aws

Guide de l’utilisateur

Incident Manager

Incident Manager: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Systems Manager Incident Manager ?

Incident Manager, un outil AWS Systems Manager intégré, est conçu pour vous aider à atténuer les incidents affectant vos applications hébergées sur AWS.

Dans le contexte d'un incident AWS, on entend toute interruption ou réduction imprévue de la qualité des services qui peut avoir un impact significatif sur les opérations commerciales. Il est donc essentiel que les entreprises établissent une stratégie de réponse pour atténuer efficacement les incidents et s'en remettre, et mettent en œuvre des mesures pour prévenir de futurs incidents.

Le gestionnaire d'incidents permet de réduire le délai de résolution des incidents en :

- Fournir des plans automatisés pour impliquer efficacement les personnes chargées de répondre aux incidents.
- Fournir des données de dépannage pertinentes.
- Activation des actions de réponse automatisées à l'aide de runbooks d'automatisation prédéfinis.
- Fournir des méthodes pour collaborer et communiquer avec toutes les parties prenantes.

Les fonctionnalités et les flux de travail intégrés à Incident Manager sont basés sur les meilleures pratiques de réponse aux incidents développées par Amazon presque depuis sa création. Incident Manager Services AWS s'intègre à Amazon CloudWatch AWS CloudTrail, AWS Systems Manager, et Amazon EventBridge.

Composants et fonctionnalités principaux

Cette section décrit les fonctionnalités d'Incident Manager que vous utilisez pour configurer vos plans de réponse aux incidents.

Plan de réponse

Un plan d'intervention fonctionne comme un modèle qui définit ce qui doit être mis en place en cas d'incident. Il comprend des informations telles que :

- Qui est tenu d'intervenir en cas d'incident.
- La réponse automatisée établie pour atténuer l'incident.

- L'outil de collaboration que les intervenants doivent utiliser pour communiquer et recevoir des notifications automatiques concernant l'incident.

Détection des incidents

Vous pouvez configurer les CloudWatch alarmes Amazon et les EventBridge événements Amazon pour créer des incidents lorsque des conditions ou des modifications affectant vos AWS ressources sont détectées.

Support d'automatisation de Runbook

Vous pouvez lancer des runbooks d'automatisation depuis Incident Manager pour automatiser votre réponse critique aux incidents et fournir des étapes détaillées aux premiers intervenants.

Engagement et escalade

Un plan d'engagement indique à tout le monde qu'il convient de notifier pour chaque incident unique. Vous pouvez spécifier les contacts individuels que vous avez ajoutés à Incident Manager ou spécifier un calendrier d'astreinte que vous avez créé dans Incident Manager. Les plans d'engagement précisent également une trajectoire d'escalade afin de garantir la visibilité auprès des parties prenantes et une participation active au cours du processus de réponse aux incidents.

Horaires d'astreinte

Un calendrier d'astreinte dans Incident Manager consiste en une ou plusieurs rotations que vous créez pour le calendrier. Pour chaque rotation, vous pouvez inclure jusqu'à 30 contacts. Lorsqu'il est ajouté à un plan d'escalade ou à un plan d'intervention, le calendrier d'astreinte définit qui est averti lorsqu'un incident nécessitant l'intervention d'un intervenant survient. Les horaires d'astreinte vous permettent de bénéficier d'une couverture complète, redondante, 24 heures sur 24, 7 jours sur 7, selon les besoins de votre intervention en cas d'incident.

Collaboration active

Les équipes de réponse aux incidents répondent activement aux incidents grâce à l'intégration du client Amazon Q Developer dans les applications de chat. Dans les applications de chat, Amazon Q Developer prend en charge la création de canaux de discussion pour Incident Manager qui utilisent Slack, Microsoft Teams, ou Amazon Chime. Les intervenants peuvent communiquer directement entre eux, recevoir des notifications automatisées concernant les incidents et, dans Slack and Microsoft Teams: exécute directement certaines opérations de l'interface de ligne de commande (CLI) d'Incident Manager.

Diagnostic de l'incident

Les intervenants peuvent consulter les up-to-date informations dans la console Incident Manager lors d'un incident. Sur la base des modifications apportées aux informations, les intervenants peuvent ensuite créer des éléments de suivi et y remédier à l'aide des runbooks d'automatisation.

Conclusions provenant d'autres services

Pour aider les intervenants à diagnostiquer les incidents, vous pouvez activer la fonctionnalité Résultats dans Incident Manager. Les résultats sont des informations sur AWS CodeDeploy les déploiements et les mises à jour de AWS CloudFormation stack survenus au moment d'un incident et impliquant une ou plusieurs ressources probablement liées à l'incident. Le fait de disposer de ces informations réduit le temps nécessaire pour évaluer les causes potentielles, ce qui peut réduire le temps moyen de rétablissement (MTTR) après un incident.

Analyse post-incident

Une fois qu'un incident est résolu, vous utilisez une analyse post-incident pour identifier les améliorations à apporter à votre réponse aux incidents, notamment le délai de détection et d'atténuation. Une analyse peut également vous aider à comprendre la cause première des incidents. Incident Manager crée des mesures de suivi recommandées que vous pouvez utiliser pour améliorer votre réponse aux incidents.

Avantages de l'utilisation d'Incident Manager

Découvrez les avantages de l'utilisation d'Incident Manager dans le cadre de vos opérations de détection et de réponse aux incidents.

Cette section décrit les avantages que votre organisation peut tirer de la mise en œuvre d'un plan de réponse Incident Manager.

Diagnostiquez les problèmes de manière efficace et immédiate

CloudWatch Les alarmes Amazon et EventBridge les événements Amazon que vous configurez peuvent créer des incidents automatiquement en cas d'interruption imprévue ou de réduction de la qualité de vos services.

CloudWatch les alarmes détectent et signalent les modifications apportées à la valeur de la métrique ou de l'expression par rapport à un seuil sur un certain nombre de périodes. EventBridge les événements sont créés à la suite de modifications apportées à un environnement, à une application ou à un service que vous avez spécifié dans une EventBridge règle. Lorsque vous créez une alarme

ou un événement, vous pouvez spécifier une action pour un incident à créer dans Incident Manager et le plan de réponse approprié pour faciliter l'engagement, l'escalade et l'atténuation de l'incident.

Incident Manager permet de collecter et de suivre automatiquement les métriques liées à un incident, grâce à l'utilisation de CloudWatch métriques. Outre les métriques automatisées générées pour l'incident lorsqu'il est créé par le biais CloudWatch d'une alarme, vous pouvez ajouter des métriques manuellement en temps réel, afin de fournir un contexte et des données supplémentaires aux intervenants lors d'un incident.

Utilisez la chronologie des incidents d'Incident Manager pour afficher les points d'intérêt par ordre chronologique. Les intervenants peuvent également utiliser la chronologie pour ajouter des événements personnalisés afin de décrire ce qu'ils ont fait ou ce qui s'est passé. Les points d'intérêt automatisés incluent :

- Une CloudWatch alarme ou une EventBridge règle crée un incident.
- Les mesures relatives aux incidents sont communiquées à Incident Manager.
- Les intervenants sont mobilisés.
- Les étapes de Runbook se sont terminées avec succès.

Engagez-vous efficacement

Incident Manager réunit les intervenants en cas d'incident grâce à l'utilisation de contacts, de calendriers d'appel, de plans d'escalade et de canaux de discussion. Vous définissez des contacts individuels directement dans Incident Manager et définissez les préférences de contact (e-mail, SMS ou voix). Vous ajoutez des contacts aux rotations des horaires d'astreinte afin de déterminer qui est chargé de traiter les incidents au cours d'une période donnée. À l'aide de vos contacts définis et de vos horaires d'astreinte, vous créez des plans d'escalade pour engager les intervenants nécessaires au bon moment lors d'un incident.

Collaborez en temps réel

La communication lors d'un incident est la clé d'une résolution plus rapide. Utilisation d'un développeur Amazon Q dans les applications de chat configurées pour être utilisées Slack, Microsoft Teams, ou Amazon Chime, vous pouvez réunir les intervenants sur leur canal de discussion connecté préféré, où ils interagissent directement avec l'incident et entre eux. Incident Manager affiche également les actions en temps réel des intervenants sur le canal de discussion, fournissant ainsi un contexte aux autres.

Automatisez la restauration des services

Incident Manager permet à vos intervenants de se concentrer sur les tâches clés requises pour résoudre un incident grâce à l'utilisation de runbooks d'automatisation. Dans Incident Manager, les runbooks sont une série prédéfinie d'actions entreprises pour résoudre un incident. Ils combinent la puissance des tâches automatisées avec des étapes manuelles selon les besoins, ce qui permet aux intervenants d'être plus disponibles pour analyser et réagir à l'impact.

Prévenir les futurs incidents

Grâce à l'analyse post-incident d'Incident Manager, votre équipe peut développer des plans de réponse plus robustes et apporter des modifications à vos applications afin de prévenir de futurs incidents et interruptions de service. L'analyse post-incident permet également un apprentissage itératif et une amélioration des runbooks, des plans de réponse et des métriques.

Services connexes

Incident Manager s'intègre à plusieurs services Services AWS et outils tiers pour vous aider à détecter et à résoudre les incidents, à interagir indirectement avec ses opérations d'API et à gérer l'infrastructure. Pour plus d'informations, veuillez consulter Intégrations de produits et de services avec Incident Manager.

Accès au gestionnaire d'incidents

Vous pouvez accéder à Incident Manager de l'une des manières suivantes :

- La console Incident Manager
- AWS CLI— Pour des informations générales, reportez-vous à la section Getting started with the AWS CLI in the AWS Command Line Interface User Guide. Pour plus d'informations sur les commandes CLI pour Incident Manager, voir ssm-incidents et ssm-contactsdans la référence de AWS CLI commande.
- API Incident Manager — Pour plus d'informations, consultez la référence de l'AWS Systems Manager Incident Manager API.
- AWS SDKs— Pour plus d'informations, voir Outils sur lesquels s'appuyer AWS.

Régions et quotas du gestionnaire d'incidents

Incident Manager n'est pas pris en Régions AWS charge dans tous les cas par Systems Manager.

Pour consulter des informations sur les régions et les quotas d'Incident Manager, consultez la section AWS Systems Manager Incident Manager Points de terminaison et quotas dans le Référence générale d'Amazon Web Services.

Tarification pour Incident Manager

L'utilisation d'Incident Manager est payante. Pour plus d'informations, consultez la section Tarification de AWS Systems Manager.

> **Note**
>
> Les autres Services AWS AWS contenus et les contenus tiers mis à disposition dans le cadre de ce service peuvent être soumis à des frais distincts et régis par des conditions supplémentaires.

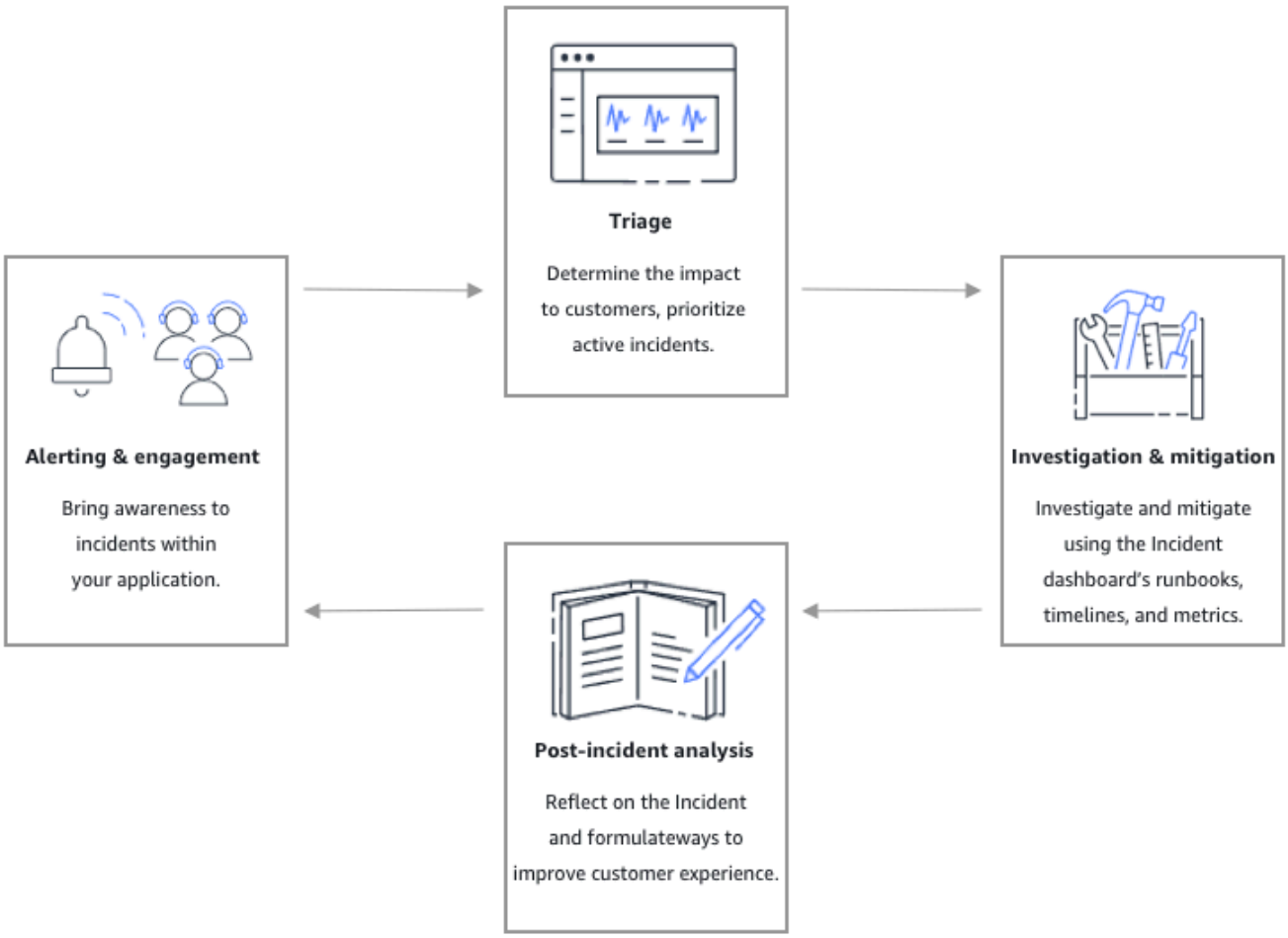
Pour obtenir une vue d' Trusted Advisor ensemble d'un service qui vous aide à optimiser les coûts, la sécurité et les performances de votre AWS environnement, consultez AWS Trusted Advisorle guide de AWS Support l'utilisateur.

Cycle de vie des incidents dans Incident Manager

AWS Systems Manager Incident Manager fournit un step-by-step cadre basé sur les meilleures pratiques pour identifier et réagir aux incidents, tels que les pannes de service ou les menaces de sécurité. L'objectif principal d'Incident Manager est d'aider à rétablir les services ou applications concernés à la normale le plus rapidement possible grâce à une solution complète de gestion du cycle de vie des incidents.

Comme illustré dans l'illustration suivante, Incident Manager fournit des outils et des meilleures pratiques pour chaque phase du cycle de vie des incidents :

- Alertes et engagement
- Tri
- Enquête et atténuation
- Analyse post-incident



Alertes et engagement

La phase d'alerte et d'engagement du cycle de vie des incidents vise à sensibiliser vos applications et services aux incidents. Cette phase commence avant qu'un incident ne soit détecté et nécessite une compréhension approfondie de vos applications. Vous pouvez utiliser CloudWatchles métriques Amazon pour surveiller les données relatives aux performances de vos applications, ou utiliser Amazon EventBridge pour agréger les alertes provenant de différentes sources, applications et services. Une fois que vous avez configuré la surveillance de vos applications, vous pouvez commencer à émettre des alertes sur les indicateurs qui s'écartent de la norme historique. Pour en savoir plus sur les meilleures pratiques en matière de surveillance, voirSurveillance.

Pour aider les intervenants à diagnostiquer les incidents, vous pouvez activer la fonctionnalité Résultats dans Incident Manager. Les résultats sont des informations sur AWS CodeDeploy les déploiements et les mises à jour de AWS CloudFormation stack survenus au moment d'un

incident. Le fait de disposer de ces informations réduit le temps nécessaire pour évaluer les causes potentielles, ce qui peut réduire le temps moyen de rétablissement (MTTR) après un incident.

Maintenant que vous surveillez les incidents dans vos applications, vous pouvez définir un plan de réponse aux incidents à utiliser lors d'un incident. Pour en savoir plus sur la création de plans d'intervention, voirCréation et configuration de plans de réponse dans Incident Manager. Amazon EventBridge Events or CloudWatch Alarms peut créer automatiquement un incident en utilisant des plans de réponse comme modèle. Pour en savoir plus sur la création d'incidents, voirCréation d'incidents automatiquement ou manuellement dans Incident Manager.

Les plans d'intervention lancent des plans d'escalade et des plans d'engagement connexes pour impliquer les premiers intervenants dans l'incident. Pour plus d'informations sur la configuration de plans d'escalade, consultezCréation d'un plan d'escalade. Simultanément, Amazon Q Developer dans les applications de chat avertit les intervenants via un canal de discussion les dirigeant vers la page détaillée de l'incident. À l'aide du canal de discussion et des détails de l'incident, l'équipe peut communiquer et trier un incident. Pour plus d'informations sur la configuration des canaux de discussion dans Incident Manager, consultezTâche 2 : créer un canal de discussion dans Amazon Q Developer dans les applications de chat.

Tri

Le triage est le moment où les premiers intervenants tentent de déterminer l'impact sur les clients. La vue détaillée de l'incident dans la console Incident Manager fournit aux intervenants des chronologies et des mesures pour les aider à évaluer l'incident. L'évaluation de l'impact d'un incident jette également les bases du temps de réponse, de résolution et de communication en cas d'incident. Les intervenants hiérarchisent les incidents en utilisant des cotes d'impact comprises entre 1 (critique) et 5 (aucun impact).

Votre organisation peut définir la portée exacte de chaque évaluation d'impact comme bon vous semble. Le tableau suivant fournit des exemples de la manière dont chaque niveau d'impact peut généralement être défini.

Code d'impact	Nom de l'impact	Exemple de portée définie
1	`Critical`	Défaillance complète de l'application qui a un impact sur la plupart des clients.

Code d'impact	Nom de l'impact	Exemple de portée définie
2	`High`	Défaillance complète de l'application ayant un impact sur un sous-ensemble de clients.
3	`Medium`	Défaillance partielle de l'application ayant un impact sur le client.
4	`Low`	Pannes intermittentes ayant un impact limité sur les clients.
5	`No Impact`	Les clients ne sont actuellem ent pas concernés, mais des mesures urgentes sont nécessaires pour éviter tout impact.

Enquête et atténuation

La vue détaillée de l'incident fournit à votre équipe des runbooks, des chronologies et des indicateurs. Pour savoir comment gérer un incident, consultez leAfficher les détails de l'incident dans la console.

Les runbooks fournissent généralement des étapes d'investigation et peuvent automatiquement extraire des données ou essayer des solutions couramment utilisées. Les Runbooks fournissent également des étapes claires et répétables que votre équipe a jugées utiles pour atténuer les incidents. L'onglet runbook se concentre sur l'étape actuelle du runbook et affiche les étapes passées et futures.

Incident Manager s'intègre à Systems Manager Automation pour créer des runbooks. Utilisez runbooks pour effectuer l'une des opérations suivantes :

- Gérer les instances et les AWS ressources
- Exécuter automatiquement des scripts
- Gérez les AWS CloudFormation ressources

Pour plus d'informations sur les types d'actions pris en charge, consultez la référence des actions d'automatisation de Systems Manager dans le guide de AWS Systems Manager l'utilisateur.

L'onglet Chronologie indique les actions entreprises. La chronologie enregistre chacune avec un horodatage et des détails créés automatiquement. Pour ajouter des événements personnalisés à la chronologie, consultez la Chronologie section de la page de détails de l'incident de ce guide de l'utilisateur.

L'onglet Diagnostic affiche les métriques renseignées automatiquement et les métriques ajoutées manuellement. Cette vue fournit des informations précieuses sur les activités de votre application lors d'un incident.

L'onglet Engagements vous permet d'ajouter des contacts supplémentaires à l'incident et de fournir les ressources nécessaires pour que le contact engagé soit rapidement mis au courant une fois impliqué dans l'incident. Les contacts sont engagés par le biais de plans d'escalade définis ou de plans d'engagement personnels.

À l'aide d'un canal de discussion, vous pouvez interagir directement avec votre incident et avec les autres intervenants de votre équipe. En utilisant Amazon Q Developer dans les applications de chat, vous pouvez configurer des canaux de discussion dans. Slack, Microsoft Teams, et Amazon Chime. Entrée Slack and Microsoft Teams canaux, les intervenants peuvent interagir avec les incidents directement depuis le canal de discussion à l'aide d'un certain nombre de `ssm-incidents` commandes. Pour de plus amples informations, veuillez consulter Interaction via le canal de discussion.

Analyse post-incident

Incident Manager fournit un cadre permettant de réfléchir à un incident, de prendre les mesures nécessaires pour empêcher que l'incident ne se reproduise à l'avenir et d'améliorer les activités de réponse aux incidents dans leur ensemble. Les améliorations peuvent inclure :

- Modifications apportées aux applications impliquées dans un incident. Votre équipe peut utiliser ce temps pour améliorer le système et le rendre plus tolérant aux pannes.
- Modifications apportées à un plan de réponse aux incidents. Prenez le temps d'intégrer les leçons apprises.
- Modifications apportées aux runbooks. Votre équipe peut étudier en profondeur les étapes nécessaires à la résolution et les étapes que vous pouvez automatiser.

- Modifications apportées aux alertes. Après un incident, votre équipe a peut-être remarqué des points critiques dans les indicateurs que vous pouvez utiliser pour alerter l'équipe plus rapidement en cas d'incident.

Incident Manager facilite ces améliorations potentielles en utilisant un ensemble de questions d'analyse post-incident et d'éléments d'action associés à la chronologie de l'incident. Pour en savoir plus sur l'amélioration par l'analyse, voirPerforming a post-incident analysis in Incident Manager.

Configuration de AWS Systems Manager Incident Manager

Nous vous recommandons de configurer AWS Systems Manager Incident Manager dans le compte que vous utilisez pour gérer vos opérations. Avant d'utiliser Incident Manager pour la première fois, effectuez les tâches suivantes :

Rubriques

Inscrivez-vous pour un Compte AWS

Si vous n'en avez pas Compte AWS, procédez comme suit pour en créer un.

Pour vous inscrire à un Compte AWS

1. Ouvrez l'https://portal.aws.amazon.com/billing/inscription.
2. Suivez les instructions en ligne.

   Une partie de la procédure d'inscription consiste à recevoir un appel téléphonique ou un message texte et à saisir un code de vérification sur le clavier du téléphone.

   Lorsque vous vous inscrivez à un Compte AWS, un Utilisateur racine d'un compte AWSest créé. Par défaut, seul l’utilisateur racine a accès à l’ensemble des Services AWS et des ressources de ce compte. La meilleure pratique de sécurité consiste à attribuer un accès administratif à un utilisateur, et à utiliser uniquement l’utilisateur racine pour effectuer les tâches nécessitant un accès utilisateur racine.

AWS vous envoie un e-mail de confirmation une fois le processus d'inscription terminé. À tout moment, vous pouvez consulter l'activité actuelle de votre compte et gérer votre compte en accédant à https://aws.amazon.com/et en choisissant Mon compte.

Création d'un utilisateur doté d'un accès administratif

Une fois que vous vous êtes inscrit à un utilisateur administratif Compte AWS, que vous Utilisateur racine d'un compte AWS l'avez sécurisé AWS IAM Identity Center, que vous l'avez activé et que vous en avez créé un, afin de ne pas utiliser l'utilisateur root pour les tâches quotidiennes.

Sécurisez votre Utilisateur racine d'un compte AWS

1. Connectez-vous en AWS Management Consoletant que propriétaire du compte en choisissant Utilisateur root et en saisissant votre adresse Compte AWS e-mail. Sur la page suivante, saisissez votre mot de passe.

   Pour obtenir de l'aide pour vous connecter en utilisant l'utilisateur racine, consultez Connexion en tant qu'utilisateur racine dans le Guide de l'utilisateur Connexion à AWS .
2. Activez l'authentification multifactorielle (MFA) pour votre utilisateur racine.

   Pour obtenir des instructions, consultez la section Activer un périphérique MFA virtuel pour votre utilisateur Compte AWS root (console) dans le guide de l'utilisateur IAM.

Création d'un utilisateur doté d'un accès administratif

1. Activez IAM Identity Center.

   Pour obtenir des instructions, consultez Activation d' AWS IAM Identity Center dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Dans IAM Identity Center, octroyez un accès administratif à un utilisateur.

   Pour un didacticiel sur l'utilisation du Répertoire IAM Identity Center comme source d'identité, voir Configurer l'accès utilisateur par défaut Répertoire IAM Identity Center dans le Guide de AWS IAM Identity Center l'utilisateur.

Connexion en tant qu'utilisateur doté d'un accès administratif

- Pour vous connecter avec votre utilisateur IAM Identity Center, utilisez l'URL de connexion qui a été envoyée à votre adresse e-mail lorsque vous avez créé l'utilisateur IAM Identity Center.

Pour obtenir de l'aide pour vous connecter en utilisant un utilisateur d'IAM Identity Center, consultez la section Connexion au portail AWS d'accès dans le guide de l'Connexion à AWS utilisateur.

Attribution d'un accès à d'autres utilisateurs

1. Dans IAM Identity Center, créez un ensemble d'autorisations qui respecte la bonne pratique consistant à appliquer les autorisations de moindre privilège.

   Pour obtenir des instructions, consultez Création d'un ensemble d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
2. Attribuez des utilisateurs à un groupe, puis attribuez un accès par authentification unique au groupe.

   Pour obtenir des instructions, consultez Ajout de groupes dans le Guide de l'utilisateur AWS IAM Identity Center .

Octroi d'un accès par programmation

Les utilisateurs ont besoin d'un accès programmatique s'ils souhaitent interagir avec AWS l'extérieur du AWS Management Console. La manière d'accorder un accès programmatique dépend du type d'utilisateur qui y accède AWS.

Pour accorder aux utilisateurs un accès programmatique, choisissez l'une des options suivantes.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
Identité de la main-d'œuvre (Utilisateurs gérés dans IAM Identity Center)	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Configuration du AWS CLI à utiliser AWS IAM Identity Center dans le

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
		guide de AWS Command Line Interface l'utilisateur. • Pour AWS SDKs, outils, et AWS APIs, voir Authentification IAM Identity Center dans le guide de référence AWS SDKs et Tools.
IAM	Utilisez des informations d'identification temporaires pour signer les demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de la section Utilisation d'informations d'identification temporaires avec AWS les ressources du Guide de l'utilisateur IAM.

Quel utilisateur a besoin d'un accès programmatique ?	Pour	Par
IAM	(Non recommandé) Utilisez des informations d'identification à long terme pour signer des demandes programmatiques adressées au AWS CLI AWS SDKs, ou AWS APIs.	Suivez les instructions de l'interface que vous souhaitez utiliser. • Pour le AWS CLI, voir Authentification à l'aide des informations d'identification utilisateur IAM dans le Guide de l'AWS Command Line Interface utilisateur. • Pour les outils AWS SDKs et, voir Authentifier à l'aide d'informations d'identif ication à long terme dans le guide de référence des outils AWS SDKs et. • Pour AWS APIs, voir Gestion des clés d'accès pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôle requis pour la configuration d'Incident Manager

Avant de commencer, votre compte doit disposer de l'autorisation `iam:CreateServiceLinkedRole` IAM. Incident Manager utilise cette autorisation pour créer le `AWSServiceRoleforIncidentManager` dans votre compte. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Incident Manager.

Commencer à utiliser Incident Manager

Cette section explique comment se préparer dans la console Incident Manager. Vous devez terminer Se préparer dans la console avant de pouvoir l'utiliser pour la gestion des incidents. L'assistant vous explique comment configurer votre ensemble de réplication, au moins un contact et un plan d'escalade, ainsi que votre premier plan de réponse. Les guides suivants vous aideront à comprendre Incident Manager et le cycle de vie des incidents :

- Qu'est-ce que c'est AWS Systems Manager Incident Manager ?
- Cycle de vie des incidents dans Incident Manager

Prérequis

Si vous utilisez Incident Manager pour la première fois, consultez leConfiguration de AWS Systems Manager Incident Manager. Nous vous recommandons de configurer Incident Manager dans le compte que vous utilisez pour gérer vos opérations.

Nous vous recommandons de terminer la configuration rapide de Systems Manager avant de lancer l'assistant de préparation d'Incident Manager. Utilisez la configuration rapide de Systems Manager pour configurer les AWS services et fonctionnalités fréquemment utilisés conformément aux meilleures pratiques recommandées. Incident Manager utilise les fonctionnalités de Systems Manager pour gérer les incidents qui vous sont associés Comptes AWS et bénéficie de la configuration préalable de Systems Manager.

Préparez-vous, magicien

La première fois que vous utilisez Incident Manager, vous pouvez accéder à l'assistant de préparation depuis la page d'accueil du service Incident Manager. Pour accéder à l'assistant de préparation une fois la configuration terminée, choisissez Préparer sur la page de liste des incidents.

1. Ouvrez la console Incident Manager.
2. Sur la page d'accueil du service Incident Manager, choisissez Get prepared.

Paramètres généraux

1. Sous Paramètres généraux, choisissez Configurer.

2. Lisez les termes et conditions. Si vous acceptez les conditions générales d'Incident Manager, sélectionnez J'ai lu et j'accepte les conditions générales d'Incident Manager, puis cliquez sur Suivant.
3. Dans la zone Régions, votre région actuelle Région AWS apparaît comme la première région de votre jeu de réplication. Pour ajouter d'autres régions à votre ensemble de réplication, choisissez-les dans la liste des régions.

   Nous recommandons d'inclure au moins deux régions. Si une région est temporairement indisponible, les activités liées à l'incident peuvent toujours être redirigées vers l'autre région.

   > **Note**
   >
   > La création du jeu de réplication crée le rôle `AWSServiceRoleforIncidentManager` lié au service dans votre compte. Pour de plus amples informations sur ce rôle, veuillez consulter Utilisation de rôles liés à un service pour Incident Manager.

4. Pour configurer le chiffrement de votre ensemble de réplication, effectuez l'une des opérations suivantes :

   > **Note**
   >
   > Toutes les ressources d'Incident Manager sont cryptées. Pour en savoir plus sur le chiffrement de vos données, consultezProtection des données dans Incident Manager. Pour plus d'informations sur votre ensemble de réplication Incident Manager, consultezConfiguration du jeu de réplication Incident Manager.

   - Pour utiliser une clé AWS détenue, choisissez Utiliser une clé AWS possédée.
   - Pour utiliser votre propre AWS KMS clé, choisissez Choisir une clé existante AWS KMS key. Pour chaque région sélectionnée à l'étape 3, choisissez une AWS KMS clé ou entrez un AWS KMS Amazon Resource Name (ARN).

     > **Tip**
     >
     > Si vous n'en avez pas de disponible AWS KMS key, choisissez Créer un AWS KMS key.

5. (Facultatif) Dans la zone Balises, ajoutez une ou plusieurs balises au jeu de réplication. Une balise inclut une clé et, éventuellement, une valeur.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Pour de plus amples informations, veuillez consulter Marquage des ressources dans Incident Manager.

6. (Facultatif) Dans la zone d'accès au service, pour activer la fonctionnalité Résultats, cochez la case Créer un rôle de service pour les résultats de ce compte.

   Une constatation est une information concernant un déploiement de code ou une modification de l'infrastructure survenus à peu près au même moment où un incident a été créé. Une découverte peut être examinée en tant que cause potentielle de l'incident. Les informations relatives à ces causes potentielles sont ajoutées à la page des détails de l'incident. Les informations relatives à ces déploiements et modifications étant à portée de main, les intervenants n'ont pas besoin de les rechercher manuellement.

   > **Tip**
   >
   > Pour afficher les informations relatives au rôle à créer, choisissez Afficher les détails des autorisations.

7. Sélectionnez Créer.

   Pour en savoir plus sur les ensembles de réplication et la résilience, consultezRésilience dans AWS Systems Manager Incident Manager.

Contacts (facultatif pendant la section Préparation)

Le gestionnaire d'incidents engage les contacts lors d'un incident. Pour plus d'informations sur les contacts, consultezCréation et configuration de contacts dans Incident Manager.

1. Choisissez Créer un contact.
2. Dans Nom, entrez le nom du contact.
3. Dans Alias unique, entrez un alias pour identifier ce contact.
4. Dans la section Canal de contact., procédez comme suit pour définir la manière dont le contact est engagé lors d'incidents :

a. Dans Type, choisissez E-mail, SMS ou Voix.

b. Dans Nom de la chaîne, entrez un nom unique pour vous aider à identifier la chaîne.

c. Pour plus de détails, entrez l'adresse e-mail ou le numéro de téléphone du contact.

   Les numéros de téléphone doivent comporter de 9 à 15 caractères et commencer + par le code du pays et le numéro d'abonné.

d. Pour créer un autre canal de contact, choisissez Ajouter un canal de contact. Nous recommandons de définir au moins deux canaux pour chaque contact.

5. Dans la zone Plan d'engagement, procédez comme suit pour définir les canaux par lesquels vous souhaitez informer le contact et le temps d'attente d'un accusé de réception via chaque canal.

> **Note**
>
> Nous vous recommandons de définir au moins deux canaux dans le plan d'engagement.

   a. Pour Nom de la chaîne de contact, choisissez une chaîne que vous avez spécifiée dans la zone de la chaîne de contact.

   b. Pour le temps d'engagement (min), entrez le nombre de minutes à attendre avant d'activer le canal de contact.

      Nous vous recommandons de sélectionner au moins un appareil à utiliser au début d'un engagement, en spécifiant un temps d'attente **0** (zéro) minute.

   c. Pour ajouter d'autres canaux de contact au plan d'engagement, choisissez Ajouter un engagement.

6. (Facultatif) Dans la zone Tags, ajoutez un ou plusieurs tags au contact. Une balise inclut une clé et, éventuellement, une valeur.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Pour de plus amples informations, veuillez consulter Marquage des ressources dans Incident Manager.

7. Pour créer l'enregistrement du contact et envoyer les codes d'activation aux canaux de contact définis, choisissez Créer.

8. (Facultatif) Sur la page d'activation du canal de contact, entrez le code d'activation envoyé à chaque canal.

   Vous pouvez générer de nouveaux codes d'activation ultérieurement si vous n'êtes pas en mesure de les saisir maintenant.

9. Pour ajouter des contacts supplémentaires, choisissez Créer un contact et répétez les étapes précédentes.

(Facultatif pendant la période de préparation) Plans d'escalade

1. Choisissez Créer un plan d'escalade.

   Un plan d'escalade passe par l'intermédiaire de vos contacts lors d'un incident, garantissant ainsi que le gestionnaire d'incidents engage les bons intervenants lors d'un incident. Pour plus d'informations sur les plans d'escalade, consultezCréation d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager.

2. Dans Nom, entrez un nom unique pour le plan d'escalade.
3. Pour Alias, entrez un alias unique pour vous aider à identifier le plan d'escalade.
4. Dans la zone Étape 1, procédez comme suit :

   a. Pour les canaux d'escalade, choisissez les canaux de contact avec lesquels vous souhaitez vous engager.

   b. Si vous souhaitez qu'un contact soit en mesure d'arrêter la progression des étapes du plan d'escalade, sélectionnez L'accusé de réception arrête la progression du plan.

   c. Pour ajouter d'autres canaux à une étape, choisissez Ajouter un canal d'escalade.

5. Pour créer une nouvelle étape dans le plan d'escalade, choisissez Ajouter une étape et ajoutez les détails de l'étape.
6. (Facultatif) Dans la zone Balises, ajoutez une ou plusieurs balises au plan d'escalade. Une balise inclut une clé et, éventuellement, une valeur.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Pour de plus amples informations, veuillez consulter Marquage des ressources dans Incident Manager.

7. Choisissez Créer un plan d'escalade.

Plan de réponse

> **Note**
>
> Vous devrez peut-être retourner à la page de démarrage du gestionnaire d'incidents et choisir Préparer pour continuer.

1. Choisissez Créer un plan de réponse.

   Utilisez le plan de réponse pour rassembler les contacts et les plans d'escalade que vous avez créés.

   Au cours de cet assistant de démarrage, les sections suivantes sont facultatives, en particulier si c'est la première fois que vous configurez un plan de réponse :

   - Canal de chat
   - Livres de course
   - Fiançailles
   - Intégrations tierces

   Pour plus d'informations sur l'ajout ultérieur de ces éléments aux plans d'intervention, voirPréparation aux incidents dans Incident Manager.
2. Dans Nom, entrez un nom unique et identifiable pour le plan de réponse. Le nom est utilisé pour créer l'ARN du plan de réponse ou dans les plans de réponse sans nom d'affichage.
3. (Facultatif) Dans Nom d'affichage, entrez un nom pour vous aider à identifier ce plan de réponse lors de la création d'incidents.
4. Dans Titre, entrez un titre pour aider à identifier le type d'incident lié à ce plan d'intervention.

   La valeur que vous spécifiez est incluse dans le titre de chaque incident. L'alarme ou l'événement à l'origine de l'incident est également ajouté au titre.
5. Pour Impact, sélectionnez le niveau d'impact que vous attendez pour les incidents liés à ce plan de réponse, tel que **`Critical`** ou**`Low`**.
6. (Facultatif) Dans Résumé, entrez une brève description qui est utilisée pour fournir une vue d'ensemble de l'incident. Incident Manager saisit automatiquement les informations pertinentes dans le résumé lors d'un incident.

7. (Facultatif) Pour la chaîne de déduplication, entrez une chaîne de déduplication. Incident Manager utilise cette chaîne pour empêcher la même cause première de créer plusieurs incidents dans le même compte.

   Une chaîne de déduplication est un terme ou une expression que le système utilise pour vérifier la présence d'incidents dupliqués. Si vous spécifiez une chaîne de déduplication, Incident Manager recherche les incidents ouverts contenant la même chaîne dans le `dedupeString` champ lorsqu'il crée l'incident. Si un doublon est détecté, Incident Manager déduplique le nouvel incident dans l'incident existant.

   > **Note**
   >
   > Par défaut, Incident Manager déduplique automatiquement plusieurs incidents créés par la même alarme Amazon CloudWatch ou le même événement Amazon. EventBridge Il n'est pas nécessaire de saisir votre propre chaîne de déduplication pour empêcher la duplication de ces types de ressources.

8. (Facultatif) Dans la zone Balises d'incident, ajoutez une ou plusieurs balises au plan de réponse. Une balise inclut une clé et, éventuellement, une valeur.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Pour de plus amples informations, veuillez consulter Marquage des ressources dans Incident Manager.
9. Sélectionnez les contacts et les plans d'escalade à appliquer à l'incident dans le menu déroulant Engagements.
10. Choisissez Créer un plan de réponse.

Après avoir créé un plan de réponse, vous pouvez associer les CloudWatch alarmes Amazon ou les EventBridge événements Amazon au plan de réponse. Cela créera automatiquement un incident basé sur une alarme ou un événement. Pour de plus amples informations, veuillez consulter Création d'incidents automatiquement ou manuellement dans Incident Manager.

Gestion des incidents par région Comptes AWS et par région dans Incident Manager

Vous pouvez configurer Incident Manager, un outil intégré AWS Systems Manager, pour qu'il fonctionne avec plusieurs Régions AWS comptes. Cette section décrit les meilleures pratiques entre régions et entre comptes, les étapes de configuration et les limites connues.

Rubriques

Gestion des incidents entre les régions

Incident Manager prend en charge la création automatique et manuelle d'incidents dans plusieurs cas Régions AWS. Lors de votre première intégration à Incident Manager à l'aide de l'assistant de préparation, vous pouvez en spécifier jusqu'à trois Régions AWS pour votre ensemble de réplication. Pour les incidents créés automatiquement par les CloudWatch alarmes Amazon ou les EventBridge événements Amazon, Incident Manager tente de créer un incident identique Région AWS à la règle ou à l'alarme de l'événement. Si Incident Manager connaît une panne dans cette région, l'incident est créé EventBridge automatiquement CloudWatch ou automatiquement dans une autre région vers laquelle vos données sont répliquées.

> **Important**
>
> Prenez note des informations importantes suivantes.
>
> - Nous vous recommandons d'en spécifier au moins deux Régions AWS dans votre jeu de réplication. Si vous ne spécifiez pas au moins deux régions, le système ne créera pas d'incidents pendant la période pendant laquelle Incident Manager n'est pas disponible.
> - Les incidents créés par un basculement entre régions n'invoquent pas les runbooks spécifiés dans les plans de réponse.

Pour plus d'informations sur l'intégration à Incident Manager et sur la spécification de régions supplémentaires, consultezCommencer à utiliser Incident Manager.

Gestion des incidents entre comptes

Incident Manager utilise AWS Resource Access Manager (AWS RAM) pour partager les ressources du gestionnaire d'incidents entre les comptes de gestion et d'application. Cette section décrit les meilleures pratiques entre comptes, comment configurer la fonctionnalité multicomptes pour Incident Manager et les limites connues de la fonctionnalité multicomptes dans Incident Manager.

Un compte de gestion est le compte à partir duquel vous effectuez la gestion des opérations. Dans une configuration organisationnelle, le compte de gestion possède les plans d'intervention, les contacts, les plans d'escalade, les runbooks et les autres AWS Systems Manager ressources.

Un compte d'application est le compte qui possède les ressources qui constituent vos applications. Ces ressources peuvent être des EC2 instances Amazon, des tables Amazon DynamoDB ou toute autre ressource que vous utilisez pour créer des applications dans le. AWS Cloud Les comptes d'applications possèdent également les CloudWatch alarmes Amazon et les EventBridge événements Amazon qui créent des incidents dans Incident Manager.

AWS RAM utilise les partages de ressources pour partager les ressources entre les comptes. Vous pouvez partager le plan de réponse et les ressources de contact entre les comptes dans AWS RAM. En partageant ces ressources, les comptes d'applications et les comptes de gestion peuvent interagir avec les engagements et les incidents. Le partage d'un plan de réponse permet de partager tous les incidents passés et futurs créés à l'aide de ce plan d'intervention. Le partage d'un contact permet de partager tous les engagements passés et futurs du contact ou du plan de réponse.

Bonnes pratiques

Suivez ces bonnes pratiques lorsque vous partagez les ressources de votre gestionnaire d'incidents entre plusieurs comptes :

- Mettez régulièrement à jour le partage des ressources avec les plans d'intervention et les contacts.
- Passez régulièrement en revue les principes de partage des ressources.
- Configurez le gestionnaire d'incidents, les runbooks et les canaux de discussion dans votre compte de gestion.

Configuration et configuration de la gestion des incidents entre comptes

Les étapes suivantes décrivent comment configurer et configurer les ressources d'Incident Manager et comment les utiliser pour les fonctionnalités multicomptes. Vous avez peut-être configuré certains

services et ressources pour la fonctionnalité multi-comptes par le passé. Utilisez ces étapes comme liste de contrôle des exigences avant de commencer votre premier incident à l'aide des ressources multicomptes.

1. (Facultatif) Créez des organisations et des unités organisationnelles à l'aide de AWS Organizations. Suivez les étapes décrites dans le didacticiel : Création et configuration d'une organisation dans le guide de AWS Organizations l'utilisateur.
2. (Facultatif) Utilisez Quick Setup, un outil AWS Systems Manager intégré, pour définir les AWS Identity and Access Management rôles appropriés à utiliser lors de la configuration de vos runbooks multicomptes. Pour plus d'informations, consultez Quick Setup dans le Guide de l'utilisateur AWS Systems Manager .
3. Suivez les étapes répertoriées dans la section Exécuter des automatisations en plusieurs Régions AWS comptes dans le Guide de l'AWS Systems Manager utilisateur pour créer des runbooks dans vos documents d'automatisation de Systems Manager. Un runbook peut être géré soit par un compte de gestion, soit par l'un de vos comptes d'application. En fonction de votre cas d'utilisation, vous devrez installer le AWS CloudFormation modèle approprié pour les rôles nécessaires à la création et à l'affichage des runbooks lors d'un incident.
   - Exécution d'un runbook dans le compte de gestion. Le compte de gestion doit télécharger et installer le AWS-SystemsManager-AutomationReadOnlyRole CloudFormation modèle. Lors de l'installation AWS-SystemsManager-AutomationReadOnlyRole, spécifiez le compte IDs de tous les comptes d'applications. Ce rôle permettra aux comptes de votre application de lire l'état du runbook depuis la page des détails de l'incident. Le compte de l'application doit installer AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation modèle. La page de détails de l'incident utilise ce rôle pour obtenir l'état de l'automatisation à partir du compte de gestion.
   - Exécution d'un runbook dans un compte d'application. Le compte de gestion doit télécharger et installer le AWS-SystemsManager-AutomationAdministrationReadOnlyRole CloudFormation modèle. Ce rôle permet au compte de gestion de lire l'état du runbook dans le compte de l'application. Le compte de l'application doit télécharger et installer AWS-SystemsManager-AutomationReadOnlyRole CloudFormation modèle. Lors de l'installation`AWS-SystemsManager-AutomationReadOnlyRole`, spécifiez l'ID du compte de gestion et des autres comptes de l'application. Le compte de gestion et les autres comptes d'application assument ce rôle pour lire l'état du runbook.
4. (Facultatif) Dans chaque compte d'application de l'organisation, téléchargez et installez AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole CloudFormation modèle. Lors de l'installation AWS-SystemsManager-IncidentManagerIncidentAccessServiceRole, spécifiez

l'ID de compte du compte de gestion. Ce rôle fournit les autorisations dont Incident Manager a besoin pour accéder aux informations relatives aux AWS CodeDeploy déploiements et aux mises à jour de la AWS CloudFormation pile. Ces informations sont signalées sous forme de conclusions relatives à un incident si la fonctionnalité Résultats est activée. Pour de plus amples informations, veuillez consulter Identifier les causes potentielles des incidents provenant d'autres services en tant que « constatations » dans Incident Manager.

5. Pour configurer et créer des contacts, des plans d'escalade, des canaux de discussion et des plans de réponse, suivez les étapes détaillées dansPréparation aux incidents dans Incident Manager.
6. Ajoutez vos contacts et les ressources du plan de réponse à votre partage de ressources existant ou à un nouveau partage de ressources AWS RAM. Pour plus d'informations, consultez Démarrer avec AWS RAM dans le Guide de l'utilisateur AWS RAM . L'ajout de plans de réponse AWS RAM permet aux comptes d'applications d'accéder aux incidents et aux tableaux de bord des incidents créés à l'aide des plans de réponse. Les comptes d'applications peuvent également associer des CloudWatch alarmes et EventBridge des événements à un plan de réponse. L'ajout des contacts et des plans d'escalade AWS RAM permet aux comptes d'applications de consulter les engagements et d'engager les contacts depuis le tableau de bord des incidents.
7. Ajoutez des fonctionnalités multicomptes et interrégions à votre CloudWatch console. Pour connaître les étapes à suivre et obtenir des informations, consultez la CloudWatch console multi-comptes inter-régions dans le guide de CloudWatch l'utilisateur Amazon. L'ajout de cette fonctionnalité garantit que les comptes d'application et le compte de gestion que vous avez créés peuvent consulter et modifier les indicateurs des tableaux de bord des incidents et des analyses.
8. Créez un bus d' EventBridge événements Amazon multicomptes. Pour connaître les étapes à suivre et obtenir des informations, consultez la section Envoi et réception d' EventBridge événements Amazon entre AWS comptes. Vous pouvez ensuite utiliser ce bus d'événements pour créer des règles d'événements qui détectent les incidents dans les comptes d'applications et créent des incidents dans le compte de gestion.

Limites

Les limites connues de la fonctionnalité multi-comptes d'Incident Manager sont les suivantes :

- Le compte qui crée une analyse post-incident est le seul à pouvoir la consulter et la modifier. Si vous utilisez un compte d'application pour créer une analyse post-incident, seuls les membres

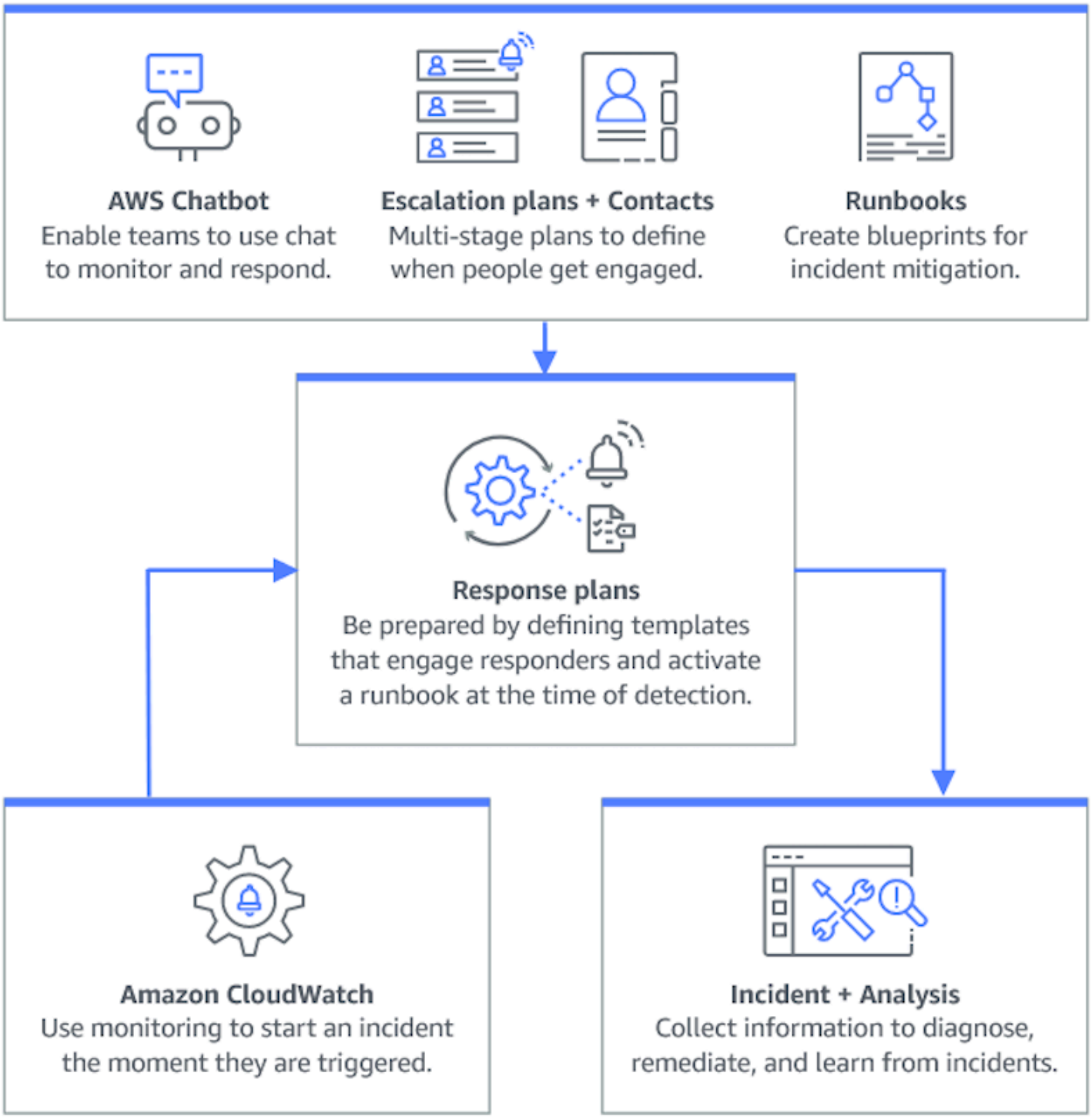
de ce compte peuvent la consulter et la modifier. Il en va de même si vous utilisez un compte de gestion pour créer une analyse post-incident.

- Les événements de chronologie ne sont pas renseignés pour les documents automatisés exécutés dans les comptes d'applications. Les mises à jour des documents d'automatisation exécutés dans les comptes d'applications sont visibles dans l'onglet Runbook de l'incident.

- Les rubriques Amazon Simple Notification Service ne peuvent pas être utilisées entre comptes. Les rubriques Amazon SNS doivent être créées dans la même région et dans le même compte que le plan de réponse dans lequel elles sont utilisées. Nous vous recommandons d'utiliser le compte de gestion pour créer toutes les rubriques SNS et tous les plans de réponse.
- Les plans d'escalade ne peuvent être créés qu'à l'aide des contacts du même compte. Un contact qui a été partagé avec vous ne peut pas être ajouté à un plan d'escalade dans votre compte.
- Les balises appliquées aux plans d'intervention, aux enregistrements d'incidents et aux contacts ne peuvent être consultées et modifiées qu'à partir du compte du propriétaire de la ressource.

Préparation aux incidents dans Incident Manager

La planification d'un incident commence bien avant le cycle de vie de l'incident. Comme le montre l'illustration suivante, avant de commencer à répondre aux incidents, vous devez vous préparer en configurant des canaux de discussion, en créant des plans d'escalade, en spécifiant les contacts et en déterminant les runbooks d'automatisation à utiliser pour répondre aux incidents. Utilisez ensuite un plan de réponse qui précise le mode de surveillance et indique si les réponses sont automatisées. Une fois la correction terminée, vous pouvez analyser l'incident et la réponse à l'incident afin d'affiner votre plan de réponse pour les futurs incidents.



Rubriques

- Surveillance
- Configuration des ensembles de réplication et des résultats dans Incident Manager
- Création et configuration de contacts dans Incident Manager

- Gestion de la rotation des intervenants à l'aide de calendriers d'astreinte dans Incident Manager
- Création d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager
- Création et intégration de canaux de discussion pour les intervenants dans Incident Manager
- Intégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents
- Création et configuration de plans de réponse dans Incident Manager
- Identifier les causes potentielles des incidents provenant d'autres services en tant que « constatations » dans Incident Manager

Surveillance

La surveillance de l'état de vos applications AWS hébergées est essentielle pour garantir le temps de disponibilité et les performances des applications. Lorsque vous déterminez des solutions de surveillance, tenez compte des points suivants :

- Criticité de la fonctionnalité — Si le système devait tomber en panne, quel en serait l'impact critique pour les utilisateurs en aval.
- Caractère commun des défaillances — Quelle est la fréquence des défaillances d'un système ? Les systèmes nécessitant des interventions fréquentes doivent être étroitement surveillés.
- Latence accrue : augmentation ou diminution du temps nécessaire à l'exécution d'une tâche.
- Mesures côté client et côté serveur : en cas de divergence entre les mesures associées sur le client et sur le serveur.
- Défaillances de dépendance : défaillances auxquelles votre équipe peut et doit se préparer.

Après avoir créé des plans de réponse, vous pouvez utiliser vos solutions de surveillance pour suivre automatiquement les incidents dès qu'ils se produisent dans votre environnement. Pour plus d'informations sur le suivi et la création d'incidents, consultezAfficher les détails de l'incident dans la console Incident Manager.

Pour plus d'informations sur l'architecture d'applications et de charges de travail d'infrastructure sécurisées, performantes, résilientes et efficaces, consultez le Well-Architected.AWS

Configuration des ensembles de réplication et des résultats dans Incident Manager

Une fois que vous avez terminé l'assistant de préparation d'Incident Manager, vous pouvez gérer certaines options sur la page Paramètres. Ces options incluent votre jeu de réplication, les balises appliquées au jeu de réplication et la fonctionnalité Findings.

Rubriques

Configuration du jeu de réplication Incident Manager

Le jeu de réplication Incident Manager réplique vos données sur de nombreuses personnes Régions AWS afin d'effectuer les opérations suivantes :

- Augmenter la redondance entre régions
- Permettez à Incident Manager d'accéder aux ressources de différentes régions et de réduire le temps de latence pour vos utilisateurs.
- Chiffrez vos données à l'aide d'une clé gérée par le client Clé gérée par AWS ou de votre propre clé.

  Toutes les ressources d'Incident Manager sont cryptées par défaut. Pour en savoir plus sur le chiffrement de vos ressources, consultezProtection des données dans Incident Manager.

Pour commencer à utiliser Incident Manager, créez d'abord votre ensemble de réplication à l'aide de l'assistant de préparation. Pour en savoir plus sur la préparation dans Incident Manager, consultez lePréparez-vous, magicien.

Modification de votre jeu de réplication

À l'aide de la page Paramètres du gestionnaire d'incidents, vous pouvez modifier votre ensemble de réplication. Vous pouvez ajouter des régions, supprimer des régions et activer ou désactiver la protection contre la suppression des ensembles de réplication. Vous ne pouvez pas modifier la clé utilisée pour chiffrer vos données. Pour modifier la clé, supprimez et recréez le jeu de réplication.

Ajouter une région

1. Ouvrez la console Incident Manager, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Choisissez Ajouter une région.
3. Sélectionnez la région.
4. Choisissez Ajouter.

Supprimer une région

1. Ouvrez la console Incident Manager, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sélectionnez la région que vous souhaitez supprimer.
3. Choisissez Supprimer.
4. Entrez Supprimer dans la zone de texte, puis choisissez Supprimer.

Suppression de votre jeu de réplication

La suppression de la dernière région de votre jeu de réplication entraîne la suppression de l'ensemble de réplication dans son intégralité. Avant de pouvoir supprimer la dernière région, désactivez la protection contre la suppression en désactivant la protection contre la suppression sur la page Paramètres. Après avoir supprimé votre jeu de réplication, vous pouvez en créer un nouveau à l'aide de l'assistant de préparation.

Pour supprimer une région de votre jeu de réplication, attendez 24 heures après l'avoir créée. Toute tentative de suppression d'une région de votre jeu de réplication moins de 24 heures après sa création entraîne l'échec de la suppression.

La suppression de votre jeu de réplication entraîne la suppression de toutes les données d'Incident Manager.

Supprimer le jeu de réplication

1. Ouvrez la console Incident Manager, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Sélectionnez la dernière région de votre jeu de réplication.
3. Choisissez Supprimer.

4. Entrez Supprimer dans la zone de texte, puis choisissez Supprimer.

Gestion des balises pour un ensemble de réplication

Les balises sont des métadonnées facultatives que vous affectez à une ressource. Utilisez des balises pour classer une ressource de différentes manières, par exemple en fonction de son objectif, de son propriétaire ou de son environnement.

Pour gérer les balises d'un ensemble de réplication

1. Ouvrez la console Incident Manager, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Dans la zone Balises, choisissez Modifier.
3. Pour ajouter une balise, procédez comme suit :
    a. Sélectionnez Ajouter une nouvelle balise.
    b. Entrez une clé et une valeur facultative pour le tag.
    c. Choisissez Enregistrer.
4. Pour supprimer un tag, procédez comme suit :
    a. Sous le tag que vous souhaitez supprimer, choisissez Supprimer.
    b. Choisissez Enregistrer.

Gestion de la fonctionnalité des résultats

La fonctionnalité Résultats aide les intervenants de votre organisation à identifier les causes profondes potentielles des incidents peu après le début des incidents. Actuellement, Incident Manager fournit des résultats pour les AWS CodeDeploy déploiements et les mises à jour de la AWS CloudFormation pile.

Pour la prise en charge des résultats entre comptes, après avoir activé la fonctionnalité, vous devez effectuer une étape de configuration supplémentaire dans chaque compte d'application de l'organisation.

Pour utiliser cette fonctionnalité, vous devez laisser Incident Manager créer un rôle de service incluant les autorisations requises pour accéder aux données en votre nom.

Pour activer la fonctionnalité Résultats

1. Ouvrez la console Incident Manager, puis sélectionnez Paramètres dans le volet de navigation de gauche.
2. Dans la zone Résultats, sélectionnez Créer un rôle de service.
3. Passez en revue les informations relatives au rôle de service à créer, puis choisissez Create.

Pour désactiver la fonctionnalité Résultats

Pour arrêter d'utiliser la fonctionnalité Résultats, supprimez le `IncidentManagerIncidentAccessServiceRole` rôle de chaque compte sur lequel il a été créé.

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation de gauche, choisissez Rôles.
3. Dans la zone de recherche, saisissez **`IncidentManagerIncidentAccessServiceRole`**.
4. Choisissez le nom du rôle, puis choisissez Supprimer.
5. Entrez le nom du rôle dans la boîte de dialogue pour confirmer que vous souhaitez supprimer le rôle, puis choisissez Supprimer.

Création et configuration de contacts dans Incident Manager

AWS Systems Manager Incident Manager les contacts interviennent en cas d'incident. Un contact peut disposer de plusieurs canaux que le gestionnaire d'incidents peut utiliser lors d'un incident. Vous pouvez définir le plan d'engagement d'un contact pour décrire comment et quand Incident Manager engage le contact avec le contact.

Rubriques

- Canaux de contact
- Plans d'engagement
- Créer un contact
- Importer les coordonnées dans votre carnet d'adresses

Canaux de contact

Les canaux de contact sont les différentes méthodes utilisées par Incident Manager pour engager un contact.

Incident Manager prend en charge les canaux de contact suivants :

- E-mails
- Service de messages courts (SMS)
- Voix

Activation du canal de contact

Pour protéger votre confidentialité et votre sécurité, Incident Manager vous envoie un code d'activation de l'appareil lorsque vous créez des contacts. Pour activer vos appareils lors d'un incident, vous devez d'abord les activer. Pour ce faire, entrez le code d'activation de l'appareil sur la page de création de contact.

Certaines fonctionnalités d'Incident Manager incluent des fonctionnalités permettant d'envoyer des notifications à un canal de contact. En utilisant ces fonctionnalités, vous consentez à ce que ce service envoie des notifications concernant les interruptions de service ou d'autres événements aux canaux de contact inclus dans le flux de travail spécifié. Cela inclut les notifications envoyées à un contact dans le cadre d'une rotation du calendrier d'astreinte. Les notifications peuvent être envoyées par e-mail, SMS ou appel vocal, comme indiqué dans les coordonnées d'un contact. En utilisant ces fonctionnalités, vous confirmez que vous êtes autorisé à ajouter les canaux de contact que vous fournissez à Incident Manager.

Désabonnement

Vous pouvez annuler ces notifications à tout moment en supprimant un appareil mobile comme canal de contact. Les destinataires individuels des notifications peuvent également annuler les notifications à tout moment en retirant l'appareil de leur contact.

Pour supprimer un canal de contact d'un contact

1. Accédez à la console Incident Manager et choisissez Contacts dans le menu de navigation de gauche.
2. Sélectionnez le contact avec le canal de contact que vous souhaitez supprimer et choisissez Modifier.

3. Choisissez Supprimer à côté du canal de contact que vous souhaitez supprimer.
4. Choisissez Mettre à jour.

Désactivation du canal de contact

Pour désactiver un appareil, répondez à UNSUBSCRIBE. Le fait de répondre à UNSUBSCRIBE empêche Incident Manager d'activer votre appareil.

Réactivation du canal de contact

1. Répondez START au message d'Incident Manager.
2. Accédez à la console Incident Manager et choisissez Contacts dans le menu de navigation de gauche.
3. Sélectionnez le contact avec le canal de contact que vous souhaitez supprimer et choisissez Modifier.
4. Choisissez Activer les appareils.
5. Entrez le code d'activation envoyé à l'appareil par Incident Manager.
6. Choisissez Activer.

Plans d'engagement

Les plans d'engagement définissent le moment où Incident Manager engage les canaux de contact. Vous pouvez utiliser les canaux de contact plusieurs fois à différentes étapes dès le début d'un engagement. Vous pouvez utiliser des plans d'engagement dans un plan d'escalade ou un plan de réponse. Pour en savoir plus sur les plans d'escalade, consultezCréation d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager.

Créer un contact

Pour créer un contact, procédez comme suit.

1. Ouvrez la console Incident Manager et choisissez Contacts dans le menu de navigation de gauche.
2. Choisissez Créer un contact.
3. Entrez le nom complet du contact et fournissez un alias unique et identifiable.

4. Définissez un canal de contact. Nous vous recommandons d'avoir au moins deux types de canaux de contact différents.

   a. Choisissez le type : e-mail, SMS ou voix.

   b. Entrez un nom identifiable pour le canal de contact.

   c. Fournissez les détails du canal de contact, tels que l'e-mail : arosalez@example.com

5. Pour définir plusieurs canaux de contact, choisissez Ajouter un canal de contact. Répétez l'étape 4 pour chaque nouveau canal de contact ajouté.

6. Définissez un plan d'engagement.

   > **Important**
   >
   > Pour engager un contact, vous devez définir un plan d'engagement.

   a. Choisissez le nom d'une chaîne de contact.

   b. Définissez le nombre de minutes à attendre entre le début de l'engagement et le moment où Incident Manager engage ce canal de contact.

   c. Pour ajouter un autre canal de contact, choisissez Ajouter un engagement.

7. Après avoir défini votre plan d'engagement, choisissez Créer. Incident Manager envoie un code d'activation à chacun des canaux de contact définis.

8. (Facultatif) Pour activer les canaux de contact, entrez le code d'activation envoyé par Incident Manager à chaque canal de contact défini.

9. (Facultatif) Pour envoyer un nouveau code d'activation, choisissez Envoyer un nouveau code.

10. Choisissez Finish (Terminer).

Après avoir défini un contact et activé ses canaux de contact, vous pouvez ajouter des contacts aux plans d'escalade pour former une chaîne d'escalade. Pour en savoir plus sur les plans d'escalade, consultezCréation d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager. Vous pouvez ajouter des contacts à un plan de réponse pour un engagement direct. Pour en savoir plus sur la création de plans d'intervention, consultezCréation et configuration de plans de réponse dans Incident Manager.

Importer les coordonnées dans votre carnet d'adresses

Lorsqu'un incident est créé, Incident Manager peut informer les intervenants en utilisant des notifications vocales ou par SMS. Pour que les intervenants voient que la notification d'appel ou de SMS provient d'Incident Manager, nous recommandons à tous les intervenants de télécharger le fichier au format de carte virtuelle Incident Manager (.vcf) dans le carnet d'adresses de leurs appareils mobiles. Le fichier est hébergé sur Amazon CloudFront et est disponible dans la partition AWS commerciale.

Pour télécharger le fichier .vcf du gestionnaire d'incidents

1. Sur votre appareil mobile, choisissez ou entrez l'URL suivante : https://d26vhuvd5b89k2.cloudfront.net/ aws-incident-manager .vcf.
2. Enregistrez ou importez le fichier dans le carnet d'adresses de votre appareil mobile.

Gestion de la rotation des intervenants à l'aide de calendriers d'astreinte dans Incident Manager

Un calendrier d'astreinte dans Incident Manager définit qui est averti lorsqu'un incident nécessitant l'intervention d'un opérateur survient. Un programme d'astreinte comprend une ou plusieurs rotations que vous créez pour le calendrier. Chaque rotation peut inclure jusqu'à 30 contacts.

Après avoir créé un calendrier d'astreinte, vous pouvez l'inclure en tant qu'escalade dans votre plan d'escalade. Lorsqu'un incident associé à ce plan d'escalade se produit, Incident Manager en informe l'opérateur (ou les opérateurs) qui sont sur appel conformément au calendrier. Ce contact peut alors accuser réception de l'engagement. Dans votre plan d'escalade, vous pouvez désigner un ou plusieurs horaires d'astreinte, ainsi qu'un ou plusieurs contacts individuels, à travers plusieurs étapes d'escalade. Pour de plus amples informations, veuillez consulter Création d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager.

> **Tip**
>
> À titre de bonne pratique, nous recommandons d'ajouter des contacts et des horaires d'astreinte comme canaux d'escalade dans un plan d'escalade. Vous devez ensuite choisir un plan d'escalade comme engagement dans un plan de réponse. Cette approche fournit la couverture la plus complète en matière de réponse aux incidents dans votre organisation.

Chaque programme d'astreinte prend en charge jusqu'à huit rotations. Les rotations peuvent se chevaucher ou s'exécuter simultanément. Cela augmente le nombre d'opérateurs invités à intervenir en cas d'incident. Vous pouvez également créer des rotations consécutives. Cela prend en charge des scénarios tels que la gestion des incidents « follow the sun » dans le cadre desquels des groupes du monde entier proposent le même service.

Utilisez les rubriques de cette section pour vous aider à créer et à gérer les plannings d'astreinte pour vos opérations de réponse aux incidents.

Rubriques

Création d'un calendrier d'astreinte et d'une rotation dans Incident Manager

Créez un calendrier d'astreinte avec une ou plusieurs rotations de contacts à engager pour répondre aux incidents pendant leur quart de travail.

Avant de commencer

Avant de créer un calendrier d'astreinte, assurez-vous d'avoir créé au préalable les contacts que vous souhaitez ajouter aux rotations du calendrier. Pour plus d'informations, voirCréation et configuration de contacts dans Incident Manager.

Comptabilisation des modifications apportées à l'heure d'été (DST)

Lorsque vous créez une rotation, vous spécifiez le fuseau horaire global qui sert de base aux heures et dates de couverture des quarts de travail que vous spécifiez pour cette rotation. Vous pouvez utiliser n'importe quel fuseau horaire défini par l'Internet Assigned Numbers Authority (IANA). Par exemple : `America/Los_Angeles`, `UTC` et `Asia/Seoul`. Vous pouvez ajouter plusieurs rotations à un calendrier d'astreinte. Toutefois, lorsque les intervenants pour chaque rotation sont situés géographiquement dans des fuseaux horaires différents, gardez à l'esprit les modifications de l'heure d'été auxquelles chaque rotation peut être soumise.

Par exemple, `America/Los_Angeles` et `Europe/Dublin` observez les différents horaires de l'heure d'été. Par conséquent, le décalage horaire entre les deux zones peut varier de 6 à 8 heures, selon la période de l'année. Par exemple, un planning d' follow-the-sunastreinte comporte une rotation dans le `America/Los_Angeles` fuseau horaire et une rotation dans `Europe/`

`Dublin` le fuseau horaire. Dans cet exemple, l'horaire peut comporter un écart d'une heure ou un chevauchement d'une heure en raison des modifications de l'heure d'été.

Pour éviter ces situations, nous recommandons l'approche suivante :

1. Utilisez un seul fuseau horaire pour toutes les rotations dans le cadre d'un calendrier d'astreinte.
2. Calculez les heures locales lorsque vous affectez des intervenants en dehors de ce fuseau horaire particulier.

Si vous décidez d'affecter chaque rotation à son fuseau horaire local, consultez le calendrier avant l'heure d'été. Ajustez ensuite les temps de rotation selon les besoins pour éviter tout écart ou chevauchement involontaire dans votre couverture d'astreinte avant que les modifications de l'heure d'été ne prennent effet.

Pour créer un calendrier d'astreinte

1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Choisissez Créer un calendrier d'astreinte.
4. Dans Nom du calendrier, entrez un nom pour vous aider à identifier le calendrier, tel que**`MyApp Primary On-call Schedule`**.
5. Pour Alias de calendrier, entrez un alias pour ce calendrier unique dans le calendrier actuel Région AWS, tel que**`my-app-primary-on-call-schedule`**.
6. (Facultatif) Dans la zone Balises, appliquez une ou plusieurs paires nom-clé de balise et valeur au calendrier des appels.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Par exemple, vous pouvez étiqueter un calendrier pour identifier la période pendant laquelle il s'exécute, les types d'opérateurs qu'il contient ou le plan d'escalade qu'il prend en charge. Pour plus d'informations sur le balisage des ressources d'Incident Manager, consultezMarquage des ressources dans Incident Manager.
7. Continuez en ajoutant une ou plusieurs rotations au calendrier des astreintes.

Création d'une rotation pour un calendrier d'astreinte dans Incident Manager

Une rotation dans un calendrier d'astreinte indique le moment où le quart de travail entre en vigueur. Il spécifie également les contacts par lesquels les décalages pivotent. Vous pouvez inclure jusqu'à huit rotations dans un seul programme d'astreinte.

Vous pouvez ajouter à une rotation toutes les personnes que vous avez créées en tant que contact dans Incident Manager. Pour plus d'informations sur la gestion de vos contacts, consultezCréation et configuration de contacts dans Incident Manager.

Lorsque vous configurez votre rotation, vous pouvez voir à quoi ressemble le calendrier global dans un calendrier d'aperçu sur le côté droit de la page.

Pour créer une rotation pour un calendrier d'astreinte

1. Dans la section Rotation 1 de la page Créer un calendrier d'astreinte, pour Nom de la rotation, entrez un nom identifiant la rotation, tel que**`00:00 - 7:59 Support`**, ou**`Dublin Support Group`**.
2. Pour Date de début, entrez la date à laquelle cette rotation devient active dans un `YYYY/MM/DD` format tel que`2023/07/14`.
3. Pour Fuseau horaire, sélectionnez le fuseau horaire global qui sert de base aux heures et dates de couverture des quarts de travail que vous spécifiez pour cette rotation.

   Vous pouvez utiliser n'importe quel fuseau horaire défini par l'Internet Assigned Numbers Authority (IANA). Par exemple : « America/Los_Angeles", "UTC", "Asia/Seoul ». Pour plus d'informations, consultez la base de données des fuseaux horaires sur le site web de l'IANA.

   > **Warning**
   >
   > Vous pouvez baser chaque rotation sur son propre fuseau horaire. Cependant, toute modification de l'heure d'été dans les fuseaux horaires que vous sélectionnez peut avoir une incidence sur les fenêtres de couverture prévues. Pour plus d'informations, consultez la section Prise en compte des modifications de l'heure d'été (DST) plus haut dans cette rubrique.

4. Pour Heure de début de rotation, entrez l'heure à laquelle le décalage de cette rotation commence au `hh:mm` format 24 heures, tel que`16:00`.

Notez les différences d'heure locale pour les contacts situés dans des fuseaux horaires différents de celui que vous avez spécifié. Par exemple, si vous choisissez `America/Los_Angeles` comme fuseau horaire et `00:00` comme heure de début de rotation, cela est égal à 08h00 à Dublin, en Irlande, et à 13h30 à Mumbai, en Inde.

5. Pour Heure de fin de rotation, entrez l'heure à laquelle le quart de travail de cette rotation prend fin au `hh:mm` format 24 heures, tel que`23:59`.

> **Note**
>
> Le délai entre le début et la fin d'une rotation doit être d'au moins 30 minutes.

6. (Facultatif) Pour définir la durée de la rotation sur 24 heures, sélectionnez une couverture de 24 heures et entrez l'heure de début de cette rotation dans le champ Heure de début de rotation. La valeur de l'heure de fin de rotation est automatiquement mise à jour.

   Par exemple, si vous souhaitez que votre service de garde bénéficie d'une couverture 24 heures sur 24 avec un changement de quart de travail à 11 h, choisissez une couverture 24 heures sur 24 et entrez **`11:00`** l'heure de début.

7. Pour les jours actifs, sélectionnez les jours de la semaine pendant lesquels cette rotation est active. Si votre forfait sur appel exclut la couverture de fin de semaine par exemple, sélectionnez tous les jours sauf le dimanche et le samedi.

8. Continuez en ajoutant des contacts à la rotation.

Ajouter des contacts à une rotation dans un calendrier d'astreinte dans Incident Manager

Pour chaque rotation de votre calendrier d'astreinte, vous pouvez ajouter un ou plusieurs contacts, jusqu'à un total de 30. Vous choisissez parmi les contacts définis dans votre configuration Incident Manager.

Lorsque vous ajoutez un contact à une rotation, celui-ci peut recevoir des notifications dans le cadre de ses tâches d'astreinte. Les notifications peuvent être envoyées par e-mail, SMS ou appel vocal, comme indiqué dans les coordonnées d'un contact.

Pour plus d'informations sur la gestion de vos contacts et les options de notification des contacts, consultezCréation et configuration de contacts dans Incident Manager.

Pour ajouter des contacts à une rotation dans un calendrier d'astreinte

1. Sur la page Créer un calendrier d'astreinte, dans la section Contacts pour la rotation, choisissez Ajouter ou supprimer des contacts.
2. Dans la boîte de dialogue Ajouter ou supprimer des contacts, sélectionnez les alias des contacts à inclure dans la rotation.

   L'ordre dans lequel vous sélectionnez les contacts est celui dans lequel ils sont répertoriés pour la première fois dans le calendrier de rotation. Vous pouvez modifier l'ordre après avoir ajouté des contacts.
3. Choisissez Confirmer.
4. Pour modifier la position d'un contact dans l'ordre, sélectionnez le bouton radio correspondant à cet utilisateur et utilisez les boutons Haut () et Bas () pour mettre à jour l'ordre des contacts.
5. Continuez en spécifiant la récurrence du décalage individuel et la durée de la rotation.

Spécification de la récurrence et de la durée du décalage et ajout de balises à une rotation dans Incident Manager

La récurrence du décalage indique la fréquence à laquelle les contacts d'une rotation entrent et sortent d'un appel. La durée des récurrences peut être spécifiée en nombre de jours, de semaines ou de mois.

Pour spécifier la récurrence et la longueur du décalage et ajouter des balises à une rotation

1. Sur la page Créer un calendrier d'astreinte, dans la section Paramètres de récurrence pour la rotation, procédez comme suit :

   - Pour le type de récurrence Shift, spécifiez si le quart de travail de chaque astreinte dure un certain nombre de jours, de semaines ou de mois en choisissant parmi `Daily`, `Weekly`, et. `Monthly`
   - Pour Durée du quart de travail, entrez le nombre de jours, de semaines ou de mois d'un quart de travail.

Par exemple, si vous choisissez `Daily` et entrez**1**, le service d'astreinte de chaque contact dure une journée. Si vous le souhaitez `Weekly` et si vous vous inscrivez**3**, le service de garde de chaque contact dure trois semaines.

2. (Facultatif) Dans la zone Balises, appliquez une ou plusieurs paires nom-clé de balise et valeur à la rotation.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Par exemple, vous pouvez étiqueter une rotation pour identifier l'emplacement des contacts qui lui sont assignés, le type de couverture qu'elle est censée fournir ou le plan d'escalade qu'elle prendra en charge. Pour plus d'informations sur le balisage des ressources d'Incident Manager, consultezMarquage des ressources dans Incident Manager.
3. (Recommandé) Utilisez l'aperçu du calendrier pour vous assurer qu'il n'y a aucune interruption involontaire dans la couverture de votre calendrier d'astreinte.
4. Sélectionnez Create (Créer).

Vous pouvez désormais ajouter le calendrier d'astreinte en tant que canal d'escalade dans un plan d'escalade. Pour plus d'informations, veuillez consulter Création d'un plan d'escalade.

Gestion d'un calendrier d'astreinte existant dans Incident Manager

Utilisez le contenu de cette section pour vous aider à travailler avec les horaires d'astreinte que vous avez déjà créés.

Rubriques

- Afficher les détails du calendrier des appels
- Modification d'un planning d'astreinte
- Copier un planning d'astreinte
- Création d'une dérogation pour une rotation des horaires sur appel
- Supprimer un planning d'astreinte

Afficher les détails du calendrier des appels

Vous pouvez accéder au at-a-glance résumé d'un calendrier d'appel sur la page Afficher les détails du calendrier d'appel. Cette page contient également des informations sur les personnes actuellement sur appel et sur les prochaines personnes à appeler. La page inclut un affichage du calendrier qui indique quels contacts sont en cours d'appel à un moment donné.

Pour consulter les détails du calendrier des appels

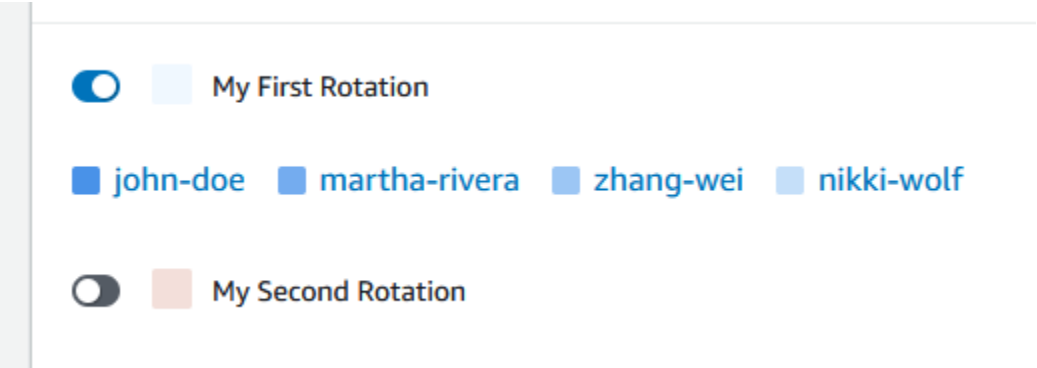
1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Dans la ligne correspondant au calendrier des astreintes à afficher, effectuez l'une des opérations suivantes :

   - Pour ouvrir une vue récapitulative du calendrier, choisissez l'alias du calendrier.

     -ou-

     Sélectionnez le bouton radio correspondant à la ligne, puis choisissez Afficher.
   - Pour ouvrir une vue du calendrier dans le calendrier, choisissez Afficher le calendrier

     Dans l'affichage du calendrier, choisissez le nom d'un contact à une date précise dans le calendrier pour voir les détails du quart de travail attribué ou créer une dérogation,.
   - Pour activer ou désactiver l'affichage d'une rotation spécifique dans le calendrier, cliquez sur le bouton situé à côté du nom de la rotation.



Modification d'un planning d'astreinte

Vous pouvez mettre à jour la configuration d'un calendrier d'astreinte et de ses rotations, à l'exception des détails suivants :

- L'alias du calendrier
- Noms des rotations
- Dates de début de rotation

Pour utiliser un calendrier existant comme base pour un nouveau calendrier avec la possibilité de modifier ces valeurs, vous pouvez copier le calendrier à la place. Pour plus d'informations, veuillez consulter Copier un planning d'astreinte.

Pour modifier un calendrier d'astreinte

1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Effectuez l'une des actions suivantes :
   - Sélectionnez le bouton radio dans la ligne correspondant au calendrier des appels à modifier, puis choisissez Modifier.
   - Choisissez l'alias du calendrier des appels pour ouvrir la page Afficher les détails du calendrier des appels, puis choisissez Modifier.
4. Apportez les modifications nécessaires au calendrier des astreintes et à ses rotations. Vous pouvez modifier les options de configuration de rotation telles que les heures de début et de fin, les contacts et la récurrence. Vous pouvez ajouter ou supprimer des rotations dans le calendrier selon vos besoins. L'aperçu du calendrier reflète vos modifications au fur et à mesure que vous les apportez.

   Pour plus d'informations sur l'utilisation des options de la page, consultezCréation d'un calendrier d'astreinte et d'une rotation dans Incident Manager.
5. Choisissez Mettre à jour.

> **Important**
>
> Si vous modifiez un calendrier contenant des dérogations, vos modifications peuvent avoir une incidence sur celles-ci. Pour vous assurer que vos dérogations restent configurées

comme prévu, nous vous recommandons de revoir attentivement vos dérogations de quart de travail après avoir mis à jour le calendrier.

Copier un planning d'astreinte

Pour utiliser la configuration d'un planning d'astreinte existant comme point de départ d'un nouveau planning, vous pouvez créer une copie du calendrier et le modifier selon vos besoins.

Pour copier un planning d'astreinte

1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Sélectionnez le bouton radio dans la rangée pour copier le calendrier des appels.
4. Choisissez Copier.
5. Apportez les modifications nécessaires au calendrier et à ses rotations. Vous pouvez modifier, ajouter ou supprimer des rotations selon vos besoins.

   > **Note**
   >
   > Lorsque vous copiez un planning existant, vous devez spécifier de nouvelles dates de début pour chaque rotation. Les plannings copiés ne prennent pas en charge les rotations dont les dates de début sont antérieures.

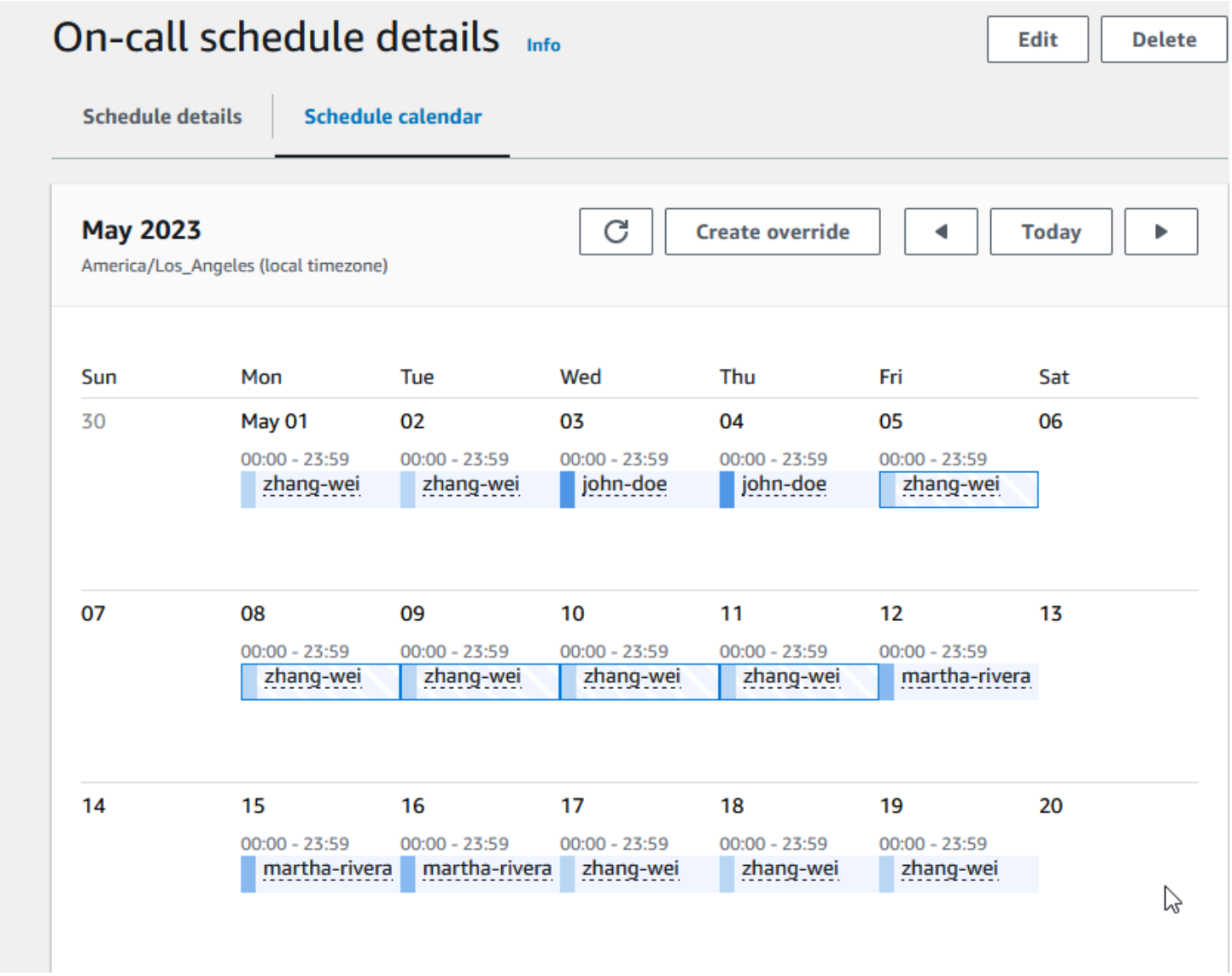
   Pour plus d'informations sur l'utilisation des options de la page, consultezCréation d'un calendrier d'astreinte et d'une rotation dans Incident Manager.
6. Choisissez Create copy (Créer une copie).

Création d'une dérogation pour une rotation des horaires sur appel

Si vous devez apporter des modifications ponctuelles à un calendrier de rotation existant, vous pouvez créer une dérogation. Une dérogation vous permet de remplacer tout ou partie du quart de travail d'un contact par un autre contact. Vous pouvez également créer une dérogation qui s'étend sur plusieurs équipes.

Vous ne pouvez affecter à une dérogation que des contacts déjà affectés à la rotation.

Dans l'aperçu du calendrier, les décalages annulés sont affichés sur un arrière-plan rayé au lieu d'un arrière-plan uni. L'image suivante montre que le contact nommé Zhang Wei est sur appel lors d'une dérogation. La dérogation inclut une partie des quarts de travail de John Doe et Martha Rivera, du 5 au 11 mai.



Pour créer une dérogation pour un calendrier d'astreinte

1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Dans la ligne correspondant au calendrier des astreintes à afficher, effectuez l'une des opérations suivantes :
   - Choisissez l'alias du calendrier, puis cliquez sur l'onglet Calendrier du calendrier.

- Choisissez Afficher le calendrier

4. Effectuez l'une des actions suivantes :
   - Choisissez Create override.
   - Choisissez le nom d'un contact dans l'aperçu du calendrier, puis choisissez Override shift.
5. Dans la boîte de dialogue Create shift override, procédez comme suit :

   > **Note**
   >
   > Une dérogation doit durer au moins 30 minutes. Vous ne pouvez spécifier une dérogation que pour les quarts de travail qui auront lieu dans les six mois à venir.

   a. Pour Sélectionner une rotation, sélectionnez le nom de la rotation dans laquelle créer une dérogation.
   b. Pour Date de début, sélectionnez ou entrez la date à laquelle la dérogation commence.
   c. Pour Heure de début, entrez l'heure à laquelle la dérogation commence au `hh:mm` format.
   d. Pour Date de fin, sélectionnez ou entrez la date à laquelle la dérogation prend fin.
   e. Pour Heure de fin, entrez l'heure à laquelle la dérogation prend fin, au `hh:mm` format.
   f. Pour Sélectionner un contact de remplacement, sélectionnez le nom du contact de rotation qui est appelé pendant la période de dérogation.
6. Choisissez Create override.

Après avoir créé une dérogation, vous pouvez l'identifier grâce à son arrière-plan rayé. Lorsque vous choisissez le nom du contact pour un quart de travail remplacé, une boîte d'information l'identifie comme un quart de travail remplacé. Vous pouvez choisir Supprimer la dérogation pour la supprimer et rétablir l'assignation d'astreinte d'origine.

Supprimer un planning d'astreinte

Lorsque vous n'avez plus besoin d'un calendrier d'astreinte particulier, vous pouvez le supprimer d'Incident Manager.

Si des plans d'escalade ou des plans de réponse utilisent actuellement le calendrier d'astreinte comme canal d'escalade, vous devez le supprimer de ces plans avant de supprimer le calendrier.

Pour supprimer un planning d'astreinte

1. Ouvrez la console Incident Manager.
2. Dans le menu de navigation de gauche, sélectionnez Horaires d'appel.
3. Sélectionnez le bouton radio dans la ligne correspondant au programme d'astreinte à supprimer.
4. Sélectionnez Delete (Supprimer).
5. Dans le programme Supprimer les appels ? boîte de dialogue, entrez **`confirm`** dans la zone de texte.
6. Sélectionnez Supprimer.

Création d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager

AWS Systems Manager Incident Manager fournit des voies d'escalade par le biais de vos contacts ou de vos horaires d'astreinte définis, collectivement appelés canaux d'escalade. Vous pouvez associer plusieurs canaux d'escalade à un incident en même temps. Si les contacts désignés dans le canal d'escalade ne répondent pas, Incident Manager passe au groupe de contacts suivant. Vous pouvez également choisir si un plan cesse d'augmenter une fois qu'un utilisateur a confirmé son engagement. Vous pouvez ajouter des plans d'escalade à un plan de réponse afin que l'escalade commence automatiquement au début d'un incident. Vous pouvez également ajouter des plans d'escalade à un incident actif.

Rubriques

Étapes

Les plans d'escalade utilisent des étapes où chaque étape dure un nombre défini de minutes. Chaque étape contient les informations suivantes :

- Durée : durée pendant laquelle le plan attend le début de l'étape suivante. La première étape du plan d'escalade commence dès le début de l'engagement.
- Canal d'escalade — Un canal d'escalade est soit un contact unique, soit un calendrier d'astreinte composé de plusieurs contacts qui alternent les responsabilités selon un calendrier défini. Le plan

d'escalade engage chaque canal en utilisant son plan d'engagement défini. Vous pouvez configurer chaque canal d'escalade pour arrêter la progression du plan d'escalade avant qu'il ne passe à l'étape suivante. Chaque étape peut comporter plusieurs canaux d'escalade.

Pour plus d'informations sur la configuration de contacts individuels, consultezCréation et configuration de contacts dans Incident Manager. Pour plus d'informations sur la création d'horaires d'astreinte, consultezGestion de la rotation des intervenants à l'aide de calendriers d'astreinte dans Incident Manager.

Création d'un plan d'escalade

1. Ouvrez la console Incident Manager et choisissez Escalation Plans dans le menu de navigation de gauche.
2. Choisissez Créer un plan d'escalade.
3. Dans Nom, entrez un nom unique pour le plan d'escalade, tel que**`My Escalation Plan`**.
4. Pour Alias, entrez un alias pour vous aider à identifier le plan, par exemple**`my-escalation-plan`**.
5. Pour la durée de l'étape, entrez le nombre de minutes pendant lequel Incident Manager doit attendre avant de passer à l'étape suivante.
6. Pour le canal d'escalade, choisissez un ou plusieurs contacts ou horaires d'astreinte à contacter au cours de cette étape.
7. (Facultatif) Pour permettre à un contact d'arrêter le plan d'escalade une fois qu'il a accusé réception de l'engagement, sélectionnez L'accusé de réception arrête la progression du plan.
8. Pour ajouter un autre canal à cette étape, choisissez Ajouter un canal d'escalade.
9. Pour ajouter une autre étape au plan d'escalade, choisissez Ajouter une étape.
10. Répétez les étapes 5 à 9 jusqu'à ce que vous ayez fini d'ajouter les canaux d'escalade et les étapes souhaités pour ce plan d'escalade.
11. (Facultatif) Dans la zone Balises, appliquez une ou plusieurs paires nom-clé de balise et valeur au plan d'escalade.

    Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes façons, par exemple, par objectif, par propriétaire ou par environnement. Par exemple, vous pouvez étiqueter un plan d'escalade pour identifier le type d'incidents pour lesquels il doit être utilisé, les types de canaux d'escalade qu'il

contient ou le plan d'escalade qu'il prend en charge. Pour plus d'informations sur le balisage des ressources d'Incident Manager, consultezMarquage des ressources dans Incident Manager.

12. Choisissez Créer un plan d'escalade.

Création et intégration de canaux de discussion pour les intervenants dans Incident Manager

Incident Manager, un outil intégré AWS Systems Manager, permet aux intervenants en cas d'incident de communiquer directement par le biais de canaux de discussion lors d'un incident. Un canal de discussion est un salon de discussion que vous configurez dans Amazon Q Developer dans des applications de chat. Vous connectez ensuite ce canal à un plan de réponse dans Incident Manager.

Lors d'un incident, les intervenants utilisent le canal de discussion pour communiquer entre eux à propos de l'incident. Incident Manager transmet également toutes les mises à jour et notifications concernant l'incident directement sur le canal de discussion. Il envoie ces notifications en utilisant un ou plusieurs sujets Amazon Simple Notification Service (Amazon SNS) que vous spécifiez dans la configuration de votre salon de discussion.

Amazon Q Developer dans les applications de chat et Incident Manager prend en charge les canaux de discussion dans les applications suivantes :

- Slack
- Microsoft Teams
- Amazon Chime

Le processus de configuration d'un canal de discussion à utiliser dans le cadre de vos incidents comprend des tâches relevant de trois services Amazon Web Services différents.

Tâches

- Tâche 1 : créer ou mettre à jour des rubriques Amazon SNS pour votre canal de discussion
- Tâche 2 : créer un canal de discussion dans Amazon Q Developer dans les applications de chat
- Tâche 3 : ajouter le canal de discussion à un plan de réponse dans Incident Manager
- Interaction via le canal de discussion

Tâche 1 : créer ou mettre à jour des rubriques Amazon SNS pour votre canal de discussion

Amazon SNS est un service géré qui fournit des messages des éditeurs aux abonnés (également appelés producteurs et consommateurs). Les éditeurs communiquent de façon asynchrone avec les abonnés en envoyant un message à une rubrique, qui est un point d'accès logique et un canal de communication. Incident Manager utilise un ou plusieurs sujets que vous associez à un plan de réponse pour envoyer des notifications concernant un incident aux intervenants.

Dans un plan de réponse, vous pouvez inclure une ou plusieurs rubriques Amazon SNS dans les notifications d'incidents. La meilleure pratique consiste à créer une rubrique SNS dans chaque rubrique Région AWS que vous avez ajoutée à votre jeu de réplication.

> **Tip**
>
> Pour un flux de travail de configuration plus linéaire, nous vous recommandons de configurer d'abord vos rubriques Amazon SNS pour une utilisation avec Incident Manager. Une fois configuré, vous pouvez créer le canal de discussion.

Pour créer ou mettre à jour des sujets Amazon SNS pour votre canal de discussion

1. Suivez les étapes décrites dans la rubrique Création d'un Amazon SNS du guide du développeur Amazon Simple Notification Service.

   > **Note**
   >
   > Après avoir créé le sujet, vous le modifiez pour mettre à jour sa politique d'accès.

2. Sélectionnez le sujet que vous avez créé, puis notez ou copiez le nom de ressource Amazon (ARN) du sujet, dans un format tel que`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
3. Choisissez Modifier, puis développez la section Politique d'accès pour configurer des autorisations d'accès supplémentaires au-delà des autorisations par défaut.
4. Ajoutez l'instruction suivante au tableau des déclarations de la politique :

   ```
   {
       "Sid": "IncidentManagerSNSPublishingPermissions",
   ```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "SNS:Publish",
    "Resource": "sns-topic-arn",
    "Condition": {
        "StringEqualsIfExists": {
            "AWS:SourceAccount": "account-id"
        }
    }
}
```

Remplacez le *placeholder values* comme suit :

- *sns-topic-arn*est le nom de ressource Amazon (ARN) du sujet que vous avez créé pour cette région, au format`arn:aws:sns:us-east-2:111122223333:My_SNS_topic`.
- *account-id*est l'identifiant de l' Compte AWS entreprise dans laquelle vous travaillez, par exemple`111122223333`.

5. Sélectionnez Enregistrer les modifications.
6. Répétez le processus dans chaque région incluse dans votre jeu de réplication.

Tâche 2 : créer un canal de discussion dans Amazon Q Developer dans les applications de chat

Vous pouvez créer un canal de discussion dans Slack, Microsoft Teams, ou Amazon Chime. Vous n'avez besoin que d'un canal de discussion pour chaque plan de réponse.

Pour vos canaux de discussion, nous vous recommandons de suivre le principe du moindre privilège (ne pas accorder aux utilisateurs plus d'autorisations que ce qui est nécessaire pour effectuer leurs tâches). Vous devez également vérifier régulièrement l'adhésion de votre développeur Amazon Q aux canaux de discussion des applications de chat. Les évaluations permettent de vérifier que seuls les intervenants appropriés et les autres parties prenantes ont accès à vos canaux de discussion.

Entrée Slack chaînes et Microsoft Teams canaux créés dans Amazon Q Developer dans les applications de chat, les personnes chargées de répondre aux incidents peuvent exécuter un certain nombre de commandes CLI d'Incident Manager directement depuis Slack or Microsoft

Teams application. Pour de plus amples informations, veuillez consulter Interaction via le canal de discussion.

> **Important**
>
> Les utilisateurs que vous ajoutez à votre canal de discussion doivent être les mêmes contacts que ceux figurant sur votre plan d'escalade ou de réponse. Vous pouvez également ajouter des utilisateurs supplémentaires aux canaux de discussion, tels que les parties prenantes et les observateurs des incidents.

Pour obtenir des informations générales sur Amazon Q Developer dans les applications de chat, consultez la section Qu'est-ce qu'Amazon Q Developer dans les applications de chat dans le Guide de l'administrateur d'Amazon Q Developer dans les applications de chat.

Choisissez parmi les applications suivantes pour créer votre chaîne :

Slack

Les étapes de cette procédure fournissent les paramètres d'autorisation recommandés pour permettre à tous les utilisateurs du canal d'utiliser les commandes de chat avec Incident Manager. À l'aide des commandes de chat prises en charge, vos intervenants peuvent mettre à jour l'incident et interagir avec celui-ci directement depuis Slack canal de discussion. Pour plus d'informations, veuillez consulter Interaction via le canal de discussion.

Pour créer un canal de discussion dans Slack

- Suivez les étapes décrites dans le didacticiel : Commencez avec Slackdans le guide d'administration d'Amazon Q Developer in chat applications et incluez les éléments suivants dans votre configuration.
  - À l'étape 10, pour les paramètres du rôle, choisissez Rôle du canal.
  - À l'étape 10d, pour les modèles de politique, sélectionnez les autorisations du gestionnaire d'incidents.
  - À l'étape 11, pour les politiques de garde-corps des chaînes, pour le nom de la politique, sélectionnez. `AWSIncidentManagerResolverAccess`
  - À l'étape 12, dans la section Rubriques SNS, procédez comme suit :
    - Pour la région 1, sélectionnez Région AWS celle qui est incluse dans votre jeu de réplication.

- Pour les rubriques 1, sélectionnez la rubrique SNS que vous avez créée dans cette région à utiliser pour envoyer des notifications d'incident au canal de discussion.
- Pour chaque région supplémentaire de votre ensemble de réplication, choisissez Ajouter une autre région et ajoutez les rubriques Régions et SNS supplémentaires.

Microsoft Teams

Les étapes de cette procédure fournissent les paramètres d'autorisation recommandés pour permettre à tous les utilisateurs du canal d'utiliser les commandes de chat avec Incident Manager. À l'aide des commandes de chat prises en charge, vos intervenants peuvent mettre à jour l'incident et interagir avec celui-ci directement depuis Microsoft Teams canal de discussion. Pour plus d'informations, veuillez consulter Interaction via le canal de discussion.

Pour créer un canal de discussion dans Microsoft Teams

- Suivez les étapes décrites dans le didacticiel : Commencez avec Microsoft Teamsdans le guide de l'administrateur des applications de chat Amazon Q pour les développeurs et incluez les éléments suivants dans votre configuration :
  - À l'étape 10, pour les paramètres du rôle, choisissez Rôle du canal.
  - À l'étape 10d, pour les modèles de politique, sélectionnez les autorisations du gestionnaire d'incidents.
  - À l'étape 11, pour les politiques de garde-corps des chaînes, pour le nom de la politique, sélectionnez. `AWSIncidentManagerResolverAccess`
  - À l'étape 12, dans la section Rubriques SNS, procédez comme suit :
    - Pour la région 1, sélectionnez Région AWS celle qui est incluse dans votre jeu de réplication.
    - Pour les rubriques 1, sélectionnez la rubrique SNS que vous avez créée dans cette région à utiliser pour envoyer des notifications d'incident au canal de discussion.
    - Pour chaque région supplémentaire de votre ensemble de réplication, choisissez Ajouter une autre région et ajoutez les rubriques Régions et SNS supplémentaires.

Amazon Chime

Pour créer un canal de discussion dans Amazon Chime

- Suivez les étapes décrites dans le didacticiel : Commencez à utiliser Amazon Chime dans le guide de l'administrateur des applications de chat Amazon Q pour les développeurs et incluez les éléments suivants dans votre configuration :
  - À l'étape 11, pour les modèles de politique, sélectionnez les autorisations du gestionnaire d'incidents.
  - À l'étape 12, dans la section Rubriques SNS, sélectionnez les rubriques SNS qui enverront des notifications au webhook Amazon Chime :
    - Pour la région 1, sélectionnez Région AWS celle qui est incluse dans votre jeu de réplication.
    - Pour les rubriques 1, sélectionnez la rubrique SNS que vous avez créée dans cette région à utiliser pour envoyer des notifications d'incident au canal de discussion.
    - Pour chaque région supplémentaire de votre ensemble de réplication, choisissez Ajouter une autre région et ajoutez les rubriques Régions et SNS supplémentaires.

> **Note**
>
> Commandes de chat, que les intervenants en cas d'incident peuvent utiliser dans Slack and Microsoft Teams canaux de discussion, ne sont pas pris en charge dans Amazon Chime.

Tâche 3 : ajouter le canal de discussion à un plan de réponse dans Incident Manager

Lorsque vous créez ou mettez à jour un plan de réponse, vous pouvez ajouter des canaux de discussion permettant aux intervenants de communiquer et de recevoir des mises à jour.

Lorsque vous suivez les étapes Création d'un plan de réponse décrites dans la section (Facultatif) Spécification d'un canal de discussion pour répondre aux incidents, sélectionnez le canal que vous souhaitez utiliser pour les incidents liés à ce plan de réponse.

Interaction via le canal de discussion

Pour les chaînes en Slack and Microsoft Teams, Incident Manager permet aux intervenants d'interagir avec les incidents directement depuis le canal de discussion à l'aide des `ssm-incidents` commandes suivantes :

- incident de début
- list-response-plan
- get-response-plan
- create-timeline-event
- delete-timeline-event
- get-incident-record
- get-timeline-event
- list-incident-records
- list-timeline-events
- list-related-items
- update-related-items
- update-incident-record
- update-timeline-event

Pour exécuter des commandes dans le canal de discussion d'un incident actif, utilisez le format suivant. Remplacez *`cli-options`* par toutes les options à inclure pour une commande.

```
@aws ssm-incidents cli-options
```

Par exemple :

```
@aws ssm-incidents start-incident --response-plan-arn arn:aws:ssm-
incidents::111122223333:response-plan/test-response-plan-chat --region us-east-2
```

```
@aws ssm-incidents create-timeline-event --event-data "\"example timeline event"\" --
event-time 2023-03-31 T20:30:00.000  --event-type Custom Event --incident-record-arn
 arn:aws:ssm-incidents::111122223333:incident-record/MyResponsePlanChat/98c397e6-7c10-
aa10-9b86-f199aEXAMPLE
```

```
@aws ssm-incidents list-incident-records
```

Intégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents

Vous pouvez utiliser les runbooks d'AWS Systems Manager Automation, un outil de AWS Systems Manager, pour automatiser les tâches d'application et d'infrastructure courantes dans votre AWS Cloud environnement.

Chaque runbook définit un flux de travail d'exécution composé des actions que Systems Manager exécute sur vos nœuds gérés ou sur d'autres types de AWS ressources. Vous pouvez utiliser des runbooks pour automatiser la maintenance, le déploiement et la correction de vos AWS ressources.

Dans Incident Manager, un runbook permet de répondre aux incidents et de les atténuer, et vous spécifiez un runbook à utiliser dans le cadre d'un plan de réponse.

Dans vos plans de réponse, vous pouvez choisir parmi des dizaines de runbooks préconfigurés pour les tâches fréquemment automatisées, ou vous pouvez créer des runbooks personnalisés. Lorsque vous spécifiez un runbook dans la définition d'un plan de réponse, le système peut démarrer automatiquement le runbook au début d'un incident.

> **Important**
>
> Les incidents créés par un basculement entre régions n'invoquent pas les runbooks spécifiés dans les plans de réponse.

Pour plus d'informations sur Systems Manager Automation, les runbooks et l'utilisation des runbooks avec Incident Manager, consultez les rubriques suivantes :

- Pour ajouter un runbook à un plan de réponse, consultezCréation et configuration de plans de réponse dans Incident Manager.
- Pour en savoir plus sur les runbooks, consultez AWS Systems Manager Automation dans le guide de l'AWS Systems Manager utilisateur et le manuel de référence des runbooks AWS Systems Manager Automation.
- Pour plus d'informations sur le coût d'utilisation des runbooks, consultez la section Tarification de Systems Manager.

- Pour plus d'informations sur l'appel automatique des runbooks lorsqu'un incident est créé par une CloudWatch alarme Amazon ou un EventBridge événement Amazon, consultez Tutorial : Using Systems Manager Automation runbooks with Incident Manager.

Rubriques

Autorisations IAM requises pour démarrer et exécuter les flux de travail Runbook

Incident Manager nécessite des autorisations pour exécuter des runbooks dans le cadre de votre réponse aux incidents. Pour fournir ces autorisations, vous utilisez les rôles AWS Identity and Access Management (IAM), le rôle de service Runbook et l'Automation. *`AssumeRole`*

Le rôle de service Runbook est un rôle de service obligatoire. Ce rôle fournit à Incident Manager les autorisations dont il a besoin pour accéder au flux de travail du runbook et le démarrer.

L'automatisation `AssumeRole` fournit les autorisations nécessaires pour exécuter les commandes individuelles spécifiées dans le runbook.

> **Note**
>
> Si non `AssumeRole` est spécifié, Systems Manager Automation tente d'utiliser le rôle de service Runbook pour les commandes individuelles. Si vous ne spécifiez pas de`AssumeRole`, vous devez ajouter les autorisations nécessaires au rôle de service Runbook. Si vous ne le faites pas, le runbook ne pourra pas exécuter ces commandes. Toutefois, pour des raisons de sécurité, nous vous recommandons d'utiliser une solution séparée`AssumeRole`. Avec un autre`AssumeRole`, vous pouvez limiter les autorisations nécessaires que vous devez ajouter à chaque rôle.

Pour plus d'informations sur l'automatisation`AssumeRole`, consultez la section « Configuration d'un accès à un rôle de service (assumer un rôle) pour les automatisations » dans le guide de l'AWS Systems Manager utilisateur.

Vous pouvez créer vous-même l'un ou l'autre type de rôle manuellement dans la console IAM.- Vous pouvez également laisser Incident Manager créer l'un ou l'autre type de rôle pour vous lorsque vous créez ou mettez à jour un plan de réponse.

Autorisations relatives aux rôles du service Runbook

Les autorisations relatives aux rôles de service Runbook sont fournies par le biais d'une politique similaire à la suivante.

La première instruction permet à Incident Manager de démarrer le `StartAutomationExecution` fonctionnement de Systems Manager. Cette opération s'exécute ensuite sur les ressources représentées par les trois formats Amazon Resource Name (ARN).

La deuxième instruction permet au rôle de service Runbook d'assumer un rôle dans un autre compte lorsque ce runbook s'exécute dans le compte concerné. Pour plus d'informations, consultez la section Exécution d'automatisations dans plusieurs comptes Régions AWS et dans le Guide de l'AWS Systems Manager utilisateur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "ssm:StartAutomationExecution",
      "Resource": [
        "arn:aws:ssm:*:{{DocumentAccountId}}:automation-definition/{{DocumentName}}:*",
        "arn:aws:ssm:*:{{DocumentAccountId}}:document/{{DocumentName}}:*",
        "arn:aws:ssm:*::automation-definition/{{DocumentName}}:*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-AutomationExecutionRole",
      "Condition": {
        "StringEquals": {
          "aws:CalledViaLast": "ssm.amazonaws.com"
```

```
        }
      }
    }
  ]
}
```

AssumeRole Autorisations d'automatisation

Lorsque vous créez ou mettez à jour un plan de réponse, vous pouvez choisir parmi plusieurs politiques AWS gérées à associer à celles créées par AssumeRole Incident Manager. Ces politiques fournissent des autorisations pour exécuter un certain nombre d'opérations courantes utilisées dans les scénarios d'exécution d'Incident Manager. Vous pouvez choisir une ou plusieurs de ces politiques gérées afin de fournir des autorisations pour votre `AssumeRole` politique. Le tableau suivant décrit les politiques que vous pouvez choisir lorsque vous créez un `AssumeRole` depuis la console Incident Manager.

Nom de la politique gérée par AWS	Description de la politique
`AmazonSSMAutomationRole`	Accorde des autorisations au service Systems Manager Automation pour exécuter les activités définies dans les runbooks. Attribuez cette politique aux administrateurs et aux utilisateurs avancés de confiance.
`AWSIncidentManagerResolverAccess`	Autorise les utilisateurs à démarrer, consulter et mettre à jour des incidents. Vous pouvez également les utiliser pour créer des événements chronologiques pour les clients et des éléments connexes dans le tableau de bord des incidents.

Vous pouvez utiliser ces politiques gérées pour accorder des autorisations pour de nombreux scénarios courants de réponse aux incidents. Toutefois, les autorisations requises pour les tâches spécifiques dont vous avez besoin peuvent varier. Dans ces cas, vous devez fournir des autorisations de politique supplémentaires pour votre`AssumeRole`. Pour plus d'informations, consultez le manuel de référence AWS Systems Manager Automation Runbook.

Utilisation des paramètres du runbook

Lorsque vous ajoutez un runbook à un plan de réponse, vous pouvez spécifier les paramètres que le runbook doit utiliser lors de l'exécution. Les plans de réponse prennent en charge les paramètres avec des valeurs statiques et dynamiques. Pour les valeurs statiques, vous saisissez la valeur lorsque vous définissez le paramètre dans le plan de réponse. Pour les valeurs dynamiques, le système détermine la valeur de paramètre correcte en collectant des informations provenant de l'incident. Incident Manager prend en charge les paramètres dynamiques suivants :

`Incident ARN`

Lorsqu'Incident Manager crée un incident, le système capture l'Amazon Resource Name (ARN) de l'enregistrement d'incident correspondant et le saisit pour ce paramètre dans le runbook.

> **Note**
>
> Cette valeur ne peut être affectée qu'aux paramètres de type `String`. Si elle est affectée à un paramètre d'un autre type, le runbook ne s'exécute pas.

`Involved resources`

Lorsque Incident Manager crée un incident, le ARNs système capture les ressources impliquées dans l'incident. Ces ressources ARNs sont ensuite affectées à ce paramètre dans le runbook.

À propos des ressources associées

Incident Manager peut renseigner les valeurs des paramètres ARNs du runbook avec les AWS ressources spécifiées dans les CloudWatch alarmes, les EventBridge événements et les incidents créés manuellement. Cette section décrit les différents types de ressources qu'Incident Manager peut capturer ARNs lors du remplissage de ce paramètre.

CloudWatch alarmes

Lorsqu'un incident est créé à partir CloudWatch d'une action d'alarme, Incident Manager extrait automatiquement les types de ressources suivants à partir des métriques associées. Il remplit ensuite les paramètres choisis avec les ressources impliquées suivantes :

AWS service	Type de ressource
Amazon DynamoDB	Index secondaires globaux Streams Tables
Amazon EC2	Images instances
AWS Lambda	Alias de fonctions Versions de la fonction Fonctions
Amazon Relational Database Service (Amazon RDS)	Clusters instances de base de données
Amazon Simple Storage Service (Amazon S3)	Compartiments

EventBridge règles

Lorsque le système crée un incident à partir d'un EventBridge événement, Incident Manager renseigne les paramètres choisis avec la `Resources` propriété associée à l'événement. Pour plus d'informations, consultez les EventBridgeévénements Amazon dans le guide de EventBridge l'utilisateur Amazon.

Incidents créés manuellement

Lorsque vous créez un incident à l'aide de l'action d'StartIncidentAPI, Incident Manager renseigne les paramètres choisis en utilisant les informations contenues dans l'appel d'API. Plus précisément, il renseigne les paramètres en utilisant des éléments du type `INVOLVED_RESOURCE` transmis dans le `relatedItems` paramètre.

> **Note**
>
> La `INVOLVED_RESOURCES` valeur ne peut être affectée qu'à des paramètres de type`StringList`. Si elle est affectée à un paramètre d'un autre type, le runbook ne s'exécute pas.

Définir un runbook

Lors de la création d'un runbook, vous pouvez suivre les étapes indiquées ici ou suivre le guide plus détaillé fourni dans la section Working with runbooks du guide de l'utilisateur de Systems Manager. Si vous créez un runbook multi-comptes et multirégions, consultez la section Exécuter des automatisations dans plusieurs comptes dans le Guide Régions AWS de l'utilisateur de Systems Manager.

Définir un runbook

1. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Sélectionnez Create automation (Créer une automatisation).
4. Entrez un nom de runbook unique et identifiable.
5. Entrez une description du runbook.
6. Fournissez un rôle IAM que le document d'automatisation doit assumer. Cela permet au runbook d'exécuter des commandes automatiquement. Pour plus d'informations, consultez Configuration de l'accès à un rôle de service pour les flux de travail d'automatisation.
7. (Facultatif) Ajoutez tous les paramètres d'entrée par lesquels le runbook commence. Vous pouvez utiliser des paramètres dynamiques ou statiques lors du démarrage d'un runbook. Les paramètres dynamiques utilisent les valeurs de l'incident lors duquel le runbook a été démarré. Les paramètres statiques utilisent la valeur que vous fournissez.
8. (Facultatif) Ajoutez un type de cible.
9. (Facultatif) Ajoutez des balises.
10. Renseignez les étapes que le runbook effectuera lors de son exécution. Chaque étape nécessite :

    - Un nom

- Description de l'objectif de l'étape.
- Action à exécuter pendant l'étape. Les runbooks utilisent le type d'action Pause pour décrire une étape manuelle.
- (Facultatif) Propriétés de commande.

11. Après avoir ajouté toutes les étapes requises du runbook, choisissez Create Automation.

Pour activer la fonctionnalité multi-comptes, partagez le runbook de votre compte de gestion avec tous les comptes d'applications qui utilisent le runbook lors d'un incident.

Partager un runbook

1. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Dans la liste des documents, choisissez le document que vous souhaitez partager, puis sélectionnez Afficher les détails. Sur l'onglet Permissions (Autorisations), vérifiez que vous êtes le propriétaire du document. Seul le propriétaire d'un document peut le partager.
4. Sélectionnez Edit (Modifier).
5. Pour partager la commande publiquement, sélectionnez Public, puis Save. Pour partager la commande en privé, choisissez Privé, entrez l' Compte AWS ID, choisissez Ajouter une autorisation, puis sélectionnez Enregistrer.

Modèle de runbook d'Incident Manager

Incident Manager fournit le modèle de runbook suivant pour aider votre équipe à commencer à créer des runbooks dans le cadre de l'automatisation de Systems Manager. Vous pouvez utiliser ce modèle tel quel ou le modifier pour inclure des détails spécifiques à votre application et à vos ressources.

Trouvez le modèle de runbook d'Incident Manager

1. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Dans la zone Documents, entrez **`AWSIncidents-`** dans le champ de recherche pour afficher tous les runbooks d'Incident Manager.

> **Tip**
>
> Entrez **`AWSIncidents-`** sous forme de texte libre au lieu d'utiliser l'option de filtre de préfixe du nom du document.

Utilisation d'un modèle

1. Ouvrez la console Systems Manager à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Choisissez le modèle que vous souhaitez mettre à jour dans la liste des documents.
4. Choisissez l'onglet Contenu, puis copiez le contenu du document.
5. Dans le panneau de navigation, cliquez sur Documents.
6. Sélectionnez Create automation (Créer une automatisation).
7. Entrez un nom unique et identifiable.
8. Choisissez l'onglet Éditeur.
9. Choisissez Modifier.
10. Collez ou saisissez les informations copiées dans la zone de l'éditeur de documents.
11. Sélectionnez Create automation (Créer une automatisation).

`AWSIncidents-CriticalIncidentRunbookTemplate`

`AWSIncidents-CriticalIncidentRunbookTemplate`Il s'agit d'un modèle qui fournit le cycle de vie des incidents d'Incident Manager en étapes manuelles. Ces étapes sont suffisamment génériques pour être utilisées dans la plupart des applications, mais suffisamment détaillées pour que les intervenants puissent commencer à résoudre les incidents.

Création et configuration de plans de réponse dans Incident Manager

Les plans de réponse vous permettent de planifier la manière de répondre à un incident ayant un impact sur vos utilisateurs. Un plan de réponse fonctionne comme un modèle qui inclut des

informations sur les personnes à engager, la gravité attendue de l'événement, les runbooks automatiques à lancer et les mesures à surveiller.

Bonnes pratiques

Vous pouvez réduire l'impact des incidents sur vos équipes en planifiant les incidents à l'avance. Les équipes doivent prendre en compte les meilleures pratiques suivantes lors de la conception d'un plan de réponse.

- Engagement rationalisé : identifiez l'équipe la plus appropriée pour un incident. Si vous interagissez avec une liste de distribution trop large ou si vous engagez les mauvaises équipes, vous risquez de créer de la confusion et de faire perdre du temps aux intervenants lors d'un incident.
- Escalade fiable — Pour vos engagements dans le cadre d'un plan de réponse, nous vous recommandons de sélectionner un plan d'engagement plutôt que des contacts ou des calendriers d'astreinte. Le plan d'engagement doit spécifier les contacts individuels ou les horaires d'astreinte (qui contiennent plusieurs contacts rotatifs) à engager lors d'incidents. Étant donné que les intervenants spécifiés dans votre plan d'engagement peuvent parfois être injoignables, vous devez configurer des répondeurs de secours dans votre plan de réponse pour couvrir ces scénarios. Avec les contacts de secours, si les contacts principaux et secondaires ne sont pas disponibles ou s'il existe d'autres lacunes imprévues dans la couverture, Incident Manager informe tout de même un contact de l'incident.
- Runbooks : utilisez les runbooks pour fournir des étapes répétables et compréhensibles qui réduisent le stress ressenti par un intervenant lors d'un incident.
- Collaboration — Utilisez les canaux de discussion pour rationaliser la communication lors d'incidents. Les canaux de discussion aident les intervenants à se tenir au courant des informations. Ils peuvent également partager des informations avec d'autres intervenants par le biais de ces canaux.

Création d'un plan de réponse

Utilisez la procédure suivante pour créer un plan de réponse et automatiser la réponse aux incidents.

Pour créer un plan d'intervention

1. Ouvrez la console Incident Manager, puis dans le volet de navigation, sélectionnez Response plans.

2. Choisissez Créer un plan de réponse.
3. Dans Nom, entrez un nom de plan de réponse unique et identifiable à utiliser dans l'Amazon Resource Name (ARN) du plan de réponse.
4. (Facultatif) Dans Nom d'affichage, entrez un nom plus lisible pour aider à identifier le plan de réponse lorsque vous créez des incidents.
5. Continuez en spécifiant les valeurs par défaut pour les enregistrements d'incidents.

Spécification des valeurs par défaut des incidents

Pour vous aider à gérer les incidents plus efficacement, vous pouvez définir des valeurs par défaut. Incident Manager applique ces valeurs à tous les incidents associés à un plan de réponse.

Pour spécifier les valeurs par défaut des incidents

1. Dans le champ Titre, saisissez le titre de cet incident afin de vous aider à l'identifier sur la page d'accueil du Gestionnaire d'incidents.
2. Pour Impact, choisissez un niveau d'impact pour indiquer l'étendue potentielle des incidents créés à partir de ce plan de réponse, tel que Critique ou Faible. Pour plus d'informations sur les évaluations d'impact dans Incident Manager, consultezTri.
3. (Facultatif) Dans Résumé, entrez un bref résumé du type d'incidents créés à partir de ce plan de réponse.
4. (Facultatif) Pour la chaîne de déduplication, entrez une chaîne de déduplication. Incident Manager utilise cette chaîne pour empêcher la même cause première de créer plusieurs incidents dans le même compte.

   Une chaîne de déduplication est un terme ou une expression que le système utilise pour vérifier la présence d'incidents dupliqués. Si vous spécifiez une chaîne de déduplication, Incident Manager recherche les incidents ouverts contenant la même chaîne dans le `dedupeString` champ lors de la création de l'incident. Si un doublon est détecté, Incident Manager déduplique le nouvel incident dans l'incident existant.

   > **Note**
   >
   > Par défaut, Incident Manager déduplique automatiquement plusieurs incidents créés par la même alarme Amazon CloudWatch ou le même événement Amazon. EventBridge Il

n'est pas nécessaire de saisir votre propre chaîne de déduplication pour empêcher la duplication de ces types de ressources.

5. (Facultatif) Sous Balises d'incident, ajoutez des clés de balise et des valeurs à attribuer aux incidents créés à partir de ce plan de réponse.

   Vous devez être autorisé à `TagResource` autoriser la ressource d'enregistrement des incidents à définir des balises d'incident dans le plan de réponse.

6. Continuez en spécifiant un canal de discussion facultatif permettant aux résolveurs de communiquer entre eux au sujet des incidents.

(Facultatif) Spécification d'un canal de discussion pour répondre aux incidents

Lorsque vous incluez un canal de discussion dans un plan de réponse, les intervenants reçoivent des mises à jour sur les incidents via le canal. Ils peuvent interagir avec l'incident directement depuis le canal de discussion en utilisant les commandes de chat.

En utilisant Amazon Q Developer dans les applications de chat, vous pouvez créer un canal pour Slack, pour Microsoft Teams, ou pour qu'Amazon Chime puisse l'utiliser dans vos plans de réponse. Pour plus d'informations sur la création d'un canal de discussion dans Amazon Q Developer dans les applications de chat, consultez le Guide de l'administrateur d'Amazon Q Developer dans les applications de chat.

Important

Incident Manager doit être autorisé à publier sur la rubrique Amazon Simple Notification Service (Amazon SNS) d'un canal de discussion. Si vous n'êtes pas autorisé à publier sur cette rubrique SNS, vous ne pouvez pas l'ajouter au plan de réponse. Incident Manager publie une notification de test dans la rubrique SNS pour vérifier les autorisations.

Pour plus d'informations sur les canaux de discussion, consultezCréation et intégration de canaux de discussion pour les intervenants dans Incident Manager.

Pour spécifier un canal de discussion pour répondre aux incidents

1. Pour le canal de discussion, sélectionnez un canal de discussion Amazon Q Developer dans les applications de chat où les intervenants peuvent communiquer lors d'un incident.

> **Tip**
>
> Pour créer un nouveau canal de discussion dans Amazon Q Developer dans les applications de chat, choisissez Configurer un nouveau client Chatbot.

2. Pour les sujets SNS du canal de chat, choisissez des sujets SNS supplémentaires sur lesquels publier pendant l'incident. L'ajout de sujets SNS en plusieurs fois Régions AWS augmente la redondance au cas où une région serait en panne au moment de l'incident.
3. Continuez en sélectionnant les contacts, les horaires d'astreinte et les plans d'escalade à engager lors d'un incident.

(Facultatif) Sélectionnez les ressources pour participer à la réponse aux incidents

Il est important d'identifier les intervenants les plus appropriés en cas d'incident. À titre de bonne pratique, nous vous recommandons de procéder comme suit :

1. Ajoutez des contacts et des horaires d'astreinte comme canaux d'escalade dans un plan d'escalade.

> **Note**
>
> Actuellement, la possibilité d'ajouter un contact partagé depuis un autre compte à un plan de réponse n'est pas prise en charge.

2. Choisissez un plan d'escalade comme engagement dans un plan de réponse.

Pour plus d'informations sur les contacts et les plans d'escalade, consultez Création et configuration de contacts dans Incident Manager etCréation d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager.

Pour sélectionner les ressources à engager dans la réponse aux incidents

1. Pour les engagements, choisissez autant de plans d'escalade, de calendriers d'astreinte et de contacts individuels que vous le souhaitez.
2. Continuez en spécifiant éventuellement un runbook à exécuter dans le cadre de l'atténuation de vos incidents.

(Facultatif) Spécification d'un runbook pour l'atténuation des incidents

Vous pouvez utiliser les runbooks d'AWS Systems Manager Automation, un outil de AWS Systems Manager, pour automatiser les tâches d'application et d'infrastructure courantes dans votre AWS Cloud environnement.

Chaque runbook définit un flux de travail de runbook. Un flux de travail Runbook inclut les actions que Systems Manager exécute sur vos nœuds gérés ou sur d'autres types de AWS ressources. Dans Incident Manager, un runbook permet de répondre aux incidents et de les atténuer.

Pour plus d'informations sur l'utilisation des runbooks dans les plans de réponse,Intégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents.

Pour spécifier un runbook pour l'atténuation des incidents, procédez comme suit :

1. Pour Runbook, effectuez l'une des opérations suivantes :

   - Choisissez Cloner le runbook depuis le modèle pour créer une copie du runbook par défaut d'Incident Manager. Pour le nom du runbook, entrez un nom descriptif pour le nouveau runbook.
   - Choisissez Sélectionner un runbook existant. Sélectionnez le propriétaire, le Runbook et la version à utiliser.

   > **Tip**
   >
   > Pour créer un runbook à partir de zéro, choisissez Configurer un nouveau runbook. Pour plus d'informations sur la création de runbooks, consultez Intégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents.

2. Dans la zone Paramètres, indiquez tous les paramètres demandés pour le runbook que vous avez sélectionné.

   Les paramètres disponibles sont ceux spécifiés par le runbook. Un runbook peut nécessiter des paramètres différents d'un autre. Certains paramètres peuvent être obligatoires et d'autres facultatifs.

   Dans de nombreux cas, vous pouvez choisir de saisir manuellement une valeur statique pour un paramètre, telle qu'une liste d' EC2 instances Amazon IDs. Vous pouvez également laisser Incident Manager fournir les valeurs de paramètres générées dynamiquement par un incident.

3. (Facultatif) Pour AutomationAssumeRole, spécifiez le rôle AWS Identity and Access Management (IAM) à utiliser. Ce rôle doit disposer des autorisations nécessaires pour exécuter les commandes individuelles spécifiées dans le runbook.

   > **Note**
   >
   > Si non `AssumeRole` est spécifié, Incident Manager tente d'utiliser le rôle de service Runbook pour exécuter les commandes individuelles spécifiées dans le runbook.

   Choisissez parmi les options suivantes :

   - Entrez une valeur ARN — Entrez manuellement le nom de ressource Amazon (ARN) d'un AssumeRole, au format`arn:aws:iam::`*`account-id`*`:role/`*`assume-role-name`*. Par exemple, **`arn:aws:iam::123456789012:role/MyAssumeRole`**.
   - Utiliser un rôle de service existant : choisissez un rôle avec les autorisations requises dans la liste des rôles existants de votre compte.
   - Créer un nouveau rôle de service : choisissez parmi les politiques AWS gérées à associer à votre AssumeRole. Après avoir sélectionné cette option, pour les politiques AWS gérées, choisissez une ou plusieurs politiques dans la liste.

     Vous pouvez accepter le nom par défaut suggéré pour le nouveau rôle ou saisir le nom de votre choix.

     > **Note**
     >
     > Ce nouveau rôle de service Runbook est associé au runbook spécifique que vous avez sélectionné. Il ne peut pas être utilisé avec différents runbooks. Cela est dû au fait que la section Ressources de la politique ne prend pas en charge les autres runbooks.

4. Pour le rôle de service Runbook, spécifiez le rôle IAM à utiliser pour fournir les autorisations nécessaires pour accéder et démarrer le flux de travail pour le runbook lui-même.

   Au minimum, le rôle doit autoriser l'`ssm:StartAutomationExecution`action pour votre runbook spécifique. Pour que le runbook fonctionne sur plusieurs comptes, le rôle doit également autoriser l'`sts:AssumeRole`action pour le `AWS-SystemsManager-`

`AutomationExecutionRole` rôle que vous avez créé au cours Gestion des incidents par région Comptes AWS et par région dans Incident Manager de cette opération.

Choisissez parmi les options suivantes :

- Créer un nouveau rôle de service : Incident Manager crée pour vous un rôle de service Runbook qui inclut les autorisations minimales requises pour démarrer le flux de travail Runbook.

  Pour Nom du rôle, vous pouvez accepter le nom par défaut suggéré ou saisir le nom de votre choix. Nous vous recommandons d'utiliser le nom suggéré ou de conserver le nom du runbook dans le nom. Cela est dû au fait que le nouveau runbook AssumeRole est associé au runbook spécifique que vous avez sélectionné et peut ne pas inclure les autorisations requises pour les autres runbooks.
- Utiliser un rôle de service existant : un rôle IAM que vous ou Incident Manager avez créé précédemment accorde les autorisations nécessaires.

  Dans Nom du rôle, sélectionnez le nom du rôle existant à utiliser.

5. Développez les options supplémentaires et choisissez l'une des options suivantes pour spécifier l' Compte AWS endroit où le flux de travail Runbook doit s'exécuter.

   - Compte du propriétaire du plan de réponse : lancez le flux de travail Runbook dans Compte AWS celui qui l'a créé.
   - Compte concerné : lancez le flux de travail Runbook dans le compte qui a déclenché ou signalé l'incident.

     Choisissez Compte impacté lorsque vous utilisez Incident Manager pour des scénarios entre comptes et que le runbook doit accéder aux ressources du compte concerné pour y remédier.

6. Poursuivez en intégrant éventuellement un PagerDuty service dans le plan de réponse.

(Facultatif) Intégrer un PagerDuty service dans le plan de réponse

Pour intégrer un PagerDuty service dans le plan de réponse

Lorsque vous intégrez Incident Manager à PagerDuty, PagerDuty crée un incident correspondant chaque fois qu'Incident Manager crée un incident. L'incident dans PagerDuty utilise le flux de travail

de pagination et les politiques d'escalade que vous y avez définis en plus de ceux définis dans Incident Manager. PagerDuty joint les événements chronologiques d'Incident Manager sous forme de notes sur votre incident.

1. Développez les intégrations tierces, puis cochez la case Activer PagerDuty l'intégration.
2. Pour Select secret, sélectionnez le secret dans AWS Secrets Manager lequel vous stockez les informations d'identification pour accéder à votre PagerDuty compte.

   Pour plus d'informations sur le stockage de vos PagerDuty informations d'identification dans un secret de Secrets Manager, consultezStockage AWS Secrets Manager secret des informations d' PagerDuty accès.
3. Pour le PagerDuty service, sélectionnez le service dans votre PagerDuty compte où vous souhaitez créer l' PagerDuty incident.
4. Continuez en ajoutant des balises facultatives et en créant le plan de réponse.

Ajouter des balises et créer le plan de réponse

Pour ajouter des balises et créer le plan de réponse

1. (Facultatif) Dans la zone Balises, appliquez une ou plusieurs paires nom/valeur clé de balise au plan de réponse.

   Les balises sont des métadonnées facultatives que vous affectez à une ressource. Les balises vous permettent de classer une ressource de différentes manières, par exemple en fonction de son objectif, de son propriétaire ou de son environnement. Par exemple, vous pouvez étiqueter un plan de réponse pour identifier le type d'incident qu'il est censé atténuer, les types de canaux d'escalade qu'il contient ou le plan d'escalade qui y sera associé. Pour plus d'informations sur le balisage des ressources d'Incident Manager, consultezMarquage des ressources dans Incident Manager.
2. Choisissez Créer un plan de réponse.

Identifier les causes potentielles des incidents provenant d'autres services en tant que « constatations » dans Incident Manager

Dans Incident Manager, une constatation est une information concernant un AWS CodeDeploy déploiement ou une mise à jour de AWS CloudFormation pile survenus au moment d'un incident et impliquant une ou plusieurs ressources probablement liées à l'incident. Chaque découverte peut être examinée en tant que cause potentielle de l'incident. Les informations relatives à ces causes potentielles sont ajoutées à la page des détails de l'incident. Les informations relatives à ces déploiements et modifications étant facilement accessibles, les intervenants n'ont pas besoin de les rechercher manuellement. Cela réduit le temps nécessaire pour évaluer les causes potentielles, ce qui peut réduire le temps moyen de rétablissement (MTTR) après un incident.

Actuellement, Incident Manager prend en charge la collecte des résultats à partir de deux Services AWS : AWS CodeDeployet AWS CloudFormation.

Findings est une fonctionnalité optionnelle. Vous pouvez l'activer dans l'assistant de préparation, lors de votre première intégration à Incident Manager, ou ultérieurement sur la page Paramètres.

Lorsque vous activez la fonctionnalité Résultats, Incident Manager crée un rôle de service pour vous. Ce rôle de service inclut les autorisations nécessaires pour récupérer les résultats de CodeDeploy et CloudFormation.

Pour utiliser les résultats dans un scénario multi-comptes, activez la fonctionnalité dans le compte de gestion. Ensuite, chaque compte d'application d'une organisation AWS Resource Access Manager (AWS RAM) doit créer un rôle de service correspondant.

Consultez les rubriques suivantes pour vous aider à utiliser la fonctionnalité Résultats.

Rubriques

- Activez et créez un rôle de service pour les résultats
- Configurer les autorisations pour la prise en charge des résultats entre comptes

Activez et créez un rôle de service pour les résultats

Lorsque vous activez la fonctionnalité Résultats, Incident Manager crée un rôle de service nommé `IncidentManagerIncidentAccessServiceRole` en votre nom. Ce rôle de service fournit les autorisations dont Incident Manager a besoin pour recueillir des informations sur CodeDeploy les

déploiements et les mises à jour de CloudFormation pile survenues au moment de la création d'un incident.

> **Note**
>
> Si vous utilisez Incident Manager avec une organisation, le rôle de service est créé dans le compte de gestion. Pour utiliser les résultats d'autres comptes de l'organisation, le rôle de service doit être créé dans chaque compte d'application. Pour plus d'informations sur l'utilisation d'un CloudFormation modèle pour créer ce rôle dans vos comptes d'applications, reportez-vous à l'étape 4 deConfiguration et configuration de la gestion des incidents entre comptes.

Ce rôle de service est associé à une politique AWS gérée. Pour plus d'informations sur les autorisations définies dans cette politique, consultezAWS politique gérée : AWSIncident ManagerIncidentAccessServiceRolePolicy.

Pour plus d'informations sur l'activation des résultats lors du processus d'intégration d'Incident Manager, consultezCommencer à utiliser Incident Manager.

Pour plus d'informations sur l'activation des résultats une fois le processus d'intégration terminé, consultezGestion de la fonctionnalité des résultats.

Configurer les autorisations pour la prise en charge des résultats entre comptes

Pour utiliser la fonctionnalité Findings sur les comptes dans lesquels une organisation est configurée AWS RAM, chaque compte d'application doit configurer les autorisations permettant à Incident Manager d'assumer le rôle de service du compte de gestion en son nom.

Ces autorisations peuvent être configurées dans un compte d'application en déployant un AWS CloudFormation modèle fourni par AWS, qui crée le rôle`IncidentManagerIncidentAccessServiceRole`.

Pour plus d'informations sur le téléchargement et le déploiement de ce modèle dans un compte d'application, reportez-vous à l'étape 4 deGestion des incidents par région Comptes AWS et par région dans Incident Manager.

Création d'incidents automatiquement ou manuellement dans Incident Manager

Incident Manager, un outil intégré AWS Systems Manager, vous aide à gérer les incidents et à y répondre rapidement. Vous pouvez configurer Amazon CloudWatch et Amazon EventBridge pour créer automatiquement des incidents en fonction des CloudWatch alarmes et EventBridge des événements. Vous pouvez également créer des incidents manuellement sur la page de liste des incidents ou en utilisant l'action StartIncidentAPI du SDK AWS CLI ou du AWS SDK. Incident Manager déduplique les incidents créés à partir de la même CloudWatch alarme ou du même EventBridge événement dans le même incident.

Pour les incidents créés automatiquement par des CloudWatch alarmes ou EventBridge des événements, Incident Manager tente de créer un incident identique à la Région AWS règle d'événement ou à l'alarme. Si Incident Manager n'est pas disponible dans le Région AWS CloudWatch ou si l'incident n'est pas créé EventBridge automatiquement dans l'une des régions disponibles spécifiées dans votre jeu de réplication. Pour de plus amples informations, veuillez consulter Gestion des incidents par région Comptes AWS et par région dans Incident Manager.

Lorsque le système crée un incident, Incident Manager collecte automatiquement des informations sur les AWS ressources impliquées dans l'incident et ajoute ces informations à l'onglet Eléments associés. Si vous avez spécifié un runbook dans votre plan de réponse, lorsque le système crée un incident, Incident Manager peut envoyer au runbook les informations relatives aux AWS ressources impliquées dans l'incident. Le système peut ensuite cibler ces ressources lorsqu'il lance le runbook et tente de résoudre le problème.

Lorsque le système crée un incident, il crée également un élément de travail opérationnel parent (OpsItem) dans OpsCenter un composant de Systems Manager, et le lie à l'incident en tant qu'élément connexe. Vous pouvez l'utiliser OpsItem pour suivre les travaux connexes et les analyses des futurs incidents. Appels pour OpsCenter engager des frais. Pour plus d'informations sur les OpsCenter tarifs, consultez la section Tarification de Systems Manager.

> **Important**
>
> Prenez note des informations importantes suivantes.
>
> - Si Incident Manager n'est pas disponible, le système ne peut basculer et créer des incidents dans un autre système que Régions AWS si vous avez spécifié au moins deux

régions dans votre jeu de réplication. Pour plus d'informations sur la configuration d'un ensemble de réplication, consultezCommencer à utiliser Incident Manager.

- Les incidents créés par un basculement entre régions n'invoquent pas les runbooks spécifiés dans les plans de réponse.

Création automatique d'incidents à l'aide d' CloudWatch alarmes

CloudWatch utilise vos CloudWatch indicateurs pour vous avertir des modifications apportées à votre environnement et pour exécuter automatiquement l'action de démarrage de l'incident. CloudWatch fonctionne avec Systems Manager et Incident Manager pour créer un incident à partir d'un modèle de plan de réponse lorsqu'une alarme passe en état d'alarme. Cela nécessite les prérequis suivants :

- Incident Manager configuré et jeu de réplication créé. Cette étape crée le rôle lié au service Incident Manager dans votre compte, en fournissant les autorisations nécessaires.
- Un plan de réponse configuré pour Incident Manager. Pour savoir comment configurer les plans de réponse d'Incident Manager, consultez Création et configuration de plans de réponse dans Incident Manager la section Préparation aux incidents de ce guide.
- CloudWatch Des métriques configurées surveillant votre application. Pour en savoir plus sur les meilleures pratiques Surveillance en matière de surveillance, consultez la section Préparation des incidents de ce guide.

Pour créer une alarme avec une action Démarrer l'incident

1. Créez une alarme dans CloudWatch. Pour plus d'informations, consultez la section Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon.
2. Lorsque vous choisissez l'action à exécuter par l'alarme, sélectionnez l'action Add Systems Manager.
3. Choisissez Créer un incident et sélectionnez le plan de réponse pour cet incident.
4. Effectuez les étapes restantes dans le guide des types d'alarme que vous avez sélectionné.

> **Tip**
>
> Vous pouvez également ajouter l'action de création d'incident à n'importe quelle alarme existante.

Création automatique d'incidents à partir d' EventBridge événements

EventBridge les règles surveillent les modèles d'événements. Si l'événement correspond au modèle défini, Incident Manager crée un incident en utilisant le plan de réponse choisi.

Création d'incidents à l'aide d'événements destinés aux partenaires SaaS

Vous pouvez configurer EventBridge pour recevoir des événements provenant d'applications et de services partenaires du logiciel en tant que service (SaaS), ce qui permet une intégration par des tiers. Après avoir configuré EventBridge pour recevoir des événements de partenaires tiers, vous pouvez créer des règles qui correspondent aux événements des partenaires afin de créer des incidents. Pour consulter la liste des intégrations tierces, consultez la section Réception d'événements d'un partenaire SaaS.

Configurez EventBridge pour recevoir des événements à partir d'une intégration SaaS.

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Partner event sources (Sources d'événements partenaires).
3. Utilisez la barre de recherche pour trouver le partenaire que vous recherchez et choisissez Configurer pour ce partenaire.
4. Choisissez Copy (Copier) pour copier votre ID de compte dans le presse-papiers.

> **Note**
>
> Pour intégrer Salesforce, suivez les étapes décrites dans le guide de AppFlow l'utilisateur Amazon.

5. Accédez au site web du partenaire et suivez les instructions pour créer une source d'événement partenaire. Utilisez votre ID de compte à cette fin. La source de l'événement que vous créez n'est disponible que sur votre compte.
6. Revenez à la EventBridge console et choisissez Partner event sources dans le volet de navigation.
7. Sélectionnez le bouton en regard de la source d'événement partenaire, puis choisissez Associate with event bus (Associer au bus d'événement).

Créez une règle qui se déclenche en fonction des événements d'un partenaire SaaS

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Saisissez un nom et une description pour la règle.

   Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.
5. Pour Event bus, choisissez le bus d'événement correspondant à ce partenaire.
6. Pour Type de règle, choisissez Règle avec un modèle d'événement.
7. Choisissez Suivant.
8. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
9. Pour Modèle d'événement, choisissez Formulaire de modèle d'événement.
10. Pour Event source, choisissez EventBridgedes partenaires
11. Pour Partenaires, choisissez le nom du partenaire.
12. Pour Event type (Type d'événement), choisissez All Events (Tous les événements) ou choisissez le type d'événement à utiliser pour cette règle. Si vous choisissez All Events (Tous les événements), tous les événements émis par cette source d'événement partenaire correspondent à la règle.

    Si vous souhaitez personnaliser le modèle d'événement, choisissez Modifier, apportez vos modifications, puis cliquez sur Enregistrer.
13. Choisissez Suivant.
14. Pour Sélectionner une cible, choisissez le plan de réponse d'Incident Manager, puis choisissez un plan de réponse.

    > **Note**
    >
    > Lorsque vous sélectionnez un plan de réponse, tous les plans de réponse que vous possédez et qui ont été partagés avec votre compte apparaissent dans la liste déroulante des plans de réponse.
15. EventBridge peut créer le rôle IAM nécessaire à l'exécution de votre règle :

- Pour créer un rôle IAM automatiquement, choisissez Create a new role for this specific resource.
- Pour utiliser un rôle IAM que vous avez créé auparavant, choisissez Utiliser le rôle existant.

16. Choisissez Suivant.
17. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez les EventBridgebalises Amazon dans le guide de EventBridge l'utilisateur Amazon.
18. Choisissez Suivant.
19. Passez en revue votre règle, puis choisissez Créer une règle.

Création d'incidents à l'aide d'événements AWS de service

EventBridge reçoit également des événements provenant des AWS services répertoriés dans la section Événements des AWS services pris en charge. De la même manière que vous configurez les règles pour les partenaires SaaS, vous pouvez les configurer pour les AWS services.

Création d'une règle qui se déclenche en fonction des événements d'un AWS service

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Saisissez un nom et une description pour la règle.

   Une règle ne peut pas avoir le même nom qu’une autre règle de la même région et sur le même bus d’événement.
5. Pour Event bus (Bus d’événement), choisissez default (défaut).
6. Pour Type de règle, choisissez Règle avec un modèle d’événement.
7. Choisissez Suivant.
8. Dans Source de l'événement, sélectionnez AWS événements ou événements EventBridge partenaires.
9. Pour Modèle d'événement, choisissez Formulaire de modèle d'événement.
10. Pour Source d'événement, choisissez Services AWS .
11. Dans Nom du service, choisissez le service qui surveille un incident.

12. Pour Event type (Type d'événement), choisissez All Events (Tous les événements) ou choisissez le type d'événement à utiliser pour cette règle. Si vous choisissez All Events (Tous les événements), tous les événements émis par cette source d'événement partenaire correspondent à la règle.

    Si vous souhaitez personnaliser le modèle d'événement, choisissez Modifier, apportez vos modifications, puis cliquez sur Enregistrer.
13. Choisissez Suivant.
14. Pour Sélectionner une cible, choisissez le plan de réponse d'Incident Manager, puis choisissez un plan de réponse.

    > **Note**
    >
    > Lorsque vous sélectionnez un plan de réponse, tous les plans de réponse que vous possédez et qui ont été partagés avec votre compte apparaissent dans la liste déroulante des plans de réponse.
15. EventBridge peut créer le rôle IAM nécessaire à l'exécution de votre règle :

    - Pour créer un rôle IAM automatiquement, choisissez Create a new role for this specific resource.
    - Pour utiliser un rôle IAM que vous avez créé auparavant, choisissez Utiliser le rôle existant.
16. Choisissez Suivant.
17. (Facultatif) Saisissez une ou plusieurs balises pour la règle. Pour plus d'informations, consultez les EventBridgebalises Amazon dans le guide de EventBridge l'utilisateur Amazon.
18. Choisissez Suivant.
19. Passez en revue votre règle, puis choisissez Créer une règle.

Création manuelle d'incidents

Les intervenants peuvent suivre manuellement un incident à l'aide de la console Incident Manager en utilisant un plan de réponse prédéfini. Suivez les étapes ci-dessous pour créer un incident.

1. Ouvrez la console Incident Manager.
2. Choisissez Démarrer l'incident.
3. Pour Plan de réponse, choisissez un plan de réponse dans la liste.

4. (Facultatif) Pour remplacer le titre fourni par le plan de réponse défini, entrez un titre d'incident.
5. (Facultatif) Pour annuler l'impact fourni par le plan de réponse défini, entrez l'impact de l'incident.

Autorisations IAM requises pour démarrer manuellement des incidents

Pour démarrer manuellement des incidents, les utilisateurs doivent être autorisés à accéder à la console Incident Manager, à consulter les plans de réponse et à démarrer des incidents. Lorsqu'un utilisateur déclenche un incident, Incident Manager utilise des sessions d'accès direct (FAS) pour effectuer l'`StartEngagement`appel dans le cadre de `StartIncident` celles-ci.

La politique IAM suivante fournit les autorisations nécessaires pour démarrer manuellement des incidents, consulter les plans de réponse avec lesquels les incidents peuvent être créés, et visualiser et modifier les incidents une fois qu'ils ont été créés.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident",
                "ssm-incidents:GetResponsePlan",
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:TagResource",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:UpdateIncidentRecord"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm-contacts:StartEngagement"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
```

```
        },
        {
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:CalledViaFirst": "ssm-incidents.amazonaws.com"
                }
            }
        }
    ]
}
```

Cette politique inclut les autorisations suivantes :

- ssm-incidents : StartIncident - Permet aux utilisateurs de démarrer manuellement un incident à l'aide de la console ou de l'API. Cela crée un nouvel enregistrement d'incident à partir d'un plan de réponse.
- ssm-incidents : GetResponsePlan - Permet aux utilisateurs de récupérer des informations sur un plan de réponse spécifique.
- ssm-incidents : ListResponsePlans - Permet aux utilisateurs de répertorier tous les plans d'intervention de leur compte.
- ssm-incidents : TagResource - Permet d'ajouter des balises aux ressources du gestionnaire d'incidents, y compris les incidents et les plans de réponse.
- ssm-incidents : GetIncidentRecord - Permet aux utilisateurs de récupérer des informations détaillées sur un incident spécifique.
- ssm-incidents : ListIncidentRecords - Permet aux utilisateurs de répertorier tous les incidents de leur compte.
- ssm-incidents : UpdateIncidentRecord - Permet aux utilisateurs de mettre à jour les détails d'un incident existant.
- ssm-contacts : StartEngagement (avec condition) - Permet au gestionnaire d'incidents de démarrer des interactions avec des contacts. La condition garantit que cela ne peut être appelé que via Incident Manager.
- ssm : CreateOpsItem (avec condition) - Permet à Incident Manager de créer un OpsItem in OpsCenter. La condition garantit que cela ne peut être appelé que via Incident Manager.

La clé de CalledViaFirst condition aws : garantit que certaines autorisations (comme`StartEngagement`) ne peuvent être utilisées que lorsque la demande passe par le service Incident Manager. Cette approche utilise le FAS plutôt que des rôles liés aux services, ce qui permet d'éviter les éventuels appels entre comptes susceptibles de présenter des risques de sécurité.

Afficher les détails de l'incident dans la console Incident Manager

AWS Systems Manager Incident Manager suit vos incidents depuis leur détection jusqu'à leur résolution, en passant par une analyse post-incident. Vous pouvez trouver tous les incidents sur la page de liste des incidents de la console Incident Manager, avec des liens directs vers les détails de l'incident.

Rubriques

Afficher la liste des incidents dans la console

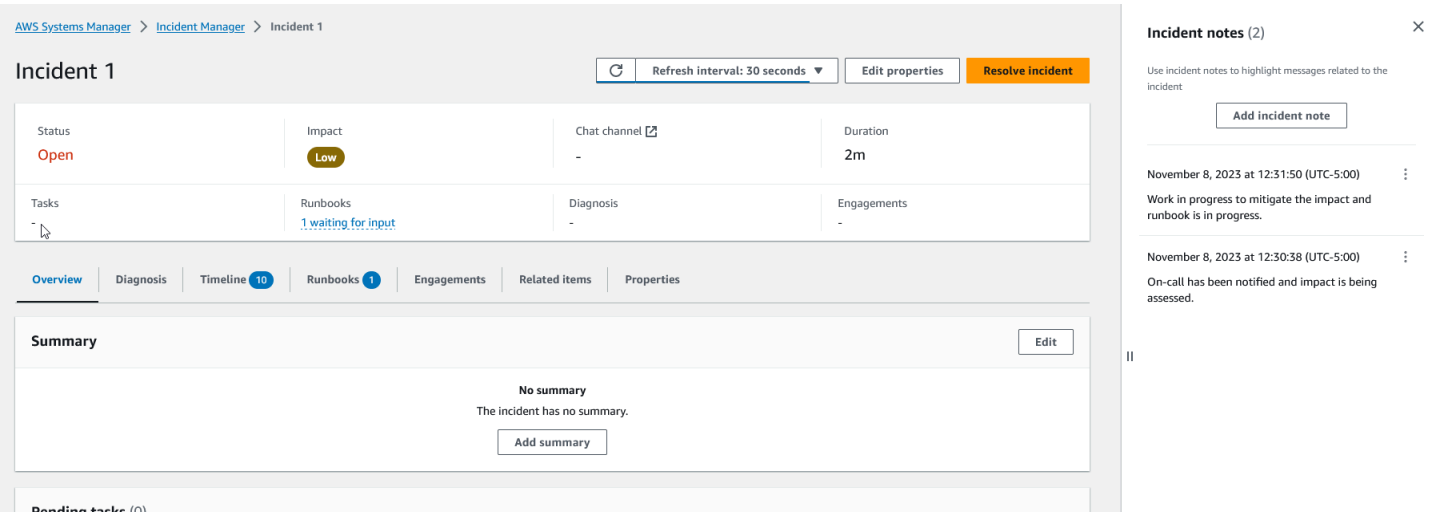
La page de liste des incidents contient trois sections : Incidents ouverts, Incidents résolus et Analyses. Vous pouvez suivre manuellement les nouveaux incidents et créer des analyses à partir de cette page. Pour en savoir plus sur le suivi manuel d'un incident, consultez Création manuelle d'incidents la section Création d'incidents de ce guide. Pour en savoir plus sur l'analyse post-incident, consultez la Performing a post-incident analysis in Incident Manager section de ce guide.

Les détails de l'incident affichent les incidents ouverts sous forme de vignettes avec le titre, l'impact, la durée et le canal de discussion correspondant à cet incident. Une fois que vous avez résolu un incident, il est transféré dans la liste des incidents résolus. Les analyses se trouvent dans le deuxième onglet.

Afficher les détails de l'incident dans la console

La page des détails de l'incident fournit des informations détaillées et des outils que vous pouvez utiliser pour gérer un incident. À partir de cette page, vous pouvez créer des runbooks pour atténuer un incident, ajouter des notes d'incident, engager d'autres résolveurs et consulter les détails de l'incident tels que les délais, les indicateurs, les propriétés et les ressources associées.

Comme le montre l'image suivante, la page des détails de l'incident comprend plusieurs sections : bannière supérieure, notes sur l'incident et sept onglets contenant des informations et des ressources supplémentaires. Par défaut, les sections Bannière supérieure et Notes d'incident sont affichées sur toutes les pages de détails de l'incident.



Cette rubrique décrit les éléments de la page de détails de l'incident et les actions que vous pouvez effectuer à partir de cette page.

Bannière supérieure

La bannière supérieure de chaque page détaillée de l'incident contient les informations suivantes :

- État : le statut actuel d'un incident peut être ouvert ou résolu.
- Impact : impact de l'incident sur votre environnement. Il peut être élevé, moyen ou faible. Pour modifier l'impact d'un incident, choisissez Modifier les propriétés.
- Canal de discussion : lien permettant d'accéder au canal de discussion où vous pouvez consulter les mises à jour et les notifications relatives aux incidents.
- Durée : délai écoulé avant qu'un intervenant ne résolve l'incident.
- Runbooks : statuts des runbooks associés à cet incident. Le statut peut être en attente de saisie, réussi ou échec. Si le statut d'un runbook est en attente de saisie, vous pouvez sélectionner le runbook pour afficher les détails des actions. Vous pouvez sélectionner « Échec » pour afficher les runbooks dont le délai est expiré, qui ont échoué ou qui ont été annulés.
- Engagements : nombre total d'engagements et statut de chaque engagement. Lorsque vous créez un engagement, son statut est Engagé. Une fois que vous avez confirmé l'engagement, le statut passe de Engagé à Reconnu. Incident Manager ne prend pas en charge la reconnaissance des engagements de tiers. Ces engagements conservent le statut Engagé.

Vous pouvez modifier le titre, l'impact et le canal de discussion de l'incident en choisissant Modifier dans le coin supérieur droit de la bannière.

Notes relatives à l'incident

La partie droite de l'écran affiche la section des notes relatives à l'incident. Grâce aux notes, vous pouvez collaborer et communiquer avec d'autres utilisateurs qui travaillent sur un incident. Vous pouvez expliquer les mesures d'atténuation que vous avez appliquées, une cause première potentielle que vous avez identifiée ou l'état actuel de l'incident. Il est recommandé d'utiliser la section Notes d'incident pour publier des mises à jour sur le statut et les mesures que vous ou d'autres prenez en cas d'incident. Si vous devez communiquer avec d'autres résolveurs en temps réel, utilisez le canal de discussion disponible dans Incident Manager.

Pour ajouter une note, cliquez sur le bouton Ajouter une note d'incident, puis saisissez votre note. Les notes peuvent contenir des mises à jour sur l'état de l'incident ou toute autre information pertinente offrant une visibilité aux autres utilisateurs. Si nécessaire, vous pouvez également modifier ou supprimer les notes d'incident.

> **Note**
>
> Tout utilisateur disposant de l'autorisation IAM pour exécuter les `ssm-incidents:DeleteTimelineEvent` actions `ssm-incidents:UpdateTimelineEvent` et peut modifier et supprimer des notes. Toutefois, lorsque vous partagez un incident avec un autre compte, la politique en matière de ressources n'inclut pas l'`ssm-incidents:DeleteTimelineEvent`action. Cela empêche l'utilisateur avec lequel vous partagez l'incident de supprimer la note. Vous pouvez consulter la piste d'audit d'une note relative aux événements d'Incident Manager dans la AWS CloudTrail console.

Onglets

La page des détails de l'incident comporte sept onglets, ce qui permet aux intervenants de localiser et de consulter plus facilement les informations lors d'un incident. Les onglets affichent un compteur dans le nom de l'onglet, qui indique le nombre de mises à jour apportées à l'onglet. Pour plus d'informations sur le contenu de chaque onglet ainsi que sur les actions disponibles, poursuivez votre lecture.

Présentation

L'onglet Vue d'ensemble est la page d'accueil pour les intervenants. Il contient le résumé de l'incident, une liste des événements chronologiques récents et l'étape actuelle du runbook.

Les intervenants utilisent le résumé pour savoir quelles mesures ont été prises, les résultats de tout changement, les prochaines étapes possibles et les informations sur l'impact de l'incident. Pour mettre à jour le résumé, choisissez Modifier dans le coin supérieur droit de la section Résumé.

> **Important**
>
> Si plusieurs répondeurs modifient le champ récapitulatif simultanément, le répondant qui soumet ses dernières modifications remplace toutes les autres entrées.

La section Événements chronologiques récents contient une chronologie renseignée par Incident Manager avec les cinq événements les plus récents. Utilisez cette section pour comprendre le statut de l'incident et ce qui s'est produit récemment. Pour consulter une chronologie complète, passez à l'onglet Chronologie.

La page d'aperçu affiche également l'étape du runbook en cours. Il peut s'agir d'une étape automatique exécutée dans votre AWS environnement ou d'un ensemble d'instructions manuelles destinées aux intervenants. Pour consulter le runbook complet, y compris les étapes précédentes et à venir, choisissez l'onglet Runbook.

Diagnostic

L'onglet Diagnostic contient des informations essentielles sur vos applications et systèmes AWS hébergés, notamment des informations sur les métriques et, si activé, les résultats.

Travailler avec des métriques

Incident Manager utilise Amazon CloudWatch pour renseigner les statistiques et les graphiques d'alarme figurant sur cet onglet. Pour en savoir plus sur les meilleures pratiques de gestion des incidents pour définir les alarmes et les mesures, consultez Surveillance la section Planification des incidents de ce guide de l'utilisateur.

Pour ajouter des métriques

- Choisissez Ajouter dans le coin supérieur droit de cet onglet.
  - Pour ajouter une métrique à partir d'un tableau de CloudWatch bord existant, choisissez À partir d'un tableau de CloudWatch bord existant.

    a. Choisissez un tableau de bord. Cela ajoute toutes les métriques et alarmes qui font partie du tableau de bord choisi.

b. (Facultatif) Vous pouvez également sélectionner des mesures dans le tableau de bord pour afficher des mesures spécifiques.

- Ajoutez une seule métrique en sélectionnant From CloudWatch et en collant une source de mesures. Pour copier une source de mesures :

  a. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
  b. Dans le panneau de navigation, sélectionnez Métriques.
  c. Dans l'onglet Toutes les mesures, entrez un terme de recherche dans le champ de recherche, tel qu'un nom de métrique ou un nom de ressource, puis choisissez Enter.

     Par exemple, si vous recherchez la `CPUUtilization` métrique, vous verrez les espaces de noms et les dimensions associés à cette métrique.
  d. Choisissez l'un des résultats de votre recherche pour afficher les statistiques.
  e. Choisissez l'onglet Source et copiez la source.

Les graphiques d'alarmes métriques ne peuvent être ajoutés aux détails de l'incident que par le biais du plan de réponse correspondant ou en sélectionnant À partir du tableau de CloudWatch bord existant lors de l'ajout d'une métrique.

Pour supprimer des métriques, choisissez Supprimer, puis choisissez les métriques que vous souhaitez supprimer dans le menu déroulant Metrics fourni.

Afficher les résultats provenant de AWS CodeDeploy et AWS CloudFormation

Une fois que les résultats sont activés et que toutes les autorisations requises sont configurées, tous les résultats susceptibles d'être liés à un incident spécifique sont joints à l'incident. Les intervenants peuvent consulter les informations relatives à ces résultats sur la page des détails de l'incident.

Pour consulter les résultats de CodeDeploy et CloudFormation

1. Ouvrez la console Incident Manager.
2. Choisissez le nom de l'incident à étudier.
3. Dans l'onglet Diagnostic, dans la zone Résultats, comparez les heures de début de tout résultat signalé avec l'heure de début de l'incident.
4. Pour afficher plus de détails sur un résultat, dans la colonne Référence, cliquez sur le lien vers le CloudFormation résultat CodeDeploy ou.

Chronologie

Utilisez l'onglet Chronologie pour suivre les événements survenus lors d'un incident. Incident Manager renseigne automatiquement les événements chronologiques qui identifient les événements importants survenus au cours de l'incident. Les intervenants peuvent ajouter des événements personnalisés en fonction des occurrences détectées manuellement. Au cours de l'analyse post-incident, l'onglet chronologie fournit des informations précieuses sur la manière de mieux se préparer et de répondre aux incidents à l'avenir. Pour plus d'informations sur l'analyse post-incident, consultezPerforming a post-incident analysis in Incident Manager.

Pour ajouter un événement chronologique personnalisé, choisissez Ajouter. Sélectionnez une date à l'aide du calendrier, puis entrez une heure. Toutes les heures sont indiquées dans votre fuseau horaire local. Fournissez une brève description de l'événement qui apparaît dans la chronologie.

Pour modifier un événement personnalisé existant, sélectionnez-le sur la chronologie, puis choisissez Modifier. Vous pouvez modifier l'heure, la date et la description des événements personnalisés. Vous ne pouvez modifier que des événements personnalisés.

Livres de course

L'onglet Runbooks de la page des détails de l'incident permet aux intervenants de consulter les étapes du runbook et de créer de nouveaux runbooks.

Pour démarrer un nouveau runbook, choisissez Start runbook dans la section Runbooks. Utilisez le champ de recherche pour trouver le runbook que vous souhaitez démarrer. Fournissez tous les paramètres requis et la version du runbook que vous souhaitez utiliser lors du démarrage du runbook. Les Runbooks démarrés lors d'un incident depuis l'onglet Runbooks utilisent les autorisations du compte actuellement connecté.

Pour accéder à la définition d'un runbook dans Systems Manager, choisissez le titre du runbook sous Runbooks. Pour accéder à l'instance en cours d'exécution du runbook dans Systems Manager, choisissez les détails d'exécution sous Détails d'exécution. Ces pages affichent le modèle utilisé pour démarrer le runbook et les détails spécifiques de l'instance actuellement en cours d'exécution du document d'automatisation.

La section des étapes du Runbook affiche la liste des étapes que le runbook sélectionné effectue automatiquement ou que les répondeurs exécutent manuellement. Les étapes se développent au fur et à mesure qu'elles deviennent l'étape en cours, affichant les informations requises pour terminer l'étape ou des détails sur le but de l'étape. Les étapes du runbook automatique sont résolues une fois

l'automatisation terminée. Les étapes manuelles obligent les intervenants à choisir Étape suivante au bas de chaque étape. Une fois qu'une étape est terminée, le résultat de l'étape apparaît sous forme de liste déroulante.

Pour annuler l'exécution d'un runbook, choisissez Annuler un runbook. Cela arrêtera l'exécution du runbook et n'effectuera aucune autre étape du runbook.

Fiançailles

L'onglet Engagements des détails de l'incident stimule l'engagement des intervenants et des équipes. Dans cet onglet, vous pouvez voir qui a été engagé, qui a répondu, ainsi que quels intervenants seront engagés dans le cadre d'un plan d'escalade. Les intervenants peuvent contacter d'autres contacts directement depuis cet onglet. Pour en savoir plus sur la création de contacts et les plans d'escalade, consultez les Création d'un plan d'escalade pour l'engagement des intervenants dans Incident Manager sections Création et configuration de contacts dans Incident Manager et de ce guide.

Vous pouvez configurer des plans de réponse avec des contacts et des plans d'escalade pour démarrer automatiquement l'engagement dès le début d'un incident. Pour en savoir plus sur la configuration des plans d'intervention, consultez la Création et configuration de plans de réponse dans Incident Manager section de ce guide.

Vous trouverez des informations sur chaque contact dans le tableau. Ce tableau contient les informations suivantes :

- Nom — Liens vers la page des coordonnées qui affiche leurs méthodes de contact et leur plan d'engagement.
- Plan d'escalade : liens vers le plan d'escalade qui a engagé le contact.
- Source du contact — Identifie le service qui a engagé ce contact, tel que AWS Systems Manager ou PagerDuty.
- Engagé : indique quand le plan a engagé un contact ou quand engager un contact dans le cadre d'un plan d'escalade.
- Confirmé — Indique si le contact a accusé réception de l'engagement.

Pour accuser réception d'un engagement, le répondant peut effectuer l'une des opérations suivantes :

- Appel téléphonique — Entrez **1** lorsque vous y êtes invité.

- SMS — Répondez au message avec le code fourni ou saisissez le code fourni dans l'onglet Engagements de l'incident.
- E-mail — Entrez le code fourni dans l'onglet Engagements de l'incident.

Éléments connexes

L'onglet Eléments associés est utilisé pour collecter des ressources liées à l'atténuation des incidents. Ces ressources peuvent être ARNs des liens vers des ressources externes ou des fichiers chargés dans des compartiments Amazon S3. Le tableau affiche un titre descriptif et un ARN, un lien ou les détails du bucket. Avant d'utiliser des compartiments S3, consultez les meilleures pratiques de sécurité pour Amazon S3 dans le guide de l'utilisateur Amazon S3.

Lorsque vous chargez des fichiers dans un compartiment Amazon S3, le contrôle des versions est activé ou suspendu sur ce compartiment. Lorsque le contrôle de version est activé sur le compartiment, les fichiers chargés avec le même nom qu'un fichier existant sont ajoutés en tant que nouvelle version du fichier. Si le contrôle de version est suspendu, les fichiers chargés avec le même nom qu'un fichier existant remplacent le fichier existant. Pour en savoir plus sur la gestion des versions, consultez la section Utilisation de la gestion des versions dans les compartiments S3 du guide de l'utilisateur Amazon S3.

Lorsque vous supprimez un élément lié à un fichier, celui-ci est supprimé de l'incident mais pas du compartiment Amazon S3. Pour en savoir plus sur la suppression d'objets d'un compartiment Amazon S3, consultez Supprimer des objets Amazon S3 dans le guide de l'utilisateur Amazon S3.

Propriétés

L'onglet Propriétés fournit les informations suivantes sur l'incident.

Dans la section Propriétés de l'incident, vous pouvez consulter les informations suivantes :

- État — Décrit l'état actuel de l'incident. L'incident peut être ouvert ou résolu.
- Heure de début : heure à laquelle l'incident a été créé dans Incident Manager.
- Heure de résolution : heure à laquelle l'incident a été résolu dans Incident Manager.
- Amazon Resource Name (ARN) : ARN de l'incident. Utilisez l'ARN lorsque vous référencez l'incident depuis le chat ou avec les commandes AWS Command Line Interface (AWS CLI).
- Plan de réponse — Identifie le plan de réponse pour l'incident sélectionné. Le choix du plan de réponse ouvre la page de détails du plan d'intervention.

- Parent OpsItem : identifie la OpsItem personne créée comme étant le parent de l'incident. Un parent OpsItem peut avoir plusieurs incidents connexes et des mesures de suivi. La sélection du parent OpsItem ouvre la page de OpsItems détails dans OpsCenter.
- Analyse — Identifie l'analyse créée à partir de cet incident. Créez une analyse à partir d'un incident résolu afin d'améliorer votre processus de réponse aux incidents. Choisissez l'analyse pour ouvrir la page des détails de l'analyse.
- Propriétaire : compte sur lequel l'incident a été créé.

Dans la section Balises, vous pouvez afficher et modifier les clés de balise et les valeurs associées à l'enregistrement de l'incident. Pour plus d'informations sur les balises dans Incident Manager, consultezMarquage des ressources dans Incident Manager.

Performing a post-incident analysis in Incident Manager

L'analyse post-incident vous aide à identifier les améliorations à apporter à votre réponse aux incidents, notamment en termes de délais de détection et d'atténuation. Une analyse peut également vous aider à comprendre la cause première des incidents. Incident Manager crée des actions recommandées pour améliorer votre réponse aux incidents.

Avantages d'une analyse post-incident

- Améliorez la réponse aux incidents
- Comprendre la cause première du problème
- Traitez les causes profondes à l'aide d'actions réalisables
- Analyser l'impact des incidents
- Capturez et partagez les apprentissages au sein d'une organisation

Les raisons pour lesquelles il ne faut pas utiliser une analyse

Une analyse est irréprochable et n'appelle pas les gens par leur nom.

« Peu importe ce que nous découvrons, nous comprenons et croyons sincèrement que chacun a fait de son mieux, compte tenu de ce qu'il savait à l'époque, de ses compétences et de ses capacités, des ressources disponibles et de la situation actuelle. » - Norm Kerth, Rétrospectives de projets : manuel pour l'examen en équipe

Détails de l'analyse

La page des détails de l'analyse vous guide dans la collecte d'informations, l'évaluation des améliorations et la création d'actions à entreprendre. La page des détails de l'analyse est similaire aux détails de l'incident, avec quelques différences importantes telles que les indicateurs historiques, la chronologie modifiable et les questions visant à améliorer les incidents futurs.

Présentation

L'aperçu est un résumé de l'incident. Ce résumé inclut le contexte, ce qui s'est passé, pourquoi cela s'est produit, comment cela a été atténué, la durée et les principales mesures à prendre pour éviter

que l'incident ne se reproduise. La vue d'ensemble est de haut niveau. Vous découvrirez plus de détails dans l'onglet Questions de l'analyse.

Métriques

Utilisez l'onglet métriques pour visualiser les indicateurs clés de votre application pendant toute la durée de l'incident. Vous pouvez ajouter ici des graphiques métriques contenant une ou plusieurs métriques représentées dans le même graphique. Les métriques utilisées lors d'un incident sont automatiquement renseignées dans cet onglet. Nous vous recommandons d'ajouter une description, un titre et des annotations des moments clés de l'incident.

Voici quelques points temporels clés que vous pouvez prendre en compte lors de l'analyse d'un graphique métrique :

- Modification du déploiement
- Modification de la configuration
- Heure de début de l'incident
- Heure de l'alarme
- Heure de l'engagement
- Heure de début des mesures d'atténuation
- Délai de résolution de l'incident

Limites

- CloudWatch les alarmes et les expressions métriques ne sont pas importées à partir d'un incident.
- Les métriques situées dans une région non prise en charge par Incident Manager ne sont pas importées à partir de l'incident.
- Les métriques des comptes d'applications nécessitent de configurer le `CloudWatch-CrossAccountSharingRole` avant de créer l'analyse. Pour plus d'informations sur le rôle, consultez la section CloudWatch Console inter-comptes inter-régions dans le guide de l' CloudWatch utilisateur.

Chronologie

Décrivez les moments clés de la chronologie au fur et à mesure que vous approfondissez votre compréhension de l'incident. La chronologie des incidents est automatiquement renseignée dans cet

onglet. Vous pouvez supprimer les points temporels qui ne sont pas pertinents pour l'analyse. Vous pouvez également ajouter et modifier des points temporels pour décrire plus précisément l'incident et son impact.

Utilisez l'onglet chronologie pour répondre aux questions que vous trouverez dans l'onglet Questions concernant la réponse à l'incident.

Questions

Utilisez les questions du gestionnaire d'incidents pour accélérer le délai de résolution des incidents dans votre application et réduire leur fréquence. Au fur et à mesure que vous répondez aux questions, mettez à jour les onglets Métriques et Chronologie pour plus de précision. Les questions portent sur les aspects essentiels de la réponse aux incidents :

- Détection — Pourriez-vous améliorer le délai de détection ? Existe-t-il des mises à jour des métriques et des alarmes qui permettraient de détecter l’incident plus rapidement ?
- Diagnostic — Pouvez-vous accélérer le diagnostic ? Y a-t-il des mises à jour de vos plans de réponse ou de vos plans d’escalade qui permettraient d’impliquer plus rapidement les bons intervenants ?
- Atténuation — Pouvez-vous réduire le délai d'atténuation ? Y a-t-il des étapes du runbook que vous pourriez ajouter ou améliorer ?
- Prévention — Pouvez-vous empêcher de futurs incidents de se produire ? Pour découvrir les causes profondes d'un incident, Amazon utilise l'approche des 5 raisons pour enquêter sur les problèmes.

Actions

Incident Manager crée des actions recommandées que vous pouvez consulter au fur et à mesure que vous répondez aux questions. Vous pouvez choisir d'accepter et d'exécuter ces actions depuis cet onglet ou de les ignorer. Vous pouvez consulter les actions rejetées en choisissant Actions rejetées. Les éléments d'action sont un type OpsItem de élément lié à l'analyse et à l'incident dans OpsCenter.

Liste de contrôle

Avant de clore une analyse, utilisez la liste de contrôle pour passer en revue les mesures que doit prendre un intervenant. Lorsque les intervenants exécutent les actions de la liste de contrôle, l'icône située à côté de l'action passe d'une ellipse à une coche, indiquant que l'action est terminée. Si vous

n'avez pas terminé les éléments de la liste de contrôle, Incident Manager affiche un message pour confirmer que le répondant souhaite clore l'analyse sans la terminer.

Modèles d'analyse

Un modèle d'analyse fournit un ensemble de questions qui explorent en profondeur la cause première des incidents. Vous pouvez utiliser les réponses à ces questions pour améliorer les performances des applications et la réponse aux incidents.

AWS modèle standard

Incident Manager fournit un modèle standard de questions basé sur les meilleures pratiques en matière de réponse aux AWS incidents et d'analyse des problèmes, intituléAWSIncidents-PostIncidentAnalysisTemplate.

Création d'un modèle d'analyse

Nous vous encourageons à utiliser le AWSIncidents-PostIncidentAnalysisTemplate modèle par défaut et à ajouter des questions ou des sections supplémentaires adaptées à vos cas d'utilisation. Créez des modèles d'analyse basés sur le modèle par défaut Utilisez ce modèle comme point de départ pour créer des modèles d'analyse dans votre compte de gestion. Vous pouvez ensuite dupliquer vos modèles d'analyse dans chaque région dans laquelle vous avez activé Incident Manager.

Création d'un modèle d'analyse

1. Appelez l'GetDocumentaction et utilisez ses Name paramètres pour le téléchargerAWSIncidents-PostIncidentAnalysisTemplate. Pour plus d'informations sur la GetDocument syntaxe, consultez la section Systems Manager API Reference.
2. Le contenu de la réponse contient les éléments de base JSON pour l'analyse. Utilisez les éléments de base des questions pour insérer des questions supplémentaires dans l'analyse. Nous vous recommandons d'ajouter des questions ou des sections dans la Incident questions section.
3. Pour créer le nouveau modèle, utilisez l'CreateDocumentopération avec le JSON mis à jour à l'étape précédente. Vous devez inclure ce qui suit, où se *Analysis_Template_Name* trouve le nom de votre modèle,

   - DocumentFormat: "JSON"

- `DocumentType: "ProblemAnalysisTemplate"`
- `Name: "Analysis_Template_Name"`

Création d'une analyse

1. Pour créer une analyse, choisissez Créer une analyse sur la page des détails de l'incident d'un incident clôturé.
2. Choisissez le modèle d'analyse à partir duquel créer cette analyse, puis entrez un nom descriptif de l'analyse.
3. Sélectionnez Create (Créer).

Imprimer une analyse d'incident formatée

Vous pouvez générer une copie d'une analyse complète ou incomplète formatée pour l'impression. Vous pouvez également enregistrer cette copie au format PDF. Vous pouvez imprimer une analyse à la fois. L'impression par lots de plusieurs analyses n'est actuellement pas prise en charge.

Pour imprimer une analyse formatée

1. Ouvrez la console Incident Manager.
2. Choisissez l'onglet Analyse.
3. Choisissez le titre de l'analyse que vous souhaitez imprimer.
4. Dans le coin supérieur droit de la page détaillée de l'analyse, choisissez Imprimer.
5. Dans la boîte de dialogue Imprimer l'analyse des incidents, effacez les sections de l'analyse que vous ne souhaitez pas inclure dans la version imprimée. Par défaut, toutes les sections sont sélectionnées.
6. Choisissez Imprimer pour ouvrir les commandes d'impression locales de votre appareil.
7. Choisissez votre destination ou format d'impression. Vous pouvez choisir une imprimante locale ou réseau, ou vous pouvez enregistrer l'analyse au format PDF. Apportez les modifications nécessaires aux options d'impression restantes, puis choisissez Imprimer.

> **Note**
>
> Les commandes d'impression locales font référence à l'interface utilisateur fournie par votre navigateur Web et votre appareil.
> Les destinations d'impression sont celles configurées pour votre appareil et accessibles depuis celui-ci.

Tutoriels Incident Manager

Ces didacticiels AWS Systems Manager Incident Manager vous aident à créer un système de gestion des incidents plus robuste. Ces didacticiels couvrent les activités courantes qui se produisent lors d'un incident ou soutiennent la réponse à un incident.

Rubriques

- Tutoriel : Utilisation des runbooks Systems Manager Automation avec Incident Manager
- Tutoriel : Gestion des incidents de sécurité dans Incident Manager

Tutoriel : Utilisation des runbooks Systems Manager Automation avec Incident Manager

Vous pouvez utiliser les runbooks AWS Systems Manager d'automatisation pour simplifier les tâches courantes de maintenance, de déploiement et de correction des AWS services. Dans ce didacticiel, vous allez créer un runbook personnalisé pour automatiser la réponse à un incident dans Incident Manager. Le scénario de ce didacticiel implique une CloudWatch alarme Amazon assignée à une EC2 métrique Amazon. Lorsque l'instance entre dans un état qui déclenche l'alarme, Incident Manager exécute automatiquement les tâches suivantes :

1. Crée un incident dans Incident Manager.
2. Lance un runbook qui tente de résoudre le problème.
3. Publie les résultats du runbook sur la page des détails de l'incident dans Incident Manager.

Le processus décrit dans ce didacticiel peut également être utilisé avec des EventBridge événements Amazon et d'autres types de AWS ressources. En automatisant votre réponse aux alarmes et aux événements, vous pouvez réduire l'impact d'un incident sur votre organisation et ses ressources.

Ce didacticiel explique comment modifier une CloudWatch alarme attribuée à une EC2 instance Amazon dans le cadre d'un plan de réponse d'Incident Manager. Si aucune alarme, instance ou plan de réponse n'est configuré, nous vous recommandons de configurer ces ressources avant de commencer. Pour plus d'informations, consultez les rubriques suivantes :

- Utilisation des CloudWatch alarmes Amazon dans le guide de CloudWatch l'utilisateur Amazon
- EC2 Instances Amazon dans le guide de EC2 l'utilisateur Amazon

- EC2Instances Amazon dans le guide de EC2 l'utilisateur Amazon
- Création et configuration de plans de réponse dans Incident Manager

> **Important**
>
> Vous devrez engager des coûts en créant des AWS ressources et en utilisant les étapes d'automatisation du runbook. Pour en savoir plus, consultez Pricing AWS (Tarification).

Rubriques

Tâche 1 : Création du runbook

Utilisez la procédure suivante pour créer un runbook dans la console Systems Manager. Lorsqu'il est invoqué à partir d'un incident du gestionnaire d'incidents, le runbook redémarre une EC2 instance Amazon et met à jour l'incident avec des informations sur l'exécution du runbook. Avant de commencer, vérifiez que vous êtes autorisé à créer un runbook. Pour plus d'informations, consultez la section Configuration de l'automatisation dans le guide de AWS Systems Manager l'utilisateur.

> **Important**
>
> Consultez les informations importantes suivantes concernant la création du runbook de ce didacticiel :
>
> - Le runbook est destiné à un incident créé à partir d'une source CloudWatch d'alarme. Si vous utilisez ce runbook pour d'autres types d'incidents, par exemple des incidents créés manuellement, l'événement chronologique de la première étape du runbook ne sera pas trouvé et le système renvoie une erreur.
> - Le runbook nécessite que l' CloudWatch alarme inclue une dimension appelée`InstanceId`. Les alarmes relatives aux métriques des EC2 instances Amazon ont cette dimension. Si vous utilisez ce runbook avec d'autres métriques (ou avec d'autres

sources d'incidents, par exemple EventBridge), vous devez modifier l'`JsonDecode2`étape pour qu'elle corresponde aux données capturées dans votre scénario.

- Le runbook tente de résoudre le problème qui a déclenché l'alarme en redémarrant l'instance Amazon. EC2 En cas d'incident réel, il se peut que vous ne souhaitiez pas redémarrer l'instance. Mettez à jour le runbook avec les mesures correctives spécifiques que vous souhaitez que le système prenne.

Pour plus d'informations sur la création de runbooks, consultez la section Utilisation des runbooks dans le Guide de l'AWS Systems Manager utilisateur.

Pour créer un runbook

1. Ouvrez la AWS Systems Manager console à l'adresse https://console.aws.amazon.com/systems-manager/.
2. Dans le panneau de navigation, cliquez sur Documents.
3. Choisissez Automation.
4. Dans Nom, entrez un nom descriptif pour le runbook, tel que**`IncidentResponseRunbook`**.
5. Sélectionnez l'onglet Éditeur, puis Modifier.
6. Collez le contenu suivant dans l'éditeur :

```
description: This runbook attempts to restart an Amazon EC2 instance that caused an
 incident.
schemaVersion: '0.3'
parameters:
  IncidentRecordArn:
    type: String
    description: The incident
mainSteps:
  - name: ListTimelineEvents
    action: 'aws:executeAwsApi'
    outputs:
      - Selector: '$.eventSummaries[0].eventId'
        Name: eventId
        Type: String
    inputs:
      Service: ssm-incidents
      Api: ListTimelineEvents
      incidentRecordArn: '{{IncidentRecordArn}}'
```

```
      filters:
        - key: eventType
          condition:
            equals:
              stringValues:
                - SSM Incident Trigger
    description: This step retrieves the ID of the first timeline event with the
CloudWatch alarm details.
  - name: GetTimelineEvent
    action: 'aws:executeAwsApi'
    inputs:
      Service: ssm-incidents
      Api: GetTimelineEvent
      incidentRecordArn: '{{IncidentRecordArn}}'
      eventId: '{{ListTimelineEvents.eventId}}'
    outputs:
      - Name: eventData
        Selector: $.event.eventData
        Type: String
    description: This step retrieves the timeline event itself.
  - name: JsonDecode
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
        import json

        def script_handler(events, context):
          data = json.loads(events["eventData"])
          return data
      InputPayload:
        eventData: '{{GetTimelineEvent.eventData}}'
    outputs:
      - Name: rawData
        Selector: $.Payload.rawData
        Type: String
    description: This step parses the timeline event data.
  - name: JsonDecode2
    action: 'aws:executeScript'
    inputs:
      Runtime: python3.8
      Handler: script_handler
      Script: |-
```

```
        import json

        def script_handler(events, context):
          data = json.loads(events["rawData"])
          return data
      InputPayload:
        rawData: '{{JsonDecode.rawData}}'
    outputs:
      - Name: InstanceId
        Selector:
'$.Payload.detail.configuration.metrics[0].metricStat.metric.dimensions.InstanceId'
        Type: String
    description: This step parses the CloudWatch event data.
  - name: RestartInstance
    action: 'aws:executeAutomation'
    inputs:
      DocumentName: AWS-RestartEC2Instance
      DocumentVersion: $DEFAULT
      RuntimeParameters:
        InstanceId: '{{JsonDecode2.InstanceId}}'
    description: This step restarts the Amazon EC2 instance
```

7. Sélectionnez Create automation (Créer une automatisation).

Tâche 2 : Création d'un rôle IAM

Utilisez le didacticiel suivant pour créer un rôle AWS Identity and Access Management (IAM) qui autorise Incident Manager à lancer un runbook spécifié dans un plan de réponse. Le runbook présenté dans ce didacticiel redémarre une instance Amazon EC2 . Vous spécifierez ce rôle IAM dans la tâche suivante lorsque vous connecterez le runbook à votre plan de réponse.

Création d'un rôle IAM qui lance un runbook à partir d'un plan de réponse

1. Ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Sous Type d'entité fiable, vérifiez que le AWS service est sélectionné.
4. Sous Cas d'utilisation, dans le champ Cas d'utilisation pour d'autres AWS services, entrez**`Incident Manager`**.
5. Choisissez Incident Manager, puis Next.

6. Sur la page Ajouter des autorisations, choisissez Créer une politique. L'éditeur d'autorisations s'ouvre dans une nouvelle fenêtre ou un nouvel onglet du navigateur.
7. Dans l'éditeur, choisissez l'onglet JSON.
8. Copiez et collez la politique d'autorisation suivante dans l'éditeur JSON. Remplacez *account_ID* par votre ID Compte AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Resource": [
                "arn:aws:ssm:*:account_ID:automation-definition/
IncidentResponseRunbook:*",
                "arn:aws:ssm:*::automation-definition/AWS-RestartEC2Instance:*"
            ],
            "Action": "ssm:StartAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm:*:*:automation-execution/*",
            "Action": "ssm:GetAutomationExecution"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:ssm-incidents:*:*:*",
            "Action": "ssm-incidents:*"
        },
        {
            "Effect": "Allow",
            "Resource": "arn:aws:iam::*:role/AWS-SystemsManager-
AutomationExecutionRole",
            "Action": "sts:AssumeRole"
        },
        {
            "Effect": "Allow",
            "Resource": "*",
            "Action": [
                "ec2:StopInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:StartInstances"
            ]
```

```
        }
    ]
}
```

9. Choisissez Suivant : Balises.
10. (Facultatif) Si nécessaire, ajoutez des balises à votre politique.
11. Choisissez Suivant : Vérification.
12. Dans le champ Nom, entrez un nom qui vous aide à identifier ce rôle comme étant utilisé pour ce didacticiel.
13. (Facultatif) Entrez une description dans le champ Description.
14. Choisissez Create Policy (Créer une politique).
15. Revenez à la fenêtre ou à l'onglet du navigateur correspondant au rôle que vous créez. La page Ajouter des autorisations s'affiche.
16. Cliquez sur le bouton d'actualisation (situé à côté du bouton Créer une politique), puis entrez le nom de la politique d'autorisation que vous avez créée dans la zone de filtre.
17. Choisissez la politique d'autorisation que vous avez créée, puis cliquez sur Suivant.
18. Sur la page Nom, révision et création, pour Nom du rôle, entrez un nom qui vous aide à identifier ce rôle comme étant utilisé pour ce didacticiel.
19. (Facultatif) Entrez une description dans le champ Description.
20. Passez en revue les détails du rôle, ajoutez des balises si nécessaire et choisissez Create role.

Tâche 3 : connexion du runbook à votre plan d'intervention

En connectant le runbook à votre plan de réponse Incident Manager, vous garantissez un processus d'atténuation cohérent, reproductible et rapide. Le runbook sert également de point de départ aux résolveurs pour déterminer leur prochaine ligne de conduite.

Pour attribuer le runbook à votre plan de réponse

1. Ouvrez la console Incident Manager.
2. Choisissez les plans de réponse.
3. Pour Plan de réponse, choisissez un plan de réponse existant, puis sélectionnez Modifier. Si vous n'avez pas de plan d'intervention existant, choisissez Créer un plan de réponse pour créer un nouveau plan.

Renseignez les champs suivants :

a. Dans la section Runbook, choisissez Select existing runbook.

b. Pour Propriétaire, vérifiez que Owned by me est sélectionné.

c. Pour Runbook, choisissez le runbook dans lequel vous l'avez créé. Tâche 1 : Création du runbook

d. Pour Version, choisissez Par défaut au moment de l'exécution.

e. Dans la section Entrées, pour le IncidentRecordArnparamètre, choisissez Incident ARN.

f. Dans la section Autorisations d'exécution, choisissez le rôle IAM dans Tâche 2 : Création d'un rôle IAM lequel vous l'avez créé.

4. Enregistrez vos modifications.

Tâche 4 : Affecter une CloudWatch alarme à votre plan d'intervention

Utilisez la procédure suivante pour attribuer une CloudWatch alarme pour une EC2 instance Amazon à votre plan de réponse.

Pour attribuer une CloudWatch alarme à votre plan d'intervention

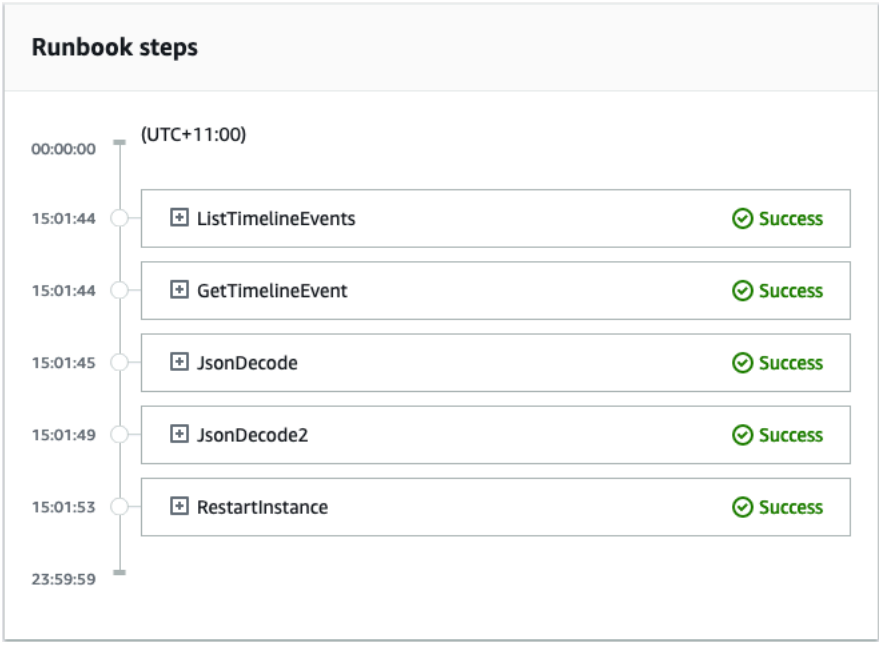
1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le volet de navigation, sous Alarmes, sélectionnez Toutes les alarmes.
3. Choisissez une alarme pour une EC2 instance Amazon que vous souhaitez connecter à votre plan de réponse.
4. Sélectionnez Actions, puis Edit (Modifier). Vérifiez que la métrique possède une dimension appelée`InstanceId`.
5. Choisissez Suivant.
6. Pour l'assistant de configuration des actions, choisissez l'action Add Systems Manager.
7. Choisissez Créer un incident.
8. Choisissez le plan de réponse que vous avez créé dansTâche 3 : connexion du runbook à votre plan d'intervention.
9. Sélectionnez Update alarm (Mettre à jour une alerte).

Tâche 5 : vérification des résultats

Pour vérifier que l' CloudWatch alarme crée un incident puis traite le runbook spécifié dans votre plan de réponse, vous devez déclencher l'alarme. Une fois que vous avez déclenché l'alarme et que le traitement du runbook est terminé, vous pouvez vérifier les résultats du runbook à l'aide de la procédure suivante. Pour plus d'informations sur le déclenchement d'une alarme, reportez-vous set-alarm-stateà la référence des AWS CLI commandes.

1. Ouvrez la console Incident Manager.
2. Choisissez l'incident créé par l' CloudWatch alarme.
3. Choisissez l'onglet Runbooks.
4. Consultez les actions effectuées sur votre EC2 instance Amazon dans la section des étapes de Runbook.

   L'image suivante montre comment les étapes effectuées par le runbook que vous avez créé dans ce didacticiel sont signalées dans la console. Chaque étape est répertoriée avec un horodatage et un message d'état.



   Pour afficher tous les détails de l' CloudWatch alarme, étendez l'étape JsonDecode2, puis développez Output.

> **Important**
>
> Vous devez nettoyer toutes les modifications de ressources que vous avez mises en œuvre au cours de ce didacticiel et que vous ne souhaitez pas conserver. Cela inclut les modifications apportées aux ressources du gestionnaire d'incidents, telles que les plans de ressources et les incidents, les modifications apportées aux CloudWatch alarmes et le rôle IAM que vous avez créé pour ce didacticiel.

Tutoriel : Gestion des incidents de sécurité dans Incident Manager

Vous pouvez utiliser AWS Security Hub Amazon EventBridge et Incident Manager ensemble pour identifier et gérer les incidents de sécurité dans vos applications AWS hébergées. Ce didacticiel explique comment configurer une EventBridge règle qui crée un incident en fonction des résultats envoyés automatiquement par Security Hub.

> **Note**
>
> Ce didacticiel utilise EventBridge Security Hub. L'utilisation de ces services peut entraîner des frais.

Prérequis

- Configurez Security Hub. Pour plus d'informations, consultez Configuration de AWS Security Hub.
- Créez ou mettez à jour des résultats dans Security Hub. Pour plus d'informations, voir Conclusions dans AWS Security Hub.
- Configurez un plan de réponse qu'Incident Manager utilisera comme modèle lors de la création de votre incident de sécurité. Pour de plus amples informations, veuillez consulter Préparation aux incidents dans Incident Manager.

Pour ce didacticiel, nous utilisons un modèle prédéfini pour créer la EventBridge règle. Pour créer la règle à l'aide d'un modèle personnalisé, consultez la section Utilisation d'un modèle personnalisé pour créer la règle dans le guide de AWS Security Hub l'utilisateur.

Création d'une EventBridge règle

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Dans le volet de navigation, choisissez Règles.
3. Choisissez Créer une règle.
4. Saisissez un Nom et une Description pour la règle.

   Une règle ne peut pas avoir le même nom qu'une autre règle de la même région et sur le même bus d'événement.
5. Pour Event bus (Bus d'événement), choisissez default (défaut).
6. Pour Type de règle, choisissez Règle avec un modèle d'événement.
7. Choisissez Suivant.
8. Dans Source de l'événement, choisissez AWS des événements ou des événements EventBridge partenaires.
9. Pour Modèle d'événement, choisissez Formulaire de modèle d'événement.
10. Pour Source d'événement, choisissez Services AWS .
11. Pour le AWS service, choisissez Security Hub.
12. Dans Type d'événement, choisissez Security Hub Findings - Imported.
13. Par défaut, EventBridge configure le modèle d'événement sans aucune valeur de filtre. Pour chaque attribut, l'*`attribute name`*option Tous est sélectionnée. Mettez à jour ces filtres pour créer des incidents basés sur les résultats de sécurité qui ont le plus d'impact sur votre environnement.
14. Cliquez sur Next (Suivant).
15. Pour Types de cibles, choisissez service AWS .
16. Pour Sélectionner une cible, choisissez le plan de réponse d'Incident Manager.
17. Pour Plan de réponse, choisissez un plan de réponse à utiliser comme modèle pour les incidents créés.
18. EventBridge peut créer le rôle IAM nécessaire à l'exécution de votre règle.

    - Pour créer automatiquement un rôle IAM, choisissez Créer un nouveau rôle pour la ressource spécifique.
    - Pour utiliser un rôle IAM qui existe déjà dans votre compte, choisissez Utiliser un rôle existant.
19. (Facultatif) Saisissez une ou plusieurs balises pour la règle.

20. Choisissez Suivant.
21. Consultez les détails de la règle et choisissez Create rule (Créer une règle).

Maintenant que vous avez créé cette EventBridge règle, les résultats de sécurité correspondant aux valeurs d'attribut que vous avez définies créeront des incidents dans Incident Manager. Vous pouvez trier, gérer, surveiller et créer une analyse post-incident à partir de ces incidents.

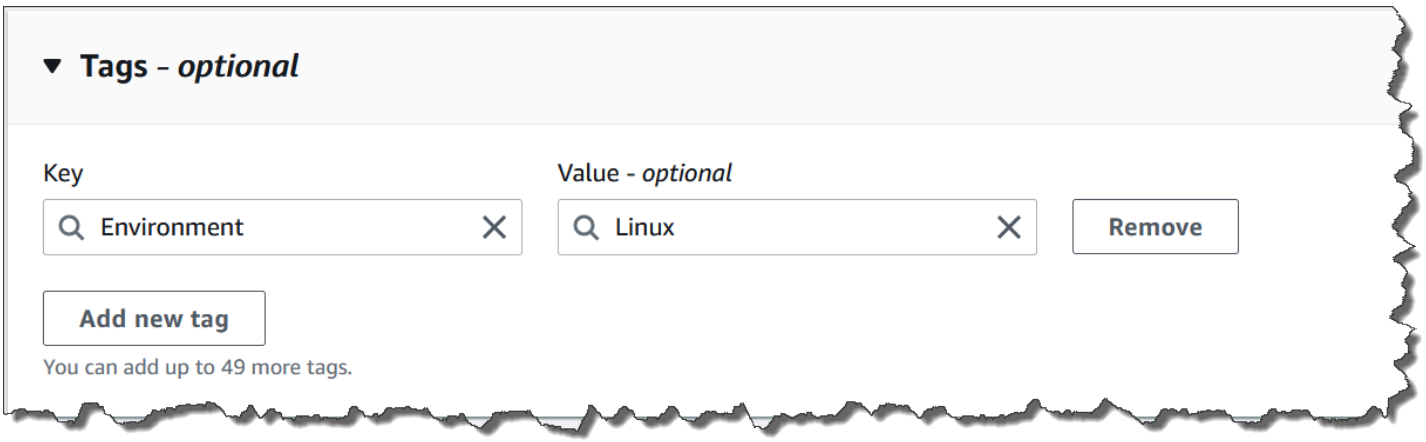
Marquage des ressources dans Incident Manager

Les balises sont des métadonnées facultatives que vous pouvez attribuer aux ressources de votre Incident Manager dans les Régions AWS limites spécifiées dans votre ensemble de réplication. Vous pouvez attribuer des balises aux plans de réponse, aux enregistrements d'incidents et aux contacts. Vous pouvez également ajouter des balises aux horaires d'astreinte et aux rotations. Vous pouvez également ajouter des balises au kit de réplication lui-même. Les balises vous permettent de classer et de contrôler l'accès à ces ressources de différentes manières. Chaque balise est constituée d'une clé et d'une valeur facultative que vous définissez. Nous vous recommandons de concevoir un ensemble de clés de balise répondant à vos besoins pour chaque type de ressource Incident Manager. L'utilisation d'un ensemble cohérent de clés de balise vous permet de gérer plus facilement ces ressources et de gérer l'accès à celles-ci. Vous pouvez rechercher et filtrer les ressources en fonction des balises. Pour plus d'informations sur le contrôle de l'accès aux ressources à l'aide de balises, consultez la section Contrôle de l'accès aux AWS ressources à l'aide de balises dans le guide de l'utilisateur IAM.

Vous pouvez spécifier des balises dans la section Incident par défaut lors de la création d'un plan de réponse. Ces balises sont appliquées à l'enregistrement de l'incident lorsqu'un incident est créé à l'aide du plan de réponse.

> **Note**
>
> Les balises n'ont aucune signification sémantique. Ils sont interprétés strictement comme une chaîne de caractères.

Vous pouvez ajouter ou supprimer des balises à l'aide de la console Incident Manager. La capture d'écran suivante montre la zone Tags d'une page de console, avec des champs pour ajouter des clés et des valeurs de balise, ainsi que des boutons pour ajouter et supprimer des balises.



Pour utiliser les balises par programmation, utilisez les actions d'API suivantes :

- TagResource
- UntagResource
- ListTagsForResource

> **Important**
>
> Les balises appliquées aux plans d'intervention, aux enregistrements d'incidents, aux contacts, aux plannings d'astreinte et aux rotations, ainsi qu'aux ensembles de réplication ne peuvent être consultées et modifiées qu'à partir du compte du propriétaire de la ressource.

Sécurité dans AWS Systems Manager Incident Manager

La sécurité du cloud AWS est la priorité absolue. En tant que AWS client, vous bénéficiez de centres de données et d'architectures réseau conçus pour répondre aux exigences des entreprises les plus sensibles en matière de sécurité.

La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud :

- Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui s'exécute Services AWS dans le AWS Cloud. AWS vous fournit également des services que vous pouvez utiliser en toute sécurité. Des auditeurs tiers testent et vérifient régulièrement l'efficacité de notre sécurité dans le cadre des programmes de AWS conformité Programmes de de conformité. Pour en savoir plus sur les programmes de conformité qui s'appliquent à AWS Systems Manager Incident Manager, voir AWS Services concernés par programme de conformitéAWS .
- Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez. Vous êtes également responsable d'autres facteurs, y compris de la sensibilité de vos données, des exigences de votre entreprise, ainsi que de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de l'utilisation d'Incident Manager. Les rubriques suivantes expliquent comment configurer Incident Manager pour répondre à vos objectifs de sécurité et de conformité. Vous apprenez également à utiliser d'autres outils Services AWS qui vous aident à surveiller et à sécuriser les ressources de votre gestionnaire d'incidents.

Rubriques

- Analyse de la configuration et des vulnérabilités dans Incident Manager
- Bonnes pratiques en matière de sécurité dans AWS Systems Manager Incident Manager

Protection des données dans Incident Manager

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Systems Manager Incident Manager. 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. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

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

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail. Pour plus d'informations sur l'utilisation des CloudTrail sentiers pour capturer AWS des activités, consultez la section Utilisation des CloudTrail sentiers dans le guide de AWS CloudTrail l'utilisateur.
- 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 sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-3 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 Norme FIPS (Federal Information Processing Standard) 140-3.

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Nom. Cela inclut lorsque vous travaillez avec Incident Manager ou autre Services AWS à l'aide de la console AWS CLI, de l'API ou AWS SDKs. Toutes les données que vous entrez dans des balises ou des champs de texte 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.

Par défaut, Incident Manager chiffre les données en transit à l'aide du protocole SSL/TLS.

Chiffrement des données

Incident Manager utilise des clés AWS Key Management Service (AWS KMS) pour chiffrer vos ressources Incident Manager. Pour plus d'informations AWS KMS, consultez le guide du AWS KMS développeur. AWS KMS combine du matériel et des logiciels sécurisés et hautement disponibles pour fournir un système de gestion des clés adapté au cloud. Incident Manager chiffre vos données à l'aide de la clé que vous avez spécifiée et chiffre les métadonnées à l'aide d'une clé AWS détenue. Pour utiliser Incident Manager, vous devez configurer votre ensemble de réplication, y compris la configuration du chiffrement. Incident Manager nécessite le chiffrement des données pour être utilisé.

Vous pouvez utiliser une clé AWS détenue pour chiffrer votre jeu de réplication ou vous pouvez utiliser votre propre clé gérée par le client que vous avez créée AWS KMS pour chiffrer les régions de votre jeu de réplication. Incident Manager prend uniquement en charge les AWS KMS clés de chiffrement symétriques pour chiffrer les données que vous y créez. AWS KMS Incident Manager ne prend pas en charge AWS KMS les clés contenant des éléments clés importés, les magasins de clés personnalisés, le code d'authentification des messages basé sur le hachage (HMAC) ou tout autre type de clé. Si vous utilisez des clés gérées par le client, vous utilisez la AWS KMS console ou AWS KMS APIs pour créer de manière centralisée les clés gérées par le client et définir les politiques clés qui contrôlent la manière dont Incident Manager peut utiliser les clés gérées par le client. Lorsque vous utilisez une clé gérée par le client pour le chiffrement avec Incident Manager, la clé gérée par le AWS KMS client doit se trouver dans la même région que les ressources. Pour en savoir plus sur la configuration du chiffrement des données dans Incident Manager, consultezPréparez-vous, magicien.

L'utilisation de clés gérées par le AWS KMS client entraîne des frais supplémentaires. Pour plus d'informations, consultez la section AWS KMS Concepts - Clés KMS dans le guide du AWS Key Management Service développeur et AWS KMS les tarifs.

> **Important**
>
> Si vous utilisez une AWS KMS key (clé KMS) pour chiffrer votre jeu de réplication et les données d'Incident Manager, mais que vous décidez ultérieurement de supprimer le jeu de réplication, assurez-vous de supprimer le jeu de réplication avant de désactiver ou de supprimer la clé KMS.

Pour permettre à Incident Manager d'utiliser votre clé gérée par le client pour chiffrer vos données, vous devez ajouter les déclarations de politique suivantes à la politique clé de votre clé gérée par le client. Pour en savoir plus sur la configuration et la modification des politiques clés de votre compte, consultez la section Utilisation des politiques clés AWS KMS dans le Guide du AWS Key Management Service développeur. La politique fournit les autorisations suivantes :

- Permet à Incident Manager d'effectuer des opérations en lecture seule AWS KMS key pour trouver le nom d'Incident Manager dans votre compte.
- Permet à Incident Manager d'utiliser la clé KMS pour créer des autorisations et décrire la clé, mais uniquement lorsqu'il agit pour le compte des principaux du compte autorisés à utiliser Incident Manager. Si les principaux responsables spécifiés dans la déclaration de politique ne sont pas autorisés à utiliser les clés KMS et à utiliser Incident Manager, l'appel échoue, même s'il provient du service Incident Manager.

```
{
"Sid": "Allow CreateGrant through AWS Systems Manager Incident Manager",
"Effect": "Allow",
"Principal": {
  "AWS": "arn:aws:iam::111122223333:user/ssm-lead"
},
"Action": [
  "kms:CreateGrant",
  "kms:DescribeKey"
],
"Resource": "*",
"Condition": {
  "StringLike": {
    "kms:ViaService": [
      "ssm-incidents.amazonaws.com",
      "ssm-contacts.amazonaws.com"
    ]
```

```
        }
      }
    }
```

Remplacez la `Principal` valeur par le principal IAM qui a créé votre ensemble de réplication.

Incident Manager utilise un contexte de chiffrement dans toutes les AWS KMS demandes d'opérations cryptographiques. Vous pouvez utiliser ce contexte de chiffrement pour identifier les événements du CloudTrail journal pour lesquels Incident Manager utilise vos clés KMS. Incident Manager utilise le contexte de chiffrement suivant :

- `contactArn=`*`ARN of the contact or escalation plan`*

Identity and Access Management pour AWS Systems Manager Incident Manager

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser les ressources d'Incident Manager. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez dans Incident Manager.

Utilisateur du service : si vous utilisez le service Incident Manager pour effectuer votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de plus en plus de fonctionnalités d'Incident Manager pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans Incident Manager, consultezRésolution des problèmes AWS Systems Manager Incident Manager d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des ressources du gestionnaire d'incidents dans votre entreprise, vous avez probablement un accès complet à Incident Manager. C'est à vous de déterminer les fonctionnalités et les ressources du gestionnaire d'incidents auxquels les utilisateurs du service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d'IAM. Pour en savoir plus sur la manière dont votre entreprise peut utiliser IAM avec Incident Manager, consultezComment AWS Systems Manager Incident Manager fonctionne avec IAM.

Administrateur IAM : si vous êtes administrateur IAM, vous souhaiterez peut-être en savoir plus sur la manière dont vous pouvez rédiger des politiques pour gérer l'accès à Incident Manager. Pour consulter des exemples de politiques basées sur l'identité d'Incident Manager que vous pouvez utiliser dans IAM, consultez. Exemples de politiques basées sur l'identité pour AWS Systems Manager Incident Manager

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec

des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer des demandes vous-même, consultez AWS Signature Version 4 pour les demandes d'API dans le Guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour plus d'informations, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Authentification multifactorielle AWS dans IAM dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur racine, consultez Tâches nécessitant des informations d'identification d'utilisateur racine dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme telles que des mots de passe et des clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons d'effectuer une rotation des clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez nommer un groupe IAMAdminset lui donner les autorisations nécessaires pour administrer les ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour plus d'informations, consultez Cas d'utilisation pour les utilisateurs IAM dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Pour assumer temporairement un rôle IAM dans le AWS Management Console, vous pouvez passer d'un rôle d'utilisateur à un rôle IAM (console). Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Méthodes pour endosser un rôle dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré : pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.
- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains

services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

- Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
- Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une EC2 instance et qui envoient des demandes AWS CLI d' AWS API. Cela est préférable au stockage des clés d'accès dans l' EC2 instance. Pour attribuer un AWS rôle à une EC2 instance et le rendre disponible pour toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes exécutés sur l' EC2 instance d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utiliser un rôle IAM pour accorder des autorisations aux applications exécutées sur des EC2 instances Amazon dans le guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette

ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACLs)

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et AWS WAF Amazon VPC sont des exemples de services compatibles. ACLs Pour en savoir plus ACLs, consultez la présentation de la liste de contrôle d'accès (ACL) dans le guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.
- Politiques de contrôle des services (SCPs) : SCPs politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans AWS Organizations. AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer des politiques de contrôle des services (SCPs) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités

figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les Organizations et consultez SCPs les politiques de contrôle des services dans le Guide de AWS Organizations l'utilisateur.

- Politiques de contrôle des ressources (RCPs) : RCPs politiques JSON que vous pouvez utiliser pour définir le maximum d'autorisations disponibles pour les ressources de vos comptes sans mettre à jour les politiques IAM associées à chaque ressource que vous possédez. Le RCP limite les autorisations pour les ressources des comptes membres et peut avoir un impact sur les autorisations effectives pour les identités, y compris Utilisateur racine d'un compte AWS, qu'elles appartiennent ou non à votre organisation. Pour plus d'informations sur les Organizations RCPs, y compris une liste de ces Services AWS supports RCPs, consultez la section Resource control policies (RCPs) dans le guide de AWS Organizations l'utilisateur.
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez Politiques de session dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment AWS Systems Manager Incident Manager fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à Incident Manager, découvrez quelles fonctionnalités IAM peuvent être utilisées avec Incident Manager.

Fonctionnalités IAM que vous pouvez utiliser avec AWS Systems Manager Incident Manager

Fonctionnalité IAM	Assistance pour le gestionnaire d'incidents
Politiques basées sur l'identité	Oui

Fonctionnalité IAM	Assistance pour le gestionnaire d'incidents
Politiques basées sur les ressources	Oui
Actions de politique	Oui
Ressources de politique	Oui
Clés de condition d'une politique	Non
ACLs	Non
ABAC (étiquettes dans les politiques)	Non
Informations d'identification temporaires	Oui
Autorisations de principal	Oui
Rôles de service	Oui
Rôles liés à un service	Oui

Pour obtenir une vue d'ensemble de la façon dont Incident Manager et les autres AWS services fonctionnent avec la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Incident Manager ne prend pas en charge les politiques qui refusent l'accès aux ressources partagées à l'aide AWS RAM.

Politiques basées sur l'identité pour Incident Manager

Prend en charge les politiques basées sur l'identité : oui

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Définition d'autorisations IAM personnalisées avec des politiques gérées par le client dans le Guide de l'utilisateur IAM.

Avec les politiques IAM basées sur l'identité, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. Vous ne pouvez pas spécifier le principal dans une politique basée sur une identité, car celle-ci s'applique à l'utilisateur ou au rôle auquel elle est attachée. Pour découvrir tous les éléments que vous utilisez dans une politique JSON, consultez Références des éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.

Exemples de politiques basées sur l'identité pour Incident Manager

Pour consulter des exemples de politiques basées sur l'identité d'Incident Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Systems Manager Incident Manager

Politiques basées sur les ressources dans Incident Manager

Prend en charge les politiques basées sur les ressources : oui

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Par exemple, les politiques de confiance de rôle IAM et les politiques de compartiment Amazon S3 sont des politiques basées sur les ressources. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Pour permettre un accès intercompte, vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une politique basée sur les ressources. L'ajout d'un principal intercompte à une politique basée sur les ressources ne représente qu'une partie de l'instauration de la relation d'approbation. Lorsque le principal et la ressource sont différents Comptes AWS, un administrateur IAM du compte sécurisé doit également accorder à l'entité principale (utilisateur ou rôle) l'autorisation d'accéder à la ressource. Pour ce faire, il attache une politique basée sur une identité à l'entité. Toutefois, si une politique basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre politique basée sur l'identité n'est requise. Pour plus d'informations, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Le service Incident Manager ne prend en charge que deux types de politiques basées sur les ressources, appelées à l'aide de la AWS RAM console ou de l' PutResourcePolicy action, qui est

attachée à un plan de réponse ou à un contact. Cette politique définit quels principaux peuvent effectuer des actions sur les plans de réponse, les contacts, les plans d'escalade et les incidents. Incident Manager utilise des politiques basées sur les ressources pour partager les ressources entre les comptes.

Incident Manager ne prend pas en charge les politiques qui refusent l'accès aux ressources partagées à l'aide AWS RAM.

Pour savoir comment associer une politique basée sur les ressources à un plan d'intervention ou à un contact, voir. Gestion des incidents par région Comptes AWS et par région dans Incident Manager

Exemples de politiques basées sur les ressources dans Incident Manager

Pour consulter des exemples de politiques basées sur les ressources d'Incident Manager, consultez. Exemples de politiques basées sur les ressources pour AWS Systems Manager Incident Manager

Actions politiques pour Incident Manager

Prend en charge les actions de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Action` d'une politique JSON décrit les actions que vous pouvez utiliser pour autoriser ou refuser l'accès à une politique. Les actions de stratégie portent généralement le même nom que l'opération AWS d'API associée. Il existe quelques exceptions, telles que les actions avec autorisations uniquement qui n'ont pas d'opération API correspondante. Certaines opérations nécessitent également plusieurs actions dans une politique. Ces actions supplémentaires sont nommées actions dépendantes.

Intégration d'actions dans une politique afin d'accorder l'autorisation d'exécuter les opérations associées.

Pour consulter la liste des actions d'Incident Manager, consultez la section Actions définies par AWS Systems Manager Incident Manager dans la référence d'autorisation de service.

Les actions de politique dans Incident Manager utilisent les préfixes suivants avant l'action :

```
ssm-incidents
```

```
ssm-contacts
```

Pour indiquer plusieurs actions dans une seule déclaration, séparez-les par des virgules.

```
"Action": [
      "ssm-incidents:GetResponsePlan",
      "ssm-contacts:GetContact"
         ]
```

Vous pouvez aussi spécifier plusieurs actions à l'aide de caractères génériques (*). Par exemple, pour spécifier toutes les actions qui commencent par le mot `Get`, incluez l'action suivante :

```
"Action": "ssm-incidents:Get*"
```

Pour consulter des exemples de politiques basées sur l'identité d'Incident Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Systems Manager Incident Manager

Incident Manager utilise des actions dans deux espaces de noms différents, ssm-incidents et ssm-contacts. Lorsque vous créez des politiques pour Incident Manager, veillez à utiliser l'espace de noms correspondant à l'action. Le SSM-Incidents est utilisé pour le plan de réponse et les actions liées aux incidents. SSM-Contacts est utilisé pour les actions liées aux contacts et à l'engagement des contacts. Par exemple :

- `ssm-contacts:GetContact`
- `ssm-incidents:GetResponsePlan`

Ressources relatives aux politiques pour Incident Manager

Prend en charge les ressources de politique : oui

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément de politique JSON `Resource` indique le ou les objets auxquels l'action s'applique. Les instructions doivent inclure un élément `Resource` ou `NotResource`. Il est recommandé de définir une ressource à l'aide de son Amazon Resource Name (ARN). Vous pouvez le faire pour des actions

qui prennent en charge un type de ressource spécifique, connu sous la dénomination autorisations de niveau ressource.

Pour les actions qui ne sont pas compatibles avec les autorisations de niveau ressource, telles que les opérations de liste, utilisez un caractère générique (*) afin d'indiquer que l'instruction s'applique à toutes les ressources.

```
"Resource": "*"
```

Pour consulter la liste des types de ressources Incident Manager et leurs caractéristiques ARNs, consultez la section Ressources définies par AWS Systems Manager Incident Manager dans la référence d'autorisation de service. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Systems Manager Incident Manager.

Pour consulter des exemples de politiques basées sur l'identité d'Incident Manager, consultez. Exemples de politiques basées sur l'identité pour AWS Systems Manager Incident Manager

Les ressources du gestionnaire d'incidents sont utilisées pour créer des incidents, collaborer sur les canaux de discussion, résoudre les incidents et impliquer les intervenants. Si un utilisateur a accès à un plan de réponse, il a accès à tous les incidents créés à partir de celui-ci. Si un utilisateur a accès à un contact ou à un plan d'escalade, il peut faire participer le ou les contacts au plan d'escalade.

Clés de conditions de politique pour Incident Manager

Prend en charge les clés de condition de politique spécifiques au service : Non

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

L'élément `Condition` (ou le bloc `Condition`) vous permet de spécifier des conditions lorsqu'une instruction est appliquée. L'élément `Condition` est facultatif. Vous pouvez créer des expressions conditionnelles qui utilisent des opérateurs de condition, tels que les signes égal ou inférieur à, pour faire correspondre la condition de la politique aux valeurs de la demande.

Si vous spécifiez plusieurs éléments `Condition` dans une instruction, ou plusieurs clés dans un seul élément `Condition`, AWS les évalue à l'aide d'une opération `AND` logique. Si vous spécifiez plusieurs valeurs pour une seule clé de condition, AWS évalue la condition à l'aide d'une `OR`

opération logique. Toutes les conditions doivent être remplies avant que les autorisations associées à l'instruction ne soient accordées.

Vous pouvez aussi utiliser des variables d'espace réservé quand vous spécifiez des conditions. Par exemple, vous pouvez accorder à un utilisateur IAM l'autorisation d'accéder à une ressource uniquement si elle est balisée avec son nom d'utilisateur IAM. Pour plus d'informations, consultez Éléments d'une politique IAM : variables et identifications dans le Guide de l'utilisateur IAM.

AWS prend en charge les clés de condition globales et les clés de condition spécifiques au service. Pour voir toutes les clés de condition AWS globales, voir les clés de contexte de condition AWS globales dans le guide de l'utilisateur IAM.

Listes de contrôle d'accès (ACLs) dans Incident Manager

Supports ACLs : Non

Les listes de contrôle d'accès (ACLs) contrôlent les principaux (membres du compte, utilisateurs ou rôles) autorisés à accéder à une ressource. ACLs sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Contrôle d'accès basé sur les attributs (ABAC) avec Incident Manager

Supporte l'ABAC (balises dans les politiques) : Non

Le contrôle d'accès par attributs (ABAC) est une stratégie d'autorisation qui définit des autorisations en fonction des attributs. Dans AWS, ces attributs sont appelés balises. Vous pouvez associer des balises aux entités IAM (utilisateurs ou rôles) et à de nombreuses AWS ressources. L'étiquetage des entités et des ressources est la première étape d'ABAC. Vous concevez ensuite des politiques ABAC pour autoriser des opérations quand l'identification du principal correspond à celle de la ressource à laquelle il tente d'accéder.

L'ABAC est utile dans les environnements qui connaissent une croissance rapide et pour les cas où la gestion des politiques devient fastidieuse.

Pour contrôler l'accès basé sur des étiquettes, vous devez fournir les informations d'étiquette dans l'élément de condition d'une politique utilisant les clés de condition `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` ou `aws:TagKeys`.

Si un service prend en charge les trois clés de condition pour tous les types de ressources, alors la valeur pour ce service est Oui. Si un service prend en charge les trois clés de condition pour certains types de ressources uniquement, la valeur est Partielle.

Pour plus d'informations sur ABAC, consultez Définition d'autorisations avec l'autorisation ABAC dans le Guide de l'utilisateur IAM. Pour accéder à un didacticiel décrivant les étapes de configuration de l'ABAC, consultez Utilisation du contrôle d'accès par attributs (ABAC) dans le Guide de l'utilisateur IAM.

Utilisation d'informations d'identification temporaires avec Incident Manager

Prend en charge les informations d'identification temporaires : oui

Certains Services AWS ne fonctionnent pas lorsque vous vous connectez à l'aide d'informations d'identification temporaires. Pour plus d'informations, y compris celles qui Services AWS fonctionnent avec des informations d'identification temporaires, consultez Services AWS la section relative à l'utilisation d'IAM dans le guide de l'utilisateur d'IAM.

Vous utilisez des informations d'identification temporaires si vous vous connectez à l' AWS Management Console aide d'une méthode autre qu'un nom d'utilisateur et un mot de passe. Par exemple, lorsque vous accédez à AWS l'aide du lien d'authentification unique (SSO) de votre entreprise, ce processus crée automatiquement des informations d'identification temporaires. Vous créez également automatiquement des informations d'identification temporaires lorsque vous vous connectez à la console en tant qu'utilisateur, puis changez de rôle. Pour plus d'informations sur le changement de rôle, consultez Passage d'un rôle utilisateur à un rôle IAM (console) dans le Guide de l'utilisateur IAM.

Vous pouvez créer manuellement des informations d'identification temporaires à l'aide de l' AWS API AWS CLI or. Vous pouvez ensuite utiliser ces informations d'identification temporaires pour y accéder AWS. AWS recommande de générer dynamiquement des informations d'identification temporaires au lieu d'utiliser des clés d'accès à long terme. Pour plus d'informations, consultez Informations d'identification de sécurité temporaires dans IAM.

Autorisations principales interservices pour Incident Manager

Prend en charge les sessions d'accès direct (FAS) : oui

Lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux

actions. Pour plus de détails sur une politique lors de la formulation de demandes FAS, consultez Transmission des sessions d'accès.

Rôles de service pour Incident Manager

Prend en charge les rôles de service : oui

Un rôle de service est un rôle IAM qu'un service endosse pour accomplir des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer un rôle de service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.

> **Warning**
>
> La modification des autorisations associées à un rôle de service peut perturber les fonctionnalités d'Incident Manager. Modifiez les rôles de service uniquement lorsque Incident Manager fournit des instructions à cet effet.

Choix d'un rôle IAM dans Incident Manager

Lorsque vous créez une ressource de plan de réponse dans Incident Manager, vous devez choisir un rôle pour permettre à Incident Manager d'exécuter un document d'automatisation de Systems Manager en votre nom. Si vous avez déjà créé un rôle de service ou un rôle lié à un service, Incident Manager vous fournit une liste de rôles parmi lesquels choisir. Il est important de choisir un rôle qui autorise l'accès à l'exécution de vos instances de documents automatisés. Pour de plus amples informations, veuillez consulter Intégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents. Lorsque vous créez un canal de discussion Amazon Q Developer dans les applications de chat à utiliser lors d'un incident, vous pouvez sélectionner un rôle de service qui vous permet d'utiliser des commandes directement depuis le chat. Pour en savoir plus sur la création de canaux de discussion pour la collaboration en cas d'incident, consultezCréation et intégration de canaux de discussion pour les intervenants dans Incident Manager. Pour en savoir plus sur les politiques IAM dans Amazon Q Developer dans les applications de chat, consultez la section Gestion des autorisations pour exécuter des commandes à l'aide d'Amazon Q Developer dans les applications de chat dans le guide d'administration d'Amazon Q Developer dans les applications de chat.

Rôles liés aux services pour Incident Manager

Prend en charge les rôles liés aux services : Oui

Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés au service apparaissent dans votre Compte AWS fichier et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

Pour plus d'informations sur la création ou la gestion des rôles liés au service Incident Manager, consultez. Utilisation de rôles liés à un service pour Incident Manager

Exemples de politiques basées sur l'identité pour AWS Systems Manager Incident Manager

Par défaut, les utilisateurs et les rôles ne sont pas autorisés à créer ou à modifier des ressources Incident Manager. Ils ne peuvent pas non plus effectuer de tâches à l'aide de l'API AWS Management Console, AWS Command Line Interface (AWS CLI) ou de AWS l'API. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Pour apprendre à créer une politique basée sur l'identité IAM à l'aide de ces exemples de documents de politique JSON, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Pour plus de détails sur les actions et les types de ressources définis par Incident Manager, y compris le format de chaque type de ressource, voir Actions, ressources et clés de condition AWS Systems Manager Incident Manager dans la référence d'autorisation de service. ARNs

Rubriques

- Bonnes pratiques en matière de politiques
- Utilisation de la console Incident Manager
- Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations
- Accès à un plan de réponse

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer des ressources Incident Manager dans votre compte. Ces actions peuvent entraîner des frais pour votre Compte AWS. Lorsque vous créez ou modifiez des politiques basées sur l'identité, suivez ces instructions et recommandations :

- Commencez AWS par les politiques gérées et passez aux autorisations du moindre privilège : pour commencer à accorder des autorisations à vos utilisateurs et à vos charges de travail, utilisez les politiques AWS gérées qui accordent des autorisations pour de nombreux cas d'utilisation courants. Ils sont disponibles dans votre Compte AWS. Nous vous recommandons de réduire davantage les autorisations en définissant des politiques gérées par les AWS clients spécifiques à vos cas d'utilisation. Pour plus d'informations, consultez politiques gérées par AWS ou politiques gérées par AWS pour les activités professionnelles dans le Guide de l'utilisateur IAM.
- Accordez les autorisations de moindre privilège : lorsque vous définissez des autorisations avec des politiques IAM, accordez uniquement les autorisations nécessaires à l'exécution d'une seule tâche. Pour ce faire, vous définissez les actions qui peuvent être entreprises sur des ressources spécifiques dans des conditions spécifiques, également appelées autorisations de moindre privilège. Pour plus d'informations sur l'utilisation d'IAM pour appliquer des autorisations, consultez politiques et autorisations dans IAM dans le Guide de l'utilisateur IAM.
- Utilisez des conditions dans les politiques IAM pour restreindre davantage l'accès : vous pouvez ajouter une condition à vos politiques afin de limiter l'accès aux actions et aux ressources. Par exemple, vous pouvez écrire une condition de politique pour spécifier que toutes les demandes doivent être envoyées via SSL. Vous pouvez également utiliser des conditions pour accorder l'accès aux actions de service si elles sont utilisées par le biais d'un service spécifique Service AWS, tel que AWS CloudFormation. Pour plus d'informations, consultez Conditions pour éléments de politique JSON IAM dans le Guide de l'utilisateur IAM.
- Utilisez l'Analyseur d'accès IAM pour valider vos politiques IAM afin de garantir des autorisations sécurisées et fonctionnelles : l'Analyseur d'accès IAM valide les politiques nouvelles et existantes de manière à ce que les politiques IAM respectent le langage de politique IAM (JSON) et les bonnes pratiques IAM. IAM Access Analyzer fournit plus de 100 vérifications de politiques et des recommandations exploitables pour vous aider à créer des politiques sécurisées et fonctionnelles. Pour plus d'informations, consultez Validation de politiques avec IAM Access Analyzer dans le Guide de l'utilisateur IAM.
- Exiger l'authentification multifactorielle (MFA) : si vous avez un scénario qui nécessite des utilisateurs IAM ou un utilisateur root, activez l'authentification MFA pour une sécurité accrue. Compte AWS Pour exiger la MFA lorsque des opérations d'API sont appelées, ajoutez des conditions MFA à vos politiques. Pour plus d'informations, consultez Sécurisation de l'accès aux API avec MFA dans le Guide de l'utilisateur IAM.

Pour plus d'informations sur les bonnes pratiques dans IAM, consultez Bonnes pratiques de sécurité dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de la console Incident Manager

Pour accéder à la AWS Systems Manager Incident Manager console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et de consulter les détails des ressources du gestionnaire d'incidents de votre Compte AWS. Si vous créez une politique basée sur l'identité qui est plus restrictive que l'ensemble minimum d'autorisations requis, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs ou rôles) tributaires de cette politique.

Il n'est pas nécessaire d'accorder des autorisations de console minimales aux utilisateurs qui appellent uniquement l'API AWS CLI ou l' AWS API. Autorisez plutôt l'accès à uniquement aux actions qui correspondent à l'opération d'API qu'ils tentent d'effectuer.

Pour garantir que les utilisateurs et les rôles peuvent résoudre les incidents à l'aide de la console Incident Manager, associez également la politique `IncidentManagerResolverAccess` AWS gérée par Incident Manager aux entités. Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

```
IncidentManagerResolverAccess
```

Autorisation accordée aux utilisateurs pour afficher leurs propres autorisations

Cet exemple montre comment créer une politique qui permet aux utilisateurs IAM d'afficher les politiques en ligne et gérées attachées à leur identité d'utilisateur. Cette politique inclut les autorisations permettant d'effectuer cette action sur la console ou par programmation à l'aide de l'API AWS CLI or AWS .

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
```

```
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Accès à un plan de réponse

Dans cet exemple, vous souhaitez accorder à un utilisateur IAM de votre compte Amazon Web Services l'accès à l'un de vos plans de réponse Incident Manager. `exampleplan` Vous souhaitez également autoriser l'utilisateur à ajouter, mettre à jour et supprimer le plan de réponse.

La politique accorde les `ssm-incident:ListResponsePlan` autorisations `ssm-incidents:ListResponsePlanssssm-incidents:GetResponsePlan`, `ssm-incidents:UpdateResponsePlan` et à l'utilisateur.

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid":"ListResponsePlans",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:ListResponsePlans"
         ],
         "Resource":"arn:aws:ssm-incidents:::*"
      },
      {
         "Sid":"ViewSpecificResponsePlanInfo",
```

```
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:GetResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan"
      },
      {
         "Sid":"ManageResponsePlan",
         "Effect":"Allow",
         "Action":[
            "ssm-incidents:UpdateResponsePlan"
         ],
         "Resource":"arn:aws:ssm-incidents:*:111122223333:response-plan/exampleplan/*"
      }
   ]
}
```

Exemples de politiques basées sur les ressources pour AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager prend en charge les politiques d'autorisation basées sur les ressources pour les plans de réponse et les contacts d'Incident Manager.

Incident Manager ne prend pas en charge les politiques basées sur les ressources qui refusent l'accès aux ressources partagées à l'aide de celles-ci. AWS RAM

Pour savoir comment créer un plan d'intervention ou un contact, consultez Création et configuration de plans de réponse dans Incident Manager etCréation et configuration de contacts dans Incident Manager.

Restreindre l'accès au plan de réponse d'Incident Manager par l'organisation

L'exemple suivant accorde des autorisations aux utilisateurs de l'organisation dotés de l'identifiant de l'organisation : `o-abc123def45` pour répondre aux incidents créés à l'aide du plan de réponse`myplan`.

Le `Condition` bloc utilise les `StringEquals` conditions et la clé de `aws:PrincipalOrgID` condition, qui est une clé de condition AWS Organizations spécifique. Pour plus d'informations sur ces clés de condition, consultez la section Spécification de conditions dans une politique.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationAccess",
      "Effect": "Allow",
      "Principal": “*”,
      "Condition": {
         "StringEquals": {"aws:PrincipalOrgID":"o-abc123def45"}
      },
      "Action": [
        "ssm-incidents:GetResponsePlan",
        "ssm-incidents:StartIncident",
        "ssm-incidents:UpdateIncidentRecord",
        "ssm-incidents:GetIncidentRecord",
        "ssm-incidents:CreateTimelineEvent",
        "ssm-incidents:UpdateTimelineEvent",
        "ssm-incidents:GetTimelineEvent",
        "ssm-incidents:ListTimelineEvents",
        "ssm-incidents:UpdateRelatedItems",
        "ssm-incidents:ListRelatedItems"
      ],
      "Resource": [
        "arn:aws:ssm-incidents:*:111122223333:response-plan/myplan",
        "arn:aws:ssm-incidents:*:111122223333:incident-record/myplan/*"
      ]
    }
  ]
}
```

Fournir un accès de contact au responsable des incidents à un mandant

L'exemple suivant autorise le principal doté de l'ARN `arn:aws:iam::999988887777:root` à créer des engagements avec le contact`mycontact`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "PrincipalAccess",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::999988887777:root"
```

```
            },
            "Action": [
                "ssm-contacts:GetContact",
                "ssm-contacts:StartEngagement",
                "ssm-contacts:DescribeEngagement",
                "ssm-contacts:ListPagesByContact"
            ],
            "Resource": [
                "arn:aws:ssm-contacts:*:111122223333:contact/mycontact"
                "arn:aws:ssm-contacts:*:111122223333:engagement/mycontact/*"
            ]
        }
    ]
}
```

Prévention de la confusion entre les services par les adjoints dans Incident Manager

Le problème des adjoints confus est un problème de sécurité de l'information qui se produit lorsqu'une entité non autorisée à effectuer une action appelle une entité plus privilégiée pour effectuer l'action. Cela peut permettre à des acteurs malveillants d'exécuter des commandes ou de modifier des ressources qu'ils n'auraient pas l'autorisation d'exécuter ou d'accéder autrement.

Dans AWS, l'usurpation d'identité interservices peut mener à un scénario d'adjoint confus. L'usurpation d'identité interservices se produit lorsqu'un service (le service appelant) appelle un autre service (le service appelé). Un acteur malveillant peut utiliser le service d'appel pour modifier les ressources d'un autre service en utilisant des autorisations qu'il n'aurait pas normalement obtenues.

AWS fournit aux responsables du service un accès géré aux ressources de votre compte afin de vous aider à protéger la sécurité de vos ressources. Nous vous recommandons d'utiliser les clés de contexte de condition `aws:SourceAccount`globale `aws:SourceArn`et les clés contextuelles dans vos politiques de ressources. Ces clés limitent les autorisations qui fournissent AWS Systems Manager Incident Manager un autre service à cette ressource. Si vous utilisez les deux clés contextuelles de condition globale, la `aws:SourceAccount` valeur et le compte référencés dans la `aws:SourceArn` valeur doivent utiliser le même identifiant de compte lorsqu'ils sont utilisés dans la même déclaration de politique.

La valeur de `aws:SourceArn` doit être l'ARN de l'enregistrement d'incident concerné. Si vous ne connaissez pas l'ARN complet de la ressource, ou si vous spécifiez plusieurs ressources, utilisez la clé de condition de contexte `aws:SourceArn` global avec le `*` caractère générique pour les

parties inconnues de l'ARN. Par exemple, vous pouvez `aws:SourceArn` définir sur`arn:aws:ssm-incidents::111122223333:*`.

Dans l'exemple de politique de confiance suivant, nous utilisons la clé de `aws:SourceArn` condition pour restreindre l'accès au rôle de service en fonction de l'ARN de l'enregistrement de l'incident. Seuls les enregistrements d'incidents créés à partir du plan `myresponseplan` d'intervention peuvent utiliser ce rôle.

```
{
  "Version": "2012-10-17",
  "Statement": {
    "Effect": "Allow",
    "Principal": { "Service": "ssm-incidents.amazonaws.com" },
    "Action": "sts:AssumeRole",
    "Condition": {
      "ArnLike": {
        "aws:SourceArn": "arn:aws:ssm-incidents:*:111122223333:incident-record/
myresponseplan/*"
      }
    }
  }
}
```

Utilisation de rôles liés à un service pour Incident Manager

AWS Systems Manager Incident Manager utilise des AWS Identity and Access Management rôles liés à un service (IAM). Un rôle lié à un service est un type unique de rôle IAM directement lié à Incident Manager. Les rôles liés au service sont prédéfinis par Incident Manager et incluent toutes les autorisations dont le service a besoin pour appeler d'autres AWS services en votre nom.

Un rôle lié à un service facilite la configuration d'Incident Manager, car vous n'avez pas à ajouter manuellement les autorisations nécessaires. Incident Manager définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul le gestionnaire d'incidents peut assumer ses rôles. Les autorisations définies comprennent la politique d'approbation et la politique d'autorisation. De plus, cette politique d'autorisation ne peut pas être attachée à une autre entité IAM.

Vous pouvez supprimer un rôle lié à un service uniquement après la suppression préalable de ses ressources connexes. Cela protège les ressources de votre gestionnaire d'incidents, car vous ne pouvez pas supprimer par inadvertance l'autorisation d'accès aux ressources.

Pour plus d'informations sur les autres services qui prennent en charge les rôles liés aux services, consultez Services AWS fonctionnant avec IAM et recherchez les services où Oui figure dans la colonne Rôle lié à un service. Choisissez un Yes (oui) ayant un lien permettant de consulter les détails du rôle pour ce service.

Autorisations de rôle liées au service pour Incident Manager

Incident Manager utilise le rôle lié au service nommé. AWSServiceRoleforIncidentManager Ce rôle permet au gestionnaire d'incidents de gérer les dossiers d'incidents du gestionnaire d'incidents et les ressources associées en votre nom.

Le rôle AWSService RoleforIncidentManager lié à un service fait confiance aux services suivants pour assumer le rôle :

- `ssm-incidents.amazonaws.com`

La politique d'autorisation des rôles `AWSIncidentManagerServiceRolePolicy`permet à Incident Manager d'effectuer les actions suivantes sur les ressources spécifiées :

- Action : `ssm-incidents:ListIncidentRecords` sur toutes les ressources liées à l'action.
- Action : `ssm-incidents:CreateTimelineEvent` sur toutes les ressources liées à l'action.
- Action : `ssm:CreateOpsItem` sur toutes les ressources liées à l'action.
- Action : `ssm:AssociateOpsItemRelatedItem` sur `all resources related to the action.`
- Action : `ssm-contacts:StartEngagement` sur toutes les ressources liées à l'action.
- Action : `cloudwatch:PutMetricData` sur les CloudWatch métriques à l'intérieur des espaces de `AWS/Usage` noms `AWS/IncidentManager` et

Vous devez configurer les autorisations de manière à permettre à une entité IAM (comme un utilisateur, un groupe ou un rôle) de créer, modifier ou supprimer un rôle lié à un service. Pour plus d'informations, consultez Service-Linked Role Permissions (autorisations du rôle lié à un service) dans le Guide de l'utilisateur IAM.

Création d'un rôle lié à un service pour Incident Manager

Vous n'avez pas besoin de créer manuellement un rôle lié à un service. Lorsque vous créez un ensemble de réplication dans l'API AWS Management Console AWS CLI, le ou l' AWS API, Incident Manager crée le rôle lié au service pour vous.

Si vous supprimez ce rôle lié à un service et que vous avez ensuite besoin de le recréer, vous pouvez utiliser la même procédure pour recréer le rôle dans votre compte. Lorsque vous créez un ensemble de réplication, Incident Manager crée à nouveau le rôle lié au service pour vous.

Modification d'un rôle lié à un service pour Incident Manager

Incident Manager ne vous permet pas de modifier le rôle AWSService RoleforIncidentManager lié au service. Une fois que vous avez créé un rôle lié à un service, vous ne pouvez pas changer le nom du rôle, car plusieurs entités peuvent faire référence au rôle. Néanmoins, vous pouvez modifier la description du rôle à l'aide d'IAM. Pour plus d'informations, consultez Modification d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Supprimer un rôle lié à un service pour Incident Manager

Si vous n'avez plus besoin d'utiliser une fonction ou un service qui nécessite un rôle lié à un service, nous vous recommandons de supprimer ce rôle. De cette façon, aucune entité inutilisée n'est surveillée ou gérée activement. Cependant, vous devez nettoyer les ressources de votre rôle lié à un service avant de pouvoir les supprimer manuellement.

Pour supprimer le rôle lié à un service, vous devez d'abord supprimer le jeu de réplication. La suppression du jeu de réplication entraîne la suppression de toutes les données créées et stockées dans Incident Manager, y compris les plans de réponse, les contacts et les plans d'escalade. Vous perdrez également tous les incidents créés précédemment. Les alarmes et EventBridge les règles pointant vers des plans d'intervention supprimés ne créeront plus d'incident en cas d'alarme ou de correspondance des règles. Pour supprimer le jeu de réplication, vous devez supprimer toutes les régions du jeu.

> **Note**
>
> Si le service Incident Manager utilise le rôle lorsque vous essayez de supprimer les ressources, la suppression risque d'échouer. Si cela se produit, patientez quelques minutes et réessayez.

Pour supprimer les régions du jeu de réplication utilisé par AWSService RoleforIncidentManager

1. Ouvrez la console Incident Manager et choisissez Paramètres dans le menu de navigation de gauche.
2. Sélectionnez une région dans le jeu de réplication.
3. Sélectionnez Delete (Supprimer).
4. Pour confirmer la suppression de la région, entrez le nom de la région et choisissez Supprimer.
5. Répétez ces étapes jusqu'à ce que vous ayez supprimé toutes les régions de votre jeu de réplication. Lorsque vous supprimez la région finale, la console vous informe qu'elle supprime le jeu de réplication qui l'accompagne.

Pour supprimer manuellement le rôle lié à un service à l'aide d'IAM

Utilisez la console IAM AWS CLI, le ou l' AWS API pour supprimer le rôle lié au AWSService RoleforIncidentManager service. Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Régions prises en charge pour les rôles liés au service Incident Manager

Incident Manager prend en charge l'utilisation de rôles liés au service dans toutes les régions où le service est disponible. Pour plus d'informations, consultez AWS Régions et points de terminaison.

AWS politiques gérées pour AWS Systems Manager Incident Manager

Une politique AWS gérée est une politique autonome créée et administrée par AWS. AWS les politiques gérées sont conçues pour fournir des autorisations pour de nombreux cas d'utilisation courants afin que vous puissiez commencer à attribuer des autorisations aux utilisateurs, aux groupes et aux rôles.

N'oubliez pas que les politiques AWS gérées peuvent ne pas accorder d'autorisations de moindre privilège pour vos cas d'utilisation spécifiques, car elles sont accessibles à tous les AWS clients. Nous vous recommandons de réduire encore les autorisations en définissant des politiques gérées par le client qui sont propres à vos cas d'utilisation.

Vous ne pouvez pas modifier les autorisations définies dans les politiques AWS gérées. Si les autorisations définies dans une politique AWS gérée sont AWS mises à jour, la mise à jour affecte toutes les identités principales (utilisateurs, groupes et rôles) auxquelles la politique est attachée.

AWS est le plus susceptible de mettre à jour une politique AWS gérée lorsqu'une nouvelle politique Service AWS est lancée ou lorsque de nouvelles opérations d'API sont disponibles pour les services existants.

Pour plus d’informations, consultez Politiques gérées par AWS dans le Guide de l’utilisateur IAM.

AWS politique gérée : AWSIncident ManagerIncidentAccessServiceRolePolicy

Vous pouvez attacher `AWSIncidentManagerIncidentAccessServiceRolePolicy` à vos entités IAM. Le gestionnaire d'incidents associe également cette politique à un rôle de gestionnaire d'incidents qui permet au gestionnaire d'incidents d'effectuer des actions en votre nom.

Cette politique accorde des autorisations de lecture seule qui permettent à Incident Manager de lire les ressources de certains autres Services AWS services afin d'identifier les résultats liés aux incidents survenus dans ces services.

Détails de l’autorisation

Cette politique inclut les autorisations suivantes.

- `cloudformation`— Permet aux principes de décrire les AWS CloudFormation piles. Cela est nécessaire pour que le gestionnaire d'incidents puisse identifier les CloudFormation événements et les ressources liés à un incident.
- `codedeploy`— Permet aux principaux de lire les AWS CodeDeploy déploiements. Cela est nécessaire pour qu'Incident Manager identifie les CodeDeploy déploiements et les cibles liés à un incident.
- `autoscaling`— Permet aux principaux de déterminer si une instance Amazon Elastic Compute Cloud (EC2) fait partie d'un groupe Auto Scaling. Cela est nécessaire pour qu'Incident Manager puisse fournir des résultats pour les EC2 instances faisant partie des groupes Auto Scaling.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "IncidentAccessPermissions",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStackEvents",
                "cloudformation:DescribeStackResources",
                "codedeploy:BatchGetDeployments",
                "codedeploy:ListDeployments",
                "codedeploy:ListDeploymentTargets",
                "autoscaling:DescribeAutoScalingInstances"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus de détails sur la politique, y compris la dernière version du document de politique JSON, voir AWSIncidentManagerIncidentAccessServiceRolePolicydans le Guide de référence des politiques AWS gérées.

AWS Politique gérée par: **`AWSIncidentManagerServiceRolePolicy`**

Vous ne pouvez pas joindre de `AWSIncidentManagerServiceRolePolicy` à vos entités IAM. Cette politique est associée à un rôle lié à un service qui permet à Incident Manager d'effectuer des actions en votre nom. Pour de plus amples informations, veuillez consulter Utilisation de rôles liés à un service pour Incident Manager.

Cette politique autorise le gestionnaire d'incidents à répertorier les incidents, à créer des événements chronologiques, à créer des éléments connexes OpsItems, à y associer des éléments connexes OpsItems, à démarrer des engagements et à publier CloudWatch des statistiques relatives à un incident.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ssm-incidents`— Permet aux directeurs de répertorier les incidents et de créer des événements chronologiques. Cela est nécessaire pour que les intervenants puissent collaborer lors d'un incident sur le tableau de bord des incidents.
- `ssm`— Permet aux directeurs de créer OpsItems et d'associer des éléments connexes. Cela est nécessaire pour créer un parent au OpsItem début d'un incident.
- `ssm-contacts`— Permet aux directeurs d'entamer des engagements. Cela est nécessaire pour que le gestionnaire d'incidents puisse engager des contacts lors d'un incident.
- `cloudwatch`— Permet aux directeurs de publier des CloudWatch métriques. Cela est nécessaire pour qu'Incident Manager publie des métriques relatives à un incident et des métriques d'utilisation.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "UpdateIncidentRecordPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:CreateTimelineEvent"
            ],
            "Resource": "*"
        },
        {
            "Sid": "RelatedOpsItemPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm:CreateOpsItem",
                "ssm:AssociateOpsItemRelatedItem"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentEngagementPermissions",
            "Effect": "Allow",
            "Action": "ssm-contacts:StartEngagement",
            "Resource": "*"
        },
        {
            "Sid": "PutCloudWatchMetricPermission",
            "Effect": "Allow",
```

```
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                         "AWS/IncidentManager",
                         "AWS/Usage"
                     ]
                 }
             }
         }
     ]
}
```

Pour plus de détails sur la politique, y compris la dernière version du document de politique JSON, voir AWSIncidentManagerServiceRolePolicydans le Guide de référence des politiques AWS gérées.

AWS politique gérée : **`AWSIncidentManagerResolverAccess`**

Vous pouvez les associer `AWSIncidentManagerResolverAccess` à vos entités IAM pour leur permettre de démarrer, de visualiser et de mettre à jour des incidents. Cela leur permet également de créer des événements chronologiques pour les clients et des éléments connexes dans le tableau de bord des incidents. Vous pouvez également associer cette politique au rôle de développeur Amazon Q dans le service des applications de chat ou directement à votre rôle géré par le client associé à n'importe quel canal de discussion utilisé pour la collaboration en cas d'incident. Pour en savoir plus sur les politiques IAM dans Amazon Q Developer dans les applications de chat, consultez la section Gestion des autorisations pour exécuter des commandes à l'aide d'Amazon Q Developer dans les applications de chat dans le Guide de l'administrateur d'Amazon Q Developer dans les applications de chat.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `ssm-incidents`— Vous permet de démarrer des incidents, de répertorier les plans de réponse, de répertorier les incidents, de mettre à jour les incidents, de répertorier les événements chronologiques, de créer des événements chronologiques personnalisés, de mettre à jour des

événements chronologiques personnalisés, de supprimer des événements chronologiques personnalisés, de répertorier les éléments connexes, de créer des éléments connexes et de mettre à jour des éléments connexes.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "StartIncidentPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:StartIncident"
            ],
            "Resource": "*"
        },
        {
            "Sid": "ResponsePlanReadOnlyPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListResponsePlans",
                "ssm-incidents:GetResponsePlan"
            ],
            "Resource": "*"
        },
        {
            "Sid": "IncidentRecordResolverPermissions",
            "Effect": "Allow",
            "Action": [
                "ssm-incidents:ListIncidentRecords",
                "ssm-incidents:GetIncidentRecord",
                "ssm-incidents:UpdateIncidentRecord",
                "ssm-incidents:ListTimelineEvents",
                "ssm-incidents:CreateTimelineEvent",
                "ssm-incidents:GetTimelineEvent",
                "ssm-incidents:UpdateTimelineEvent",
                "ssm-incidents:DeleteTimelineEvent",
                "ssm-incidents:ListRelatedItems",
                "ssm-incidents:UpdateRelatedItems"
            ],
            "Resource": "*"
        }
    ]
```

```
}
```

Pour plus de détails sur la politique, y compris la dernière version du document de politique JSON, voir AWSIncidentManagerResolverAccessdans le Guide de référence des politiques AWS gérées.

Mises à jour des politiques AWS gérées par Incident Manager

Consultez les détails des mises à jour des politiques AWS gérées pour Incident Manager depuis que ce service a commencé à suivre ces modifications. Pour recevoir des alertes automatiques concernant les modifications apportées à cette page, abonnez-vous au flux RSS sur la page d'historique des documents d'Incident Manager.

Modification	Description	Date
`AWSIncidentManager ServiceRolePolicy` — Mise à jour de la politique	Incident Manager a ajouté une nouvelle autorisation qui permet à Incident Manager de publier des métriques au sein de l'`AWS/Usage` espace de noms sur votre compte.	27 janvier 2025
AWSIncidentManager IncidentAccessServiceRolePolicy — Mise à jour de la politique	Incident Manager a ajouté une nouvelle autorisat ion`AWSIncidentManager IncidentAccessServ iceRolePolicy` , à l'appui de la fonctionnalité Findings, qui lui permet de vérifier si une EC2 instance fait partie d'un groupe Auto Scaling.	20 février 2024
`AWSIncidentManager IncidentAccessServ iceRolePolicy` : nouvelle politique	Incident Manager a ajouté une nouvelle politique qui accorde à Incident Manager l'autoris ation d'appeler d'autres Services AWS personnes	17 novembre 2023

Modification	Description	Date
	dans le cadre de la gestion d'un incident.	
AWSIncidentManagerServiceRolePolicy — Mise à jour de la politique	Incident Manager a ajouté une nouvelle autorisation qui permet à Incident Manager de publier des statistiques sur votre compte.	16 déc. 2022
AWSIncidentManagerResolverAccess : nouvelle politique	Incident Manager a ajouté une nouvelle politique pour vous permettre de démarrer des incidents, de répertorier les plans de réponse, de répertorier les incidents, de mettre à jour les incidents, de répertorier les événements chronologiques, de créer des événements chronologiques personnalisés, de mettre à jour des événements chronologiques personnalisés, de répertorier les éléments connexes, de créer des éléments connexes et de mettre à jour des éléments connexes.	26 avril 2021

Modification	Description	Date
AWSIncidentManagerServiceRolePolicy : nouvelle politique	Incident Manager a ajouté une nouvelle politique pour accorder à Incident Manager l'autorisation de répertorier les incidents, de créer des événements OpsItems chronologiques, de créer OpsItems, d'associer des éléments connexes et de démarrer des engagements liés à un incident.	26 avril 2021
Incident Manager a commencé à suivre les modifications	Incident Manager a commencé à suivre les modifications apportées AWS à ses politiques gérées.	26 avril 2021

Résolution des problèmes AWS Systems Manager Incident Manager d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lors de l'utilisation d'Incident Manager et d'IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans Incident Manager
- Je ne suis pas autorisé à effectuer iam : PassRole
- Je souhaite autoriser des personnes extérieures à mon compte Amazon Web Services à accéder à mes ressources Incident Manager

Je ne suis pas autorisé à effectuer une action dans Incident Manager

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `ssm-incidents:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform: ssm-
incidents:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `ssm-incidents:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez un message d'erreur indiquant que vous n'êtes pas autorisé à effectuer l'`iam:PassRole`action, vos politiques doivent être mises à jour pour vous permettre de transmettre un rôle à Incident Manager.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour effectuer une action dans Incident Manager. Toutefois, l'action nécessite que le service ait des autorisations accordées par un rôle de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite autoriser des personnes extérieures à mon compte Amazon Web Services à accéder à mes ressources Incident Manager

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACLs), vous pouvez utiliser ces politiques pour autoriser les utilisateurs à accéder à vos ressources.

Pour plus d'informations, consultez les éléments suivants :

- Pour savoir si Incident Manager prend en charge ces fonctionnalités, consultezComment AWS Systems Manager Incident Manager fonctionne avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.
- Pour en savoir plus sur la différence entre l'utilisation des rôles et des politiques basées sur les ressources pour l'accès intercompte, consultez Accès intercompte aux ressources dans IAM dans le Guide de l'utilisateur IAM.

Utilisation de contacts partagés et de plans de réponse dans Incident Manager

Grâce au partage de contacts, en tant que propriétaire d'un contact, vous pouvez partager des informations de contact, des plans d'escalade et des engagements avec d'autres personnes Comptes AWS ou au sein d'une AWS organisation.

Grâce au partage du plan d'intervention, en tant que propriétaire du plan d'intervention, vous pouvez partager un plan d'intervention et les incidents connexes avec d'autres personnes Comptes AWS ou au sein d'une AWS organisation.

Le propriétaire d'un contact ou d'un plan de réponse peut partager des contacts et des plans de réponse avec :

- Spécifique Comptes AWS à l'intérieur ou à l'extérieur de son organisation dans AWS Organizations
- Une unité organisationnelle au sein de son organisation dans AWS Organizations
- Toute son organisation en AWS Organizations

Table des matières

Conditions préalables au partage des contacts et des plans de réponse

Pour partager un contact ou un plan de réponse avec votre organisation ou unité organisationnelle dans AWS Organizations :

- Vous devez être propriétaire de la ressource contenue dans votre Compte AWS. Vous ne pouvez pas partager un contact ou un plan de réponse qui a été partagé avec vous.
- Vous devez activer le partage avec AWS Organizations. Pour plus d'informations, veuillez consulter Activation du partage avec AWS Organizations dans le Guide de l'utilisateur AWS RAM .

Services connexes

Le partage des contacts et du plan de réponse s'intègre à AWS Resource Access Manager (AWS RAM). Avec AWS RAM, vous pouvez partager vos AWS ressources avec n'importe qui Compte AWS ou via AWS Organizations. Vous partagez les ressources que vous possédez en créant un partage de ressources. Un partage de ressources spécifie les ressources à partager, ainsi que les

consommateurs avec qui elles seront partagées. Les consommateurs peuvent être des individus Comptes AWS, des unités organisationnelles ou une organisation entière AWS Organizations.

Pour plus d'informations AWS RAM, consultez le guide de AWS RAM l'utilisateur.

Partage d'un contact ou d'un plan de réponse

Une fois que vous avez partagé un plan de réponse, les consommateurs ont accès à tous les incidents passés, actuels et futurs créés à l'aide de ce plan d'intervention.

Une fois que vous avez partagé un contact, les consommateurs ont accès aux informations de contact, au plan d'engagement, aux plans d'escalade et aux engagements pris lors d'un incident. Les consommateurs peuvent également établir un plan de contact ou d'escalade lors d'un incident.

Si vous faites partie d'une organisation AWS Organizations et que le partage au sein de votre organisation est activé, les clients de votre organisation ont automatiquement accès au contact partagé ou au plan de réponse. Dans le cas contraire, les consommateurs reçoivent une invitation à rejoindre le partage de ressources et ont accès au contact partagé ou au plan de réponse après avoir accepté l'invitation.

Vous pouvez partager un contact ou un plan de réponse dont vous êtes propriétaire à l'aide de la AWS RAM console ou du AWS CLI.

> **Note**
>
> Actuellement, la possibilité d'ajouter un contact partagé depuis un autre compte à un plan de réponse n'est pas prise en charge.

Pour partager un contact ou un plan de réponse dont vous êtes propriétaire à l'aide de la AWS RAM console

Consultez Création d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Pour partager un contact ou un plan de réponse dont vous êtes propriétaire à l'aide du AWS CLI

Utilisez la commande create-resource-share.

Arrêter de partager un contact partagé ou un plan de réponse

Lorsqu'un propriétaire de ressource arrête de partager un contact ou un plan de réponse avec un consommateur, les contacts, les plans de réponse, les plans d'escalade, les engagements et les incidents n'apparaissent plus dans la console du consommateur.

> **Note**
>
> Le consommateur continue de voir les contacts, les plans de réponse, les plans d'escalade, les engagements ou les incidents sans mise à jour, s'il les consulte dans la console, jusqu'à ce qu'il actualise la page ou qu'il quitte la page.

Pour arrêter de partager un contact partagé ou un plan de réponse dont vous êtes le propriétaire, vous devez le supprimer du partage de ressources. Vous pouvez le faire à l'aide de la AWS RAM console ou du AWS CLI.

Pour arrêter de partager un contact partagé ou un plan de réponse dont vous êtes le propriétaire à l'aide de la AWS RAM console

Consultez Mise à jour d'un partage de ressources dans le Guide de l'utilisateur AWS RAM .

Pour arrêter de partager un contact partagé ou un plan de réponse dont vous êtes le propriétaire en utilisant le AWS CLI

Utilisez la commande disassociate-resource-share.

Identification d'un contact partagé ou d'un plan de réponse

Les propriétaires et les consommateurs peuvent identifier les contacts partagés et les plans de réponse à l'aide de la console Incident Manager et AWS CLI.

Pour identifier un contact partagé ou un plan de réponse à l'aide de la console Incident Manager

> **Note**
>
> Les contacts, les plans de réponse, les plans d'escalade, les engagements et les incidents ne sont généralement pas identifiables en tant que ressource partagée dans la console Incident Manager. Aux endroits où le nom de ressource Amazon (ARN) est visible, l'ARN contient l'ID de compte du propriétaire.

Pour identifier un contact partagé ou un plan de réponse à l'aide du AWS CLI

Utilisez les ListContactscommandes ListResponsePlansou. La commande renvoie les contacts et les plans de réponse que vous possédez, ainsi que les contacts et les plans de réponse partagés avec vous. L'ARN indique l' Compte AWS ID du contact ou du propriétaire du plan de réponse.

Autorisations de contact partagé et de plan de réponse

Autorisations accordées aux propriétaires

Les propriétaires peuvent mettre à jour, consulter, partager, arrêter de partager et utiliser les contacts et les plans de réponse. Les contacts et les plans d'intervention incluent les engagements et les incidents connexes.

Autorisations accordées aux consommateurs

Les consommateurs ne peuvent utiliser et consulter que les plans de réponse et les contacts. Les contacts et les plans d'intervention incluent les engagements et les incidents connexes.

Facturation et mesures

Le propriétaire de la ressource est facturé pour la ressource. Les consommateurs ne sont pas facturés pour les ressources partagées avec eux. Le partage d'une ressource n'entraîne aucun coût supplémentaire.

Limites d'instance

Le partage d'une ressource n'a aucune incidence sur les limites de la ressource sur le compte du propriétaire ou du consommateur. Seul le compte du propriétaire est utilisé pour calculer les limites de la ressource.

Validation de conformité pour AWS Systems Manager Incident Manager

Des auditeurs tiers évaluent la sécurité et AWS Systems Manager Incident Manager la conformité de plusieurs programmes de AWS conformité. Il s'agit notamment des certifications SOC, PCI, FedRAMP, HIPAA et d'autres.

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de

conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Conformité et gouvernance de la sécurité : ces guides de mise en œuvre de solutions traitent des considérations architecturales et fournissent les étapes à suivre afin de déployer des fonctionnalités de sécurité et de conformité.
- Référence des services éligibles HIPAA : liste les services éligibles HIPAA. Tous ne Services AWS sont pas éligibles à la loi HIPAA.
- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST), le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).
- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.

- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Résilience dans AWS Systems Manager Incident Manager

L'infrastructure AWS mondiale est construite autour des AWS régions et des zones de disponibilité. AWS Les régions fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant. Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d'une zone à l'autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l'échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Incident Manager est un service mondial-régional qui ne prend actuellement pas en charge les zones de disponibilité.

Outre l'infrastructure AWS globale, Incident Manager propose plusieurs fonctionnalités pour répondre à vos besoins en matière de résilience et de sauvegarde des données. Au cours de l'assistant de préparation, il vous est demandé de configurer un ensemble de réplication. Cet ensemble de réplication régional garantit que vos données et ressources sont accessibles depuis plusieurs régions, ce qui facilite la gestion des incidents sur un réseau cloud. Cette réplication garantit également la sécurité et l'accessibilité de vos données en cas de panne de l'une de vos régions.

Pour plus d'informations sur l'utilisation du jeu de réplication Incident Manager, consultezConfiguration du jeu de réplication Incident Manager.

Sécurité de l'infrastructure dans AWS Systems Manager Incident Manager

En tant que service géré, AWS Systems Manager Incident Manager il est protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de

l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à Incident Manager via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Utilisation AWS Systems Manager Incident Manager et interface avec les points de terminaison VPC ()AWS PrivateLink

Vous pouvez établir une connexion privée entre votre VPC et créer un point de AWS Systems Manager Incident Manager terminaison VPC d'interface. Les points de terminaison d'interface sont alimentés par AWS PrivateLink. Avec AWS PrivateLink, vous pouvez accéder en privé aux opérations de l'API Incident Manager sans passerelle Internet, appareil NAT, connexion VPN ou AWS Direct Connect connexion. Les instances de votre VPC n'ont pas besoin d'adresses IP publiques pour communiquer avec les opérations de l'API Incident Manager. Le trafic entre votre VPC et Incident Manager reste sur le réseau Amazon.

Chaque point de terminaison d'interface est représenté par une ou plusieurs interfaces réseau Elastic dans vos sous-réseaux.

Pour de plus amples informations, consultez Points de terminaison VPC (AWS PrivateLink) dans le Guide de l'utilisateur Amazon VPC.

Considérations relatives aux points de terminaison VPC Incident Manager

Avant de configurer un point de terminaison VPC d'interface pour Incident Manager, assurez-vous de consulter les propriétés, les limites et les AWS PrivateLink quotas du point de terminaison d'interface dans le guide de l'utilisateur Amazon VPC.

Incident Manager permet d'appeler toutes ses actions d'API depuis votre VPC. Pour utiliser l'intégralité d'Incident Manager, vous devez créer deux points de terminaison VPC : un pour `ssm-incidents` et un pour. `ssm-contacts`

Création d'un point de terminaison VPC d'interface pour Incident Manager

Vous pouvez créer un point de terminaison VPC pour Incident Manager à l'aide de la console Amazon VPC ou du (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Création d'un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Créez un point de terminaison VPC pour Incident Manager en utilisant les noms de service pris en charge pour Incident Manager dans votre. Région AWS Les exemples suivants montrent les formats de point de terminaison d'interface pour les points IPv4 de terminaison à double pile.

IPv4 formats des terminaux

- `com.amazonaws.region.ssm-incidents`
- `com.amazonaws.region.ssm-contacts`

Formats à double pile (IPv4 et IPv6) de point de terminaison

- `aws.api.region.ssm-incidents`
- `aws.api.region.ssm-contacts`

Pour obtenir la liste des points de terminaison pris en charge pour toutes les régions, consultez la section Points de terminaison et quotas d'AWS Systems Manager Incident Manager dans le Guide de référence AWS général.

Si vous activez le DNS privé pour le point de terminaison de l'interface, vous pouvez envoyer des demandes d'API à Incident Manager en utilisant ses noms DNS régionaux par défaut au format. Les exemples suivants montrent le format des noms DNS régionaux par défaut.

- `ssm-incidents.region.amazonaws.com`
- `ssm-contacts.region.amazonaws.com`

Pour plus d'informations, consultez Accès à un service via un point de terminaison d'interface dans le Guide de l'utilisateur Amazon VPC.

Création d'une politique de point de terminaison VPC pour Incident Manager

Vous pouvez associer une politique de point de terminaison à votre point de terminaison VPC qui contrôle l'accès à Incident Manager. La politique spécifie les informations suivantes :

- Le principal qui peut exécuter des actions.
- Les actions qui peuvent être effectuées.
- Les ressources sur lesquelles ces actions peuvent être effectuées.

Pour plus d'informations, consultez Contrôle de l'accès aux services avec points de terminaison d'un VPC dans le Guide de l'utilisateur Amazon VPC.

Exemple : politique de point de terminaison VPC pour les actions du gestionnaire d'incidents

Voici un exemple de politique de point de terminaison pour Incident Manager. Lorsqu'elle est attachée à un point de terminaison, cette politique accorde l'accès aux actions répertoriées du gestionnaire d'incidents à tous les principaux sur toutes les ressources.

```
{
   "Statement":[
      {
         "Principal":"*",
         "Effect":"Allow",
         "Action":[
            "ssm-contacts:ListContacts",
            "ssm-incidents:ListResponsePlans",
            "ssm-incidents:StartIncident"
         ],
         "Resource":"*"
      }
   ]
}
```

Analyse de la configuration et des vulnérabilités dans Incident Manager

La configuration et les contrôles informatiques sont une responsabilité partagée entre vous AWS et vous, notre client. Pour plus d'informations, consultez le modèle de responsabilité AWS partagée.

Bonnes pratiques en matière de sécurité dans AWS Systems Manager Incident Manager

AWS Systems Manager Incident Manager fournit de nombreuses fonctionnalités de sécurité à prendre en compte lors de l'élaboration et de la mise en œuvre de vos propres politiques de sécurité. Les bonnes pratiques suivantes doivent être considérées comme des instructions générales et ne représentent pas une solution de sécurité complète. Étant donné que ces bonnes pratiques peuvent ne pas être appropriées ou suffisantes pour votre environnement, considérez-les comme des remarques utiles plutôt que comme des recommandations.

Rubriques

Bonnes pratiques de sécurité préventive pour Incident Manager

Implémentation d'un accès sur la base du moindre privilège

Lorsque vous accordez des autorisations, vous décidez qui obtient quelles autorisations à quelles ressources Incident Manager. Vous activez des actions spécifiques que vous souhaitez autoriser sur ces ressources. Par conséquent, accordez uniquement les autorisations nécessaires à l'exécution d'une tâche. L'implémentation d'un accès sur la base du moindre privilège est fondamentale pour réduire les risques en matière de sécurité et l'impact que pourraient avoir des d'erreurs ou des actes de malveillance.

Les outils suivants sont disponibles pour l'implémentation d'un accès sur la base du moindre privilège :

- Contrôle de l'accès aux AWS ressources à l'aide de politiques et de limites d'autorisations pour les entités IAM
- Politiques de contrôle de service

Création et gestion de contacts

Lors de l'activation des contacts, Incident Manager contacte l'appareil pour confirmer l'activation. Assurez-vous que les informations de l'appareil sont correctes avant de l'activer. Cela réduit le risque qu'Incident Manager contacte le mauvais appareil ou la mauvaise personne lors de l'activation.

Passez régulièrement en revue vos contacts et vos plans d'escalade pour vous assurer que seuls les contacts devant être contactés lors d'un incident sont contactés. Passez régulièrement en revue les contacts pour supprimer les informations périmées ou incorrectes. Si un contact ne doit plus être informé lorsqu'un incident survient, supprimez-le des plans d'escalade correspondants ou retirez-le du gestionnaire d'incidents.

Rendre les canaux de discussion privés

Vous pouvez rendre vos canaux de discussion sur les incidents privés afin de mettre en œuvre l'accès avec le moindre privilège. Envisagez d'utiliser un canal de discussion différent avec une liste d'utilisateurs détaillée pour chaque modèle de plan de réponse. Cela garantit que seuls les bons intervenants sont redirigés vers un canal de discussion susceptible de contenir des informations sensibles.

Slack les canaux créés dans Amazon Q Developer dans les applications de chat héritent des autorisations du rôle IAM utilisé pour configurer Amazon Q Developer dans les applications de chat. Cela permet aux répondeurs d'un développeur Amazon Q d'activer les applications de chat Slack canal pour appeler toute action répertoriée comme autorisée, telle que le gestionnaire d'incidents APIs et la récupération de graphiques de mesures.

Maintenir AWS les outils à jour

AWS publie régulièrement des versions mises à jour d'outils et de plugins que vous pouvez utiliser dans le cadre de vos AWS opérations. La mise à jour de ces ressources garantit que les utilisateurs et les instances de votre compte ont accès aux fonctionnalités et aux fonctions de sécurité les plus récentes de ces outils.

- AWS CLI — The AWS Command Line Interface (AWS CLI) est un outil open source qui vous permet d'interagir avec les AWS services à l'aide de commandes dans votre interface de ligne de commande. Pour mettre à jour l' AWS CLI, vous exécutez la même commande que pour installer l' AWS CLI. Nous vous recommandons de créer une tâche planifiée sur votre ordinateur local pour exécuter la commande appropriée pour votre système d'exploitation au moins une fois toutes les deux semaines. Pour plus d'informations sur les commandes d'installation, reportez-vous à la section Installation de l'interface de ligne de AWS commande dans le Guide de l'utilisateur de l'interface de ligne de AWS commande.
- AWS Tools for Windows PowerShell — Les outils pour Windows PowerShell sont un ensemble de PowerShell modules basés sur les fonctionnalités proposées par le AWS SDK pour .NET. Les outils pour Windows vous PowerShell permettent de scripter des opérations sur vos AWS ressources à partir de la ligne de PowerShell commande. Régulièrement, à mesure que des

versions mises à jour des Outils pour Windows PowerShell sont publiées, vous devez mettre à jour la version que vous exécutez localement. Pour plus d'informations, voir Mise à AWS Tools for Windows PowerShell jour du sous Windows ou Mise à AWS Tools for Windows PowerShell jour du sous Linux ou macOS.

Contenu connexe

Bonnes pratiques de sécurité pour Systems Manager

Les meilleures pratiques de Detective en matière de sécurité pour Incident Manager

Identifiez et auditez toutes les ressources de votre gestionnaire d'incidents

L'identification de vos ressources informatiques est un aspect crucial de la gouvernance et de la sécurité. Identifiez les ressources de vos Systems Manager pour évaluer leur niveau de sécurité et prendre des mesures en cas de points faibles potentiels. Créez des groupes de ressources pour les ressources de votre Incident Manager. Pour plus d'informations, consultez Que sont les groupes de ressources ? dans le Guide de l'utilisateur AWS Resource Groups .

Utiliser AWS CloudTrail

AWS CloudTrail fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans Incident Manager. À l'aide des informations collectées par AWS CloudTrail, vous pouvez déterminer la demande qui a été faite à Incident Manager, l'adresse IP à partir de laquelle la demande a été faite, qui a fait la demande, quand elle a été faite et des détails supplémentaires. Pour de plus amples informations, veuillez consulter Journalisation des appels AWS Systems Manager Incident Manager d'API à l'aide AWS CloudTrail.

Surveillez les avis AWS de sécurité

Consultez régulièrement les avis de sécurité publiés Trusted Advisor pour votre Compte AWS. Vous pouvez le faire par programmation en utilisant. describe-trusted-advisor-checks

De plus, surveillez activement l'adresse e-mail principale enregistrée pour chacun de vos Comptes AWS. AWS vous contactera, à l'aide de cette adresse e-mail, au sujet des problèmes de sécurité émergents susceptibles de vous affecter.

AWS les problèmes opérationnels ayant un impact important sont publiés sur le AWS Service Health Dashboard. Les problèmes opérationnels sont également publiés dans les comptes individuels via le

tableau de bord AWS Health Dashboard. Pour plus d'informations, consultez la documentation AWS Health.

Contenu connexe

Amazon Web Services : Présentation des procédures de sécurité (livre blanc)

Mise en route : suivez les meilleures pratiques de sécurité lors de la configuration de vos AWS ressources (blog sur AWS la sécurité)

Bonnes pratiques IAM

Bonnes pratiques en matière de sécurité dans AWS CloudTrail

Surveillance dans Incident Manager

AWS Systems Manager Incident Manager s'intègre aux services suivants qui offrent des fonctionnalités de surveillance et de journalisation :

CloudWatch métriques

Utilisez CloudWatch les métriques pour récupérer des statistiques sur les points de données pour les opérations de AWS Systems Manager Incident Manager sous la forme d'un ensemble ordonné de séries chronologiques, appelées métriques. Vous pouvez utiliser ces métriques pour vérifier que le système fonctionne comme prévu. Pour de plus amples informations, veuillez consulter Surveillance des métriques dans Incident Manager avec Amazon CloudWatch.

CloudTrail journaux

AWS CloudTrail À utiliser pour capturer des informations détaillées sur les appels passés à AWS APIs. Vous pouvez enregistrer ces appels sous forme de fichiers journaux dans Amazon Simple Storage Service. Vous pouvez utiliser ces CloudTrail journaux pour déterminer des informations telles que l'appel a été effectué, l'adresse IP source d'où provient l'appel, l'auteur de l'appel et la date de l'appel. Les CloudTrail journaux contiennent des informations sur les appels aux actions d'API pour Incident Manager. Pour plus d'informations, consultezJournalisation des appels AWS Systems Manager Incident Manager d'API à l'aide AWS CloudTrail.

Trusted Advisor

AWS Trusted Advisor peut vous aider à surveiller vos AWS ressources afin d'améliorer les performances, la fiabilité, la sécurité et la rentabilité. Quatre Trusted Advisor chèques sont disponibles pour tous les utilisateurs ; plus de 50 chèques sont disponibles pour les utilisateurs disposant d'un plan de support Business ou Enterprise. Pour Incident Manager, Trusted Advisor vérifie que la configuration d'un ensemble de réplication en utilise plusieurs Région AWS pour prendre en charge le basculement et la réponse régionaux. Pour plus d'informations, consultez AWS Trusted Advisor dans le Guide de l'utilisateur AWS Support .

Surveillance des métriques dans Incident Manager avec Amazon CloudWatch

Incident Manager fournit des statistiques agrégées que vous pouvez surveiller sur Amazon CloudWatch. Vous pouvez utiliser ces indicateurs pour identifier les tendances en matière d'incidents et de plans de réponse.

Ces métriques incluent :

- Nombre d'incidents créés sur une période donnée
- Le temps nécessaire pour répondre à ces incidents et les résoudre
- Nombre d'incidents résolus

Vous pouvez surveiller les indicateurs d'Incident Manager afin de mieux comprendre votre état de santé opérationnel et de prendre des mesures pertinentes pour garantir l'excellence opérationnelle de votre réponse aux incidents. Les métriques d'Incident Manager sont disponibles dans toutes les régions d'Incident Manager. Vos statistiques pourront être consultées sur Amazon CloudWatch pour toutes les régions que vous avez spécifiées dans votre ensemble de réplication lors de l'intégration à Incident Manager. Vous pouvez consulter les statistiques publiées dans la région indiquant que des mesures ont été prises pour l'incident. Il n'y a aucun frais supplémentaire pour ces statistiques.

Sur la CloudWatch console, vous pouvez créer des tableaux de bord avec ces indicateurs pour :

- Mesurez et passez en revue votre charge d'incidents existante
- Vérifiez si votre charge d'incidents augmente, diminue ou reste la même
- Utilisez le gestionnaire d'incidents de manière plus efficace pour réduire la fréquence, la durée et l'impact de vos incidents

Cette page décrit les métriques d'Incident Manager disponibles sur la CloudWatch console.

> **Important**
>
> Pour un événement généré par le client, si la valeur source `TriggerDetails` est nommée à l'aide de caractères non ASCII, les statistiques relatives à l'événement ne seront pas indiquées dans les CloudWatch métriques Amazon, qui ne prennent pas en charge le texte

non ASCII. `sourcene` peut être fourni que par programmation, par exemple à l'aide d'un SDK ou du. AWS CLI

Incident Manager envoie les métriques suivantes à CloudWatch.

Métrique	Description
`NumberOfCreateIncidents`	Nombre d'incidents créés. Dimensions valides : [] (dimension vide), `[ResponsePlan ]`, [], `[Impact]`, `[,Source]`, `[ResponsePlan ,Impact]`, `[ResponseP lan ,Source]` Unité : nombre
`NumberOfResolveIncidents`	Nombre d'incidents résolus. Dimensions valides : [] (dimension vide), `[ResponsePlan ]`, [], `[Impact]`, `[,Source]`, `[ResponsePlan ,Impact]`, `[ResponseP lan ,Source]` Unité : nombre
`TimeToFirstAcknowledgement`	Décalage horaire entre l'heure de création de l'incident et l'heure à laquelle l'incident a été reconnu pour la première fois. Dimensions valides : [] (dimension vide), `[ResponsePlan ]`, [], `[Impact]`, `[,Source]`, `[ResponsePlan ,Impact]`, `[ResponseP lan ,Source]` Unité : secondes
`TimeToResolveIncident`	Décalage horaire entre le moment où l'incident a été créé et celui où il a été résolu.

Métrique	Description
	Dimensions valides :] (dimension vide), [`ResponsePlan `], [], [`Impact`], [,`Source`], [`ResponsePlan ,Impact`], [`ResponsePlan ,Source`] Unité : secondes

Afficher les métriques d'Incident Manager sur la CloudWatch console

Pour consulter les métriques d'Incident Manager dans la CloudWatch console

1. Ouvrez la CloudWatch console à l'adresse https://console.aws.amazon.com/cloudwatch/.
2. Dans le panneau de navigation, sélectionnez Métriques.
3. Sélectionnez l'espace de noms `IncidentManager`.
4. Dans l'onglet Mesures, choisissez une dimension, puis choisissez une métrique.

Pour plus d'informations sur l'utilisation des CloudWatch métriques, consultez les rubriques suivantes du guide de CloudWatch l'utilisateur Amazon :

- Métriques
- Utilisation des CloudWatch métriques Amazon

Dimensions pour les métriques

Les métriques d'Incident Manager utilisent l'`IncidentManager`espace de noms et fournissent des métriques pour les dimensions suivantes :

Dimension	Description
`By Response Plan`	Affichez les statistiques agrégées par plan de réponse.
`By Impact Level`	Affichez les métriques agrégées par niveau de gravité.

Dimension	Description
`By Source`	Consultez les métriques des incidents créés manuellement, par CloudWatch alarme ou par EventBridge événement.
`Across All Incidents`	Consultez les statistiques agrégées pour tous les incidents dans la AWS région actuelle.
`Response Plan name and Source`	Consultez les statistiques agrégées pour chaque combinaison de plan de réponse et de source.
`Response Plan Name and Impact Level`	Consultez les mesures agrégées pour chaque combinaison de plan de réponse et de niveau de gravité.

Journalisation des appels AWS Systems Manager Incident Manager d'API à l'aide AWS CloudTrail

AWS Systems Manager Incident Manager est intégré à AWS CloudTrailun service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un Service AWS. CloudTrail capture tous les appels d'API pour Incident Manager sous forme d'événements. Les appels capturés incluent des appels provenant de la console Incident Manager et des appels de code vers les opérations de l'API Incident Manager. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite à Incident Manager, l'adresse IP à partir de laquelle la demande a été faite, la date à laquelle elle a été faite et des informations supplémentaires.

Chaque événement ou entrée de journal contient des informations sur la personne ayant initié la demande. Les informations relatives à l'identité permettent de déterminer :

- Si la demande a été effectuée avec des informations d'identification d'utilisateur root ou d'utilisateur root.
- Si la demande a été faite au nom d'un utilisateur du centre d'identité IAM.
- Si la demande a été effectuée avec les informations d'identification de sécurité temporaires d'un rôle ou d'un utilisateur fédéré.
- Si la requête a été effectuée par un autre Service AWS.

CloudTrail est actif dans votre compte Compte AWS lorsque vous créez le compte et vous avez automatiquement accès à l'historique des CloudTrail événements. L'historique des CloudTrail événements fournit un enregistrement consultable, consultable, téléchargeable et immuable des 90 derniers jours des événements de gestion enregistrés dans un. Région AWS Pour plus d'informations, consultez la section Utilisation de l'historique des CloudTrail événements dans le guide de AWS CloudTrail l'utilisateur. La consultation de CloudTrail l'historique des événements est gratuite.

Pour un enregistrement continu des événements de vos 90 Compte AWS derniers jours, créez un magasin de données sur les événements de Trail ou CloudTrailLake.

CloudTrail sentiers

Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Tous les sentiers créés à l'aide du AWS Management Console sont multirégionaux. Vous ne pouvez créer un journal de suivi en une ou plusieurs régions à l'aide de l' AWS CLI. Il est recommandé de créer un parcours multirégional, car vous capturez l'activité dans l'ensemble Régions AWS de votre compte. Si vous créez un journal de suivi pour une seule région, il convient de n'afficher que les événements enregistrés dans le journal de suivi pour une seule région Région AWS. Pour plus d'informations sur les journaux de suivi, consultez Créez un journal de suivi dans vos Compte AWS et Création d'un journal de suivi pour une organisation dans le AWS CloudTrail Guide de l'utilisateur.

Vous pouvez envoyer une copie de vos événements de gestion en cours à votre compartiment Amazon S3 gratuitement CloudTrail en créant un journal. Toutefois, des frais de stockage Amazon S3 sont facturés. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification. Pour obtenir des informations sur la tarification Amazon S3, consultez Tarification Amazon S3.

CloudTrail Stockages de données sur les événements du lac

CloudTrail Lake vous permet d'exécuter des requêtes SQL sur vos événements. CloudTrail Lake convertit les événements existants au format JSON basé sur les lignes au format Apache ORC. ORC est un format de stockage en colonnes qui est optimisé pour une récupération rapide des données. Les événements sont agrégés dans des magasins de données d'événement. Ceux-ci constituent des collections immuables d'événements basées sur des critères que vous sélectionnez en appliquant des sélecteurs d'événements avancés. Les sélecteurs que vous appliquez à un magasin de données d'événement contrôlent les événements qui persistent et

que vous pouvez interroger. Pour plus d'informations sur CloudTrail Lake, consultez la section Travailler avec AWS CloudTrail Lake dans le guide de AWS CloudTrail l'utilisateur.

CloudTrail Les stockages et requêtes de données sur les événements de Lake entraînent des coûts. Lorsque vous créez un magasin de données d'événement, vous choisissez l'option de tarification que vous voulez utiliser pour le magasin de données d'événement. L'option de tarification détermine le coût d'ingestion et de stockage des événements, ainsi que les périodes de conservation par défaut et maximale pour le magasin de données d'événement. Pour plus d'informations sur la CloudTrail tarification, consultez la section AWS CloudTrail Tarification.

Événements de gestion d'Incident Manager dans CloudTrail

Les événements de gestion fournissent des informations sur les opérations de gestion effectuées sur les ressources de votre Compte AWS. Ils sont également connus sous le nom opérations de plan de contrôle. Par défaut, CloudTrail enregistre les événements de gestion.

AWS Systems Manager Incident Manager enregistre toutes les opérations du plan de contrôle d'Incident Manager en tant qu'événements de gestion. Pour obtenir la liste des opérations du plan de AWS Systems Manager Incident Manager contrôle auxquelles Incident Manager se connecte CloudTrail, consultez la référence des AWS Systems Manager Incident Manager API.

Exemples d'événements Incident Manager

Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'opération d'API demandée, la date et l'heure de l'opération, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics. Les événements n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`StartIncident`action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
```

```
    "eventTime": "2024-04-22T23:20:10Z",
    "eventSource": "ssm-incidents.amazonaws.com",
    "eventName": "StartIncident",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
    "userAgent": "aws-cli/2.0.58 Python/3.7.4 Darwin/19.6.0 exe/x86_64 command/
ssmincidents.start-incident",
    "requestParameters": {
        "responsePlanArn": "arn:aws:ssm-incidents::555555555555:response-plan/security-
test-response-plan-non-dedupe-v1",
        "clientToken": "12345678-1111-2222-3333-abcdefghijkl"
    },
    "responseElements": {
        "incidentRecordArn": "arn:aws:ssm-incidents::444455556666:incident-record/
security-test-response-plan-non-dedupe-v1/abcdefgh-abcd-1234-1234-1234567890"
    },
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```


L'exemple suivant montre une entrée de CloudTrail journal illustrant l'`DeleteContactChannel`action.


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "IAMUser",
        "principalId": "1234567890abcdef0",
        "arn": "arn:aws:iam::246873129580111122223333:user/nikki_wolf",
        "accountId": "abcdef01234567890",
        "accessKeyId": "021345abcdef6789",
        "userName": "nikki_wolf"
    },
    "eventTime": "2024-04-08T02:27:21Z",
    "eventSource": "ssm-contacts.amazonaws.com",
    "eventName": "DeleteContactChannel",
    "awsRegion": "us-east-2",
    "sourceIPAddress": "192.0.2.0",
```

```
    "userAgent": "Apache-HttpClient/UNAVAILABLE (Java/1.8.0_282)",
    "requestParameters": {
        "contactChannelId": "arn:aws:ssm-contacts:us-west-2:555555555555:device/
bnuomysohc/abcdefgh-abcd-1234-1234-1234567890"
    },
    "responseElements": null,
    "requestID": "abcdefgh-1234-abcd-1234-1234567abcdef",
    "eventID": "12345678-1234-1234-abcd-abcdef1234567",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "eventCategory": "Management",
    "recipientAccountId": "12345678901234567"
}
```


Pour plus d'informations sur le contenu des CloudTrail enregistrements, voir le contenu des CloudTrail enregistrements dans le Guide de AWS CloudTrail l'utilisateur.

Intégrations de produits et de services avec Incident Manager

Incident Manager, un outil intégré AWS Systems Manager, s'intègre aux produits, services et outils suivants.

Intégration avec Services AWS

Incident Manager s'intègre aux outils Services AWS et décrits dans le tableau suivant.

AWS CDK	AWS CDK Il s'agit d'un framework de développement permettant d'utiliser du code pour définir votre infrastructure cloud et de l'utiliser AWS CloudFormation pour le provision nement. Il AWS CDK prend en charge plusieurs langages de programmation TypeScript, notamment JavaScript, Python, Java, et C#/ Net. Pour plus d'informations sur l'utilisation de AWS CDK with Incident Manager, consultez les sections suivantes de la référence des AWS CDK API : • @aws-cdk/aws-ssmincidents module • @aws-cdk/aws-ssmcontacts module
Amazon Q Developer dans les applications de chat	Amazon Q Developer dans les applications de chat permet aux équipes de développe ment de logiciels DevOps et aux équipes de développement de logiciels d'utiliser les forums de discussion des programmes de messageri e pour surveiller et répondre aux événement s opérationnels qui se produisent dans leurs applications AWS Cloud.

	En utilisant Amazon Q Developer dans les applications de chat avec Incident Manager, vous pouvez créer des canaux de discussio n que les intervenants peuvent utiliser pour surveiller les incidents et y répondre. Supports d'Amazon Q Developer dans les applications de chat Slack salons de discussion, Microsoft Teams canaux et salons de discussion Amazon Chime en tant que canaux de discussion. Dans le cadre de la création d'un canal de discussion, vous créez également un sujet dans Amazon Simple Notification Service (Amazon SNS). Amazon SNS est un service géré qui fournit des messages aux abonnés par les éditeurs. Dans les plans de réponse aux incidents, lorsque vous associez un canal de discussion que vous avez créé au plan, vous choisissez également un ou plusieurs sujets que vous avez associés au canal de discussion. Ces rubriques SNS sont utilisées pour envoyer des notifications concernant un incident aux intervenants en cas d'incident. Pour de plus amples informations, veuillez consulter Création et intégration de canaux de discussion pour les intervenants dans Incident Manager.

AWS CloudFormation	AWS CloudFormation est un service que vous pouvez utiliser pour créer un modèle contenant toutes les ressources dont vous avez besoin pour votre application, puis pour configurer et approvisionner les ressources pour vous. Il configurera également toutes les dépendanc es, afin que vous puissiez vous concentrer davantage sur votre application et moins sur la gestion des ressources. Pour plus d'informations sur l'utilisation AWS CloudFormation avec Incident Manager, consultez les rubriques suivantes du guide de AWS CloudFormation l'utilisateur : • Référence du type de ressource Incident Manager • Contacts, type de ressource, référence de type de ressource

Amazon CloudWatch	CloudWatchsurveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez les utiliser CloudWatch pour collecter et suivre les métriques, qui sont des variables que vous pouvez mesurer pour vos ressources et vos applications. Vous pouvez configurer des CloudWatch alarmes pour créer des incidents dans Incident Manager. CloudWatch fonctionne avec Systems Manager et Incident Manager pour créer un incident à partir d'un modèle de plan de réponse lorsqu'une alarme passe en état d'alarme. Pour de plus amples informations, veuillez consulter Création automatique d'incidents à l'aide d' CloudWatch alarmes.
Amazon Chime	Amazon Chime est un espace de travail en ligne qui combine les réunions, le chat et les appels professionnels. Vous pouvez vous rencontrer, discuter et passer des appels professionnels au sein et en dehors de votre organisation à l'aide d'Amazon Chime. Vous pouvez intégrer une salle Amazon Chime aux opérations de votre gestionnaire d'incidents en créant un canal de discussion pour Amazon Chime dans Amazon Q Developer dans les applications de chat, puis en ajoutant ce canal à un plan de réponse. Pour de plus amples informations, veuillez consulter Création et intégration de canaux de discussion pour les intervenants dans Incident Manager.

Amazon EventBridge	EventBridgeest un service sans serveur qui utilise des événements pour connecter les composants de l'application, ce qui vous permet de créer plus facilement des applicati ons évolutives pilotées par des événements. Vous pouvez configurer EventBridge des règles pour surveiller les modèles d'événements dans vos AWS ressources et créer un incident dans Incident Manager lorsqu'un événement correspond à un modèle que vous avez défini. Vos règles peuvent surveiller les modèles d'événements dans des dizaines d'applications Services AWS et de services tiers. Pour de plus amples informations, veuillez consulter Création automatique d'incidents à partir d' EventBridge événements.
AWS Secrets Manager	Secrets Manager vous aide à gérer, à récupérer et à alterner les informations d'identif ication de base de données, les informations d'identification des applications, les OAuth jetons, les clés d'API et d'autres secrets tout au long de leur cycle de vie. Lorsque vous intégrez Incident Manager au PagerDuty service, vous créez un secret dans Secrets Manager qui contient vos PagerDuty informations d'identification. Pour de plus amples informations, veuillez consulter Stockage AWS Secrets Manager secret des informations d' PagerDuty accès.

AWS Systems Manager	Systems Manager est un hub d'opérations que vous pouvez utiliser pour visualiser et contrôler votre infrastructure d'applications, ainsi qu'une solution end-to-end de gestion sécurisée pour les environnements cloud. Les outils Systems Manager suivants s'intègrent directement à Incident Manager : • Automatisation : un manuel d'automatisation définit les actions que Systems Manager exécute sur vos AWS ressources. Dans Incident Manager, un runbook définit une série d'étapes automatisées et manuelles à suivre pour résoudre vos incidents. Pour plus d'informations sur la création de runbooks d'automatisation à utiliser avec Incident Manager, consultezIntégration des runbooks Systems Manager Automation dans Incident Manager pour remédier aux incidents. • OpsCenter— OpsCenter fournit un emplacement central où les ingénieurs des opérations et les professionnels de l'informatique peuvent gérer les éléments de travail opérationnels OpsItems, appelés, liés aux AWS ressources. Vous pouvez créer OpsItems directement à partir d'une analyse post-incident pour suivre les travaux connexes. Pour de plus amples informations, veuillez consulter Performing a post-incident analysis in Incident Manager.

AWS Trusted Advisor	Trusted Advisorest un outil disponible pour les AWS clients disposant d'un plan de support de base ou d'un plan de support pour développe urs. Trusted Advisor inspecte votre AWS environnement, puis émet des recommand ations lorsque des opportunités se présenten t pour économiser de l'argent, améliorer la disponibilité et les performances du système ou contribuer à combler les failles de sécurité. Pour Incident Manager, Trusted Advisor vérifie que la configuration d'un ensemble de réplication en utilise plusieurs Région AWS pour prendre en charge le basculement et la réponse régionaux.

Intégration à d'autres produits et services

Vous pouvez intégrer ou utiliser Incident Manager avec les services tiers décrits dans le tableau suivant.

Jira Cloud	À l'aide de Connecteur AWS Service Management, vous pouvez intégrer Incident Manager à Jira Cloud (Atlassian), une plateform e de flux de travail tierce basée sur le cloud. Après avoir configuré l'intégration avec Jira Cloud, lorsque vous créez un nouvel incident dans Incident Manager, l'intégration crée également l'incident dans Jira Cloud. Si vous mettez à jour un incident dans Incident Manager, celui-ci apporte ces mises à jour à l'incident correspondant dans Jira Cloud. Si vous résolvez un incident dans Incident Manager ou Jira Cloud, l'intégration résout

	l'incident dans les deux services en fonction des préférences que vous configurez. Pour plus d'informations, consultez la section Intégration AWS Systems Manager Incident Manager (Jira Cloud) dans le guide de l'Connect eur AWS Service Management administrateur.
Gestion des services Jira	À l'aide de Connecteur AWS Service Management, vous pouvez intégrer Incident Manager à Jira Service Management, une plateforme de flux de travail tierce basée sur le cloud. Après avoir configuré l'intégration avec Jira Service Management, lorsque vous créez un nouvel incident dans Incident Manager, l'intégra tion crée également l'incident dans Jira Service Management. Si vous mettez à jour un incident dans Incident Manager, celui-ci apporte ces mises à jour à l'incident correspondant dans Jira Service Management. Si vous résolvez un incident dans Incident Manager ou Jira Service Management, l'intégration résout l'incident dans les deux services en fonction des préférences que vous configurez. Pour plus d'informations, consultez la section Configuration de Jira Service Management dans le Guide de l'Connecteur AWS Service Management administrateur.

Microsoft Teams	Microsoft Teamsfournit des outils collaboratifs basés sur le cloud pour la messagerie d'équipe, les conférences audio et vidéo et le partage de fichiers. Vous pouvez intégrer un Microsoft Teams accédez aux opérations de votre Incident Manager en créant un canal de discussion pour Microsoft Team dans Amazon Q Developer dans les applications de chat, puis en ajoutant ce canal à un plan de réponse. Pour de plus amples informations, veuillez consulter Création et intégration de canaux de discussion pour les intervenants dans Incident Manager.

PagerDuty	PagerDutyest un outil de réponse aux incidents qui prend en charge les flux de travail de pagination et les politiques d'escalade. Lorsque vous intégrez Incident Manager à PagerDuty, vous pouvez ajouter un PagerDuty service à votre plan de réponse. Ensuite, un incident correspondant est créé PagerDuty chaque fois qu'un incident est créé dans Incident Manager. L'incident dans PagerDuty utilise le flux de travail de pagination et les politiques d'escalade que vous y avez définis en plus de ceux définis dans Incident Manager. PagerDutyjoint les événements chronologiques d'Incident Manager sous forme de notes sur votre incident. Pour intégrer Incident Manager à Incident Manager PagerDuty, vous devez d'abord créer un secret AWS Secrets Manager contenant vos PagerDuty informations d'identification. Pour plus d'informations sur l'ajout d'une clé d' PagerDuty API REST et d'autres informati ons requises dans un code secret AWS Secrets Manager, consultezStockage AWS Secrets Manager secret des informations d' PagerDuty accès. Pour plus d'informations sur l'ajout d'un PagerDuty service depuis votre PagerDuty compte à un plan de réponse dans Incident Manager, consultez les étapes relatives à l'intégration d'un PagerDuty service dans le plan de réponse dans la rubriqueCréation d'un plan de réponse.

ServiceNow	À l'aide de Connecteur AWS Service Management, vous pouvez intégrer Incident Manager à ServiceNowune plateforme de flux de travail tierce basée sur le cloud. Après avoir configuré l'intégration avec ServiceNow, lorsque vous créez un nouvel incident dans Incident Manager, l'intégration crée également ServiceNow l'incident dans. Si vous mettez à jour un incident dans Incident Manager, celui-ci apporte ces mises à jour à l'incident correspondant dans ServiceNo w. Si vous résolvez un incident dans Incident Manager ou ServiceNow, l'intégration résout l'incident dans les deux services en fonction des préférences que vous configurez. Pour plus d'informations, consultez la section Intégration AWS Systems Manager Incident Manager ServiceNow dans le guide de Connecteur AWS Service Management l'administrateur.

Slack	Slackfournit des outils collaboratifs basés sur le cloud pour la messagerie d'équipe, les conférences audio et vidéo et le partage de fichiers. Vous pouvez intégrer un Slack accédez aux opérations de votre Incident Manager en créant un canal de discussion pour Slack dans Amazon Q Developer dans les applications de chat, puis en ajoutant ce canal à un plan de réponse. Pour de plus amples informations, veuillez consulter Création et intégration de canaux de discussion pour les intervenants dans Incident Manager.

Terraforme	HashiCorp Terraform est un outil logiciel open source d'infrastructure en tant que code (IaC) qui fournit un flux de travail d'interface de ligne de commande (CLI) pour gérer divers services cloud. Pour Incident Manager, vous pouvez utiliser Terraform pour gérer ou fournir les éléments suivants : SSM Incident Manager Contacts et ressources • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Sources de données SSM Contacts • aws_ssmcontacts_contact • aws_ssmcontacts_contact_channel • aws_ssmcontacts_plan • aws_ssmcontacts_rotation Ressources du gestionnaire d'incidents SSM • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan Sources de données SSM Incident Manager • aws_ssmincidents_replication_set • aws_ssmincidents_response_plan

Stockage AWS Secrets Manager secret des informations d' PagerDuty accès

Une fois que vous avez activé l'intégration avec PagerDuty pour un plan de réponse, Incident Manager fonctionne de la PagerDuty manière suivante :

- Incident Manager crée un incident correspondant PagerDuty lorsque vous créez un nouvel incident dans Incident Manager.
- Le flux de travail de pagination et les politiques d'escalade que vous avez créés PagerDuty sont utilisés dans l' PagerDuty environnement. Cependant, Incident Manager n'importe pas votre PagerDuty configuration.
- Incident Manager publie les événements chronologiques sous forme de notes relatives à l'incident PagerDuty, dans la limite de 2 000 notes.
- Vous pouvez choisir de résoudre automatiquement les PagerDuty incidents lorsque vous résolvez l'incident correspondant dans Incident Manager.

Pour intégrer Incident Manager à Incident Manager PagerDuty, vous devez d'abord créer un secret AWS Secrets Manager contenant vos PagerDuty informations d'identification. Ils permettent à Incident Manager de communiquer avec votre PagerDuty service. Vous pouvez ensuite inclure un PagerDuty service dans les plans de réponse que vous créez dans Incident Manager.

Ce secret que vous créez dans Secrets Manager doit contenir, dans le format JSON approprié, les éléments suivants :

- Une clé d'API provenant de votre PagerDuty compte. Vous pouvez utiliser une clé d'API REST d'accès général ou une clé d'API REST User Token.
- Une adresse e-mail utilisateur valide provenant de votre PagerDuty sous-domaine.
- La région PagerDuty de service dans laquelle vous avez déployé votre sous-domaine.

> **Note**
>
> Tous les services d'un PagerDuty sous-domaine sont déployés dans la même région de service.

Prérequis

Avant de créer le secret dans Secrets Manager, assurez-vous que vous répondez aux exigences suivantes.

Clé KMS

Vous devez chiffrer le secret que vous créez avec une clé gérée par le client que vous avez créée dans AWS Key Management Service (AWS KMS). Vous spécifiez cette clé lorsque vous créez le secret qui stocke vos PagerDuty informations d'identification.

> **Important**
>
> Secrets Manager permet de chiffrer le secret avec un Clé gérée par AWS, mais ce mode de chiffrement n'est pas pris en charge.

La clé gérée par le client doit répondre aux exigences suivantes :

- Type de clé : choisissez Symetric.
- Utilisation de la clé : choisissez Chiffrer et déchiffrer.
- Régionalité : si vous souhaitez répliquer votre plan de réponse à plusieurs Régions AWS, assurez-vous de sélectionner la clé multirégionale.

Stratégie de clé

L'utilisateur qui configure le plan de réponse doit disposer d'une autorisation pour `kms:GenerateDataKey` et `kms:Decrypt` dans la politique basée sur les ressources de la clé. Le directeur du `ssm-incidents.amazonaws.com` service doit disposer d'une autorisation pour `kms:GenerateDataKey` et `kms:Decrypt` dans la politique basée sur les ressources de la clé.

La politique suivante décrit ces autorisations. Remplacez chaque *`user input placeholder`* par vos propres informations.

```
{
    "Version": "2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM user permissions",
            "Effect": "Allow",
```

```
            "Principal": {
                "AWS": "arn:aws:iam::account-id:root"
            },
            "Action": "kms:*",
            "Resource": "*"
        },
        {
            "Sid": "Allow creator of response plan to use the key",
            "Effect": "Allow",
            "Principal": {
                "AWS": "IAM_ARN_of_principal_creating_response_plan"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "Allow Incident Manager to use the key",
            "Effect": "Allow",
            "Principal": {
                "Service": "ssm-incidents.amazonaws.com"
            },
            "Action": [
                "kms:Decrypt",
                "kms:GenerateDataKey*"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour plus d'informations sur la création d'une nouvelle clé gérée par le client, consultez la section Création de clés KMS de chiffrement symétriques dans le guide du AWS Key Management Service développeur. Pour plus d'informations sur AWS KMS les clés, consultez la section AWS KMS Concepts.

Si une clé gérée par le client existante répond à toutes les exigences précédentes, vous pouvez modifier sa politique pour ajouter ces autorisations. Pour plus d'informations sur la mise à jour de la politique d'une clé gérée par le client, consultez la section Modification d'une politique clé dans le Guide du AWS Key Management Service développeur.

> **Tip**
>
> Vous pouvez spécifier une clé de condition pour limiter encore davantage l'accès. Par exemple, la politique suivante autorise l'accès via Secrets Manager dans la région USA Est (Ohio) (us-east-2) uniquement :

```
{
    "Sid": "Enable IM Permissions",
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": ["kms:Decrypt", "kms:GenerateDataKey*"],
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "kms:ViaService": "secretsmanager.us-east-2.amazonaws.com"
        }
    }
}
```

`GetSecretValue`autorisation

L'identité IAM (utilisateur, rôle ou groupe) qui crée le plan de réponse doit disposer de l'autorisation IAM. `secretsmanager:GetSecretValue`

Pour stocker les informations d' PagerDuty accès dans un AWS Secrets Manager secret

1. Suivez les étapes de l'étape 3a de la section Créer un AWS Secrets Manager secret dans le guide de AWS Secrets Manager l'utilisateur.
2. Pour l'étape 3b, pour les paires clé/valeur, procédez comme suit :
   - Choisissez l'onglet Plaintext.
   - Remplacez le contenu par défaut de la boîte par la structure JSON suivante :

```
{
    "pagerDutyToken": "pagerduty-token",
    "pagerDutyServiceRegion": "pagerduty-region",
    "pagerDutyFromEmail": "pagerduty-email"
```

```
}
```

- Dans l'exemple JSON que vous avez collé, remplacez le *placeholder values* comme suit :
  - *pagerduty-token*: valeur d'une clé d'API REST d'accès général ou d'une clé d'API REST à jeton utilisateur de votre PagerDuty compte.

    Pour des informations connexes, consultez la section Clés d'accès aux API dans la base de PagerDuty connaissances.
  - *pagerduty-region*: région de service du centre de PagerDuty données qui héberge votre PagerDuty sous-domaine.

    Pour des informations connexes, consultez la section Régions de service dans la base de PagerDuty connaissances.
  - *pagerduty-email*: adresse e-mail valide d'un utilisateur appartenant à votre PagerDuty sous-domaine.

    Pour des informations connexes, consultez la section Gestion des utilisateurs dans la base de PagerDuty connaissances.

  L'exemple suivant montre un secret JSON complet contenant les PagerDuty informations d'identification requises :

```
{
    "pagerDutyToken": "y_NbAkKc66ryYEXAMPLE",
    "pagerDutyServiceRegion": "US",
    "pagerDutyFromEmail": "JohnDoe@example.com"
}
```

3. À l'étape 3c, pour Clé de chiffrement, choisissez une clé gérée par le client que vous avez créée et qui répond aux exigences répertoriées dans la section Prérequis précédente.
4. À l'étape 4c, pour les autorisations relatives aux ressources, procédez comme suit :
   - Développez les autorisations relatives aux ressources.
   - Choisissez Modifier les autorisations.
   - Remplacez le contenu par défaut de la boîte de politique par la structure JSON suivante :

```
{
```

```
    "Effect": "Allow",
    "Principal": {
        "Service": "ssm-incidents.amazonaws.com"
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

- Choisissez Save (Enregistrer).

5. À l'étape 4d, pour Répliquer le secret, procédez comme suit si vous avez répliqué votre plan de réponse vers plusieurs : Région AWS
   - Développez le secret de réplication.
   - Pour Région AWS, sélectionnez la région dans laquelle vous avez répliqué votre plan de réponse.
   - Pour la clé de chiffrement, choisissez une clé gérée par le client que vous avez créée ou répliquée dans cette région et qui répond aux exigences répertoriées dans la section Conditions préalables.
   - Pour chaque élément supplémentaire Région AWS, choisissez Ajouter une région, puis sélectionnez le nom de la région et la clé gérée par le client.
6. Effectuez les étapes restantes de la section Créer un AWS Secrets Manager secret dans le guide de AWS Secrets Manager l'utilisateur.

Pour plus d'informations sur la façon d'ajouter un PagerDuty service à un flux de travail relatif aux incidents d'Incident Manager, voir Intégrer un PagerDuty service dans le plan de réponse de la rubriqueCréation d'un plan de réponse.

Informations connexes

Comment automatiser la réponse aux incidents avec PagerDuty et AWS Systems Manager Incident Manager (blog sur AWS Cloud les opérations et les migrations)

Chiffrement secret AWS Secrets Manager dans le guide de AWS Secrets Manager l'utilisateur

Résolution des problèmes liés à AWS Systems Manager Incident Manager

Si vous rencontrez des problèmes lors de l'utilisation de AWS Systems Manager Incident Manager, vous pouvez utiliser les informations suivantes pour les résoudre conformément à nos meilleures pratiques. Si les problèmes que vous rencontrez ne sont pas couverts par les informations suivantes, ou s'ils persistent après avoir essayé de les résoudre, contactez AWS Support.

Rubriques

Message d'erreur : `ValidationException – We were unable to validate the AWS Secrets Manager secret`

Problème 1 : L'identité AWS Identity and Access Management (IAM) (utilisateur, rôle ou groupe) qui crée le plan de réponse ne dispose pas de l'autorisation `secretsmanager:GetSecretValue` IAM. Les identités IAM doivent disposer de cette autorisation pour valider les secrets de Secrets Manager.

- Solution : ajoutez l'`secretsmanager:GetSecretValue`autorisation manquante à la politique IAM pour l'identité IAM qui crée le plan de réponse. Pour plus d'informations, consultez la section Ajout d'autorisations d'identité IAM (console) ou Ajout de politiques IAM (AWS CLI) dans le guide de l'utilisateur IAM.

Problème 2 : le secret n'est pas associé à une politique basée sur les ressources permettant à l'identité IAM d'exécuter l'`GetSecretValue`action, ou la politique basée sur les ressources refuse l'autorisation d'accès à l'identité.

- Solution : créez ou ajoutez une `Allow` déclaration à la politique basée sur les ressources du secret qui autorise l'identité `secrets:GetSecretValue` IAM. Ou, si vous utilisez une `Deny` instruction qui inclut l'identité IAM, mettez à jour la politique afin que l'identité puisse exécuter l'action. Pour plus d'informations, voir Associer une politique d'autorisation à un AWS Secrets Manager secret dans le Guide de AWS Secrets Manager l'utilisateur.

Problème 3 : Les secrets ne sont pas associés à une politique basée sur les ressources qui autorise l'accès au principal du service Incident Manager,. `ssm-incidents.amazonaws.com`

- Solution : créez ou mettez à jour la politique basée sur les ressources pour le secret et incluez l'autorisation suivante :

```
{
    "Effect": "Allow",
    "Principal": {
        "Service": ["ssm-incidents.amazonaws.com"]
    },
    "Action": "secretsmanager:GetSecretValue",
    "Resource": "*"
}
```

Problème 4 : La clé AWS KMS key sélectionnée pour chiffrer le secret n'est pas une clé gérée par le client, ou la clé gérée par le client sélectionnée ne fournit pas les autorisations `kms:Decrypt` IAM `kms:GenerateDataKey*` au responsable du service Incident Manager. Il se peut également que l'identité IAM qui crée le plan de réponse ne dispose pas de l'autorisation IAM. `GetSecretValue`

- Solution : Assurez-vous que vous répondez aux exigences décrites dans la section Conditions préalables de la rubriqueStockage AWS Secrets Manager secret des informations d' PagerDuty accès.

Problème 5 : L'ID du secret qui contient la clé d'API REST d'accès général ou la clé d'API REST du jeton d'utilisateur n'est pas valide.

- Solution : Assurez-vous d'avoir saisi correctement l'ID du secret de Secrets Manager, sans espace de fin. Vous devez travailler dans celui Région AWS qui stocke le secret que vous souhaitez utiliser. Vous ne pouvez pas utiliser un secret supprimé.

Problème 6 : Dans de rares cas, le service Secrets Manager peut rencontrer un problème ou le gestionnaire d'incidents peut avoir des difficultés à communiquer avec lui.

- Solution : Patientez quelques minutes, puis réessayez. Vérifiez les éventuels problèmes susceptibles AWS Health Dashboardd'affecter l'un ou l'autre des services.

Autres problèmes de résolution des problèmes

Si les étapes précédentes n'ont pas permis de résoudre votre problème, vous pouvez obtenir de l'aide supplémentaire en consultant les ressources suivantes :

- Pour les problèmes IAM spécifiques à Incident Manager lorsque vous accédez à la console Incident Manager, consultezRésolution des problèmes AWS Systems Manager Incident Manager d'identité et d'accès.
- Pour les problèmes généraux d'authentification et d'autorisation lorsque vous accédez au AWS Management Console, consultez la section Résolution des problèmes liés à l'IAM dans le guide de l'utilisateur IAM.

Historique des documents pour Incident Manager

Modification	Description	Date
Modification des exigences d'autorisation pour la création manuelle d'incidents	Les autorisations IAM requises pour qu'un utilisateur crée un incident manuellement ont changé et n'utilisent plus de rôle lié à un service. Incident Manager utilise désormais des sessions d'accès direct (FAS) pour appeler dans `ssm-contacts:StartEngagement` le cadre de `ssm-incidents:StartIncident` celles-ci. Pour plus d'informations, consultez la section Autorisations IAM requises pour démarrer manuellement des incidents.	10 juin 2025
Mise à jour de la politique gérée `AWSServiceRoleforIncidentManagerPolicy`	Incident Manager a ajouté une nouvelle autorisation `AWSServiceRoleforIncidentManagerPolicy` qui permet à Incident Manager de publier des métriques dans l'espace de `AWS/Usage` noms de votre compte. Pour plus d'informations, consultez la section Mises à jour des politiques AWS gérées par Incident Manager.	28 janvier 2025

Mise à jour de la politique gérée `AWSIncidentManagerIncidentAccessServiceRolePolicy`	Incident Manager a ajouté une nouvelle autorisation `AWSIncidentManagerIncidentAccessServiceRolePolicy`, à l'appui de la fonctionnalité Findings, qui lui permet de vérifier si une EC2 instance fait partie d'un groupe Auto Scaling. Pour plus d'informations, consultez la section Mises à jour des politiques AWS gérées par Incident Manager.	20 février 2024
Support HashiCorp Terraform supplémentaire : rotations sur appel	Terraform a renforcé son support pour Incident Manager. Vous pouvez désormais provisionner ou gérer les ressources sur appel d'Incident Manager à l'aide de Terraform. Pour plus d'informations à ce sujet et sur d'autres intégrations tierces avec Incident Manager, consultez la section Intégration à d'autres produits et services.	2 février 2024

Nouvelle fonctionnalité : résultats provenant d'autres Services AWS	Les résultats vous fournissent des informations sur les modifications liées aux AWS CloudFormation stacks et aux AWS CodeDeploy déploiements survenus à peu près au moment où un incident a été créé dans Incident Manager. Dans la console Incident Manager, vous pouvez consulter des informations récapitulatives sur ces modifications et, dans de nombreux cas, accéder à des liens vers les CodeDeploy consoles CloudFormation ou pour obtenir des informations complètes sur les modifications. Les résultats réduisent le temps nécessaire pour évaluer les causes potentielles des incidents. Ils réduisent également les risques que les intervenants accèdent au mauvais compte ou à la mauvaise console pour rechercher la cause d'un incident. Cette fonctionnalité introduit également une nouvelle politique géréeAWSIncidentManagerIncidentAccessServiceRolePolicy , qui permet à Incident Manager de lire des ressources dans d'autres Services AWS	15 novembre 2023

	afin d'identifier les résultats liés aux incidents. Pour plus d’informations, consultez les rubriques suivantes : • Travailler avec les résultats • AWS politique gérée : AWSIncidentManagerIncidentAccessServiceRolePolicy	
Listes mises à jour des intégrations avec Incident Manager	La rubrique Intégrations de produits et de services avec Incident Manager a été étendue pour répertorier et décrire tous les Services AWS outils tiers que vous pouvez intégrer à Incident Manager dans vos opérations de détection et de réponse aux incidents.	9 juin 2023

Intégration avec AWS Trusted Advisor	Trusted Advisor vérifie désormais que la configuration d'un ensemble de réplication en utilise plusieurs Région AWS pour prendre en charge le basculement et la réponse régionaux. Pour les incidents créés par des CloudWatch alarmes ou EventBridge des événements, Incident Manager crée un incident au même Région AWS titre que la règle d'alarme ou d'événement. Si la gestion des incidents est temporairement indisponible dans cette région, le système tente de créer un incident dans une autre région de l'ensemble de réplications. Si l'ensemble de réplications ne comprend qu'une seule région, le système ne pourra pas créer d'enregistrement d'incident tant que la gestion des incidents est indisponible. Pour éviter cette situation, Trusted Advisor indique lorsqu'un ensemble de réplication est configuré pour une seule région. Pour plus d'informations sur l'utilisation Trusted Advisor, consultez AWS Trusted Advisorle guide de AWS Support l'utilisateur.	28 avril 2023

Utilisation Microsoft Teams comme canal de discussion dans les plans de réponse	Grâce à l'intégration avec Microsoft Teams Amazon Q Developer dans les applications de chat, vous pouvez désormais utiliser Microsoft Teams le canal de chat dans vos plans de réponse. Cela s'ajoute à la prise en charge Slack des canaux de discussion Amazon Chime. Lors d'un incident, Incident Manager envoie des notifications de statut directement à un canal de discussion pour tenir tous les intervenants informés. Les intervenants peuvent également communiquer entre eux et avec des AWS CLI commandes relatives aux incidents dans l'Microsoft Teamsapplication pour mettre à jour les incidents et interagir avec eux. Pour plus d'informations, consultez la section Utilisation des canaux de discussion dans Incident Manager.	4 avril 2023

Nouvelle fonctionnalité : horaires d'astreinte	Un calendrier d'astreinte dans Incident Manager définit qui est averti lorsqu'un incident nécessitant l'intervention d'un opérateur survient. Un programme d'astreinte comprend une ou plusieurs rotations que vous créez pour le calendrier. Chaque rotation peut inclure jusqu'à 30 contacts. Après avoir créé un calendrier d'astreinte, vous pouvez l'inclure en tant qu'escalade dans votre plan d'escalade. Lorsqu'un incident associé à ce plan d'escalade se produit, Incident Manager en informe l'opérateur (ou les opérateurs) qui sont sur appel conformément au calendrier. Pour plus d'informations, consultez la section Utilisation des horaires d'astreinte dans Incident Manager.	28 mars 2023

Imprimez une analyse d'incident formatée ou enregistrez-la au format PDF	La page d'analyse des incidents inclut désormais un bouton Imprimer pour générer une version de l'analyse formatée pour l'impression. À l'aide des destinations d'impression configurées pour votre appareil, vous pouvez enregistrer l'analyse de l'incident au format PDF ou l'envoyer vers une imprimant e locale ou réseau. Pour plus d'informations, voir Imprimer une analyse d'incident formatée.	17 janvier 2023

PagerDuty intégration : Incident Manager copie désormais les événements chronologiques des PagerDuty incidents dans les incidents	Lorsque vous activez l'intégration PagerDuty dans un plan de réponse, Incident Manager ajoute les événements chronologiques créés à partir de ce plan à l'enregistrement d'incident correspondant dans PagerDuty. PagerDuty ajoute des événements chronologiques sous forme de notes sur l'incident, jusqu'à un maximum de 2 000 notes. Pour en savoir plus sur ces modifications, consultez les rubriques suivantes : • Stockez les informations d'PagerDuty accès en AWS Secrets Manager secret • Intégrer un PagerDuty service dans le plan de réponse	15 décembre 2022
Intégration du gestionnaire d'incidents aux CloudWatch métriques.	Vous pouvez désormais publier les statistiques relatives aux incidents dans. CloudWatch Pour plus d'informations, consultez la section CloudWatchMesures. AWSIncidentManager ServiceRolePolicy Il a inclus une autorisation supplémentaire permettant à notre service de publier des statistiques en votre nom.	15 décembre 2022

Lancement des notes d'incident et mise à jour de l'écran Détails de l'incident	Vous pouvez collaborer et communiquer avec d'autres utilisateurs qui travaillent sur un incident à l'aide des notes d'incident. En outre, vous pouvez consulter les runbooks et les statuts des engagements depuis l'écran Détails de l'incident. Pour plus d'informations, consultez la section Détails de l'incident.	16 novembre 2022

Intégrez des plans d' PagerDuty escalade et des workflows de pagination dans les plans de réponse d'Incident Manager	Vous pouvez désormais intégrer Incident Manager à un plan de réponse PagerDuty et y ajouter un PagerDuty service. Après avoir configuré l'intégration, Incident Manager peut créer un incident correspondant PagerDuty pour chaque nouvel incident créé dans Incident Manager. PagerDuty utilise le flux de travail de pagination et les politiques d'escalade que vous définissez dans l' PagerDuty environnement. Pour plus d’informations, consultez les rubriques suivantes : • Intégrations de produits et de services avec Incident Manager • Stockez les informations d' PagerDuty accès en AWS Secrets Manager secret • Intégrer un PagerDuty service dans le plan de réponse de la rubrique Création d'un plan de réponse • Dépannage	16 novembre 2022

Lancement des notes d'incident et mise à jour de l'écran Détails de l'incident.	Vous pouvez collaborer et communiquer avec d'autres utilisateurs qui travaillent sur un incident à l'aide des notes d'incident. En outre, vous pouvez consulter les runbooks et les statuts des engagements depuis l'écran Détails de l'incident. Pour plus d'informations, consultez la section Détails de l'incident.	16 novembre 2022
Support de balisage pour les ensembles de réplication	Vous pouvez désormais attribuer des balises à votre ensemble de réplication dans AWS Systems Manager Incident Manager. Cela s'ajoute à la prise en charge existante pour l'attribution de balises aux plans de réponse, aux enregistrements d'incidents et aux contacts dans les zones Régions AWS spécifiées dans votre ensemble de réplication. Pour plus d'informations, consultez les rubriques suivantes : • Préparez-vous, magicien • Marquage des ressources d'Incident Manager	2 novembre 2022

Intégration du gestionnaire d'incidents à Atlassian Jira Service Management	Vous pouvez intégrer Incident Manager à Jira Service Management en utilisant le connecteur de gestion des AWS services pour Jira Service Management. Après avoir configuré l'intégration, les nouveaux incidents créés dans Incident Manager créent un incident correspondant dans Jira. Si vous mettez à jour un incident dans Incident Manager, les mises à jour sont ajoutées à l'incident correspondant dans Jira. Si vous résolvez un incident dans Incident Manager ou Jira, l'incident correspon dant est également résolu, en fonction des préférenc es configurées. Pour plus d'informations, consultez la section Configuration de Jira Service Management dans le Guide de l'administrateur du AWS Service Management Connector.	6 octobre 2022

Support de balisage amélioré	Incident Manager prend en charge l'attribution de balises aux plans de réponse, aux enregistrements d'incidents et aux contacts Régions AWS spécifiés dans votre ensemble de réplication. Incident Manager prend également en charge l'attribution automatiq ue de balises aux incidents créés à partir des plans de réponse. Pour plus d'informa tions, consultez la section Marquage des ressources d'Incident Manager.	28 juin 2022

Intégration d'Incident Manager avec ServiceNow	Vous pouvez intégrer Incident Manager à ServiceNowl'aide du connecteur AWS de gestion des services pour ServiceNow. Après avoir configuré l'intégration, les nouveaux incidents créés dans Incident Manager créent un incident correspondant dans ServiceNow. Si vous mettez à jour un incident dans Incident Manager, les mises à jour sont ajoutées à l'incident correspondant dans ServiceNow. Si vous résolvez un incident dans Incident Manager ou ServiceNow, l'incident correspondant est également résolu, en fonction des préférences configuré es. Pour plus d'informations, consultez la section Intégrati on d' AWS Systems Manager Incident Manager dans ServiceNow.	9 juin 2022

Importer les coordonnées	Lorsqu'un incident est créé, Incident Manager peut informer les intervenants en utilisant des notifications vocales ou par SMS. Pour que les intervenants voient que la notification d'appel ou de SMS provient d'Incident Manager, nous recommandons à tous les intervenants de télécharger le fichier au format de carte virtuelle Incident Manager (.vcf) dans le carnet d'adresses de leurs appareils mobiles. Pour plus d'informations, voir Importer les coordonnées dans votre carnet d'adresses.	18 mai 2022

Améliorations de nombreuses fonctionnalités pour améliorer la création et la résolution des incidents	Incident Manager a apporté les améliorations suivantes aux fonctionnalités afin d'améliorer la création et la résolution des incidents : • Création automatique d'incidents dans d'autres régions Régions AWS : si le gestionnaire d'incidents n'est pas disponible Région AWS lorsqu'Amazon CloudWatch ou Amazon EventBridge créent un incident, ces services créent désormais automatiquement l'incident dans l'une des régions disponibles spécifiées dans votre ensemble de réplication. Pour plus d'informations, consultez la section Gestion des incidents entre régions. • Renseignez automatiquement les paramètres du runbook avec les métadonnées des incidents : vous pouvez désormais configurer Incident Manager pour collecter des informations sur les AWS ressources issues des incidents. Incident Manager peut ensuite renseigner les paramètres du runbook avec les informations collectée	17 mai 2022

	s. Pour plus d'informations, consultez Tutoriel : Utilisation des runbooks d'automatisation de Systems Manager avec Incident Manager. • Collecte automatique AWS des informations sur les ressources : lorsque le système crée un incident, Incident Manager collecte désormais automatiquement des informations sur les AWS ressources impliquées dans l'incident. Incident Manager ajoute ensuite ces informations à l'onglet Eléments associés.	
Support multi-runbook	Incident Manager prend désormais en charge l'exécution de plusieurs runbooks lors d'un incident pour la page de détails de l'incident.	14 janvier 2022
Incident Manager a été lancé dans un nouveau Régions AWS	Incident Manager est désormais disponible dans les nouvelles régions suivantes : us-west-1, sa-east-1, ap-northeast-2, ap-south-1, ca-central-1, eu-west-2 et eu-west-3. Pour plus d'informations sur les régions et les quotas d'Incident Manager, consultez le guide de Références générales AWS référence.	8 novembre 2021

Confirmation d'engagement sur la console	Vous pouvez désormais accuser réception des engagements directement depuis la console Incident Manager.	5 août 2021
Onglet Propriétés	Incident Manager a introduit un onglet de propriétés sur la page des détails de l'incident, fournissant plus d'informations sur les incidents OpsItem, le parent et l'analyse post-inci dent associée.	3 août 2021
Lancement d'Incident Manager	Incident Manager est une console de gestion des incidents conçue pour aider les utilisateurs à atténuer les incidents affectant leurs applications AWS hébergées et à s'en remettre.	10 mai 2021

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.