventBridge
- Ingérez les alarmes des APM grâce à l'intégration directe d'Amazon SNS

> **Note**
>
> Les CloudFormation modèles nécessitent des modifications. Ces modifications sont expliquées dans les rubriques précédentes. Pour plus d'informations sur le format de charge utile requis pour envoyer des alertes APM à AWS Incident Detection and Response, consultez. Exigences de charge utile pour l'ingestion d'alertes APM avec EventBridge

Exigences de charge utile pour l'ingestion d'alertes APM avec EventBridge

D'où proviennent les alertes APM issues de la détection et de la réponse aux incidents ?

AWS Incident Detection and Response installe une règle gérée sur le bus d'événements auquel vous envoyez votre charge utile transformée finale. Il est recommandé de créer un bus d'événements personnalisé à cette fin.

Dans quel format les charges utiles doivent-elles être utilisées ?

Les paires clé:valeur JSON minimales 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-identifier": "Your alarm name from your APM",
    }
}
```

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

Avant la 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}
 <= 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, `source` cela indique `detail-type` les détails de l'APM d'où provient l'alerte. Ceux-ci doivent être modifiés avant l'ingestion. La `incident-detection-response-identifier` clé n'est pas encore présente et doit également être ajoutée avant l'ingestion.

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

Après transformation :


```
{
    "version": "0",
    "id": "7f5e0fc1-e917-2b5d-a299-50f4735f1283",
    "detail-type": "ams.monitoring/generic-apm",
    "source": "GenericAPMEvent",
    "account": "123456789012",
    "time": "2023-10-25T14:42:25Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "incident-detection-response-identifier": "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}
 <= 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`ams.monitoring/generic-apm`, la source est maintenant`GenericAPMEvent`, et en détail, il y a une nouvelle paire clé:valeur :. `incident-detection-response-identifier`

La `incident-detection-response-identifier` valeur est extraite du nom de l'alerte en fonction de la charge utile envoyée par votre APM. Les chemins des noms d'alertes APM sont différents d'un APM à l'autre. Une fonction Lambda doit être configurée pour prendre le nom de l'alarme à partir du chemin correct dans la charge utile APM JSON reçue par Lambda et l'utiliser comme valeur. `incident-detection-response-identifier`

`incident-detection-response-identifier`les valeurs doivent être uniques par type d'alarme envoyé à AWS Incident Detection and Response. Chaque nom unique défini sur le `incident-detection-response-identifier` doit être fourni à l'équipe de détection et de réponse aux incidents d'AWS lors de l'intégration. Les événements dont la valeur de la `incident-detection-response-identifier` clé est inconnue ou manquante ne sont pas traités.

Ingérez les alarmes des APM grâce à l'intégration directe EventBridge

La rubrique suivante décrit le processus d'envoi d'alarmes à AWS Incident Detection and Response à partir d'outils de surveillance des performances des applications (APM) directement intégrés à Amazon EventBridge. Pour une liste complète des APM directement intégrés à Amazon EventBridge, consultez Amazon EventBridge integrations.

Vous pouvez déployer le CloudFormation modèle fourni ou configurer manuellement cette intégration. Avant de configurer l'intégration, vérifiez que le rôle AWS lié au service (SLR) `AWSServiceRoleForHealth_EventProcessor` est créé dans vos comptes.

Option 1 : utilisation CloudFormation

Un CloudFormation modèle est disponible pour simplifier le processus de création de l'infrastructure d'intégration requise pour intégrer les alarmes à AWS Incident Detection and Response depuis votre APM avec l'intégration Amazon EventBridge.

> **Note**
>
> - Des coûts supplémentaires sont encourus pour les ressources déployées via ce CloudFormation modèle (par exemple : Lambda et EventBridge). Pour plus d'informations sur la tarification de ces services, consultez la section AWS Tarification.
> - Déployez ce CloudFormation modèle dans tous les AWS comptes et régions dans lesquels AWS Incident Detection and Response doit d'intégrer des alarmes. Les incidents et les dossiers de support sont ouverts sur le AWS compte d'où l'alerte APM a été reçue.
> - Ce document utilise New Relic comme exemple, mais le CloudFormation modèle peut être utilisé pour n'importe quel APM intégrant le SaaS à Amazon. EventBridge
> - Après avoir testé l'intégration, supprimez les instructions logger.info () du `TransformLambdaFunction` pour empêcher la charge utile d'apparaître dans Amazon Logs. CloudWatch

Conditions préalables au déploiement de ce CloudFormation modèle :

- Une source d'événement partenaire doit être configurée sur Amazon EventBridge. Pour obtenir des instructions sur la configuration de votre APM en tant que source d'événements, consultez la section Recevoir des événements d'un partenaire SaaS d'Amazon EventBridge dans le guide de l' EventBridge utilisateur Amazon.
- La `TransformLambdaFunction` (fonction Lambda) du modèle doit être modifiée pour être définie `["detail"]["incident-detection-response-identifier"]` sur la valeur souhaitée en fonction du chemin JSON du nom de l'alerte dans la charge utile APM.

Étapes préalables :

1. Ouvrez la EventBridge console. Dans le menu Intégration, sélectionnez Sources d'événements partenaires.
   - Recherchez votre APM dans le champ Amazon EventBridge Partners.
   - Choisissez Configuration, puis suivez les instructions fournies.
     - Remarque : la dernière étape consiste à choisir Associer à Event Bus dans la console pour la source d'événements Partner. La sélection de cette option crée automatiquement un bus d'événements partenaires portant le même nom que la source d'événements partenaire (les noms doivent correspondre).
   - Copiez le nom du Partner Event Bus ou de la source. Le bus d'événements ou la source est utilisé comme paramètre, nomméPartnerEventBusNameParameter, lors du déploiement du CloudFormation modèle.
     - Exemple pour New Relic : aws.partner/newrelic.com/1234567/source_name
   - Copiez la première partie du Partner Event Bus ou de la source à saisir PartnerEventBusPrefixParameter lors du déploiement du CloudFormation modèle.
     - L'exemple de New Relic est aws.partner/newrelic.com
2. Téléchargez et modifiez le CloudFormation modèle.
   - Localisez le TransformLambdaFunction dans le modèle
   - def lambda_handler(event, context)Sous-défini sur event["detail"]["incident-detection-response-identifier"] le chemin json où le nom de l'alarme apparaît dans la charge utile JSON de l'alarme APM. Chaque APM suivra un chemin différent. Vous trouverez quelques exemples ci-dessous, mais vos charges utiles spécifiques peuvent différer.
     - Exemple de nouvelle relique :event["detail"]["incident-detection-response-identifier"] = event["detail"]["workflowName"].
     - Exemple de Datadog : event["detail"]["incident-detection-response-identifier"] = event["detail"]["meta"]["monitor"]["name"]
     - Exemple Splunk : event["detail"]["incident-detection-response-identifier"] = event["detail"]["ruleName"]
   - Enregistrez le CloudFormation modèle.

Déploiement du CloudFormation modèle :

1. Ouvrez la CloudFormation console dans votre compte cible et dans votre région.

2. Choisissez Créer une pile, avec de nouvelles ressources (standard)
   - Sélectionnez Choisir un modèle existant, Charger un fichier modèle, Choisir un fichier, puis téléchargez le CloudFormation modèle que vous avez enregistré localement.
3. Spécifiez les détails de la pile :
   - Entrez un nom de pile (Exemple :`NewRelicIntegrationForIDR`).
   - Spécifiez les valeurs des paramètres obtenues lors de la réalisation des prérequis.
     - APMNameParameter(Exemple :`NewRelic`)
     - PartnerEventBusNameParameter(Exemple :`aws.partner/newrelic.com/1234567/source_name`)
     - PartnerEventBusPrefixParameter(Exemple :`aws.partner/newrelic.com`)
   - Choisissez Suivant.
4. Configurez les options de pile :
   - Faites défiler la page vers le bas et cochez la case pour autoriser la création CloudFormation de ressources IAM avec des noms personnalisés.
5. Vérifiez et créez :
   - Vérifiez que les valeurs des paramètres sont correctement configurées et choisissez Soumettre.
6. La CloudFormation pile déploie les ressources nécessaires pour intégrer vos événements APM à AWS Incident Detection and Response. Attendez que l'état de la pile s'affiche`CREATE_COMPLETE`.
7. La CloudFormation pile crée les ressources suivantes, en supposant que les valeurs d'exemple aient été saisies dans les paramètres de New Relic et aient été exécutées dans la US-EAST-1 région.
   - CustomEventBus: NewRelic-AWSIncidentDetectionResponse-EventBus
   - EventBridgeRule: lois. partner/newrelic. com/1234567/nom_source | NewRelic-AWSIncidentDetectionResponse-EventBridgeRule
   - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
   - TransformLambdaFunction: NewRelic-AWSIncidentDetectionResponse-Lambda-Transform
   - TransformLambdaPermission: NewRelicIntegrationForIDR-TransformLambdaPermission - [chaîne_aléatoire]

Tests d'intégration

Après avoir déployé la pile, testez l'intégration en envoyant une charge utile de test depuis votre APM :

1. Accédez à la console Lambda et sélectionnez la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` fonction. Choisissez l'onglet Surveiller.
2. Recherchez un appel réussi dans les graphiques métriques.
3. Choisissez View Amazon CloudWatch Logs pour vérifier dans les flux de journaux la présence de votre charge utile de test ou d'éventuelles erreurs.

Partage de l'ARN de votre bus d'événements avec AWS Incident Detection and Response

1. Ouvrez la EventBridge console Amazon. Sélectionnez Event Bus.
2. Copiez l'ARN du bus d'événements personnalisé créé dans le cadre de la CloudFormation pile (exemple : *`arn:aws:events:us-east-1:123456789123:event-bus/NewRelic-AWSIncidentDetectionResponse-EventBus`*.)
   - Ajoutez cet ARN au champ « EventBridge Event Bus ARN » de la section « Third-Party APM Alarms » de votreQuestionnaire sur l'ingestion d'alarmes - Aperçu.
3. Au cours du processus d'intégration, AWS Incident Detection and Response crée une EventBridge règle gérée sur ce bus d'événements personnalisé pour ingérer vos alarmes APM.

Option 2 : intégration manuelle

Procédez comme suit pour chaque AWS compte et AWS région d'où AWS Incident Detection and Response doit ingérer des alarmes. AWS Incident Detection and Response recommande de configurer les alarmes dans le même AWS compte et dans la même région que les ressources de votre application afin d'identifier et d'étudier plus rapidement les ressources touchées. Les incidents et les dossiers de support sont ouverts sur le AWS compte d'où l'alerte APM a été reçue.

1. Créez un bus d'événements pour les EventBridge partenaires en configurant votre APM en tant que source d'événements EventBridge partenaires Amazon (par exemple,`aws.partner/apm_name/integrationName`). Pour obtenir des instructions sur la configuration de votre APM en tant que source d'événements, consultez la section Réception d'événements d'un partenaire SaaS avec Amazon EventBridge.
2. Effectuez l'une des actions suivantes :

- (Recommandé) Créez un bus d'événements EventBridge personnalisé nommé`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
- (Alternative) Utilisez le bus d' EventBridgeévénements par défaut au lieu d'un bus d'événements personnalisé.

AWS Incident Detection and Response installera une règle gérée (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sur le bus d'événements personnalisé ou par défaut via le `AWSServiceRoleForHealth_EventProcessor` SLR. La source de la règle sera le bus d'événements personnalisé ou par défaut, la destination de la règle sera AWS Incident Detection and Response, et la règle correspondra au modèle d'ingestion d'événements APM tiers.

3. Créez une fonction Lambda nommée `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` pour transformer les événements du bus d'événements de votre partenaire. Les événements transformés seront conformes à la règle géréeAWSHealthEventProcessorEventSource-DO-NOT-DELETE.
   - Les événements transformés incluent un identifiant AWS unique de détection et de réponse aux incidents, et définissent la source et le type de détail de l'événement selon les valeurs requises. Cela permet à la structure de charge utile JSON transformée de correspondre au modèle de règles gérées.
   - Définissez la cible de la fonction Lambda sur le bus d'événements personnalisé (recommandé) créé à l'étape 2 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 AWS Incident Detection and Response. La source de la règle est le bus d'événements partenaire que vous avez créé à l'étape 1 (`aws.partner/apm_name/integrationName`). La cible de la règle est la fonction Lambda que vous avez créée à l'étape 3 ()`[apm_name]-AWSIncidentDetectionResponse-LambdaFunction`. Pour obtenir des instructions sur la définition de votre EventBridge règle, consultez les EventBridge règles d'Amazon.

Pour un exemple étape par étape expliquant comment configurer manuellement les intégrations du bus d'événements des partenaires avec AWS Incident Detection and Response, consultez Intégration des notifications de Datadog et Splunk.

Ingérez les alarmes des APM sans intégration directe avec EventBridge

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

Vous pouvez déployer un CloudFormation modèle ou configurer manuellement l'intégration. Avant de configurer l'intégration, vérifiez que le rôle AWS lié au service (SLR) `AWSServiceRoleForHealth_EventProcessor` est créé dans vos comptes.

Option 1 : utilisation CloudFormation Modèle

Un CloudFormation modèle est disponible pour simplifier le processus de création de l'infrastructure d'intégration requise pour intégrer les alarmes à AWS Incident Detection and Response depuis votre APM qui n'est pas directement intégré à Amazon EventBridge.

Considérations à prendre en compte avant de déployer ce CloudFormation modèle

- Cette solution utilise un autorisateur Lambda API Gateway pour comparer un jeton secret transmis dans la charge utile de votre APM à un jeton entrant. AWS Secrets Manager Si le jeton ne correspond pas, une politique avec un refus explicite sera renvoyée. Pour plus d'informations, consultez la section Autorisateurs Lambda.
- Dans le cadre du modèle de responsabilité AWS partagée, il est de votre responsabilité de vous assurer que vous utilisez une approche d'authentification qui répond aux exigences de sécurité de votre organisation. Nous vous recommandons d'utiliser AWS Secrets Manager un service similaire, au lieu de stocker des informations sensibles telles que des clés d'API ou des jetons d'autorisation sous forme de variables codées en dur. Pour plus d'informations, veuillez consulter Création et gestion des secrets avec AWS Secrets Manager.
- Pour un exemple supplémentaire d'implémentation du code d'authentification des Hash-Based messages (HMAC), consultez receive-webhooks sur la page Github d'aws-samples. Pour plus d'informations sur la mise en œuvre de l'autorisation par jeton, consultez l'exemple de fonction Lambda d'autorisation TOKEN dans la documentation d'API Gateway.
- La solution utilise RateLimitBurstLimit, et Quota dans API Gateway pour contrôler les volumes de demandes. Ces outils limitent le nombre de demandes pouvant être traitées dans un délai défini. Cela permet d'éviter la surcharge du système et de maintenir la stabilité du service. Pour plus d'informations sur le throttling, consultez le guide du développeur d'API Gateway.
- Envisagez d'utiliser le AWS Web Application Firewall (WAF) pour protéger l'API Gateway des adresses IP erronées connues. Cela réduit le risque que des attaquants inondent l'API de fausses requêtes susceptibles de bloquer les événements réels du journal.

- AWS Secrets Manager les valeurs des jetons doivent être stockées dans votre outil de surveillance des performances des applications (APM) sous forme d'en-tête HTTP. Veillez à effectuer une rotation régulière du jeton en tant que bonne pratique en matière de sécurité.
- Des coûts supplémentaires seront encourus pour les ressources déployées via ce CloudFormation modèle (par exemple : Lambda et EventBridge). Pour plus d'informations sur la tarification de ces services, consultez la section AWS Tarification.
- Après avoir testé l'intégration, supprimez les instructions logger.info () de la (fonction `TransformLambdaFunction` Lambda) pour empêcher les charges utiles d'apparaître dans Amazon Logs. CloudWatch
- Déployez ce CloudFormation modèle dans tous les AWS comptes et régions dont AWS Incident Detection and Response doit ingérer des alarmes.

Préparation du CloudFormation modèle :

Remarque : Les étapes d'intégration utilisent Dynatrace comme exemple, mais ce modèle peut être utilisé pour n'importe quel APM capable d'envoyer des charges utiles à une API Gateway.

1. Téléchargez et ouvrez le CloudFormation modèle.
2. `APIGWUsagePlan`Localisez-le dans le modèle. Passez en revue les valeurs configurées pour `RateLimitBurstLimit`, et `Quota Limit` qui sont définies sur 20, 50 et 2000 par défaut. Ajustez les valeurs en fonction de vos besoins.
3. `AuthorizerLambdaFunction`Localisez-le dans le modèle. Cette fonction Lambda sert d'exemple de mécanisme d'authentification. Il extrait une valeur de jeton d'un en-tête appelé`authorizationToken`, qui est transmis par votre APM. Vous pouvez modifier ce code pour l'aligner sur les politiques de sécurité et les exigences de votre organisation en matière d'APM.
4. `TransformLambdaFunction`Repérez-le dans le modèle. Remplacez le chemin du dictionnaire`raw_json["detail"]["ProblemTitle"]`, par le chemin du nom de votre alarme envoyé dans la charge utile JSON depuis votre APM. Laissez les choses telles quelles pour Dynatrace.

Déploiement du CloudFormation modèle :

1. Ouvrez la CloudFormation console dans votre compte cible et Région AWS.
2. Choisissez Créer une pile, avec de nouvelles ressources (standard).

- Sélectionnez Choisir un modèle existant, Charger un fichier modèle, Choisir un fichier, puis téléchargez le CloudFormation modèle que vous avez enregistré localement.

3. Spécifiez les détails de la pile :
   - Entrez un nom de pile (par exemple, *`DynatraceIntegrationForIDR`*.)
   - APMNameParameter (exemple, *`Dynatrace`*.)
   - Choisissez Suivant.
4. Configurez les options de pile :
   - Faites défiler la page vers le bas et cochez la case pour autoriser la création CloudFormation de ressources IAM avec des noms personnalisés.
5. Vérifiez et créez :
   - Vérifiez que les valeurs des paramètres sont correctement configurées et choisissez Soumettre.
6. La CloudFormation pile déploie les ressources nécessaires pour intégrer vos événements APM à AWS Incident Detection and Response. Attendez que le statut de la CloudFormation pile soit CREATE_COMPLETE.
7. La CloudFormation pile crée les ressources ci-dessous en supposant que la valeur d'exemple `Dynatrace` a été saisie dans les paramètres et exécutée dans la US-EAST-1 région.
   - Nom du secret : DynatraceMySecretTokenName (une valeur secrète aléatoire sera créée pour la clé secrète APMSecureToken)
   - Ressources API Gateway :
     - Nom de l'API : Dynatrace-AWSIncidentDetectionResponse-APIGW
     - Nom de la scène : Dynatrace-Stage-Prod
     - Autorisateurs : Dynatrace-APIGW-Authorizer
     - Plan d'utilisation : APIGW_ Throttling_Plan
   - Fonctions Lambda :
     - Fonction d'autorisation : Dynatrace-AWSIncidentDetectionResponse-Lambda-Authorizer
     - Fonction de transformation : Dynatrace-AWSIncidentDetectionResponse-Lambda-Transform
   - EventBus Nom personnalisé : Dynatrace-AWSIncidentDetectionResponse-EventBus
   - Rôle IAM :
     - TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-us-east-1
     - AuthorizerLambdaExecutionRole: IDR-AuthorizerLambdaExecutionRole-us-east-1
8. Enregistrez l'URL du webhook et la valeur du jeton :

- Ouvrez la console API Gateway et choisissez le nom de l'API créé dans le cadre de la CloudFormation pile.
- Choisissez Stages dans le menu de navigation de gauche, développez le nom de l'étape à l'aide du signe +, puis choisissez POST. Enregistrez l'URL Invoke. Configurez cette URL dans votre APM comme destination pour envoyer des webhooks en cas d'événements d'alarme.
- Ouvrez la AWS Secrets Manager console et choisissez le nom secret créé dans le cadre de la CloudFormation pile. (Exemple : DynatraceMySecretTokenName.)
  - Dans l'onglet Valeur secrète, choisissez Extraire la valeur secrète. Vous verrez la clé secrète sous la forme APMSecureToken. Enregistrez la valeur secrète. Ne partagez cette valeur secrète avec personne.

Tests d'intégration

Après avoir déployé la pile, testez l'intégration en envoyant une charge utile de test depuis votre APM :

1. Accédez à la console Lambda et sélectionnez `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` la fonction. Choisissez l'onglet Surveiller.
2. Recherchez un appel réussi dans les graphiques métriques.
3. Choisissez View Amazon CloudWatch Logs pour vérifier dans les flux de journaux la présence de votre charge utile de test ou d'éventuelles erreurs.

Partage de l'ARN de votre bus d'événements avec AWS Incident Detection and Response

1. Ouvrez la EventBridge console Amazon. Sélectionnez Event Bus.
2. Copiez l'ARN du bus d'événements personnalisé créé dans le cadre de la CloudFormation pile, exemple : *`arn:aws:events:us-east-1:123456789123:event-bus/Dynatrace-AWSIncidentDetectionResponse-EventBus`*.
   - Ajoutez cet ARN au champ « EventBridge Event Bus ARN » de la section « Third-Party APM Alarms » de votreQuestionnaire sur l'ingestion d'alarmes - Aperçu.
3. Au cours du processus d'intégration, AWS Incident Detection and Response créera une EventBridge règle gérée sur ce bus d'événements personnalisé afin d'ingérer vos alarmes APM.

Option 2 : intégration manuelle

Suivez les étapes ci-dessous pour configurer l'intégration avec AWS Incident Detection and Response.

1. Créez un Amazon API Gateway pour accepter la charge utile de votre APM.
2. Définissez une fonction Lambda pour l'autorisation à l'aide d'un jeton d'authentification.
3. Effectuez l'une des actions suivantes :
   - (Recommandé) Créez un bus d'événements EventBridge personnalisé nommé`$YourApmName-AWSIncidentDetectionResponse-EventBus`.
   - (Alternative) Utilisez le bus d' EventBridge événements par défaut au lieu d'un bus d'événements personnalisé.
4. Définissez une fonction Transform Lambda pour ajouter l'identifiant AWS Incident Detection and Response à votre charge utile. Vous pouvez également utiliser cette fonction pour filtrer les événements que vous souhaitez envoyer à AWS Incident Detection and Response.
   - L'API Gateway doit appeler la fonction Transform Lambda qui transformera la charge utile transmise par l'API Gateway.
   - La fonction Transform Lambda doit écrire les événements transformés dans le bus d'événements défini au point 3 ci-dessus.
5. Configurez votre APM pour envoyer des notifications à l'URL générée par l'API Gateway.

Ingérez les alarmes des APM grâce à l'intégration directe d'Amazon SNS

Si votre APM prend en charge l'envoi d'alarmes vers les rubriques Amazon SNS, vous pouvez suivre ce guide pour intégrer vos alarmes APM à AWS Incident Detection and Response.

Vous pouvez déployer le CloudFormation modèle fourni ou configurer manuellement cette intégration. Avant de configurer l'intégration, vérifiez que le rôle AWS lié au service (SLR) `AWSServiceRoleForHealth_EventProcessor` est créé dans vos comptes.

Option 1 : utilisation CloudFormation

Un CloudFormation modèle est disponible pour simplifier le processus de création de l'infrastructure d'intégration requise pour intégrer les alarmes à AWS Incident Detection and Response depuis votre APM avec l'intégration Amazon SNS.

> **Note**
>
> - Des coûts supplémentaires seront encourus pour les ressources déployées via ce CloudFormation modèle (par exemple : Lambda et EventBridge). Pour plus d'informations sur la tarification de ces services, consultez la section AWS Tarification.
> - Ce CloudFormation modèle doit être déployé dans tous les AWS comptes et régions à partir desquels les alarmes doivent être ingérées par AWS Incident Detection and Response.
> - Les exemples fournis dans ce document concernent Grafana, mais ce modèle peut être utilisé pour tout APM directement intégré à Amazon Simple Notification Service.
> - Pour des raisons de sécurité, AWS recommande de supprimer les `logger.info()` instructions du `TransformLambdaFunction` afin d'empêcher la charge utile d'être enregistrée dans Amazon CloudWatch Logs.

Conditions préalables au déploiement de ce CloudFormation modèle :

- Une rubrique Amazon Simple Notification Service doit être créée pour recevoir les événements d'alarme de votre APM. Créez une rubrique SNS dans la console Amazon Simple Notification Service.
- Le `TransformLambdaFunction` contenu du modèle doit être modifié pour être défini `["detail"]["incident-detection-response-identifier"]` sur la valeur souhaitée en fonction de l'APM utilisé.

Réalisation des prérequis :

1. Ouvrez la console Amazon SNS, puis sélectionnez Rubriques. Copiez l'ARN de la rubrique SNS créée pour recevoir les événements d'alarme de votre APM.
   - Exemple : `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
2. Téléchargez et ouvrez le CloudFormation modèle
   - Localisez le `TransformLambdaFunction` dans le modèle
     - `def lambda_handler(event, context)`Sous-défini sur `event["detail"]["incident-detection-response-identifier"]` le chemin json où le nom de l'alarme apparaît dans la charge utile JSON de l'enregistrement SNS.

- Tout événement envoyé au `TransformLambdaFunction` via SNS a une structure de charge utile parent sous la forme. `event["Records"][n]["Sns"]["Message"]` L'origine réelle de la charge utile provenant de la source (APM) est intégrée à la structure parent.
- Exemple pour Grafana : `event["Records"][n]["Sns"]["Message"]["alerts"][n]["labels"]["alertname"]`

Déploiement du CloudFormation modèle :

1. Accédez à la CloudFormation console du compte et de la région dans lesquels vous devez configurer l'intégration.
2. Naviguez vers CloudFormation.
   - Choisissez Créer une pile, avec de nouvelles ressources (standard)
     - Sélectionnez Choisir un modèle existant, Charger un fichier modèle, Choisir un fichier, puis téléchargez le CloudFormation modèle que vous avez enregistré localement.
3. Spécifiez les détails de la pile :
   - Entrez un nom de pile Exemple : `<your-apm-name>IntegrationForIDR`
   - Spécifiez les valeurs des paramètres obtenues lors de la réalisation des prérequis
     - APMNameParameterExemple : `Grafana`
     - Exemple de paramètre TriggerSNSParameter : `arn:aws:sns:eu-west-1:012345678912:<your-apm-name>-sns`
   - Choisissez Suivant.
4. Configurez les options de pile :
   - Accédez au bas de la page et confirmez la case à cocher pour autoriser la création CloudFormation de ressources IAM avec des noms personnalisés.
5. Vérifiez et créez :
   - Vérifiez que les valeurs des paramètres sont correctement configurées, puis choisissez Soumettre.
6. La CloudFormation pile déploiera les ressources nécessaires pour intégrer vos événements APM à AWS Incident Detection and Response. Attendez que le statut de la CloudFormation pile soit CREATE_COMPLETE.
7. La CloudFormation pile crée les ressources ci-dessous en supposant que les valeurs d'exemple ont été saisies dans les paramètres de Grafana et ont été exécutées dans la EU-WEST-1 région.

- CustomEventBus: Grafana-AWSIncidentDetectionResponse-EventBus
- Abonnement SNS : arn:aws:sns:eu-west- 1:012345678912:grafana-sns : [random_string]
- TransformLambdaExecutionRole: IDR-TransformLambdaExecutionRole-eu-west-1
- TransformLambdaFunction: Grafana-AWSIncidentDetectionResponse-Lambda-Transform
- TransformLambdaPermission: GrafanaIntegrationForIDR-TransformLambdaPermission - [chaîne_aléatoire]

Tests d'intégration

Une fois la CloudFormation pile déployée avec succès, vous pouvez valider l'intégration en envoyant une charge utile de test depuis votre APM. Une fois que la charge utile de test est envoyée depuis votre APM :

1. Accédez à la console Lambda et sélectionnez la `APMNameParameter-AWSIncidentDetectionResponse-Lambda-Transform` fonction. Choisissez ensuite l'onglet Moniteur.
2. Un appel réussi doit être observé dans les graphiques métriques.
3. Sélectionnez Afficher Amazon CloudWatch Logs. Vous pouvez vérifier à partir des événements du journal dans les flux de journal que la charge utile de test envoyée par votre APM est présente ou si des erreurs ont été détectées.

Partage de l'ARN de votre bus d'événements avec AWS Incident Detection and Response

1. Accédez à la EventBridge console Amazon. Sélectionnez Event Bus.
2. Enregistrez l'ARN du bus d'événements personnalisé déployé dans le cadre de la CloudFormation pile, par exemple :`arn:aws:events:eu-west-1:012345678912:event-bus/Grafana-AWSIncidentDetectionResponse-EventBus`.
   - Fournissez l'ARN de ce bus d'événements personnalisé à AWS Incident Detection and Response dans le champ « ARN du bus d'EventBridge événements » de la section « Alarmes Third-Party APM » du Questionnaire sur l'ingestion d'alarmes - Aperçu.
3. Au cours du processus d'intégration, AWS Incident Detection and Response créera une EventBridge règle gérée sur ce bus d'événements personnalisé afin d'ingérer vos alarmes APM.

Option 2 : intégration manuelle

1. Ouvrez la console Amazon SNS et créez une rubrique SNS dans la console Amazon Simple Notification Service nommée `[apm_name]-sns` pour recevoir les événements d'alarme de votre APM. Notez l'ARN de la rubrique SNS créée.
2. Effectuez l'une des actions suivantes :
   - (Recommandé) Créez un bus d'événements EventBridge personnalisé nommé`[apm_name]-AWSIncidentDetectionResponse-EventBus`.
   - (Alternative) Utilisez le bus d' EventBridge événements par défaut au lieu d'un bus d'événements personnalisé.

   AWS Incident Detection and Response installera une règle gérée (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sur le bus d'événements personnalisé ou par défaut via le `AWSServiceRoleForHealth_EventProcessor` SLR. La source de la règle sera le bus d'événements personnalisé ou par défaut, la destination de la règle sera AWS Incident Detection and Response, et la règle correspondra au modèle d'ingestion d'événements APM tiers.
3. Créez une fonction Lambda nommée `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` pour transformer vos charges utiles SNS.
   - Les événements transformés doivent répondre aux exigences de charge utile définies dans Exigences de charge utile pour l'ingestion d'alertes APM avec EventBridge
   - Définissez la cible de la fonction Lambda sur le bus d'événements personnalisé (recommandé) créé à l'étape 2 ou sur votre bus d'événements par défaut.
4. Définissez le sujet SNS comme déclencheur pour votre fonction `$YourApmName-AWSIncidentDetectionResponse-LambdaFunction` Lambda.
   - Sur la page « Ajouter des déclencheurs », recherchez « SNS ».
   - Ajoutez l'ARN de votre rubrique SNS dédiée créée à l'étape 1.
   - Choisissez « Ajouter ».
5. Suivez votre documentation APM pour configurer une destination SNS pour vos charges utiles APM qui doivent être ingérées par AWS Incident Detection and Response.

AWS Incident Detection and Response installera une règle gérée (`AWSHealthEventProcessorEventSource-DO-NOT-DELETE`) sur le bus d'événements

personnalisé ou par défaut via le `AWSServiceRoleForHealth_EventProcessor` SLR. La source de la règle sera le bus d'événements personnalisé ou par défaut, la destination de la règle sera AWS Incident Detection and Response, et la règle correspondra au modèle d'ingestion d'événements APM tiers.

Optimisation des alarmes et réglages de surveillance

Pour garantir une précision optimale de détection des incidents, nos ingénieurs de gestion des incidents évaluent en permanence les performances des alarmes par rapport à vos charges de travail critiques. Nous vous recommandons de modifier la configuration des alarmes, que vous êtes tenu d'apporter, et nous collaborons de manière proactive avec vous et vos responsables de comptes techniques (TAM) pour affiner ces paramètres.

Lorsque les données de surveillance indiquent que les alarmes ne correspondent peut-être pas aux opérations critiques de votre entreprise, par exemple lorsque les alertes se déclenchent sans que cela ait un impact sur le client ou lorsque les états des alarmes fluctuent fréquemment, nous vous recommandons de supprimer les alarmes non critiques et d'intégrer les alarmes qui reflètent mieux l'impact critique de la charge de travail. Cela permet de maintenir l'efficacité globale de votre couverture de réponse aux incidents.

Révision des alarmes et commentaires

AWS Incident Detection and Response effectue des examens complets de vos alarmes avant de les intégrer à des fins de surveillance. Les alarmes sont évaluées par rapport à des critères d'acceptation techniques tels que les paramètres de configuration, la qualité des données et l'efficacité des alertes.

Sur la base de cet examen, deux types de commentaires sont fournis :

- Exigences de configuration obligatoires : ces modifications doivent être mises en œuvre pour que l'alarme soit acceptée.
- Recommandations d'amélioration facultatives : ces modifications améliorent l'efficacité des alarmes mais ne sont pas obligatoires pour l'acceptation des alarmes.

Après avoir reçu ces commentaires, vous pouvez décider de n'intégrer que les alarmes acceptées et celles nécessitant des améliorations facultatives, tout en travaillant en parallèle sur les modifications de configuration pour les alarmes soumises à des exigences de configuration obligatoires.

Vous pouvez également implémenter toutes les modifications avant de les mettre en ligne. Cette approche allonge le calendrier d'intégration, en fonction du nombre d'alarmes nécessitant des ajustements.

Test des alarmes (Gameday)

La dernière étape du processus d'intégration d'AWS Incident Detection and Response consiste à organiser un Gameday pour votre nouvelle charge de travail. Après les étapes d'ingestion des alarmes, AWS Incident Detection and Response confirme la date et l'heure que vous avez choisies pour commencer votre journée de jeu.

Votre Gameday a deux objectifs principaux :

- Validation fonctionnelle : confirme qu'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 actions souhaitées, telles que la création automatique d'un dossier d'assistance si vous l'avez sélectionnée lors de l'ingestion de l'alarme.
- Simulation : Le Gameday est une simulation de bout en bout de ce qui pourrait se passer lors d'un incident réel. AWS Incident Detection and Response vous donne un aperçu de la façon dont un véritable incident peut se dérouler. Le Gameday 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 Test d'alarme

Pendant le Gameday, les CloudWatch alarmes Amazon sont testées en les faisant passer manuellement à l'état Alarme à l'aide du AWS Command Line Interface. Vous pouvez également accéder au AWS CLI formulaire AWS CloudShell. AWS Incident Detection and Response fournit une liste de AWS CLI commandes que vous pouvez utiliser pendant les tests.

Exemple de 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
```

> **Note**
>
> L' Gestion des identités et des accès AWS utilisateur ou le rôle que vous utilisez pour tester les alarmes doit disposer d'une `cloudwatch:SetAlarmState` autorisation.

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 opérations CloudWatch d'API, consultez la référence CloudWatch des autorisations Amazon.

Test d'alarmes APM par un tiers

Les charges de travail qui utilisent un outil tiers de surveillance des performances des applications (APM), tel que Datadog, Splunk, New Relic ou Dynatrace, 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 vos opérateurs de comparaison pour forcer l'alarme à passer au statut ALARM. Ce statut déclenche une charge utile pour AWS Incident Detection and Response.

Le Gameday valide les points suivants

- 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 incident et les contacts que vous avez prescrits pour le runbook sont avertis.
- AWS Incident Detection and Response peut interagir avec vous selon la méthode de pont de conférence que vous avez définie.

Les alarmes se déclenchent

Une fois le Gameday terminé avec succès, AWS Incident Detection and Response envoie une communication en direct via votre dossier d'assistance à l'intégration. À partir de ce moment, vos alarmes intégrées sont surveillées et AWS Incident Detection and Response vous contactera selon les coordonnées de la charge de travail lorsque vos alarmes intégrées passeront à l'état ALARM.

Principaux résultats

- Une Go-Live correspondance est envoyée pour confirmer que votre charge de travail est désormais surveillée par AWS Incident Detection and Response.

Toutes les modifications requises identifiées pendant le Gameday, AWS Incident Detection and Response les exécute à l'aide d'un. Demander des modifications à une charge de travail intégrée dans Incident Detection and Response

Questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans Incident Detection and Response (chemin d'exception)

> **Note**
>
> Si vous ne parvenez pas à utiliser l'interface de ligne de commande client AWS Incident Detection and Response pour intégrer votre charge de travail, utilisez les questionnaires suivants pour l'intégration de la charge de travail et des alarmes.

Cette page fournit les questionnaires que vous devez remplir lors de l'intégration d'une charge de travail dans AWS Incident Detection and Response et lors de la configuration des alarmes à intégrer au service. Le questionnaire d'intégration de la charge de travail contient des informations générales sur votre charge de travail, les détails de son architecture et les contacts pour la réponse aux incidents. Dans le questionnaire d'ingestion des alarmes, vous spécifiez les alarmes critiques qui doivent déclencher la création d'incidents dans Incident Detection and Response pour votre charge de travail, ainsi que les informations du manuel indiquant qui doit être contacté et quelles mesures doivent être prises. Le fait de remplir correctement ces questionnaires est une étape clé dans la mise en place de processus de surveillance et de réponse aux incidents pour vos AWS charges de travail.

Téléchargez le questionnaire d'intégration de Workload :

- Version anglaise
- Version japonaise

Téléchargez le questionnaire sur l'ingestion d'Alarm :

- Version anglaise
- Version japonaise

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

Questions générales

Question	Exemple de réponse
Nom de l'entreprise	Amazon Inc.
Nom de cette charge de travail (inclure les abréviations éventuelles)	Amazon Retail Operations (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 and/or réglementaires de conformité applicables à cette charge de travail et à toute action requise 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
Liste des balises de AWS 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.	Nom de l'application : Optimax environnement : Production

Question	Exemple de réponse
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.	
Une liste des AWS services utilisés par cette charge de travail ainsi que le AWS compte et les régions dans lesquels ils se trouvent. **Note** Créez une nouvelle ligne pour chaque service.	Route 53 : achemine le trafic Internet vers l'ALB. Account:123456789101 Région : US-EAST-1, US-WEST-2
Une liste des AWS services utilisés par cette charge de travail ainsi que le AWS compte et les régions dans lesquels ils se trouvent. **Note** Créez une nouvelle ligne pour chaque service.	ALB : achemine le trafic entrant vers un groupe cible de conteneurs ECS. Compte : 123456789101 Région : N/A

Question	Exemple de réponse
Une liste des AWS services utilisés par cette charge de travail ainsi que le AWS compte et les régions dans lesquels ils se trouvent. **Note** Créez une nouvelle ligne pour chaque service.	ECS : infrastructure informatique pour le parc de logique métier principal. Responsable du traitement des demandes des utilisateurs entrantes et de l'envoi de requêtes à la couche de persistance. Compte : 123456789101 Région : US-EAST-1
Une liste des AWS services utilisés par cette charge de travail ainsi que le AWS compte et les régions dans lesquels ils se trouvent. **Note** Créez une nouvelle ligne pour chaque service.	RDS : le cluster Amazon Aurora stocke les données utilisateur accessibles par la couche de logique métier ECS. Compte : 123456789101 Région : US-EAST-1
Une liste des AWS services utilisés par cette charge de travail ainsi que le AWS compte et les régions dans lesquels ils se trouvent. **Note** Créez une nouvelle ligne pour chaque service.	S3 : Stocke les actifs statiques du site Web. Compte : 123456789101 Région : N/A
Détaillez tous upstream/downstream les composants non intégrés qui pourraient affecter cette charge de travail en cas de panne.	Microservice d'authentification : empêchera les utilisateurs de charger leurs dossiers médicaux car ils ne seront pas authentifiés.

Question	Exemple de réponse
Existe-t-il des AWS composants sur site ou non pour cette charge de travail ? Dans l'affirma tive, quels sont-ils et quelles sont les fonctions exécutées ?	Tout le trafic Internet in/out de AWS est acheminé via notre service proxy sur site.
Fournissez les détails de tous les plans de failover/disaster restauration manuels ou automatisés au niveau de la zone de disponibi lité et de la région.	Mode veille à chaud. Basculement automatiq ue en cas US-WEST-2 de baisse prolongée du taux de réussite.

Questionnaire sur l'ingestion d'alarmes - Aperçu

Dans le questionnaire d'ingestion d'alarmes, vous spécifiez les alarmes critiques pour votre charge de travail auxquelles vous souhaitez faire participer AWS Incident Detection and Response, ainsi que les contacts que vous souhaitez qu'un ingénieur de gestion des incidents intervienne lorsque ces alarmes se déclenchent.

Le questionnaire sur l'ingestion d'alarmes est divisé en sections suivantes :

- Section de contact : spécifiez d'abord le ou les principaux contacts à inclure dans le Support dossier créé avec AWS Incident Detection and Response lorsqu'une alarme se déclenche, ainsi que votre application de conférence préférée pour les passerelles d'incidents. Si aucune préférence de passerelle n'est fournie, AWS Incident Detection and Response créera une passerelle lors des incidents. Spécifiez ensuite les contacts d'escalade et les intervalles de temps pour les engager lorsque les contacts principaux sont injoignables. Enfin, listez tous les contacts qui devraient recevoir des mises à jour régulières sur l'état des incidents par le biais du dossier d'assistance pendant toute la durée de l'incident.
- Matrice d'alarmes : liste l'ensemble des alarmes qui déclencheront la détection et la réponse aux incidents AWS lorsqu'elles sont déclenchées. Consultez les « critères d'alarme critique » définis par AWS Incident Detection and Response lors de la sélection des alarmes à intégrer. Pour de plus amples informations, veuillez consulter Définition de l'alarme.
  - Amazon CloudWatch Alarms (laissez cette section vide si vous n'avez pas d' CloudWatch alarme Amazon)
  - Alarmes APM tierces (laissez cette section vide si vous n'avez pas d'alarmes APM tierces)

- EventBridge EventBus ARN : il s'agit de l' EventBus ARN personnalisé que vous avez créé dans Ingérez les alarmes des APM grâce à l'intégration directe EventBridge ouIngérez les alarmes des APM sans intégration directe avec EventBridge.
- Identifiants d'alarme : partagez le numéro de compte, la région et le nom de l'alarme APM.

Questionnaire sur l'ingestion d'alarmes - Questions du Runbook

Questions relatives à Runbook

Question	Exemple de réponse
AWS engage les contacts liés à la charge de travail tout au long du Support dossier. Qui est le contact principal lorsqu'une alarme se déclenche pour cette charge de travail ? Spécifiez votre application de conférence préférée et AWS nous vous demanderons ces informations lors d'un incident. **Note** Si aucune application de conférenc e préférée n'est fournie, elle AWS vous contactera lors d'un incident et vous fournira un pont Chime que vous pourrez rejoindre.	Équipe de candidature app@example.com +61 2 3456 7890
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.	1. Au bout de 10 minutes, en l'absence de réponse de la part du contact principal, contactez : John Smith - Superviseur des applications john.smith@example.com +61 2 3456 7890

Question	Exemple de réponse
	2. Au bout de 10 minutes, si John Smith ne répond pas, contactez : Jane Smith - Directrice des opérations jane.smith@example.com +61 2 3456 7890
AWS communique les mises à jour par le biais du dossier de support à intervalles réguliers tout au long de l'incident. Y a-t-il d'autres contacts qui devraient recevoir ces mises à jour ?	john.smith@example.com, jane.smith@example.com

Matrice d'alarme

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

Critères d'alerte critiques d'AWS relatifs à la détection et à la réponse aux incidents :

- Les alarmes de détection et de réponse aux incidents AWS ne doivent passer en état « alarme » qu'en cas d'impact commercial significatif sur la charge de travail surveillée (perte d'expérience revenue/degraded client) nécessitant une attention immédiate de la part de l'opérateur.
- Les alarmes de détection et de réponse aux incidents AWS 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.
- Les seuils d'alarme de détection et de réponse aux incidents AWS doivent être définis sur un seuil et une durée appropriés afin que chaque fois qu'une alarme se déclenche, une enquête soit menée. 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.

Politique d'AWS en matière de détection et de réponse aux incidents en cas de violation des critères :

Ces critères ne peuvent être évalués qu'au cas par cas au fur et à mesure que les événements se produisent. L'équipe de gestion des incidents travaille avec vos responsables de comptes techniques (TAM) pour régler 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 incidents d'AWS l'appelle après avoir envoyé un e-mail d'engagement initial.

Tableau matriciel des alarmes

Nom de la métrique/ ARN/Seuil	Description	Remarques	Actions demandées
Volume de charge de travail/ *CW Alarm ARN* / CallCount < 100 000 pour 5 points de données en 5 minutes, traiter les données manquantes comme manquantes	Cette métrique représente le nombre de demandes entrantes destinées à la charge de travail, mesuré au niveau de l'Application Load Balancer. Cette alarme est importante car des baisses importantes du nombre de demandes entrantes peuvent indiquer	L'alarme est passée à l'état « Alarme » 10 fois au cours de la semaine dernière. Cette alarme présente un risque de faux positifs. Une révision des seuils est prévue. Des problèmes ? Non ou Oui (si Non, laissez le champ vide) : cette alarme se déclenche fréquemment lors de l'exécution	Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à *SRE@example.com* Créez un AWS Support dossier pour nos services ELB et Amazon Route 53. Si une action IMMÉDIATE est nécessaire : vérifiez memory/

Nom de la métrique/ ARN/Seuil	Description	Remarques	Actions demandées
	des problèmes de connectivité réseau en amont ou des problèmes liés à notre implémentation DNS empêchant les utilisateurs d'accéder à la charge de travail.	d'une tâche par lots donnée. Résolveurs : ingénieurs de fiabilité des sites	disk l'espace libre d'EC2 et informez l'*Example*équipe par e-mail pour qu'elle redémarre l'instance, ou effectuez un vidage du journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)

Nom de la métrique/ ARN/Seuil	Description	Remarques	Actions demandées
Latence des demandes de charge de travail/ *CW Alarm ARN* / p90 Latence > 100 ms pour 5 points de données en 5 minutes, traiter les données manquantes comme manquantes	Cette métrique représente la latence p90 pour les requêtes HTTP à traiter par la charge de travail. Cette alarme représente la latence (mesure importante de l'expérience client pour le site Web).	L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière. 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. Résolveurs : ingénieurs de fiabilité des sites	Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à *SRE@example.com* Créez un AWS Support dossier pour nos services ECW et RDS. Si une action IMMÉDIATE est nécessaire : vérifiez memory/ disk l'espace libre d'EC2 et informez l'*Example*équipe par e-mail pour qu'elle redémarre l'instance, ou effectuez un vidage du journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)

Nom de la métrique/ ARN/Seuil	Description	Remarques	Actions demandées
Disponibilité des demandes de charge de travail/ *CW Alarm ARN* / Disponibilité < 95 % pour 5 points de données en 5 minutes, considérez les données manquantes comme manquantes.	Cette métrique représente la disponibilité des requêtes HTTP à traiter par la charge de travail. (nombre de requêtes HTTP 200/ nombre de demandes) par période. Cette alarme indique la disponibilité de la charge de travail.	L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière. 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. Résolveurs : ingénieurs de fiabilité des sites	Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à *SRE@example.com* Créez un AWS Support dossier pour nos services ELB et Amazon Route 53. Si une action IMMÉDIATE est nécessaire : vérifiez memory/ disk l'espace libre d'EC2 et informez l'*Example*équipe par e-mail pour qu'elle redémarre l'instance, ou effectuez un vidage du journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)
Exemple d'alarme New Relic			

Nom de la métrique/ ARN/Seuil	Description	Remarques	Actions demandées
Test d'intégration de bout en bout/ *CW Alarm ARN* / Taux d'échec de 3 % pour les métriques d'une minute sur une durée de 3 minutes, traiter les données manquantes comme manquantes Identifiant de charge de travail : flux de travail de test de bout en bout, Région AWS : US-EAST-1 , Compte AWS ID : 012345678910	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. Cette alarme indique la capacité de traiter les transactions commerciales correspondant à la charge de travail.	L'alarme est passée à l'état « Alarme » 0 fois la semaine dernière. 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. Résolveurs : ingénieurs de fiabilité des sites	Engagez l'équipe d'ingénierie de fiabilité du site en envoyant un e-mail à *SRE@example.com* Créez un AWS Support dossier pour nos services Amazon Elastic Container Service et Amazon DynamoDB. Si une action IMMÉDIATE est nécessaire : vérifiez memory/ disk l'espace libre d'EC2 et informez l'*Example*équipe par e-mail pour qu'elle redémarre l'instance, ou effectuez un vidage du journal. (si aucune action immédiate n'est nécessaire, laissez le champ vide)

Gérer les charges de travail dans le cadre de la détection et de la réponse aux incidents

Pour gérer efficacement les incidents, il est essentiel de mettre en place les processus et procédures appropriés pour intégrer, tester et maintenir vos charges de travail surveillées. Cette section couvre les étapes essentielles, notamment le développement de runbooks et de plans de réponse complets pour guider vos équipes en cas d'incident, le test et la validation approfondis des nouvelles charges de travail avant l'intégration, la demande de modifications pour mettre à jour le suivi de la charge de travail et le déchargement approprié des charges de travail lorsque cela est nécessaire.

Rubriques

Développez des guides et des plans de réponse pour répondre à un incident dans le cadre de la détection et de la réponse aux incidents

Incident Detection and Response utilise les informations capturées lors de l'intégration de votre interface de ligne de commande client AWS Incident Detection and Response 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 l'intégration de la charge de travail. Les plans de réponse sont des modèles de documents AWS Systems Manager (SSM) utilisés pour déclencher des incidents. Pour en savoir plus sur les

documents SSM, consultez la section AWS Systems Manager Documents. Pour en savoir plus sur Incident Manager, voir Qu'est-ce que c'est AWS Systems Manager Incident Manager ?

Principaux résultats :

- Finalisation de la définition de votre charge de travail sur AWS Incident Detection and Response.
- Finalisation des alarmes, des runbooks et de la définition du plan de réponse sur AWS Incident Detection and Response.

Vous pouvez également télécharger un exemple de manuel AWS Incident Detection and Response Runbook : 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
  ```
  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.
  ```
  * 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

---
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 dans le domaine de la détection et de la réponse aux incidents

> **Note**
>
> L' Gestion des identités et des accès AWS 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'ingestion des alarmes terminée, 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 qu'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 Incident Detection and Response suit 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, réglez manuellement l'alarme à l'état Alarme à l'aide du AWS Command Line Interface. Vous pouvez également accéder au AWS CLI formulaire AWS CloudShell. AWS Incident Detection and Response fournit une liste de AWS CLI commandes que vous pouvez utiliser pendant les tests.

Pour empêcher toute action indésirable, par exemple le redémarrage de l'instance Amazon EC2, désactivez toute action CloudWatch d'alarme avant de modifier l'état de l'alarme. Vous pouvez réactiver les actions CloudWatch d'alarme une fois les tests terminés. Pour en savoir plus sur la désactivation ou l'activation des actions d'alarme, consultez DisableAlarmActionset consultez EnableAlarmActionsle Amazon CloudWatch API Reference.

Exemple de 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 opérations CloudWatch d'API, consultez la référence CloudWatch des autorisations Amazon.

Alarmes APM tierces

Les charges de travail qui utilisent un outil tiers de surveillance des performances des applications (APM), tel que Datadog, Splunk, New Relic ou Dynatrace, nécessitent des instructions différentes pour simuler une alarme. Au début de la journée de jeu, 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 statut ALARM. Ce statut déclenche une charge utile pour AWS Incident Detection and Response.

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 avertis.
- AWS Incident Detection and Response peut communiquer avec vous par les moyens de conférence que vous avez prescrits.
- Toutes les alarmes et demandes d'assistance générées pendant la journée de jeu sont résolues.
- Un Go-Live e-mail est envoyé pour confirmer que votre charge de travail est désormais surveillée par AWS Incident Detection and Response.

Demander des modifications à une charge de travail intégrée dans Incident Detection and Response

Pour demander des modifications à une charge de travail intégrée, suivez les étapes suivantes pour créer un dossier de support avec AWS Incident Detection and Response.

1. Accédez au AWS Support Centre, 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 :

   Détection et réponse aux incidents AWS - *`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 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, etc.
   - Détails de la modification : Entrez les détails de la modification demandée.
8. Dans la section Contacts supplémentaires - facultatif, entrez les adresses e-mail auxquelles 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'identifiants e-mail dans la section Contacts supplémentaires - facultatif peut retarder le processus de modification.
9. Sélectionnez Soumettre.

   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 les identifiants e-mail dans la section Contacts supplémentaires - facultatif.

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

Empêcher les alarmes de déclencher la détection et la réponse aux incidents

Spécifiez les alarmes de charge de travail intégrées qui participent à la surveillance de la détection et de la réponse aux incidents AWS en les supprimant temporairement ou selon un calendrier. Par exemple, vous pouvez supprimer temporairement les alarmes de charge de travail pendant la maintenance planifiée afin d'éviter que les alarmes ne déclenchent la détection et la réponse aux incidents. Vous pouvez également supprimer les alarmes selon un calendrier si vous redémarrez tous les jours. Vous pouvez supprimer les alarmes à la source de l'alarme, telle qu'Amazon CloudWatch, ou vous pouvez soumettre une demande de modification de la charge de travail.

Rubriques

- Supprimer les alarmes à la source de l'alarme
- Soumettre une demande de modification de la charge de travail pour supprimer les alarmes
- Tutoriel : Utiliser une fonction mathématique métrique pour supprimer une alarme
- Tutoriel : Supprimer une fonction mathématique métrique pour annuler la suppression d'une alarme

Supprimer les alarmes à la source de l'alarme

Spécifiez quelles alarmes sont associées à la détection et à la réponse aux incidents et à quel moment elles le font en supprimant les alarmes à la source de l'alarme.

Rubriques

- Utiliser une fonction mathématique métrique pour supprimer une CloudWatch alarme
- Supprimer une fonction mathématique métrique pour annuler la suppression d'une alarme CloudWatch
- Exemples de fonctions mathématiques métriques et cas d'utilisation associés
- Supprimer les alarmes provenant d'un APM tiers

Utiliser une fonction mathématique métrique pour supprimer une CloudWatch alarme

Pour supprimer la surveillance de la détection des incidents et de la réponse aux CloudWatch alarmes Amazon, utilisez une fonction mathématique métrique pour empêcher les CloudWatch alarmes de passer à l'`ALARM`état pendant une période définie.

> **Note**
>
> La désactivation des actions d'alarme associées à une CloudWatch alarme ne supprime pas la surveillance de vos alarmes par la fonction de détection et de réponse aux incidents. Les modifications de l'état des alarmes sont enregistrées via Amazon EventBridge, et non par le biais CloudWatch d'actions d'alarme.

Pour utiliser une fonction mathématique métrique afin de supprimer une CloudWatch alarme, procédez comme suit :

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Alarmes, puis localisez l'alarme à laquelle vous souhaitez ajouter la fonction mathématique métrique.
3. Choisissez Actions, puis sélectionnez Modifier pour modifier l'alarme.
4. Choisissez Modifier la métrique pour modifier la métrique de l'alarme.
5. Choisissez Ajouter des données mathématiques, puis Commencer par une expression vide.
6. Entrez votre expression mathématique, puis choisissez Appliquer.
7. Désélectionnez la métrique existante surveillée par l'alarme.
8. Sélectionnez l'expression que vous venez de créer, puis sélectionnez Sélectionner une métrique.
9. Choisissez Passer à l'aperçu et créez.
10. Passez en revue vos modifications pour vous assurer que votre fonction mathématique métrique est appliquée comme prévu, puis choisissez Mettre à jour l'alarme.

Pour un exemple étape par étape de suppression d'une CloudWatch alarme à l'aide d'une fonction mathématique métrique, consultezTutoriel : Utiliser une fonction mathématique métrique pour supprimer une alarme.

Pour plus d'informations sur la syntaxe et les fonctions disponibles, consultez Syntaxe et fonctions mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon.

Supprimer une fonction mathématique métrique pour annuler la suppression d'une alarme CloudWatch

Annulez la suppression CloudWatch d'une alarme en supprimant la fonction mathématique métrique. Pour supprimer une fonction mathématique métrique d'une alarme, procédez comme suit :

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Alarmes, puis localisez l'alarme ou les alarmes dont vous souhaitez supprimer l'expression mathématique métrique.
3. Dans la section des mathématiques métriques, choisissez Modifier.
4. Pour supprimer la métrique de l'alarme, choisissez Modifier sur la métrique, puis cliquez sur le bouton X à côté de l'expression mathématique de la métrique.
5. Sélectionnez la métrique d'origine, puis sélectionnez Sélectionner la métrique.
6. Choisissez Passer à l'aperçu et créez.
7. Passez en revue vos modifications pour vous assurer que votre fonction mathématique métrique est appliquée comme prévu, puis choisissez Mettre à jour l'alarme.

Exemples de fonctions mathématiques métriques et cas d'utilisation associés

Le tableau suivant contient des exemples de fonctions mathématiques métriques, ainsi que des cas d'utilisation associés et une explication de chaque composant métrique.

Fonction mathématique métrique	Cas d'utilisation	Explication
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)`	Supprimez l'alarme entre 1 h 00 et 3 h 00 UTC tous les mardis en remplaçant les points de données réels par 0 pendant cette fenêtre.	• JOUR (m1) == 2 : garantit que c'est mardi (lundi = 1, dimanche = 7). • HEURE (m1) >= 1 && HEURE (m1) > 3 : Spécifie la plage horaire comprise entre 1 h et 3 h UTC. • IF (condition, value_if_ true, value_if_false) : si

Fonction mathématique métrique	Cas d’utilisation	Explication
		les conditions sont vraies, remplacez la valeur de la métrique par 0. Sinon, renvoyez la valeur d'origine (m1)
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 0, m1)`	Supprimez l'alarme entre 23 h 00 et 4 h 00 UTC, tous les jours en remplaçant les points de données réels par 0 pendant cette fenêtre.	• HEURE (m1) >= 23 : capture les heures à partir de 23 h UTC. • HEURE (m1) < 4 : capture les heures jusqu'à (mais sans inclure) 04:00 UTC. • || : Logic OR garantit que la condition s'applique à deux plages : tard le soir et tôt le matin. • IF (condition, value_if_true, value_if_false) : renvoie 0 pendant la période spécifiée. Conserve la valeur métrique initiale m1 en dehors de cette plage.

Fonction mathématique métrique	Cas d’utilisation	Explication
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 0, m1)`	Supprimez l'alarme entre 11 h 00 et 13 h 00 UTC tous les jours en remplaçant les points de données réels par 0 pendant cette fenêtre.	• HEURE (m1) >= 11 && HEURE (m1) < 13 : capture la plage horaire comprise entre 11 h 00 et 13 h 00 UTC. • IF (condition, value_if_ true, value_if_false) : si la condition est vraie (par exemple, l'heure est comprise entre 11 h 00 et 13 h 00 UTC), renvoie 0. Si la condition est fausse, conservez la valeur métrique d'origine (m1).
`IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 99, m1)`	Supprimez l'alarme entre 1 h 00 et 3 h 00 UTC tous les mardis en remplaçant les points de données réels par 99 pendant cette fenêtre.	• JOUR (m1) == 2 : Garantit que c'est mardi (lundi = 1, dimanche = 7). • HEURE (m1) >= 1 && HEURE (m1) < 3 : Spécifie la plage horaire comprise entre 1 h et 3 h UTC. • IF (condition, value_if_ true, value_if_false) : si les conditions sont vraies, remplacez la valeur de la métrique par 99. Sinon, renvoyez la valeur d'origine (m1).

Fonction mathématique métrique	Cas d’utilisation	Explication
`IF((HOUR(m1) >= 23 || HOUR(m1) < 4), 100, m1)`	Supprimez l'alarme entre 23 h 00 et 4 h 00 UTC, tous les jours en remplaçant les points de données réels par 100 pendant cette fenêtre.	• HEURE (m1) >= 23 : capture les heures à partir de 23 h UTC. • HEURE (m1) < 4 : capture les heures jusqu'à (mais sans inclure) 04:00 UTC. • || : Logic OR garantit que la condition s'applique à deux plages : tard le soir et tôt le matin. • IF (condition, value_if_true, value_if_false) : renvoie 100 pendant la période spécifiée. Conserve la valeur métrique initiale m1 en dehors de cette plage.
`IF((HOUR(m1) >= 11 && HOUR(m1) < 13), 99, m1)`	Supprimez l'alarme entre 11 h 00 et 13 h 00 UTC tous les jours en remplaçant les points de données réels par 99 pendant cette fenêtre.	• HEURE (m1) >= 11 && HEURE (m1) < 13 : capture la plage horaire comprise entre 11 h 00 et 13 h 00 UTC. • IF (condition, value_if_ true, value_if_false) : si la condition est vraie (par exemple, l'heure est comprise entre 11 h et 13 h UTC), renvoie 99. Si la condition est fausse, conservez la valeur métrique d'origine (m1).

Supprimer les alarmes provenant d'un APM tiers

Consultez la documentation de votre fournisseur APM tiers pour obtenir des instructions sur la manière de supprimer les alarmes. New Relic, Splunk, Dynatrace, Datadog et. SumoLogic

Soumettre une demande de modification de la charge de travail pour supprimer les alarmes

Si vous ne parvenez pas à supprimer les alarmes à la source comme décrit dans la section précédente, soumettez une demande de modification de la charge de travail pour demander à Incident Detection and Response de supprimer manuellement la surveillance de certaines ou de toutes les alarmes relatives à votre charge de travail.

Pour obtenir des instructions détaillées sur la façon de créer une demande de modification de charge de travail, voir Demander des modifications à une charge de travail intégrée dans Détection et réponse aux incidents. Lorsque vous soumettez une demande de modification de la charge de travail pour demander la suppression de vos alarmes, assurez-vous de fournir les informations requises suivantes

- Nom de charge de travail : nom de votre charge de travail.
- Identifiant (s) de compte : ID1, ID2, ID3, et ainsi de suite.
- Détails des modifications : Suppression des alarmes
- Heure de début de suppression : date, heure et fuseau horaire.
- Heure de fin de suppression : date, heure et fuseau horaire.
- Alarmes à supprimer : liste d' CloudWatch alarmes ARNs ou d'identifiants d'événements APM tiers à supprimer.

Après avoir créé la demande de modification de la charge de travail de suppression des alarmes, vous recevez les notifications suivantes de la part de Incident Detection and Response :

- Accusé de réception de votre demande de modification de la charge de travail.
- Notification lorsque les alarmes sont supprimées.
- Notification lorsque les alarmes sont réactivées pour la surveillance.

Tutoriel : Utiliser une fonction mathématique métrique pour supprimer une alarme

Le didacticiel suivant explique comment supprimer une CloudWatch alarme à l'aide des mathématiques métriques.

Exemple de scénario

Une activité est prévue entre 1 h 00 et 3 h 00 UTC le mardi prochain. Vous souhaitez créer une fonction mathématique CloudWatch métrique qui remplace les points de données réels pendant cette période par 0 (un point de données inférieur au seuil défini).

1. Évaluez les critères qui déclenchent votre alarme. La capture d'écran suivante fournit un exemple de critères d'alarme :

   L'alarme illustrée dans la capture d'écran précédente surveille la `UnHealthyHostCount` métrique pour un groupe cible d'Application Load Balancer. Cette alarme entre dans l'`ALARM`état lorsque la `UnHealthyHostCount` métrique est supérieure ou égale à 3 pour 5 points de données sur 5. L'alarme considère les données manquantes comme étant incorrectes (franchissant le seuil configuré).
2. Créez la fonction mathématique métrique.

   Dans cet exemple, l'activité planifiée a lieu entre 1 h 00 et 3 h 00 UTC le mardi suivant. Créez donc une fonction mathématique CloudWatch métrique qui remplace les points de données réels pendant cette période par 0 (un point de données inférieur au seuil défini).

   Notez que le point de données de remplacement que vous devez configurer varie en fonction de la configuration de votre alarme. Par exemple, si vous avez une alarme qui surveille le taux de réussite HTTP, avec un seuil inférieur à 98, remplacez vos points de données réels pendant l'activité planifiée par une valeur supérieure au seuil configuré, 100. Voici un exemple de fonction mathématique métrique pour ce scénario.

   ```
   IF((DAY(m1) == 2 && HOUR(m1) >= 1 && HOUR(m1) < 3), 0, m1)
   ```

   La fonction mathématique métrique précédente contient les éléments suivants :

   - JOUR (m1) == 2 : garantit que c'est mardi (lundi = 1, dimanche = 7).

- HEURE (m1) >= 1 && HEURE (m1) < 3 : Spécifie la plage horaire comprise entre 1 h et 3 h UTC.
- IF (condition, value_if_true, value_if_false) : si les conditions sont vraies, la fonction remplace la valeur de la métrique par 0. Dans le cas contraire, la valeur d'origine (m1) est renvoyée.

Pour plus d'informations sur la syntaxe et les fonctions disponibles, consultez Syntaxe et fonctions mathématiques métriques dans le guide de CloudWatch l'utilisateur Amazon

3. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
4. Choisissez Alarmes, puis localisez l'alarme à laquelle vous souhaitez ajouter la fonction mathématique métrique.
5. Dans la section des mathématiques métriques, choisissez Modifier.
6. Choisissez Ajouter des données mathématiques, puis Commencer par une expression vide.
7. Entrez votre expression mathématique, puis choisissez Appliquer.

   La métrique existante surveillée automatiquement par l'alarme devient m1 et votre expression mathématique est e1, comme illustré dans l'exemple suivant :

8. (Facultatif) Modifiez l'étiquette de l'expression mathématique métrique pour aider les autres utilisateurs à comprendre sa fonction et pourquoi elle a été créée, comme indiqué dans l'exemple suivant :

9. Désélectionnez m1, sélectionnez e1, puis sélectionnez Sélectionner une métrique. Cela permet de configurer l'alarme pour qu'elle surveille directement l'expression mathématique au lieu de la métrique sous-jacente.
10. Choisissez Passer à l'aperçu et créez.
11. Vérifiez que l'alarme est configurée comme prévu, puis choisissez Mettre à jour l'alarme pour enregistrer la modification.

Dans l'exemple précédent, sans l'application de la fonction mathématique métrique, la `UnHealthyHostCount` métrique réelle aurait été signalée lors de l'activité planifiée. Cela aurait entraîné l'entrée en `ALARM` état de l' CloudWatch alarme et l'activation de la détection et de la réponse aux incidents, comme le montre l'exemple suivant :

Lorsque la fonction mathématique métrique est en place, les points de données réels sont remplacés par 0 pendant l'activité, et l'alarme reste active, ce qui supprime 0K l'engagement de détection et de réponse aux incidents.

Tutoriel : Supprimer une fonction mathématique métrique pour annuler la suppression d'une alarme

Si vous supprimez une CloudWatch alarme pour une activité ponctuelle, supprimez la fonction mathématique métrique de l'alarme une fois l'activité terminée afin de reprendre le suivi régulier de l'alarme. Pour supprimer l'alarme selon un calendrier régulier, par exemple, si vous avez une routine de correction hebdomadaire planifiée qui entraîne le redémarrage de l'instance le même jour et à la même heure chaque semaine, laissez la fonction mathématique métrique en place.

Le didacticiel suivant explique comment supprimer une fonction mathématique métrique pour annuler la suppression d'une CloudWatch alarme.

1. Connectez-vous à la CloudWatch console AWS Management Console et ouvrez-la à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Choisissez Alarmes, puis localisez l'alarme à laquelle vous souhaitez ajouter la fonction mathématique métrique.
3. Dans la section des mathématiques métriques, choisissez Modifier.
4. Pour supprimer la suppression de l'alarme, sélectionnez le bouton x à côté de l'expression mathématique métrique.
5. Sélectionnez la métrique pour reprendre le suivi de la métrique réelle, puis choisissez Select metric.
6. Choisissez Passer à l'aperçu et créez.
7. Vérifiez que l'alarme est configurée comme prévu, puis choisissez Mettre à jour l'alarme pour enregistrer la modification.

Décharger une charge de travail de la fonction de détection et de réponse aux incidents

Pour décharger une charge de travail d'AWS Incident Detection and Response, créez un nouveau dossier de support pour chaque charge de travail. Lorsque vous créez le dossier de support, gardez à l'esprit les points suivants :

- Pour décharger une charge de travail enregistrée sur un seul AWS compte, créez le dossier d'assistance soit à partir du compte de la charge de travail, soit à partir de votre compte payeur.
- Pour décharger une charge de travail qui couvre plusieurs AWS comptes, créez le dossier d'assistance à partir de votre compte payeur. Dans le corps du dossier d'assistance, listez tous les identifiants de compte à déconnecter.

> **Important**
>
> Si vous créez un dossier d'assistance pour décharger une charge de travail d'un compte incorrect, 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 Centre, 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 incidents AWS - *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, etc.
- Motif du désenclavement : indiquez le motif du déchargement de la charge de travail.

8. Dans la section Contacts supplémentaires - facultatif, entrez les adresses e-mail auxquelles vous souhaitez recevoir de la correspondance concernant cette demande de désenclavement.
9. Sélectionnez Soumettre.

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. Pour en savoir plus sur l'utilisation de l'interface de ligne de commande client AWS Incident Detection and Response afin d'automatiser ces étapes, consultez la CLI pour AWS Incident Detection and Response.
- Post-onboarding phase : 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 incidents avec détection et réponse aux incidents

AWS Incident Detection and Response vous propose une surveillance proactive et une gestion des incidents 24 heures sur 24, 7 jours sur 7, assurées par une équipe désignée de gestionnaires d'incidents. Le schéma suivant décrit le processus standard de gestion des incidents lorsqu'une alarme d'application déclenche un incident, y compris la génération d'alarmes, AWS l'engagement du gestionnaire d'incidents, la résolution des incidents et l'examen post-incident.

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 extrait 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 qu'il 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 à l'incident. Pour plus d'informations sur la demande de réponse à un incident, consultezDemander une 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 du Services AWS pour déterminer si l'alarme est liée à des problèmes liés à l' Services AWS utilisation 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 les bons AWS experts pour obtenir de l'aide. Dans la mesure où AWS Incident Detection and Response surveille Services AWS spécifiquement pour vos applications, AWS Incident Detection and Response peut déterminer que l'incident est lié à un Service AWS problème avant qu'un Service AWS événement ne soit déclaré. Dans ce scénario, le responsable des incidents vous conseille sur l'état de l' Service AWS événement Service AWS, déclenche le flux de travail de gestion des incidents et assure le 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 l' Service AWS événement.

   Parfois, les alarmes se déclenchent et se rétablissent rapidement. Dans ce scénario, le responsable des incidents envoie une correspondance indiquant que l'alarme est rétablie, mais ne vous contacte pas. Toutefois, si une alarme se déclenche plusieurs fois dans les 15 minutes, le

gestionnaire des incidents vous contacte conformément aux instructions de votre manuel, même si l'alarme se rétablit.

3. Résolution des incidents : le responsable des incidents coordonne l'incident au sein des AWS équipes requises et veille à ce que vous restiez en contact avec les bons AWS experts jusqu'à ce que l'incident soit atténué ou résolu.
4. Examen post-incident (si demandé) : après un incident, AWS 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 RCA en plus du 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 Support support case on behalf of the customer.
At 2023-02-04T03:32:00 UTC, ** the customer's SRE team, and 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 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 a 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.

Rubriques

Fournir un accès à AWS Support Center Console pour les équipes de candidature

AWS Incident Detection and Response communique avec vous en Support cas de problème pendant le cycle de vie d'un incident. Pour correspondre avec les responsables des incidents, vos équipes doivent avoir accès au Support centre.

Pour plus d'informations sur le provisionnement de l'accès, voir Gérer l'accès au Support centre dans le guide de l'Support utilisateur.

Demander une réponse à un incident

Si un incident critique survient sur votre charge de travail et qu'il 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 à l'incident. 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, à l'aide de l' AWS Support Center Console AWS Support API ou. AWS Support App in Slack

Le schéma suivant illustre le flux de travail de bout en bout pour un AWS client demandant une assistance en cas d'incident à l'équipe de détection et de réponse aux incidents, en détaillant les étapes allant de la demande initiale à l'investigation, à l'atténuation et à la résolution.

Pour demander une réponse à un incident ayant un impact actif sur votre charge de travail, créez un Support dossier. Une fois le dossier d'assistance soulevé, AWS Incident Detection and Response vous invite à participer à une conférence avec les 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

Pour demander une réponse à un incident, procédez comme suit :

1. Ouvrez le AWS Support Center Consolepour créer un nouveau dossier de support.
2. Dans le champ Objet, entrez un bref résumé de l'incident. Par exemple, `AWS Incident Detection and Response - Active Incident - workload_name`.
3. Dans le champ Description, entrez les détails de l'incident. Nous vous recommandons d'inclure les informations suivantes dans votre dossier d'assistance :
   - ARN (s) AWS des ressources concernées, nom de la charge de travail et fonction de celle-ci
   - Description de l'impact sur l'entreprise
   - (Facultatif) L'URL de votre pont de conférence préféré. Si vous ne fournissez pas les détails du pont, AWS Incident Detection and Response crée un pont de AWS conférence et vous envoie une invitation avec l'URL du pont.
4. (Facultatif) Joignez des fichiers qui peuvent aider à décrire l'incident, tels que des captures d'écran ou des extraits de journal.
5. Configurez les champs de classification des cas suivants :
   - Type de boîtier : Technique
   - Service : Détection et réponse aux incidents
   - Catégorie : Incident actif
   - Gravité : panne Business-critical du système
6. Fournissez un contexte supplémentaire pour aider AWS Incident Detection and Response à impliquer plus rapidement les AWS experts, notamment en ce qui concerne les personnes touchées Service AWS Région AWS, l'impact commercial, l'heure de début de l'impact et les ressources concernées.
7. Sélectionnez Soumettre.
8. AWS Incident Detection and Response accuse réception de votre dossier dans les cinq minutes et vous invite à participer à une conférence avec les AWS experts appropriés.

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

Vous pouvez utiliser l' AWS Support API pour créer des dossiers de support par programmation. Pour plus d'informations, consultez la section À propos de l' AWS Support API dans le guide de AWS Support l'utilisateur.

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

Pour utiliser le AWS Support App in Slack pour demander une réponse à un incident, procédez comme suit :

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

```
/awssupport create
```

3. Entrez un sujet pour cet incident. Par exemple, saisissez 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. Dans le champ Severity, sélectionnez Business-critical System Down.
10. Entrez éventuellement jusqu'à 10 contacts supplémentaires dans le champ Contacts supplémentaires à notifier, séparés par des virgules. Ces contacts supplémentaires reçoivent des copies des courriers électroniques concernant cet incident.
11. Choisissez Examiner.
12. Un nouveau message qui n'est visible que par vous apparaît dans la chaîne Slack. Passez en revue les détails du dossier, puis choisissez Créer un dossier.
13. Votre numéro de dossier est fourni dans un nouveau message du AWS Support App in Slack.
14. Incident Detection and Response accuse réception de votre dossier dans les 5 minutes et vous invite à participer à une conférence avec les AWS experts appropriés.
15. La correspondance provenant de Incident Detection and Response est mise à jour dans le fil de discussion du dossier.

Gérez les cas d'assistance relatifs à la détection et à la réponse aux incidents grâce au AWS Support App in Slack

Vous pouvez ainsi gérer vos Support dossiers dans Slack AWS Support App in Slack, recevoir des notifications concernant de nouveaux incidents déclenchés par des alarmes sur votre charge de travail AWS Incident Detection and Response, et créer des demandes de réponse aux incidents.

Pour configurer le AWS Support App in Slack, suivez les instructions fournies dans le guide de Support l'utilisateur.

> **Important**
>
> - Pour recevoir des notifications dans Slack concernant tous les incidents déclenchés par une alarme sur votre charge de travail, vous devez configurer les comptes AWS Support App in Slack pour tous les comptes de votre charge de travail intégrés à AWS Incident

Detection and Response. Support : les dossiers de support sont créés dans le compte d'origine de l'alarme de charge de travail.

- Plusieurs dossiers d'assistance très sévères peuvent être ouverts en votre nom lors d'un incident afin d'impliquer les 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 Incident Detection and Response lors d'un incident.

Rubriques

Notifications d'incidents déclenchées par une alarme dans Slack

Après avoir configuré le AWS Support App in Slack dans votre canal Slack, vous recevez des notifications concernant les incidents déclenchés par des alarmes sur votre charge de travail surveillée par AWS Incident Detection and Response.

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 une alarme est reconnu par AWS Incident Detection and Response, une notification similaire à la suivante est générée dans Slack :

Pour consulter l'intégralité de la correspondance ajoutée par AWS Incident Detection and Response, sélectionnez Voir les détails.

D'autres mises à jour d'AWS Incident Detection and Response figurent dans le fil de discussion de l'affaire.

Choisissez Voir les détails pour consulter l'intégralité de la correspondance ajoutée par AWS Incident Detection and Response.

Création d'une demande de réponse à un incident dans Slack

Pour obtenir des instructions sur la façon de créer une demande de réponse à un incident via le AWS Support App in Slack, voirDemander une réponse à un incident.

Création de rapports en matière 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. Cette page couvre les types de données disponibles, notamment les données de configuration, les données d'incident et les données de performance.

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 post-incident

Données de performance

- Performance des 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 responsabilitéAWS partagée s'applique à la protection des données dans 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 responsabilitéAWS 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 Gestion des identités et des accès AWS (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 des certificats Layer/Transport Layer Security (SSL/TLS (Secure Sockets) pour communiquer avec AWS les ressources. 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 qu'ils contiennent Services AWS.
- 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 Support ou d'autres personnes à Services AWS l'aide de la console, de l'API, de la AWS CLI ou AWS SDKs. 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

Gestion des identités et des accès AWS (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 guide IDR.

Modifier	Description	Date
Procédure de demande de réponse aux incidents mise à jour	Mise à jour de la procédure de demande de réponse à un incident pour qu'elle correspon de à l' AWS Support Center Console interface utilisateur actuelle, ajout de directives relatives à l'URL du pont et suppression des captures d'écran obsolètes. Pour de plus amples informations, veuillez consulter Demandez une réponse à un incident à l'aide du AWS Support Center Console.	12 mai 2026
Mise à jour de l'intégration à l'approche CLI-first	Le chapitre « Commencer » a été mis à jour afin de promouvoir l'interface de ligne de commande client AWS Incident Detection and Response en tant que principale méthode d'intégration et a déconseillé le questionn aire d'intégration de la charge de travail et le questionnaire d'ingestion des alarmes comme processus d'intégration par défaut. Les questionnaires restent disponibles en tant qu'option exceptionnelle pour les clients qui ne peuvent pas utiliser la CLI IDR. Pour plus d’informations, consultez Intégrez les charges de travail à la détection et à la réponse aux incidents et Ingestion d'alarmes.	12 mai 2026
Ajout de liens vers des questionnaires japonais	Ajout de liens de Japanese-language télécharg ement pour le questionnaire d'intégration de la	20 avril 2026

Modifier	Description	Date
	charge de travail et le questionnaire d'ingestion des alarmes. Pour de plus amples informations, veuillez consulter Questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans Incident Detection and Response (chemin d'exception).	
Références d'architecture mises à jour	Les références aux diagrammes d'architecture ont été supprimées et remplacées par des détails d'architecture. Pour plus d'informations, consultez Architecture de détection et de réponse aux incidents et À propos des charges de travail dans Incident Detection and Response.	31 mars 2026
Mise à jour des charges de travail intégrées aux tests dans le domaine de la détection et de la réponse aux incidents	Ajout d'informations sur la désactivation des actions CloudWatch d'alarme avant de modifier l'état de l'alarme pendant les tests. Pour de plus amples informations, veuillez consulter Testez les charges de travail intégrées dans le domaine de la détection et de la réponse aux incidents.	2 mars 2026
Gestion des incidents actualisée avec détection et réponse aux incidents	Ajout d'informations sur le comportement récurrent des alarmes et l'engagement du gestionnaire d'incidents. Pour de plus amples informations, veuillez consulter Gestion des incidents avec détection et réponse aux incidents.	2 mars 2026

Modifier	Description	Date
Étapes mises à jour de la section Utiliser une fonction mathématique métrique pour supprimer une CloudWatch alarme	Étapes mises à jour de la section Utiliser une métrique mathématique pour supprimer une CloudWatch alarme. Pour de plus amples informations, veuillez consulter Supprimer les alarmes à la source de l'alarme.	3 février 2026
Ajout du coréen comme langue prise en charge	Le coréen a été ajouté comme langue prise en charge. Pour de plus amples informations, veuillez consulter Disponibilité des régions pour la détection et la réponse aux incidents.	22 janvier 2026
Ajout du mandarin comme langue prise en charge	Le mandarin a été ajouté comme langue prise en charge. Pour de plus amples informations, veuillez consulter Disponibilité des régions pour la détection et la réponse aux incidents.	13 janvier 2026
Ajout d'une nouvelle section : Interface de ligne de commande client AWS pour la détection et la réponse aux incidents	Ajout de la section IDR CLI et mise à jour du chapitre Get started pour inclure des informati ons sur l'interface de ligne de commande client AWS Incident Detection and Response. Pour plus d'informations, consultez la section CLI pour AWS Incident Detection and Response.	8 décembre 2025

Modifier	Description	Date
Plusieurs sections ont été mises à jour : questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans la section Détection et réponse aux incidents et prise en main dans la détection et la réponse aux incidents	Le processus de gestion des Service AWS événements ne fait plus partie d'AWS Incident Detection and Response. Les sections de ce guide de l'utilisateur ont été mises à jour pour supprimer les références à ce processus . Vous continuerez à recevoir des notificat ions d'événements liés au service via le AWS Service Health Dashboard. Les clients d'AWS Incident Detection and Response peuvent utiliser une demande de réponse aux incidents pour recevoir de l'aide lors d'événements de service, le cas échéant. Pour de plus amples informations, veuillez consulter Demander une réponse à un incident.	14 octobre 2025
Section supprimée : Gestion des incidents pour les événements de service	Le processus de gestion des Service AWS événements ne fait plus partie d'AWS Incident Detection and Response. Cette section du guide de l'utilisateur a été supprimée pour refléter cette modification. Vous continuerez à recevoir des notifications d'événements liés au service via le AWS Service Health Dashboard . Les clients d'AWS Incident Detection and Response peuvent utiliser une demande de réponse aux incidents pour recevoir de l'aide lors d'événements de service, le cas échéant. Pour de plus amples informations, veuillez consulter Demander une réponse à un incident.	14 octobre 2025

Modifier	Description	Date
Section mise à jour : disponibilité des régions pour la détection et la réponse aux incidents	AWS Incident Detection and Response est désormais disponible en AWS GovCloud (US-East) et AWS GovCloud (US-West). Pour de plus amples informations, consultez Disponibilité des régions pour la détection et la réponse aux incidents.	05 octobre 2025
Section mise à jour : questionnaires d'intégration de la charge de travail et d'ingestion d'alarmes dans Incident Detection and Response	Exemple d'adresse e-mail mis à jour pour le tableau de la matrice des alarmes.	26 août 2025
Section mise à jour : Abonnement d'une charge de travail à AWS Incident Detection and Response	La référence au champ Date de début de l'abonnement a été supprimée dans la section Description de la fenêtre Créer un dossier. Section mise à jour : Abonnement d'une charge de travail à AWS Incident Detection and Response	4 août 2025
Nouvelle fonction : empêcher les alarmes de déclencher la détection et la réponse aux incidents	Ajout de nouvelles sections aux charges de travail gérées qui fournissent des informations sur la façon de supprimer les alarmes, temporairement ou selon un calendrier Nouvelle section : Empêcher les alarmes de déclencher la détection et la réponse aux incidents	9 avril 2025
Instructions mises à jour pour demander une réponse à un incident à l'aide du AWS Support Center Console	Ajout de détails sur les informations à saisir dans le champ Description du problème. Section mise à jour : Demander une réponse à un incident	6 février 2025

Modifier	Description	Date
Ajout Régions AWS supplémentaire	Des informations supplémentaires Régions AWS ont été ajoutées à la section Disponibilité de la détection et de la réponse aux incidents. Section mise à jour : Disponibilité des régions pour la détection et la réponse aux incidents	1er novembre 2024
Mises à jour pour gérer les cas d'assistance relatifs à la détection et à la réponse aux incidents avec la AWS Support App in Slack page	Page déplacée sous Gestion des incidents, texte révisé et captures d'écran remplacées. Section mise à jour : Gérez les cas d'assistance relatifs à la détection et à la réponse aux incidents grâce au AWS Support App in Slack	10 octobre 2024
Ajout d'une nouvelle page AWS Support App in Slack Gestion des incidents mise à jour avec AWS Incident Detection and Response	Ajout d'une nouvelle page pour AWS Support App in Slack Gestion des incidents mise à jour avec AWS Incident Detection and Response pour ajouter une nouvelle section intitulée « Demander une réponse aux incidents à l'aide du AWS Support App in Slack ».	10 septembre 2024
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. Section mise à jour : Abonnement d'une charge de travail à AWS Incident Detection and Response	12 juin 2024

Modifier	Description	Date
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 Pour de plus amples informations, veuillez consulter Décharger une charge de travail de la fonction de détection et de réponse aux incidents.	28 mars 2024
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 Pour plus d'informations, consultez Abonnement d'une charge de travail à AWS Incident Detection and Response	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. Section mise à jour : Testez les charges de travail intégrées dans le domaine de la détection et de la réponse aux incidents	29 février 2024
Mise à jour : qu'est-ce qu'AWS Incident Detection and Response ?	Mise à jour de la section Qu'est-ce qu'AWS Incident Detection and Response ? Section mise à jour : Qu'est-ce qu'AWS Incident Detection and Response ?	19 février 2024

Modifier	Description	Date
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.	2 février 2024
Informations mises à jour sur l'événement de AWS service et l'intégration	Plusieurs sections ont été mises à jour avec de nouvelles informations pour l'intégration. Sections mises à jour : • Intégrez les charges de travail à la détection et à la réponse aux incidents • Abonnement d'une charge de travail à AWS Incident Detection and Response Nouvelles sections • Fournir un accès à AWS Support Center Console pour les équipes de candidature	31 janvier 2024
Ajout d'une section d'informations connexes	Ajout d'une section d'informations connexes dans le provisionnement des accès. Section mise à jour : Fournir un accès pour l'ingestion des alarmes à la détection et à la réponse aux incidents	17 janvier 2024
Exemples d'étapes mis à jour	Mise à jour de la procédure pour les étapes 2, 3 et 4 dans Exemple : intégration des notifications de Datadog et Splunk. Section mise à jour : Exemple : intégration des notifications de Datadog et Splunk	21 décembre 2023

Modifier	Description	Date
Graphisme et texte d'introduction mis à jour	Graphique mis à jour dans Ingest alarmes provenant d'APM directement intégrés à Amazon. EventBridge Section mise à jour : Développez des guides et des plans de réponse pour répondre à un incident dans le cadre de la détection et de la réponse aux incidents	21 décembre 2023
Modèle de runbook mis à jour	Le modèle de runbook a été mis à jour dans Developing runbooks for AWS Incident Detection and Response. Section mise à jour : Développez des guides et des plans de réponse pour répondre à un incident dans le cadre de la détection et de la réponse aux incidents	4 décembre 2023
Configurations d'alarme actualisées	Configurations d'alarme mises à jour avec des informations détaillées sur la configuration des CloudWatch alarmes. Nouvelle section : Créez des CloudWatch alarmes adaptées aux besoins de votre entreprise en matière de détection et de réponse aux incidents Nouvelle section : Création d' CloudWatch alarmes dans la fonction de détection et de réponse aux incidents à l'aide CloudFormation de modèles Nouvelle section : Exemples de cas d'utilisation des CloudWatch alarmes dans le cadre de la détection et de la réponse aux incidents	28 septembre 2023

Modifier	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 Nouvelle section : Demander des modifications à une charge de travail intégrée dans Incident Detection and Response Section mise à jour : Abonnement d'une charge de travail à AWS Incident Detection and Response	05 septembre 2023
Nouvelle section dans Getting Started	Ajout d'alertes d'ingestion dans AWS Incident Detection and Response.	30 juin 2023
Document original	AWS Incident Detection and Response a été publié pour la première fois	15 mars 2023

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.