Guide de l’utilisateur

AWS Health

AWS Health: Guide de l’utilisateur

Table of Contents

Qu'est-ce que c'est AWS Health ?

AWS Health fournit une visibilité continue sur les performances de vos ressources et sur la disponibilité de vos comptes Services AWS et de vos comptes. Vous pouvez utiliser les AWS Health événements pour découvrir comment les modifications des services et des ressources peuvent affecter les applications qui s'exécutent sur celles-ci AWS. AWS Health fournit des informations pertinentes et actualisées pour vous aider à gérer les événements en cours. AWS Health vous aide également à connaître les activités planifiées et à vous y préparer. Le service fournit des alertes et des notifications déclenchées par des modifications de l'état des AWS ressources, de sorte que vous bénéficiez d'une visibilité quasi instantanée sur les événements et de conseils pour accélérer le dépannage.

Tous les clients peuvent utiliser le AWS Health Dashboard AWS , alimenté par l' AWS Health API. Le tableau de bord ne nécessite aucune configuration et est prêt à être utilisé par les AWS utilisateurs authentifiés. Pour en savoir plus sur les points forts du service, consultez la AWS Health page détaillée du de bord.

AWS Health fournit une console, appelée AWS Health tableau de bord, à tous les clients. Vous n'avez pas besoin d'écrire du code ou d'effectuer d'autres actions pour configurer le tableau de bord.

Pour connaître les bases AWS Health et les termes que vous rencontrerez lors de l'utilisation du service, pour comprendre les bases de AWS Health seeConcepts pour AWS Health.

Remarques

- Le AWS Health tableau de bord est disponible pour tous les AWS clients sans frais supplémentaires.
- Tous les AWS clients peuvent recevoir AWS Health des événements via Amazon EventBridge sans frais supplémentaires.
- Si vous avez un plan Business, Enterprise On-Ramp ou Enterprise Support, vous pouvez utiliser l' AWS Health API pour intégrer des systèmes internes et tiers. Pour plus d'informations, consultez la page Référence de l'API AWS Health.
- Pour plus d'informations sur AWS Support les forfaits disponibles, consultez AWS Support.

Concepts pour AWS Health

Découvrez AWS Health les concepts et comprenez comment vous pouvez utiliser le service pour maintenir l'intégrité de vos applications, services et ressources dans votre environnement Compte AWS.

Rubriques

AWS Health événement

AWS Health les événements, également appelés événements de santé, sont des notifications AWS Health envoyées pour le compte d'autres AWS services. Vous pouvez utiliser ces événements pour en savoir plus sur les modifications à venir ou planifiées susceptibles d'affecter votre compte. Par exemple, AWS Health peut envoyer un événement si AWS Identity and Access Management (IAM) prévoit de déprécier une politique gérée ou AWS Config prévoit de déprécier une règle gérée. AWS Health envoie également des événements en cas de problèmes de disponibilité des services dans un Région AWS. Vous pouvez consulter la description de l'événement pour comprendre le problème, identifier les ressources concernées et prendre les mesures recommandées.

Il existe deux types d'événements liés à la santé :

Table des matières

Événement spécifique au compte

Les événements spécifiques à un compte sont locaux, soit pour votre Compte AWS compte, soit pour un compte de votre AWS organisation. Par exemple, en cas de problème avec un type d'instance Amazon Elastic Compute Cloud (Amazon EC2) dans une région que vous utilisez AWS Health , fournissez des informations sur l'événement et le nom des ressources concernées.

Vous pouvez trouver les événements spécifiques à votre compte depuis votre AWS Health tableau de bord, l'AWS Health API, ou utiliser Amazon EventBridge ou les notifications des AWS utilisateurs pour recevoir des notifications.

Événement public

Les événements publics sont des événements de service signalés qui ne sont pas spécifiques à un compte. Par exemple, en cas de problème de service pour Amazon Simple Storage Service (Amazon S3) dans la région USA Est (Ohio), fournissez des informations sur l'événement AWS Health , même si vous n'utilisez pas ce service ou si vous possédez des compartiments S3 dans cette région. Nous vous recommandons de consulter les notifications publiques avant de prendre des mesures à leur sujet.

Vous pouvez trouver les événements publics dans votre AWS Health tableau de bord et dans le AWS Health tableau de bord — État des services.

Si vous avez un compte, consultezCommencer à utiliser votre AWS Health tableau de bord.

Si vous n'avez pas de compte, consultez AWS Health Tableau de bord.

AWS Health Tableau de bord

Si vous en avez un Compte AWS, votre AWS Health tableau de bord affiche à la fois les événements publics et les événements spécifiques au compte.

Nous vous recommandons d'utiliser votre AWS Health tableau de bord pour en savoir plus sur les événements présentant un intérêt général, tels qu'un problème de maintenance imminent pour un service dans une région. Vous pouvez également utiliser le AWS Health tableau de bord pour en savoir plus sur les événements susceptibles de vous affecter directement, tels qu'une ressource obsolète dans votre compte.

Vous pouvez vous connecter au AWS Management Console pour consulter votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.

Pour de plus amples informations, veuillez consulter Commencer à utiliser votre AWS Health tableau de bord.

AWS Health Tableau de bord — État des services

Si vous n'avez pas de compte, vous pouvez utiliser le AWS Health Dashboard — Service health at https://health.aws.amazon.com/health/status pour consulter les événements publics. Les événements publics sont des problèmes de service signalés AWS qui fournissent des informations sur la disponibilité des services. Ce site Web ne montre que les événements publics, qui ne sont spécifiques à aucun compte. Vous n'avez pas besoin de vous connecter ou d'avoir un compte pour consulter cette page.

Pour de plus amples informations, veuillez consulter AWS Health Tableau de bord.

Code du type d'événement

Les codes de type d'événement affichés lors d'un événement Health incluent le service concerné et le type d'événement. Par exemple, si vous recevez un événement Health dont le code est le type d'`AWS_EC2_SYSTEM_MAINTENANCE_EVENT`événement, cela signifie que le service planifie un événement de maintenance susceptible de vous affecter. Utilisez ces informations pour planifier à l'avance ou prendre des mesures pour votre compte.

Catégories de types d'événements

Tous les événements de santé sont associés à une catégorie de type d'événement. Pour certains événements, la catégorie du type d'événement peut apparaître dans le code du type d'événement, tel que le `AWS_RDS_MAINTENANCE_SCHEDULED` code. Dans cet exemple, la catégorie est planifiée. Vous pouvez utiliser ces informations pour comprendre les catégories d'événements à un niveau élevé.

Il est recommandé de surveiller toutes les catégories de types d'événements. Notez que chaque catégorie apparaît pour différents types d'événements. Vous pouvez également utiliser l'opération DescribeEventTypesAPI pour trouver la catégorie de type d'événement.

Notification du compte

> Ces événements fournissent des informations sur l'administration ou la sécurité de vos comptes et services. Ces événements peuvent être informatifs ou nécessiter une action urgente de votre part.

Nous vous recommandons de prêter attention à ces types d'événements et de passer en revue toutes les actions recommandées.

Voici des exemples de codes de type d'événement pour les notifications de compte :

- `AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION`— Vous disposez d'un compartiment Amazon S3 susceptible d'autoriser un accès public.
- `AWS_BILLING_SUSPENSION_NOTICE`— Votre compte a des frais impayés et a été suspendu, ou vous avez désactivé votre compte.
- `AWS_WORKSPACES_OPERATIONAL_NOTIFICATION`— Il y a un problème de service pour Amazon WorkSpaces.

Problème

Ces événements sont des événements inattendus qui affectent les AWS services ou les ressources. Les événements courants de cette catégorie incluent les communications relatives à des problèmes opérationnels à l'origine de la dégradation du service ou à des problèmes localisés liés au niveau des ressources destinés à votre attention.

Voici des exemples de codes de type d'événement relatifs à des problèmes :

- `AWS_EC2_OPERATIONAL_ISSUE`— Un problème opérationnel lié à un service, tel que des retards dans l'utilisation d'un service.
- `AWS_EC2_API_ISSUE`— Un problème opérationnel lié à l'API d'un service, tel qu'une latence accrue lors d'une opération d'API.
- `AWS_EBS_VOLUME_ATTACHMENT_ISSUE`— Un problème localisé au niveau des ressources susceptible d'affecter vos ressources Amazon Elastic Block Store (Amazon EBS).
- `AWS_ABUSE_PII_CONTENT_REMOVAL_REPORT`— Cet événement signifie que votre compte peut être suspendu si vous n'agissez pas.

Modification planifiée

Ces événements fournissent des informations sur les modifications à venir de vos services et ressources. Ces événements incluent les événements du cycle de vie planifiés tels que end-of-support les notifications et les mises à niveau automatiques pour les différentes versions. Certains événements peuvent vous recommander de prendre des mesures pour éviter les interruptions de service, tandis que d'autres se produiront automatiquement sans aucune action de votre part. Il est possible que votre ressource soit temporairement indisponible pendant l'activité de modification planifiée. Tous les événements de cette catégorie sont des événements spécifiques au compte.

Voici des exemples de codes de type d'événement pour les modifications planifiées :

- `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`— Une EC2 instance Amazon nécessite un redémarrage.
- `AWS_SAGEMAKER_SCHEDULED_MAINTENANCE`— SageMaker L'IA nécessite un événement de maintenance, tel que la résolution d'un problème de service.
- `AWS_RDS_PLANNED_LIFECYCLE_EVENT`— Amazon RDS planifie un événement du cycle de vie planifié, tel qu'un end-of-support événement pour l'une de ses versions, qui nécessite une action du client.

> **Tip**
>
> Si vous utilisez l' AWS Health API ou le AWS Command Line Interface (AWS CLI) pour renvoyer les détails de l'événement, l'`Event`objet contient le `eventScopeCode` champ contenant la `ACCOUNT_SPECIFIC` valeur. Pour plus d'informations, consultez la page Référence de l'API AWS Health.

État de l'événement

Le statut de l'événement vous indique si l'événement Health est ouvert, fermé ou à venir. Vous pouvez consulter les événements de santé dans le AWS Health tableau de bord ou dans l' AWS Health API pendant 90 jours maximum.

Entités affectées

Les entités affectées sont les AWS ressources susceptibles d'être affectées par l'événement. Par exemple, si vous recevez un événement planifié pour la EC2 maintenance d'Amazon pour un type d'instance spécifique que vous utilisez dans votre compte, vous pouvez utiliser l'événement Health pour déterminer l'ID des instances concernées. Utilisez ces informations pour résoudre tout problème de service potentiel, tel que la création ou la dépréciation de ressources.

AWS Health événements sur Amazon EventBridge

Vous pouvez configurer des EventBridge règles Amazon pour vos comptes afin d'automatiser les actions une fois que l' AWS Health événement approprié a été reçu par un compte. Il peut s'agir

d'actions générales, telles que l'envoi de tous les messages relatifs aux événements du cycle de vie planifiés vers une interface de chat. Il peut également s'agir d'actions spécifiques, telles que le déclenchement d'un flux de travail dans un outil de gestion des services informatiques.

Pour de plus amples informations, veuillez consulter Surveillance des événements AWS Health avec Amazon EventBridge.

AWS Health API

Vous pouvez utiliser l' AWS Health API pour accéder par programmation aux informations qui apparaissent dans le AWS Health tableau de bord, telles que les suivantes :

- Obtenez des informations sur les événements susceptibles d'affecter vos AWS services et ressources
- Activer ou désactiver la fonctionnalité d'affichage organisationnel pour votre AWS organisation
- Filtrez vos événements en fonction de services spécifiques, de catégories de types d'événements et de codes de type d'événement

Pour plus d'informations, consultez la page Référence de l'API AWS Health.

> **Note**
>
> Vous devez disposer d'un plan Business, Enterprise On-Ramp ou Enterprise Support AWS Supportpour utiliser l' AWS Health API. Si vous appelez l' AWS Health API depuis un compte ne disposant pas d'un plan Business, Enterprise On-Ramp ou Enterprise Support, vous recevez un `SubscriptionRequiredException` message d'erreur.

Vue organisationnelle

Vous pouvez utiliser cette fonctionnalité pour regrouper tous les événements de santé relatifs à vos AWS comptes AWS Organizations en une seule vue dans le AWS Health tableau de bord. Vous pouvez ensuite vous connecter au compte de gestion de votre organisation ou utiliser l' AWS Health API pour consulter tous les événements susceptibles d'affecter les différents comptes et ressources. Vous pouvez activer cette fonctionnalité depuis la AWS Health console ou l'API. Pour de plus amples informations, veuillez consulter Agrégation des AWS Health événements entre les comptes.

Notifications des utilisateurs AWS

AWS Health s'intègre Notifications des utilisateurs AWSafin que vous puissiez facilement recevoir et contrôler les notifications concernant les événements affectant votre Comptes AWS et vos services. Notifications des utilisateurs propose des notifications gérées pour les AWS Health événements par défaut. Vous pouvez configurer ces abonnements pour contrôler la fréquence à laquelle vous recevez des messages par le biais d'une agrégation basée sur le temps, les types d' AWS Health événements dont vous êtes informé et l'endroit où les notifications sont envoyées. Pour commencer, ouvrez Notifications des utilisateurs dans le AWS Management Console. Pour plus d’informations, consultez Gérez AWS Health les notifications dans Notifications des utilisateurs AWS.

Commencer à utiliser votre AWS Health tableau de bord

Vous pouvez utiliser votre AWS Health tableau de bord pour en savoir plus sur AWS Health les événements. Ces événements peuvent affecter votre Services AWS ou Compte AWS. Une fois que vous êtes connecté à votre compte, le AWS Health tableau de bord affiche les informations de la manière suivante :

- Événements de votre compte — Cette page affiche les événements spécifiques à votre compte. Vous pouvez consulter les modifications en cours, récentes et planifiées. Vous pouvez également consulter les notifications et un journal des événements qui répertorie tous les événements des 90 derniers jours.
- Événements de votre organisation : cette page affiche les événements spécifiques à votre organisation dans AWS Organizations. Vous pouvez consulter les modifications en cours, récentes et planifiées pour votre organisation. Vous pouvez également consulter les notifications, ainsi qu'un journal des événements répertoriant tous les événements de l'organisation survenus au cours des 90 derniers jours.

> **Note**
>
> Si vous n'en avez pas Compte AWS, vous pouvez l'utiliser AWS Health Tableau de bord pour en savoir plus sur la disponibilité générale des services.
> Si vous avez un compte, nous vous recommandons de vous connecter à votre AWS Health tableau de bord pour obtenir des informations plus détaillées sur les événements et les modifications à venir susceptibles d'affecter vos services et ressources.

Rubriques

Configuration de votre AWS compte

Avant de pouvoir l'activer AWS Health, vous devez disposer d'un Compte AWS. Si vous n'avez pas de AWS compte, suivez les étapes ci-dessous pour en créer un.

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.

   Dans le cadre de la procédure d'inscription, vous recevrez un appel téléphonique ou un SMS et vous saisirez un code de vérification en utilisant le clavier numérique 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 .

Afficher les événements de votre compte dans le AWS Health tableau de bord

Vous pouvez vous connecter à votre compte pour obtenir des événements et des recommandations personnalisés.

Pour consulter les événements du compte dans votre AWS Health tableau de bord

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Dans le volet de navigation, pour l'état de santé de votre compte, vous pouvez choisir les options suivantes :
   a. Numéros ouverts et récents : consultez les événements récemment ouverts et clôturés.
   b. Modifications planifiées : consultez les événements à venir susceptibles d'affecter vos services et ressources.
   c. Autres notifications : consultez toutes les autres notifications et les événements en cours des sept derniers jours susceptibles d'affecter votre compte.
   d. Journal des événements : affiche tous les événements des 90 derniers jours.

Numéros ouverts et récents

Utilisez l'onglet Problèmes en cours et récents pour consulter tous les événements en cours des sept derniers jours susceptibles d'affecter votre compte.

Lorsque vous sélectionnez un événement dans le tableau de bord, le volet Détails apparaît avec des informations sur l'événement et une liste des ressources concernées. Pour de plus amples informations, veuillez consulter Détails de l'événement.

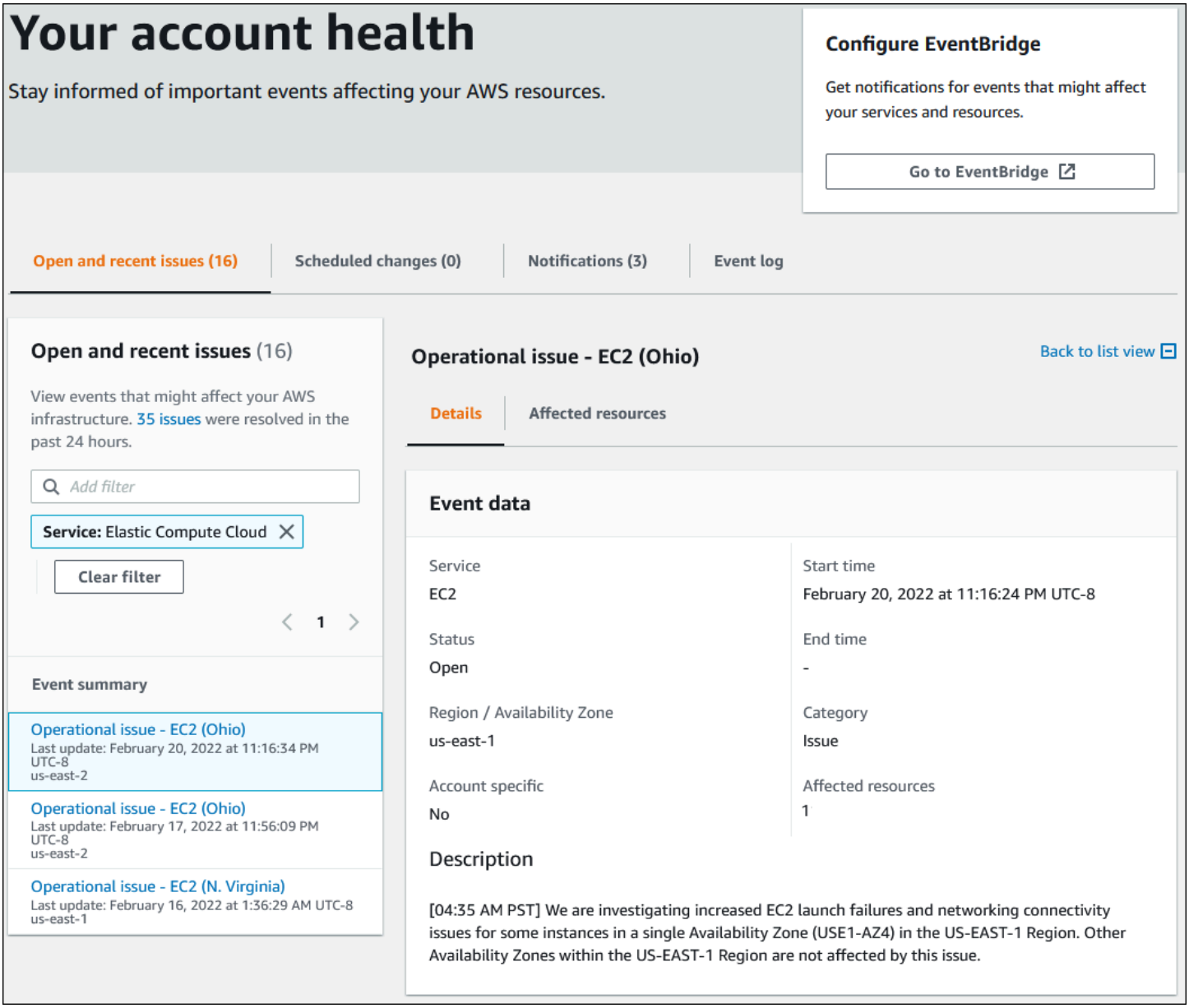
Vous pouvez filtrer les événements qui apparaissent dans n'importe quel onglet en choisissant des options dans la liste des filtres. Par exemple, vous pouvez affiner les résultats par zone de disponibilité, région, heure de fin d'événement ou date de dernière mise à jour Service AWS, etc.

Pour voir tous les événements, plutôt que ceux qui apparaissent récemment dans le tableau de bord, choisissez l'Event Log (Journal des événements)onglet.

> **Note**
>
> À l'heure actuelle, vous ne pouvez pas supprimer les notifications relatives aux événements qui apparaissent dans votre AWS Health tableau de bord. Une fois qu' Service AWS un événement a été résolu, la notification est supprimée de l'affichage de votre tableau de bord.

Example : événement lié à un problème opérationnel pour Amazon Elastic Compute Cloud (Amazon EC2)

L'image suivante montre un événement lié à des échecs de lancement et à des problèmes de connectivité pour les EC2 instances Amazon.



Changements planifiés

Utilisez l'onglet Modifications planifiées pour consulter les événements à venir susceptibles d'affecter votre compte. Ces événements peuvent inclure des activités de maintenance planifiées pour les services et des événements du cycle de vie planifiés qui nécessitent une action pour être résolus. Pour vous aider à planifier ces activités, une vue du calendrier est fournie afin que vous puissiez mapper ces modifications planifiées dans un calendrier mensuel. Des filtres sont disponibles. Pour plus d'informations sur les événements du cycle de vie planifiés, consultezÉvénements du cycle de vie planifiés pour AWS Health.

Autres notifications

Utilisez l'onglet Notifications pour consulter toutes les autres notifications et les événements en cours des sept derniers jours susceptibles d'affecter votre compte. Cela peut inclure des événements tels que des rotations de certificats, des notifications de facturation et des failles de sécurité.

Event Log (Journal des événements)

Utilisez l'onglet Journal des événements pour afficher tous les AWS Health événements. Le tableau du journal inclut des colonnes supplémentaires afin que vous puissiez filtrer par statut et heure de début.

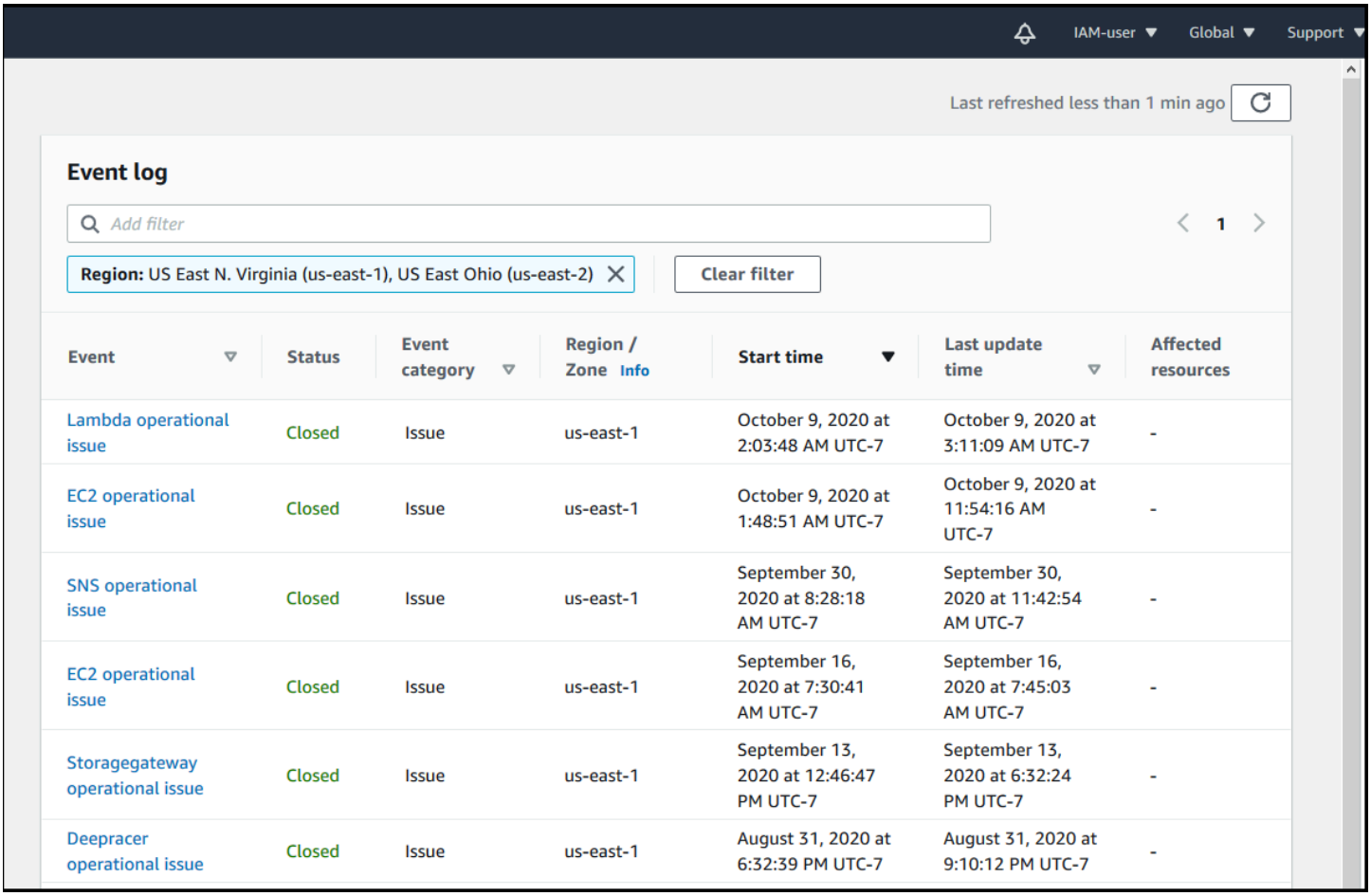
Lorsque vous choisissez un événement dans le tableau du journal des événements, le volet Détails apparaît avec des informations sur l'événement et la liste des ressources concernées. Pour de plus amples informations, veuillez consulter Détails de l’événement.

Vous pouvez choisir les options de filtre suivantes pour affiner vos résultats :

- Zone de disponibilité
- L’heure de fin
- Événement
- ARN de l'événement
- Catégorie d'événement
- Heure de la dernière mise à jour
- Région
- ID de ressource/ ARN
- Service
- L’heure de début
- Statut

Example : journal des événements

L'image suivante montre les événements récents survenus dans les régions de l'est des États-Unis (Virginie du Nord) et de l'est des États-Unis (Ohio).



Détails de l'événement

Lorsque vous choisissez un événement, deux onglets apparaissent à son sujet. L'onglet Détails affiche les informations suivantes :

- Service
- Statut
- Région/Zone de disponibilité
- Si l'événement est ou non spécifique au compte
- Heure de début et de fin
- Catégorie
- Nombre de ressources affectées
- Description et chronologie des mises à jour concernant l'événement

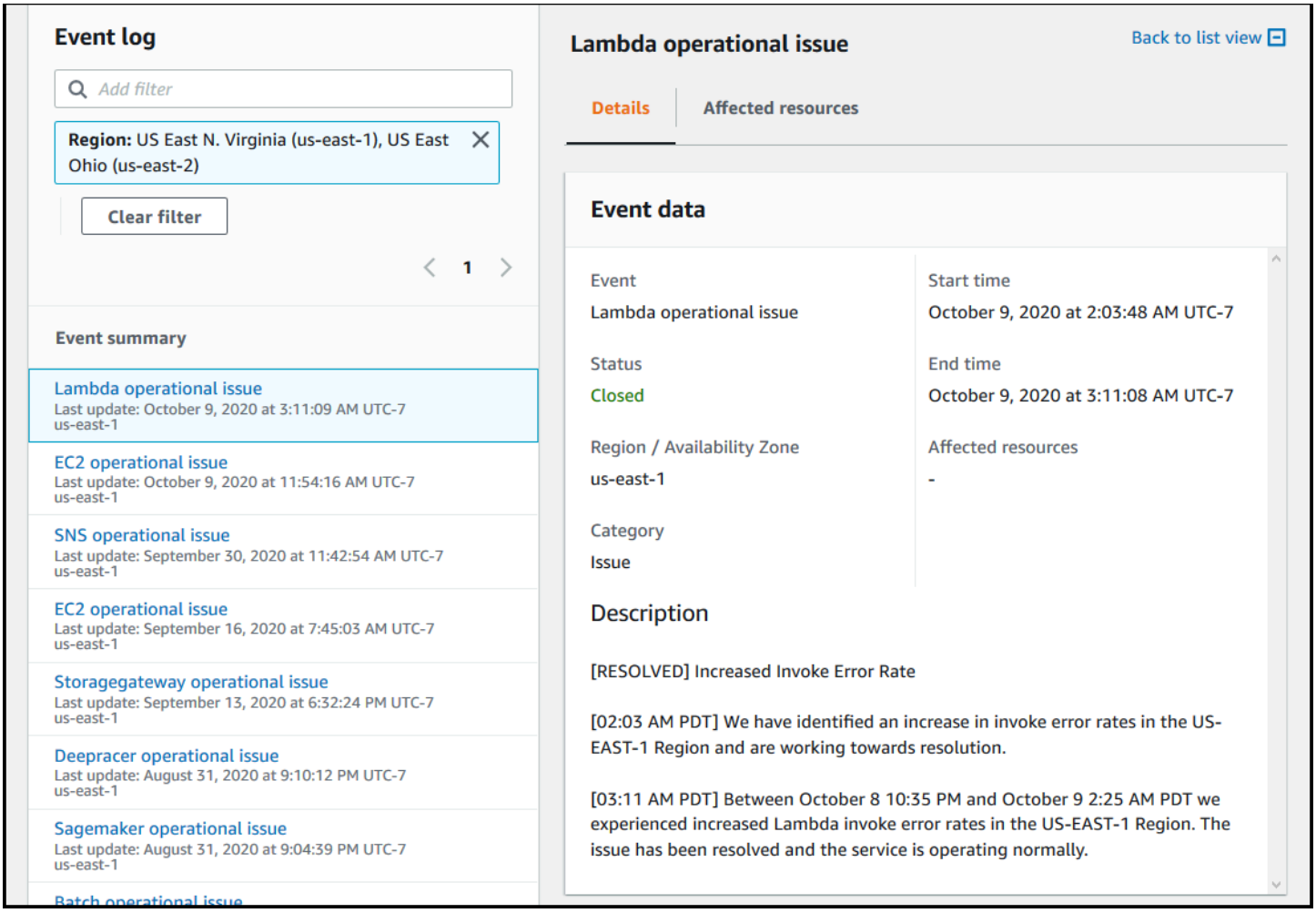
L'onglet Ressources affectées affiche les informations suivantes sur les AWS ressources affectées par l'événement :

- L'ID de ressource (par exemple, un identifiant de volume Amazon EBS tel que`vol-a1b2c34f`) ou le nom de ressource Amazon (ARN), s'il est disponible ou pertinent.
- Pour les événements du cycle de vie planifiés, cette liste des ressources concernées contient également le dernier état des ressources (en attente, inconnu ou résolu). Cette liste est généralement actualisée toutes les 24 heures, mais cela peut prendre jusqu'à 72 heures pour refléter le statut actuel.

Vous pouvez filtrer les éléments qui apparaissent dans les ressources. Vous pouvez affiner vos résultats par ID de ressource ou par ARN.

Example : AWS Health événement pour AWS Lambda

La capture d'écran suivante montre un exemple d'événement pour Lambda.



Types d'événement

Il existe deux types d' AWS Health événements :

- Les événements publics sont des événements de service qui ne sont pas spécifiques à un compte. Par exemple, en cas de problème avec Amazon EC2 dans un Région AWS, AWS Health fournit des informations sur l'événement, même si vous n'utilisez pas les services ou les ressources de cette région.
- Les événements spécifiques à un compte sont spécifiques à votre compte ou à un compte de votre organisation. Par exemple, en cas de problème avec une EC2 instance Amazon Région AWS que vous utilisez, AWS Health fournit des informations sur l'événement et la liste des EC2 instances Amazon concernées.

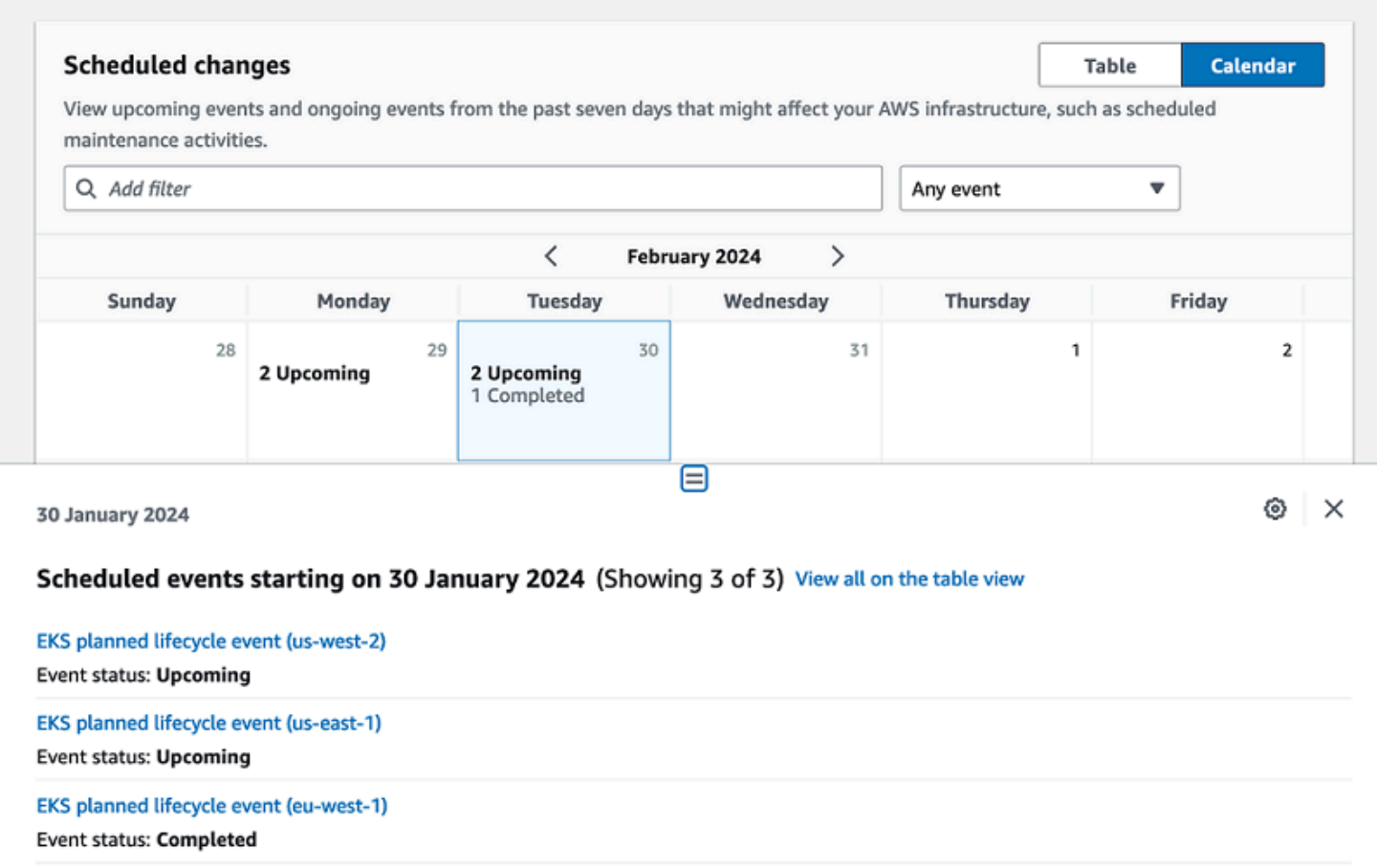
Vous pouvez utiliser les options suivantes pour déterminer si un événement est public ou spécifique à un compte :

- Dans le AWS Health tableau de bord, choisissez l'onglet Ressources affectées pour un événement. Les événements avec des ressources sont spécifiques à votre compte. Les événements sans ressources sont publics et ne sont pas spécifiques à votre compte. Pour de plus amples informations, veuillez consulter Commencer à utiliser votre AWS Health tableau de bord.
- Utilisez l' AWS Health API pour renvoyer le `eventScopeCode` paramètre. Les événements peuvent avoir la valeur `PUBLIC`, `ACCOUNT_SPECIFIC` ou `NONE`. Pour plus d'informations, consultez le DescribeEventDetailsfonctionnement dans la référence de l'AWS Health API.

Affichage du calendrier

L'affichage du calendrier est disponible dans l'onglet des modifications planifiées pour projeter AWS Health les événements dans un calendrier mensuel. Cette vue vous permet de voir les modifications planifiées jusqu'à 3 mois dans le passé et un an dans le futur.

AWS Health les événements sont affichés par date. Sélectionnez une date pour afficher un panneau latéral contenant plus de détails sur l' AWS Health événement. Les événements à venir et en cours sont affichés en noir. Les événements terminés sont affichés en gris. S'il y a plus de deux événements dans une date, seul le nombre d'événements en noir et en gris est affiché. Sélectionnez une date pour afficher la liste des AWS Health événements dans le panneau latéral. Vous pouvez sélectionner un événement dans le panneau latéral pour afficher les informations relatives à cet événement. Le panneau latéral comporte un fil d'Ariane permettant d'accéder à une vue précédente.



Vue des ressources concernées

AWS Health les événements peuvent spécifier les ressources précises qui sont affectées. Vous pouvez consulter les ressources concernées dans l'onglet Ressources concernées de l' AWS Health événement. Pour voir le statut, sélectionnez l' AWS Health événement. L'état s'affiche dans l'onglet Ressources concernées du panneau latéral. Pour les événements du cycle de vie planifiés, AWS Health les événements fournissent des mises à jour quotidiennes de l'état des ressources affectées.

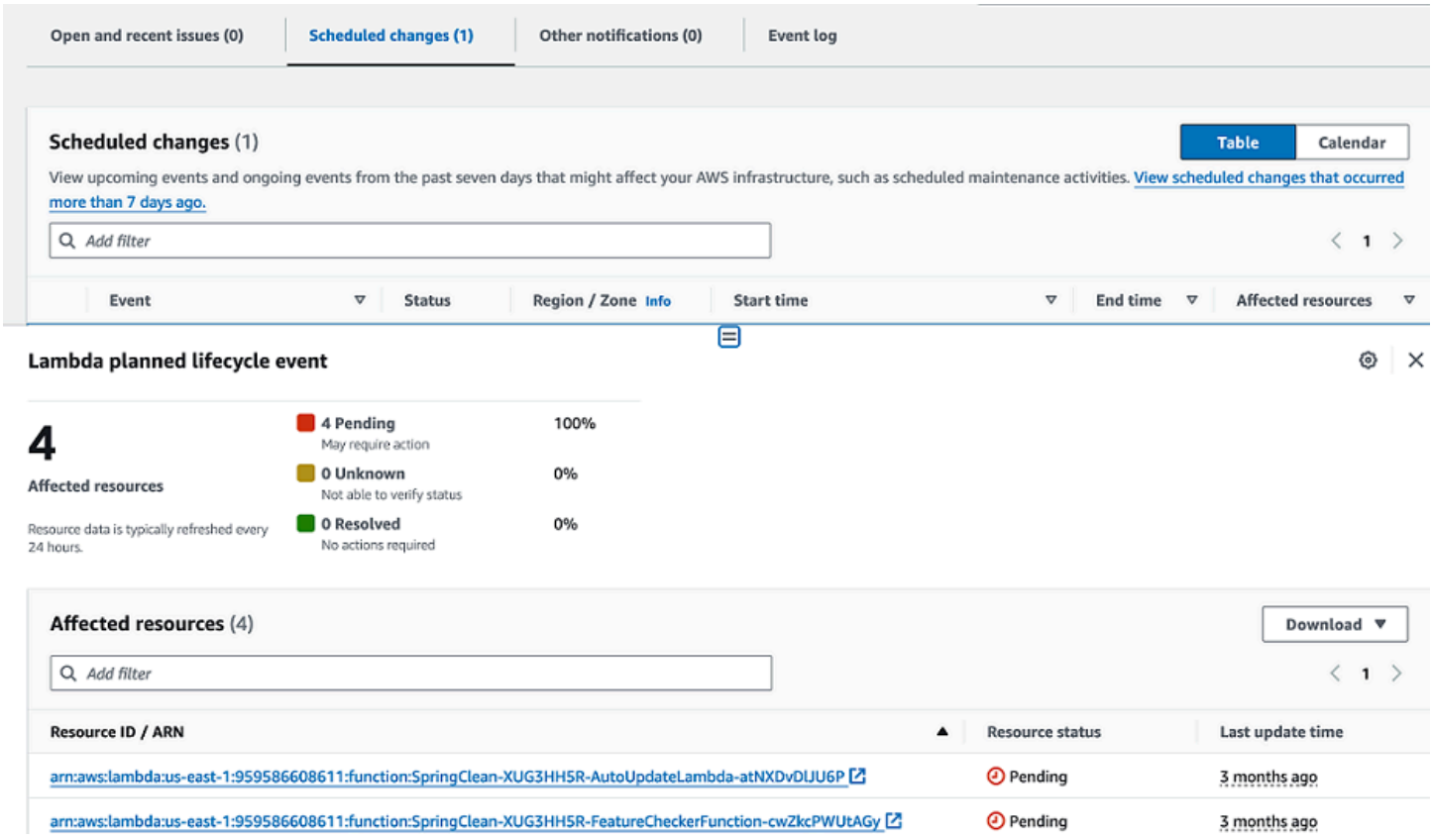
AWS Health Les événements au niveau du compte affichent un résumé de l'état des ressources concernées en haut de l'onglet Ressources concernées. La liste des ressources concernées est affichée dans un tableau avec le statut correspondant. Les événements du cycle de vie planifié sont un exemple de types d'événements qui utilisent le champ d'état des ressources. Pour en savoir plus sur les événements du cycle de vie planifiés, voirÉvénements du cycle de vie planifiés pour AWS Health.

Lorsque vous accédez à la vue de l'organisation, les AWS Health événements affichent un résumé de l'état de toutes les ressources affectées pour tous les comptes inclus. Après le résumé se

trouve une liste des comptes concernés et le nombre de ressources en attente pour ce compte. Sélectionnez le numéro de compte ou le nombre de ressources en attente pour afficher le résumé de l'affichage du compte. Le résumé de l'affichage des comptes contient des fils de navigation permettant de revenir à la liste organisationnelle des comptes concernés. Un résumé des statuts des ressources concernées est affiché en haut du panneau divisé.

Vous pouvez télécharger la liste des ressources concernées dans l'onglet Ressources concernées au format CSV ou JSON. Du point de vue organisationnel, le fichier téléchargé inclut toutes les ressources des comptes répertoriés. Accédez au niveau du compte dans la vue organisationnelle pour inclure uniquement les ressources de ce compte dans le fichier téléchargé. Chaque ressource affectée dans le fichier téléchargé inclut l' Compte AWS ID, l'EventArn, le nom de l'entité, l'EntityArn, le statut et l'heure de dernière mise à jour de la ressource. Si les filtres sont activés, le fichier téléchargé inclut uniquement les résultats filtrés.

Vous ne pouvez télécharger qu'un seul fichier à la fois. Les fichiers sont automatiquement téléchargés dans le dossier de téléchargement par défaut de votre navigateur et portent un nom de fichier prédéfini basé sur le Région AWS titre de l'événement, la date de début de l'événement et la date de téléchargement.



Réglages du fuseau horaire

Vous pouvez consulter les événements dans le AWS Health tableau de bord dans votre fuseau horaire local ou en UTC. Si vous modifiez le fuseau horaire dans votre AWS Health tableau de bord, tous les horodatages du tableau de bord et les événements publics sont mis à jour selon le fuseau horaire que vous spécifiez.

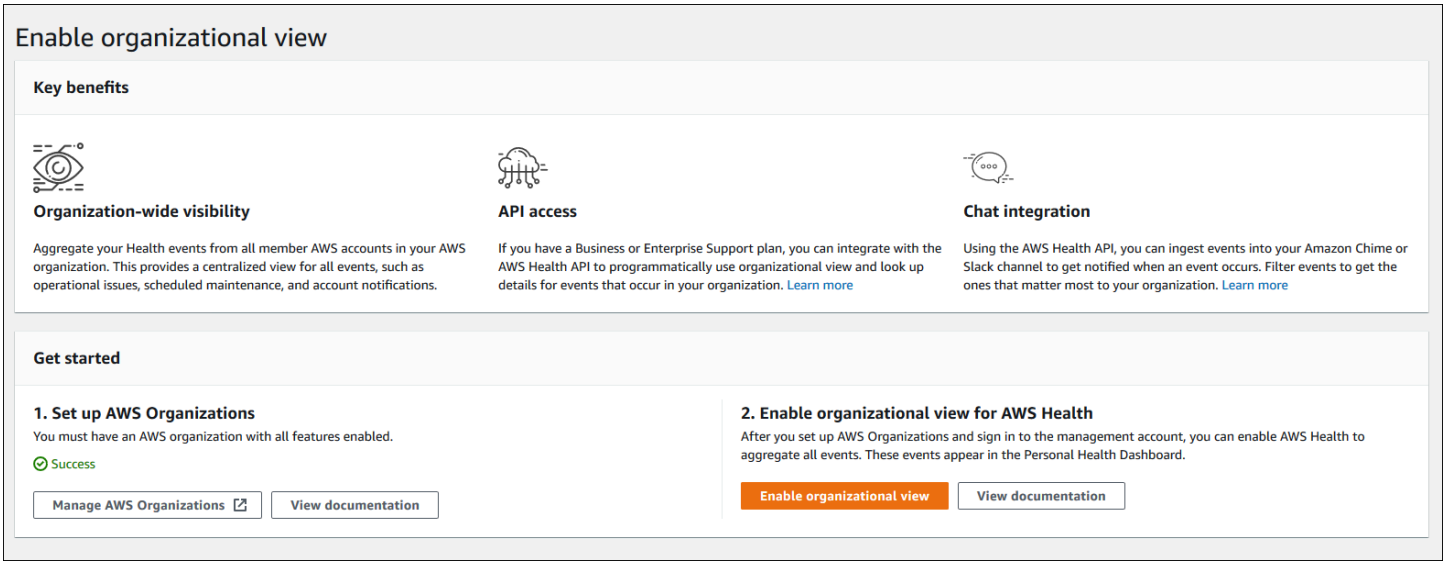
Pour mettre à jour les paramètres de votre fuseau horaire

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Au bas de la page, sélectionnez Préférences en matière de cookies.
3. Sélectionnez Autorisé pour les cookies fonctionnels. Choisissez ensuite Enregistrer les préférences.
4. Dans le volet de navigation de votre AWS Health tableau de bord, choisissez Paramètres du fuseau horaire.
5. Sélectionnez un fuseau horaire pour vos sessions AWS Health de tableau de bord. Ensuite, choisissez Enregistrer les modifications.

Santé de votre organisation

AWS Health s'intègre AWS Organizations afin que vous puissiez consulter les événements de tous les comptes faisant partie de votre organisation. Vous disposez ainsi d'une vue centralisée pour les événements qui apparaissent dans votre organisation. Vous pouvez utiliser ces événements pour surveiller les modifications apportées à vos ressources, services et applications.

Pour de plus amples informations, veuillez consulter Agrégation des AWS Health événements entre les comptes.



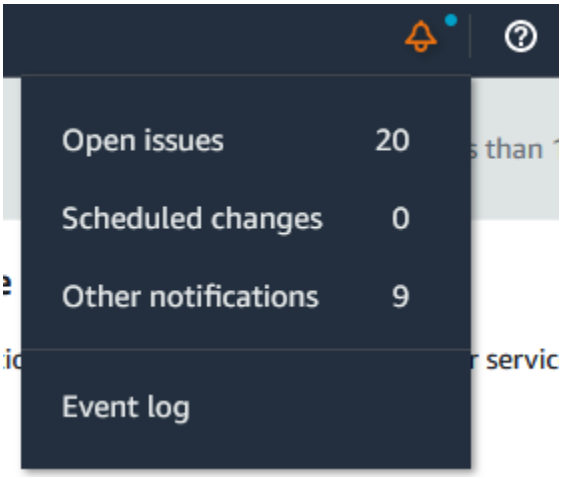
Alertes pour les AWS Health événements

Votre AWS Health tableau de bord comporte une icône en forme de cloche dans la barre de navigation de la console avec un menu d'alerte. Cette fonctionnalité affiche le nombre d' AWS Health événements récents qui apparaissent sur le tableau de bord dans chaque catégorie. Cette icône en forme de cloche apparaît sur plusieurs AWS consoles, telles que celles d'Amazon EC2, Amazon Relational Database Service (Amazon RDS) AWS Identity and Access Management , (IAM) et. AWS Trusted Advisor

Cliquez sur l'icône en forme de cloche pour voir si les récents événements ont une incidence sur votre compte. Vous pouvez ensuite choisir un événement pour accéder à votre AWS Health tableau de bord pour plus d'informations.

Example : Événements ouverts

L'image suivante montre les événements d'ouverture et de notification relatifs à un compte.



Configuration d'Amazon EventBridge

EventBridge À utiliser pour détecter les changements liés aux AWS Health événements et y réagir. Vous pouvez surveiller des AWS Health événements spécifiques qui se produisent dans votre compte, puis définir des règles afin de vous AWS Health avertir ou de prendre des mesures lorsque des événements changent.

Utiliser EventBridge avec AWS Health

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Pour accéder à la EventBridge console afin de créer une règle, effectuez l'une des opérations suivantes :
   - Dans le volet de navigation, sous Health Integrations, choisissez Amazon EventBridge.
   - Sous Configurer EventBridge, choisissez Accéder à EventBridge.
3. Suivez cette procédure pour créer des règles et surveiller les événements. Consultez Surveillance des événements AWS Health avec Amazon EventBridge.

Gérez AWS Health les notifications dans Notifications des utilisateurs AWS

AWS les notifications gérées vous Notifications des utilisateurs AWS permettent de recevoir et de gérer des notifications concernant des événements qui affectent votre Comptes AWS et vos services. Lorsque vous utilisez des notifications AWS gérées dans Notifications des utilisateurs AWS, vous pouvez spécifier les catégories d' AWS Health événements à recevoir, configurer l'affichage

organisationnel des e-mails et obtenir des notifications consolidées au lieu de plusieurs e-mails similaires. Pour plus d'informations sur la façon d'activer ce service, consultez la section Activation ou désactivation des notifications AWS gérées pour AWS Health in Notifications des utilisateurs AWS.

Vous pouvez choisir les canaux supplémentaires suivants pour recevoir vos AWS Health événements Notifications des utilisateurs AWS :

- E-mails
- Chat
- Notifications push vers le AWS Console Mobile Application

Bien que ces notifications ne soient pas aussi détaillées que les AWS Health outils directs, elles constituent un moyen efficace d'informer les parties prenantes des problèmes et des modifications.

> **Note**
>
> Pour une visibilité complète sur les détails de l' AWS Health événement IDs, y compris les ressources affectées, le statut actuel (ouvert ou fermé) et l'état des ressources, il est recommandé d'utiliser l'un des AWS Health outils suivants :
>
> - L' AWS Health API
> - La source aws.health sur Amazon EventBridge
> - Le AWS Health Dashboard
>
> Ces outils fournissent les informations les plus détaillées et en temps réel sur les événements en cours et les changements susceptibles d'affecter vos charges de travail.

Configurez votre abonnement aux notifications AWS gérées pour les AWS Health événements

Pour configurer votre abonnement aux notifications AWS gérées, procédez comme suit :

1. Ouvrez Notifications des utilisateurs dans le AWS Management Console.
2. Dans le volet de navigation, sélectionnez AWS Managed Notifications Subscriptions.

3. Si vous n'êtes pas activé Notifications des utilisateurs AWS en tant qu'expéditeur de AWS Health notifications, sélectionnez Activer AWS Health les notifications. Cela désactive les e-mails provenant de AWS Health et les active depuis Notifications des utilisateurs. Pour plus d'informations, voir Activation ou désactivation des notifications AWS gérées pour AWS HealthNotifications des utilisateurs AWS
4. Vous pouvez gérer vos notifications AWS Health d'événements par catégorie. Pour plus d'informations, voir Ajouter et supprimer des contacts de compte pour les notifications AWS gérées dans Notifications des utilisateurs AWS.

> **Note**
>
> AWS Health migre la livraison des e-mails vers des notifications AWS gérées dans Notifications des utilisateurs AWS. Voici quelques dates clés :
>
> - Jusqu'au 14 septembre 2025 : période d'inscription pour utiliser les notifications AWS gérées.
> - 15 septembre 2025 : les notifications AWS gérées sont activées pour toutes les notifications existantes Comptes AWS. Pour les nouveaux Comptes AWS, les notifications gérées sont activées par défaut. Vous pouvez activer et désactiver les notifications gérées jusqu'au 15 décembre 2025.
> - 15 décembre 2025 : les notifications AWS gérées sont activées pour tous les comptes, et vous ne pouvez plus les désactiver.
>
> Aucune action n'est requise de votre part pour continuer à recevoir des notifications concernant AWS Health des événements. Lorsque les notifications AWS gérées seront activées, certaines modifications et améliorations seront apportées. Pour plus d'informations, voir Quels sont les changements lorsque j'active les notifications AWS gérées ? dans leAWS notifications gérées dans la FAQ sur les notifications AWS utilisateur.

AWS notifications gérées dans la FAQ sur les notifications AWS utilisateur

Qu'est-ce qui change lorsque j'active les notifications AWS gérées ?

Par défaut, les e-mails concernant les notifications gérées sont envoyés aux contacts existants de votre compte (adresses e-mail root, opérationnelles, de facturation et de sécurité). Les e-mails que

vous recevez dans le cadre `health@aws.com` des `no-reply-aws@amazon.com` notifications AWS gérées proviennent de et leur format change. Si vous avez déjà configuré des règles d'e-mail pour AWS Health les notifications, telles que le routage d'un e-mail par identifiant d'expéditeur ou le retrait du contenu de l'e-mail, vous devez mettre à jour cette configuration pour qu'elle corresponde au nouveau format d'e-mail. Si vous avez besoin d'une automatisation par le biais de notifications push, nous vous recommandons d'évaluer les AWS Health événements envoyés via Amazon EventBridge comme alternative aux notifications gérées.

Comment fonctionne l'agrégation pour les e-mails et comment activer cette fonctionnalité ?

AWS les notifications gérées regroupent les AWS Health événements qui ont un impact sur plusieurs comptes au sein d'une même AWS Organizations organisation en une seule notification agrégée. Vous pouvez consulter l'organisation agrégée dans le centre de notifications du compte de gestion. Les notifications gérées envoient par e-mail la notification agrégée aux contacts du compte de gestion. Pour réduire les doublons d'e-mails, les notifications AWS gérées envoient une notification lorsque les contacts du compte sont partagés entre les comptes de gestion et les comptes des membres.

Pour activer l'agrégation, vous devez avoir AWS Organizations configuré et accordé un accès sécurisé entre votre compte de gestion et le Notifications des utilisateurs AWS service.

Pour plus d'informations, consultez la section Agrégation des notifications AWS gérées dans Notifications des utilisateurs AWS.

Dois-je activer l'accès AWS Organizations sécurisé pour recevoir des e-mails agrégés Notifications des utilisateurs AWS à partir de notifications AWS gérées ?

Oui, un accès sécurisé via Notifications des utilisateurs AWS le AWS Organizations formulaire est requis.

Quelle est la différence entre permettre un accès fiable AWS Organizations avec AWS Health et avec Notifications des utilisateurs AWS ?

La confiance organisationnelle et les privilèges d'administrateur délégués associés sont attribués par le service et servent de garde-fous contre les autorisations trop étendues. L'accès sécurisé AWS Health permet une vue organisationnelle du AWS Health Dashboard AWS Health service et des AWS Health événements envoyés via Amazon EventBridge. L'accès fiable pour Notifications des utilisateurs AWS permet d'agréger les notifications dans Notifications des utilisateurs AWS les AWS Health notifications. L'accès sécurisé n'étant pas partagé, la configuration des administrateurs délégués doit être ajoutée séparément pour chaque service.

Où puis-je activer les notifications gérées ?

Activez les notifications gérées à partir du AWS Management Console. Pour plus d'informations, voir Activation ou désactivation des notifications AWS gérées pour AWS HealthNotifications des utilisateurs AWS

Existe-t-il un moyen de conserver les e-mails en texte brut pour mon cas d'utilisation spécifique ?

Non. Les AWS Health e-mails en texte brut actuels sont désactivés une fois la migration terminée. Si vous utilisez des règles d'e-mail pour gérer différents flux de travail, nous vous recommandons d'évaluer les AWS Health événements envoyés via Amazon EventBridge comme alternative.

AWS Health Tableau de bord

Vous pouvez utiliser le AWS Health tableau de bord — État du service pour consulter l'état de santé de tous Services AWS. Cette page affiche les événements de service signalés pour les différents services Régions AWS. Vous n'avez pas besoin de vous connecter ou d'en avoir un Compte AWS pour accéder à la page AWS Health Tableau de bord — État des services.

> **Tip**
>
> Ce site Web ne montre que les événements publics, qui ne sont pas spécifiques à un Compte AWS. Si vous avez déjà un compte, nous vous recommandons de vous connecter pour consulter votre AWS Health tableau de bord et rester informé des événements susceptibles d'affecter votre compte et vos services. Pour de plus amples informations, veuillez consulter Commencer à utiliser votre AWS Health tableau de bord.

Pour consulter le AWS Health tableau de bord — État du service

1. Accédez à la page https://health.aws.amazon.com/health/d'état.

   > **Note**
   >
   > Si vous êtes déjà connecté à votre page Compte AWS, vous serez redirigé vers la page AWS Health Tableau de bord — État de votre compte.

2. Sous État du service, sélectionnez Problèmes ouverts et récents pour afficher les événements récemment signalés. Vous pouvez consulter les informations suivantes concernant l'événement :

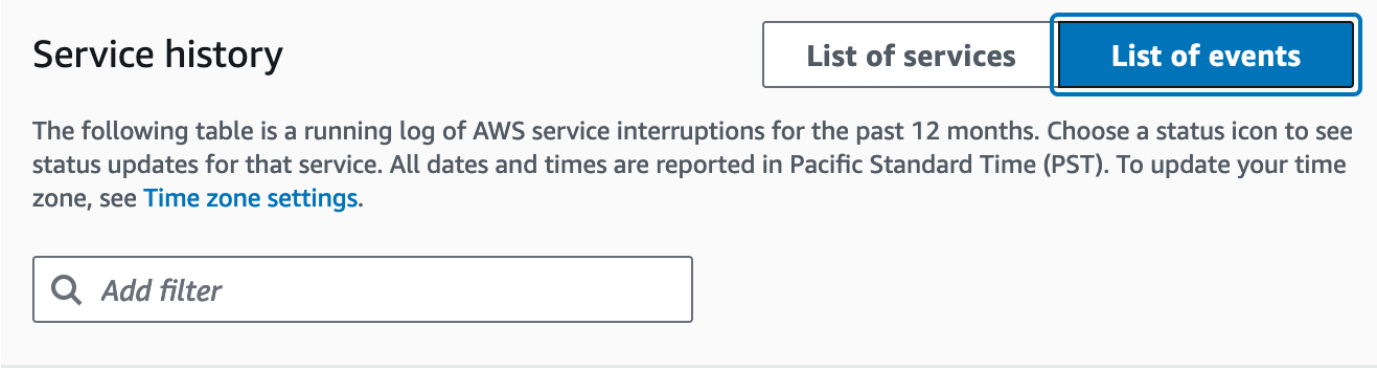
   - Le nom de l'événement et la région affectée. Par exemple, problème opérationnel : Amazon Elastic Compute Cloud (Virginie du Nord)
   - Le nom du service
   - La gravité de l'événement, telle que « impacté » ou « dégradé »
   - Chronologie des dernières mises à jour de l'événement
   - Une liste de Services AWS ceux qui sont également concernés par cet événement

> **Note**
>
> Vous pouvez consulter les événements dans votre fuseau horaire local ou en UTC. Pour plus d'informations, consultez la section Paramètres du fuseau horaire.

3. (Facultatif) À côté de l'événement, choisissez RSS pour vous abonner à un flux RSS pour cet événement. Vous recevrez des notifications concernant ce service spécifique dans le délai indiqué Région AWS.
4. Choisissez Historique des services pour afficher le tableau de l'historique des services. Ce tableau montre toutes les Service AWS interruptions des 12 derniers mois.

> **Tip**
>
> Vous pouvez filtrer par service Région AWSet par date.

5. À côté d'un événement de service en cours, cliquez sur l'icône d'état ( ) pour afficher plus d'informations sur l'événement.
6. (Facultatif) Pour l'afficher sous forme de liste d'événements historiques, cliquez sur le bouton Liste des événements. Choisissez un événement dans la colonne des événements pour afficher plus d'informations sur cet événement spécifique dans le panneau latéral contextuel.



> **Note**
>
> La sélection d'un événement public après septembre 2023 remplira l'URL du navigateur avec un lien vers cet AWS Health événement public. Après avoir sélectionné ce lien,

vous accédez à l'affichage de la liste des événements avec la fenêtre contextuelle correspondante.

7. (Facultatif) Choisissez RSS pour vous abonner à un flux RSS. Vous recevrez des notifications concernant ce service spécifique dans le délai indiqué Région AWS.
8. (Facultatif) Vous pouvez consulter les événements dans votre fuseau horaire local ou en UTC. Pour de plus amples informations, veuillez consulter Réglages du fuseau horaire.
9. (Facultatif) Si vous avez un compte, choisissez Open your account health pour vous connecter. Une fois connecté, vous pouvez consulter les événements spécifiques à votre compte. Pour de plus amples informations, veuillez consulter Commencer à utiliser votre AWS Health tableau de bord.

Événements du cycle de vie planifiés pour AWS Health

Découvrez les événements du cycle de vie planifiés pour AWS Health.

Rubriques

Quels sont les événements du cycle de vie planifiés ?

AWS Health communique les modifications importantes susceptibles d'affecter la disponibilité de vos applications. Dans le modèle de responsabilité AWS partagée, AWS prend des mesures pour maintenir le matériel et l'infrastructure sous-jacents qui soutiennent vos ressources à jour et sécurisés. Toutefois, certains changements nécessitent une action ou une coordination du client afin d'éviter tout impact sur vos applications. AWS Health vous informe à l'avance des modifications importantes telles que :

- Fin du support pour les logiciels libres - Certains Services AWS exécutent des versions open source de logiciels. Si la communauté open source met fin au support des versions logicielles, elle vous AWS indique quand vous devez prendre des mesures pour effectuer une mise à niveau et éviter tout impact sur vos applications.
  - Fin du support de la version du moteur Amazon RDS for MySQL
  - Fin du support de la version Amazon EKS Kubernetes
- Modifications affectant les ressources AWS détenues et susceptibles de nécessiter votre intervention.
  - Expiration des certificats de l'autorité de certification Amazon RDS.

> **Note**
>
> Toutes les notifications répondant à ces critères seront signalées AWS Health sous la forme d'événements du cycle de vie planifiés.

- Consommation dynamique des ressources et amélioration des métadonnées : entre le moment où vous recevez la notification et la durée de vie de l' AWS Health événement, les ressources affectées sont associées à l' AWS Health événement en tant qu'entités concernées avec un statut d'entité spécifique. Les ressources concernées sont spécifiées au format ARN, le cas échéant. Si vos ressources concernées nécessitent une intervention du client, elles sont répertoriées avec le statut « EN ATTENTE ». Si l'action requise a été effectuée sur les ressources concernées ou si les ressources ont été supprimées, le statut passe à « RÉSOLU ».

> **Note**
>
> - Les mises à jour de l'état des ressources sont effectuées de manière asynchrone et périodique et peuvent être retardées jusqu'à 72 heures dans de rares cas.
> - Dans les exceptions où les mises à jour dynamiques ne sont pas fournies, alors que les ressources ont le statut « EN ATTENTE » ou « RÉSOLU », aucun statut ne sera attribué aux ressources.
> - Les mises à jour de l'état des ressources ne sont pas prises en charge dans les régions AWS GovCloud (US) et en Chine.

À quoi dois-je m'attendre lorsque je reçois une notification d'événement lié au cycle de vie planifié ?

L' AWS Health expérience des événements planifiés du cycle de vie aide vos équipes à se renseigner sur les modifications à venir du cycle de vie et à suivre l'achèvement des actions.

Catégorie de type : Modification planifiée

Code du type d'événement : AWS_ {SERVICE} _PLANID_LIFECYCLE_EVENT

Heure de début de l'événement : L'heure de début de l'événement est la date la plus proche à laquelle vos ressources sont affectées par le changement.

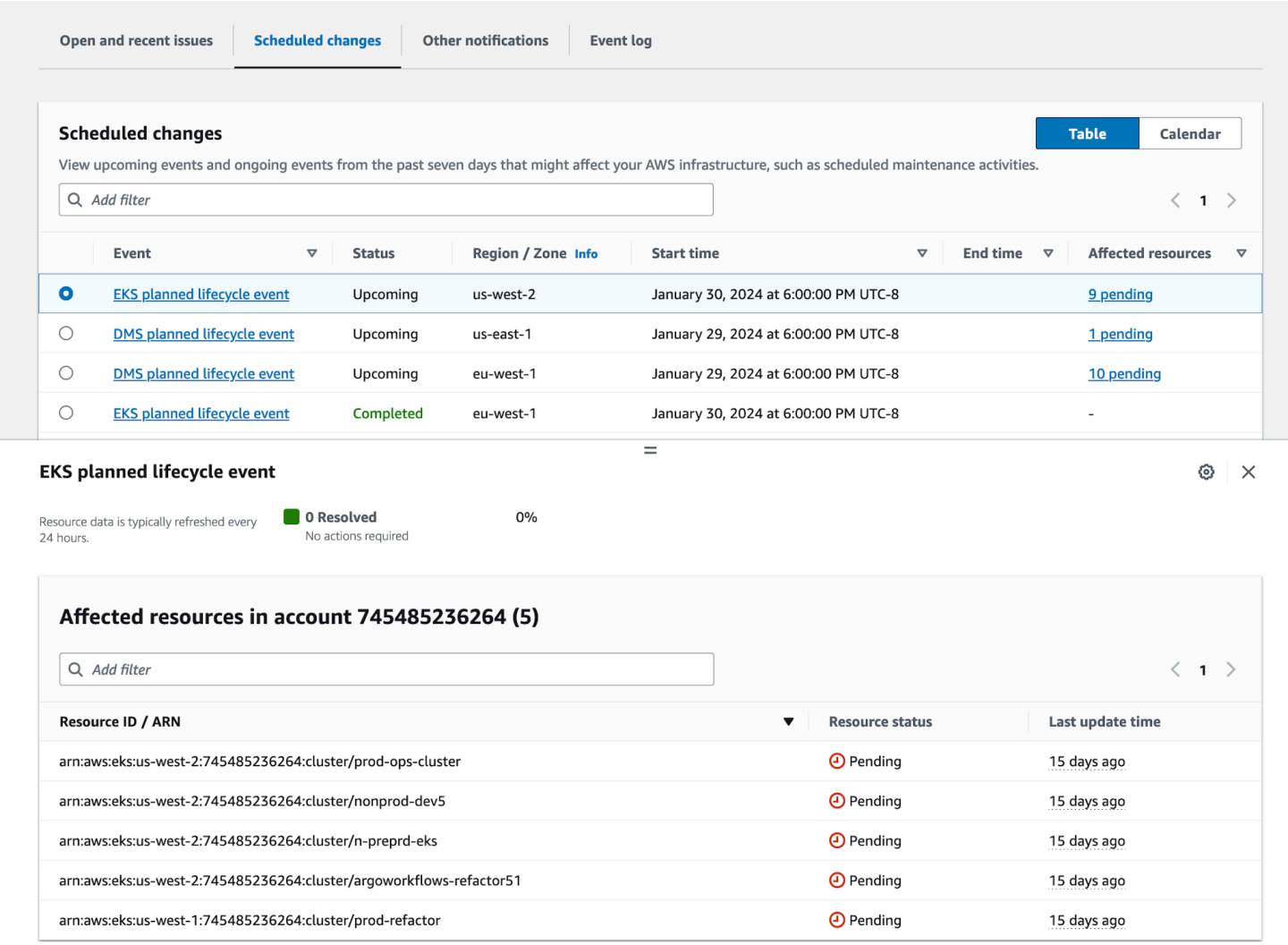
Heure de fin de l'événement : L'heure de fin de l'événement est la date à laquelle la modification prend fin pour toutes les AWS ressources. Notez que l'heure de fin n'est pas toujours spécifiée. Il est important de considérer l'heure de début comme la date de modification.

> **Note**
>
> Organisations peuvent s'attendre à recevoir un seul ARN d'événement pour chaque événement du cycle de vie planifié, groupé par région où les ressources sont concernées. Mais ils peuvent en recevoir plusieurs ARNs si l'organisation compte un grand nombre de personnes touchées Comptes AWS ou de ressources.

Visibilité précoce des événements planifiés du cycle de vie : les événements du cycle de vie planifiés sont conçus pour avoir un délai minimum de 180 jours pour les événements majeursversions/changes and 90 days for minor versions/changes, dans la mesure du possible.

Consommation dynamique des ressources et amélioration des métadonnées : entre le moment où vous recevez la notification et la durée de vie de l' AWS Health événement, les ressources affectées sont associées à l' AWS Health événement en tant qu'entités concernées avec un statut d'entité spécifique. Les ressources concernées sont spécifiées au format ARN, le cas échéant. Si vos ressources concernées nécessitent une intervention du client, elles sont répertoriées avec le statut « EN ATTENTE ». Si l'action requise a été effectuée sur les ressources concernées ou si les ressources ont été supprimées, le statut passe à « RÉSOLU ».

> **Note**
>
> - AWS Health les notifications fournissent des mises à jour de statut au fil du temps dans la mesure du possible, sauf pour les régions AWS GovCloud (US) et la Chine.
> - Les mises à jour de l'état des ressources sont effectuées de manière asynchrone et périodique et peuvent être retardées jusqu'à 72 heures dans de rares cas.

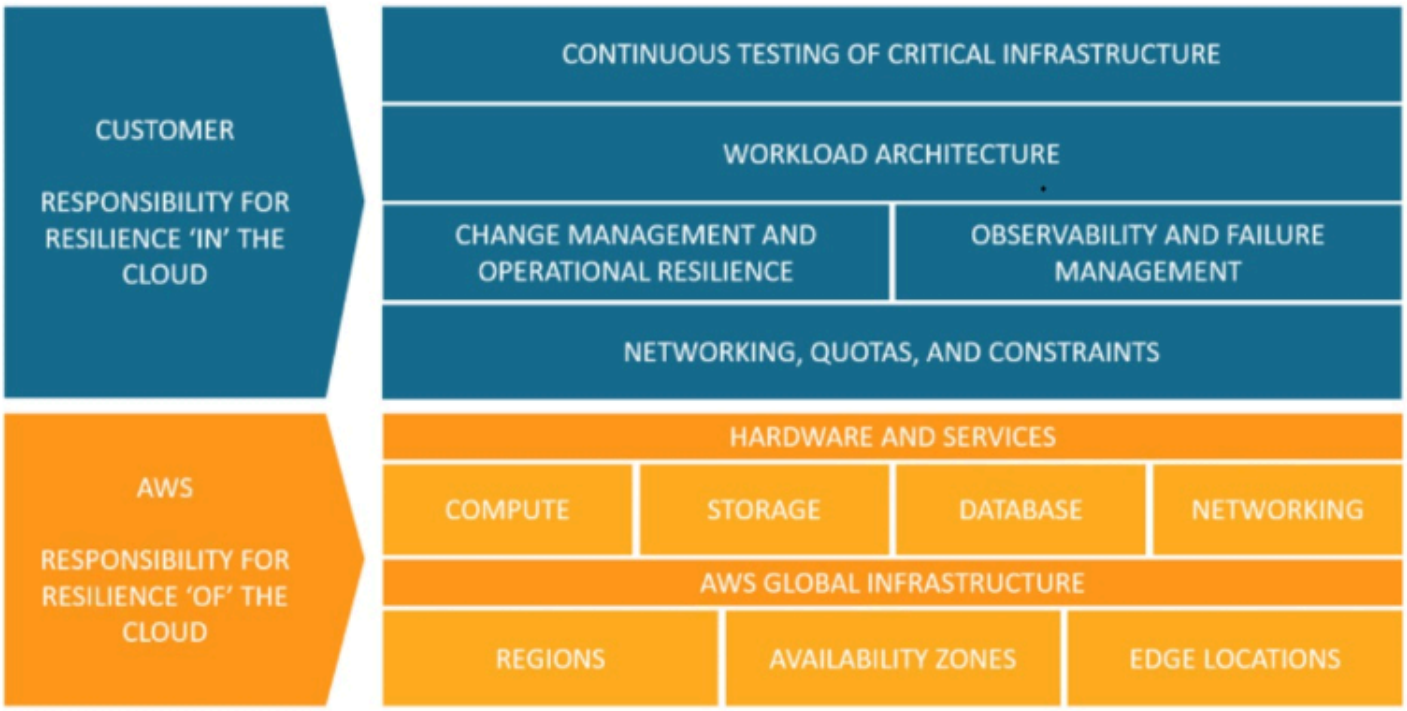


Une fois la date prévue de l'événement passée :

1. Le cas échéant, le service peut mettre en œuvre la modification décrite dans votre ressource à tout moment après la date de début de l'événement.
2. Si vous résolvez toutes les ressources avant la date de fin du support, le statut de votre AWS Health événement change`Closed`.
3. Si vous avez des ressources en suspens après la date de modification qui ne sont pas résolues, l' AWS Health événement reste ouvert pendant 4 ans après la date de début ou de fin de l'événement (selon la date la plus tardive). Passé ce délai, l' AWS Health événement est supprimé.

Modèle de responsabilité partagée pour la résilience

La sécurité et la conformité sont des responsabilités partagées entre le client AWS et le client. En fonction des services déployés, ce modèle partagé peut contribuer à alléger la charge opérationnelle du client. Cela est dû au fait qu'il AWS exploite, gère et contrôle les composants depuis le système d'exploitation hôte et la couche de virtualisation jusqu'à la sécurité physique des installations dans lesquelles le service fonctionne. Le client assume la responsabilité et la gestion du système d'exploitation client (y compris les mises à jour et les correctifs de sécurité) et des autres logiciels d'application associés, en plus de la configuration du pare-feu du groupe de sécurité fourni par AWS. Pour de plus amples informations, veuillez consulter Modèle de responsabilité partagée.



Accès aux événements du cycle de vie planifiés

Les événements du cycle de vie planifiés peuvent être consultés et surveillés via plusieurs canaux :

- Utilisez Amazon EventBridge
- Utiliser le AWS Health tableau de bord
  - Affichage du calendrier
  - Vue des ressources concernées
- Utiliser l' AWS Health API

Intégration AWS Health à d'autres systèmes à l'aide de l' AWS Health API

AWS Health est un service RESTful Web qui utilise le protocole HTTPS comme moyen de transport et le format JSON comme format de sérialisation des messages. Votre code applicatif peut effectuer des requêtes directement à l'API AWS Health . Lorsque vous utilisez directement l'API REST, vous devez écrire le code nécessaire pour signer et authentifier vos demandes. Pour plus d'informations sur les AWS Health opérations et les paramètres, consultez la référence de l'AWS Health API.

> **Note**
>
> Vous devez disposer d'un plan Business, Enterprise On-Ramp ou Enterprise Support AWS Supportpour utiliser l' AWS Health API. Si vous appelez l' AWS Health API depuis un AWS compte ne disposant pas d'un plan Business, Enterprise On-Ramp ou Enterprise Support, vous recevez un `SubscriptionRequiredException` message d'erreur.

Vous pouvez utiliser le AWS SDKs pour encapsuler les appels d' AWS Health API REST, ce qui peut simplifier le développement de vos applications. Vous spécifiez vos AWS informations d'identification, et ces bibliothèques se chargent de l'authentification et de la signature des demandes pour vous.

AWS Health fournit également un AWS Health tableau de bord AWS Management Console que vous pouvez utiliser pour afficher et rechercher des événements et des entités concernées. Consultez Commencer à utiliser votre AWS Health tableau de bord.

Rubriques

- Signature des demandes AWS Health d'API
- Choix des points de terminaison pour les demandes AWS Health d'API
- Démos : récupération des données d' AWS Health événements des sept derniers jours par programmation
- Tutoriel : Utilisation de l' AWS Health API avec des exemples Java

Signature des demandes AWS Health d'API

Lorsque vous utilisez le AWS SDKs ou le AWS Command Line Interface (AWS CLI) pour faire des demandes AWS, ces outils signent automatiquement les demandes à votre place avec la clé d'accès que vous spécifiez lors de la configuration des outils. Par exemple, si vous utilisez le AWS SDK pour Java pour la démonstration précédente des terminaux à haute disponibilité, vous n'avez pas besoin de signer vous-même les demandes.

Exemples de code Java

Pour plus d'exemples sur l'utilisation de l' AWS Health API avec le AWS SDK pour Java, consultez cet exemple de code.

Lorsque vous faites des demandes, nous vous recommandons vivement de ne pas utiliser les informations d'identification de votre compte AWS root pour accéder régulièrement à AWS Health. Vous pouvez utiliser les informations d'identification d'un utilisateur IAM. Pour plus d'informations, voir Verrouiller les clés d'accès utilisateur root de votre AWS compte dans le guide de l'utilisateur IAM.

Si vous n'utilisez pas le AWS SDKs ou le AWS CLI, vous devez signer vous-même vos demandes. Nous vous recommandons d'utiliser AWS la version 4 de Signature. Pour plus d'informations, consultez la section Signature des demandes d' AWS API dans le Références générales AWS.

Choix des points de terminaison pour les demandes AWS Health d'API

L' AWS Health API suit une architecture d'application multirégionale Architecture d'application et possède deux points de terminaison régionaux dans une configuration active-passive. Pour prendre en charge le basculement du DNS actif-passif, AWS Health fournit un point de terminaison global unique. Vous pouvez effectuer une recherche DNS sur le point de terminaison global pour déterminer le point de terminaison actif et la AWS région de signature correspondante. Cela vous permet de savoir quel point de terminaison utiliser dans votre code, afin que vous puissiez obtenir les dernières informations AWS Health.

Lorsque vous envoyez une demande au point de terminaison mondial, vous devez spécifier vos informations d' AWS accès au point de terminaison régional que vous ciblez et configurer la signature pour votre région. Dans le cas contraire, votre authentification risque d'échouer. Pour de plus amples informations, veuillez consulter Signature des demandes AWS Health d'API.

Pour les demandes IPv6 uniquement, nous recommandons d'effectuer une recherche DNS sur le point de terminaison global afin de déterminer le point de terminaison actif, Région AWS puis d'appeler le point de terminaison à double pile IPv6 pris en charge pour cette région.

Le tableau suivant représente la configuration par défaut.

Description	Région de signature	Point de terminaison	Protocole
Actif	us-east-1	health.us-east-1.amazonaws.com (IPv4-uniquement) health.us-east-1.api.aws (et pris en charge) IPv4 IPv6	HTTPS
Passif	us-east-2	health.us-east-2.amazonaws.com (IPv4-uniquement) health.us-east-2.api.aws (et pris en charge) IPv4 IPv6	HTTPS
Globale	us-east-1 **Note** Il s'agit de la région de signature du point de terminaison actif actuel.	global.health.amazonaws.com	HTTPS

Pour déterminer si un point de terminaison est le point de terminaison actif, effectuez une recherche DNS sur le CNAME du point de terminaison global, puis extrayez la AWS région du nom résolu.

Example : recherche DNS sur le point de terminaison global

La commande renvoie ensuite le point de terminaison de la région us-east-1 . Cette sortie vous indique pour quel point de terminaison vous devez utiliser AWS Health.

```
dig global.health.amazonaws.com | grep CNAME
global.health.amazonaws.com. 10 IN CNAME health.us-east-1.amazonaws.com
```

> **Tip**
>
> Les points de terminaison actifs et passifs renvoient AWS Health des données. Cependant, les AWS Health données les plus récentes ne sont disponibles qu'à partir du point de terminaison actif. Les données du point de terminaison passif seront finalement cohérentes avec le point de terminaison actif. Nous vous recommandons de redémarrer tous les flux de travail lorsque le point de terminaison actif change.

Démos : récupération des données d' AWS Health événements des sept derniers jours par programmation

Dans les exemples de code suivants, AWS Health utilise une recherche DNS sur le point de terminaison global pour déterminer le point de terminaison régional actif et la région de signature. AWS Health utilise ces informations pour récupérer un rapport des sept derniers jours de données relatives aux événements. Le code redémarre le flux de travail si le point de terminaison actif change.

Rubriques

- Démo : récupération des données d' AWS Health événements des sept derniers jours à l'aide de Java
- Démo : récupération des données d' AWS Health événements des sept derniers jours à l'aide de Python

Démo : récupération des données d' AWS Health événements des sept derniers jours à l'aide de Java

Prérequis

Vous devez installer Gradle.

Pour utiliser l'exemple Java

1. Téléchargez la démo des terminaux de AWS Health haute disponibilité sur GitHub.
2. Accédez au `high-availability-endpoint/java` répertoire du projet de démonstration.
3. Dans une fenêtre de ligne de commande, entrez la commande suivante.

```
gradle build
```

4. Entrez les commandes suivantes pour spécifier vos AWS informations d'identification.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

5. Entrez la commande suivante pour exécuter la démo.

```
gradle run
```

Example : sortie AWS Health d'événement

L'exemple de code renvoie l' AWS Health événement récent des sept derniers jours sur votre AWS compte. Dans l'exemple suivant, la sortie inclut un AWS Health événement pour le AWS Config service.

```
> Task :run
[main] INFO aws.health.high.availability.endpoint.demo.HighAvailabilityV2Workflow
 - EventDetails(Event=Event(Arn=arn:aws:health:global::event/CONFIG/
AWS_CONFIG_OPERATIONAL_NOTIFICATION/AWS_CONFIG_OPERATIONAL_NOTIFICATION_88a43e8a-
e419-4ca7-9baa-56bcde4dba3,
Service=CONFIG, EventTypeCode=AWS_CONFIG_OPERATIONAL_NOTIFICATION,
 EventTypeCategory=accountNotification, Region=global,
 StartTime=2020-09-11T02:55:49.899Z, LastUpdatedTime=2020-09-11T03:46:31.764Z,
StatusCode=open, EventScopeCode=ACCOUNT_SPECIFIC),
 EventDescription=EventDescription(LatestDescription=As part of our ongoing efforts
 to optimize costs associated with recording changes related to certain ephemeral
 workloads,
AWS Config is scheduled to release an update to relationships modeled within
 ConfigurationItems (CI) for 7 EC2 resource types on August 1, 2021.
Examples of ephemeral workloads include changes to Amazon Elastic Compute Cloud
 (Amazon EC2) Spot Instances, Amazon Elastic MapReduce jobs, and Amazon EC2
 Autoscaling.
```

```
This update will optimize CI models for EC2 Instance, SecurityGroup, Network
 Interface, Subnet, VPC, VPN Gateway, and Customer Gateway resource types to record
 direct relationships and deprecate indirect relationships.

A direct relationship is defined as a one-way relationship (A->B) between a
 resource (A) and another resource (B), and is typically derived from the Describe
 API response of resource (A).
An indirect relationship, on the other hand, is a relationship that AWS Config
 infers (B->A), in order to create a bidirectional relationship.
For example, EC2 instance -> Security Group is a direct relationship, since
 security groups are returned as part of the describe API response for an EC2
 instance.
But Security Group -> EC2 instance is an indirect relationship, since EC2 instances
 are not returned when describing an EC2 Security group.

Until now, AWS Config has recorded both direct and indirect relationships. With
 the launch of Advanced queries in March 2019, indirect relationships can easily be
 answered by running Structured Query Language (SQL) queries such as:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'sg-234213'

By deprecating indirect relationships, we can optimize the information contained
 within a
Configuration Item while reducing AWS Config costs related to relationship
 changes.
This is especially useful in case of ephemeral workloads where there is a high
 volume of configuration changes for EC2 resource types.

Which resource relationships are being removed?

Resource Type: Related Resource Type
1 AWS::EC2::CustomerGateway: AWS::VPN::Connection
2 AWS::EC2::Instance: AWS::EC2::EIP, AWS::EC2::RouteTable
3 AWS::EC2::NetworkInterface: AWS::EC2::EIP, AWS::EC2::RouteTable
4 AWS::EC2::SecurityGroup: AWS::EC2::Instance, AWS::EC2::NetworkInterface
5 AWS::EC2::Subnet: AWS::EC2::Instance, AWS::EC2::NetworkACL,
 AWS::EC2::NetworkInterface, AWS::EC2::RouteTable
```

```
6 AWS::EC2::VPC: AWS::EC2::Instance, AWS::EC2::InternetGateway,
 AWS::EC2::NetworkACL, AWS::EC2::NetworkInterface, AWS::EC2::RouteTable,
 AWS::EC2::Subnet, AWS::EC2::VPNGateway, AWS::EC2::SecurityGroup
7 AWS::EC2::VPNGateway: AWS::EC2::RouteTable, AWS::EC2::VPNConnection

Alternate mechanism to retrieve this relationship information:
The SelectResourceConfig API accepts a SQL SELECT command, performs the
 corresponding search, and returns resource configurations matching the properties.
 You can use this API to retrieve the same relationship information.
For example, to retrieve the list of all EC2 Instances related to a particular VPC
 vpc-1234abc, you can use the following query:

SELECT
 resourceId,
 resourceType
WHERE
 resourceType ='AWS::EC2::Instance'
AND
 relationships.resourceId = 'vpc-1234abc'

If you have any questions regarding this deprecation plan, please contact AWS
 Support [1]. Additional sample queries to retrieve the relationship information
 for the resources listed above is provided in [2].

[1] https://aws.amazon.com/support
[2] https://docs.aws.amazon.com/config/latest/developerguide/
examplerelationshipqueries.html),
EventMetadata={})
```

Ressources Java

- Pour plus d'informations, consultez l'interface HealthClient dans la référence de l'AWS SDK pour Java API et le code source.
- Pour plus d'informations sur la bibliothèque utilisée dans cette démonstration pour les recherches DNS, consultez le fichier dnsjava dans. GitHub

Démo : récupération des données d' AWS Health événements des sept derniers jours à l'aide de Python

Prérequis

Vous devez installer Python 3.

Pour utiliser l'exemple Python

1. Téléchargez la démo des terminaux de AWS Health haute disponibilité sur GitHub.
2. Accédez au `high-availability-endpoint/python` répertoire du projet de démonstration.
3. Dans une fenêtre de ligne de commande, entrez les commandes suivantes.

```
pip3 install virtualenv
virtualenv -p python3 v-aws-health-env
```

> **Note**
>
> Pour Python 3.3 et versions ultérieures, vous pouvez utiliser le `venv` module intégré pour créer l'environnement virtuel au lieu de l'installer`virtualenv`. Pour plus d'informations, consultez venv - Création d'environnements virtuels sur le site Web de Python.
>
> ```
> python3 -m venv v-aws-health-env
> ```

4. Entrez la commande suivante pour activer l'environnement virtuel.

```
source v-aws-health-env/bin/activate
```

5. Entrez la commande suivante pour installer les dépendances.

```
pip install -r requirements.txt
```

6. Entrez les commandes suivantes pour spécifier vos AWS informations d'identification.

```
export AWS_ACCESS_KEY_ID="AKIAIOSFODNN7EXAMPLE"
export AWS_SECRET_ACCESS_KEY="wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY"
export AWS_SESSION_TOKEN="your-aws-token"
```

7. Entrez la commande suivante pour exécuter la démo.

```
python3 main.py
```

Example : sortie AWS Health d'événement

L'exemple de code renvoie l' AWS Health événement récent des sept derniers jours sur votre AWS compte. La sortie suivante renvoie un AWS Health événement pour une notification AWS de sécurité.

```
INFO:botocore.credentials:Found credentials in environment variables.
INFO:root:Details: {'arn': 'arn:aws:health:global::event/SECURITY/
AWS_SECURITY_NOTIFICATION/AWS_SECURITY_NOTIFICATION_0e35e47e-2247-47c4-
a9a5-876544042721',
'service': 'SECURITY', 'eventTypeCode': 'AWS_SECURITY_NOTIFICATION',
 'eventTypeCategory': 'accountNotification', 'region': 'global', 'startTime':
 datetime.datetime(2020, 8, 19, 23, 30, 42, 476000,
tzinfo=tzlocal()), 'lastUpdatedTime': datetime.datetime(2020, 8, 20, 20, 44, 9,
 547000, tzinfo=tzlocal()), 'statusCode': 'open', 'eventScopeCode': 'PUBLIC'},
 description:
{'latestDescription': 'This is the second notice regarding TLS requirements on FIPS
 endpoints.\n\nWe
are in the process of updating all AWS Federal Information Processing Standard
 (FIPS) endpoints across all AWS regions
to Transport Layer Security (TLS) version 1.2 by March 31, 2021 . In order to avoid
 an interruption in service, we encourage you to act now, by ensuring that you
 connect to AWS FIPS endpoints at a TLS version of 1.2.
If your client applications fail to support TLS 1.2 it will result in connection
 failures when TLS versions below 1.2 are no longer supported.\n\nBetween now and
 March 31, 2021 AWS will remove TLS 1.0 and TLS 1.1 support from each FIPS endpoint
 where no connections below TLS 1.2 are detected over a 30-day period.
After March 31, 2021 we may deploy this change to all AWS FIPS endpoints, even if
 there continue
to be customer connections detected at TLS versions below 1.2. \n\nWe will provide
 additional updates and reminders on the AWS Security Blog, with a 'TLS' tag [1].
 If you need further guidance or assistance, please contact AWS Support [2] or your
 Technical Account Manager (TAM).
Additional information is below.\n\nHow can I identify clients that are connecting
 with TLS
1.0/1.1?\nFor customers using S3 [3], Cloudfront [4] or Application Load Balancer
 [5] you can use
your access logs to view the TLS connection information for these services, and
 identify client
connections that are not at TLS 1.2. If you are using the AWS Developer Tools on
 your clients,
```

```
you can find information on how to properly configure your client's TLS versions
 by visiting Tools to Build on AWS [7] or our associated AWS Security Blog has a
 link for each unique code language [7].\n\nWhat is Transport Layer Security (TLS)?
\nTransport Layer Security (TLS Protocols) are cryptographic protocols designed to
 provide secure communication across a computer network
[6].\n\nWhat are AWS FIPS endpoints? \nAll AWS services offer Transport Layer
 Security (TLS) 1.2 encrypted endpoints that can be used for all API calls. Some
 AWS services also offer FIPS 140-2 endpoints [9] for customers that require use
 of FIPS validated cryptographic libraries. \n\n[1] https://aws.amazon.com/blogs/
security/tag/tls/\n[2] https://aws.amazon.com/support\n[3]
https://docs.aws.amazon.com/AmazonS3/latest/dev/LogFormat.html\n[4] https://
docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/AccessLogs.html\n[5]
 https://docs.aws.amazon.com/elasticloadbalancing/latest/application/load-balancer-
access-logs.html\n[6] https://aws.amazon.com/tools\n[7] https://aws.amazon.com/
blogs/security/tls-1-2-to-become-the-minimum-for-all-aws-fips-endpoints\n[8]
https://en.wikipedia.org/wiki/Transport_Layer_Security\n[9] https://aws.amazon.com/
compliance/fips'}
```

8. Lorsque vous avez terminé, entrez la commande suivante pour désactiver la machine virtuelle.

```
deactivate
```

Ressources Python

- Pour plus d'informations à ce sujet`Health. Client`, consultez le manuel de référence de l'API du AWS SDK pour Python (Boto3).
- Pour plus d'informations sur la bibliothèque utilisée dans cette démo pour les recherches DNS, consultez le kit d'outils dnspython et son code source. GitHub

Tutoriel : Utilisation de l' AWS Health API avec des exemples Java

Les exemples de code Java suivants montrent comment initialiser un AWS Health client et récupérer des informations sur les événements et les entités.

Étape 1 : Initialiser des informations d'identification

Des informations d'identification valides sont requises pour communiquer avec l' AWS Health API. Vous pouvez utiliser la paire de clés de n'importe quel utilisateur IAM associé au AWS compte.

Créez et initialisez une AWSCredentialsinstance :

```
AWSCredentials credentials = null;
try {
       credentials = new ProfileCredentialsProvider("default").getCredentials();
} catch (Exception e) {
throw new AmazonClientException(
   "Cannot load the credentials from the credential profiles file. "
   + "Please make sure that your credentials file is at the correct "
   + "location (/home/username/.aws/credentials), and is in valid format.", e);
}
```

Étape 2 : Initialisation d'un client AWS Health API

Utilisez l'objet d'informations d'identification initialisé à l'étape précédente pour créer un client AWS Health :

```
import com.amazonaws.services.health.AWSHealthClient;

AWSHealth awsHealthClient = new AWSHealthClient(credentials);
```

Étape 3 : utiliser les opérations de AWS Health l'API pour obtenir des informations sur les événements

DescribeEvents

```
import com.amazonaws.services.health.model.DescribeEventsRequest;
import com.amazonaws.services.health.model.DescribeEventsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventsRequest request = new DescribeEventsRequest();

EventFilter filter = new EventFilter();
// Filter on any field from the supported AWS Health EventFilter model.
// Here is an example for Region us-east-1 events from the EC2 service.
filter.setServices(singletonList("EC2"));
filter.setRegions(singletonList("us-east-1"));
request.setFilter(filter);

DescribeEventsResult response = awsHealthClient.describeEvents(request);
List<Event> resultEvents = response.getEvents();
```

```
Event currentEvent = null;
for (Event event : resultEvents) {
    // Display result event data; here is a subset.
    System.out.println(event.getArn());
    System.out.println(event.getService());
    System.out.println(event.getRegion());
    System.out.println(event.getAvailabilityZone());
    System.out.println(event.getStartTime());
    System.out.println(event.getEndTime());
 }
```

DescribeEventAggregates

```
import com.amazonaws.services.health.model.DescribeEventAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEventAggregatesResult;
import com.amazonaws.services.health.model.EventAggregate;
import com.amazonaws.services.health.model.EventFilter;

DescribeEventAggregatesRequest request = new DescribeEventAggregatesRequest();
// set the aggregation field
request.setAggregateField("eventTypeCategory");

// filter more on result if needed
EventFilter filter = new EventFilter();
filter.setRegions(singleton("us-east-1"));
request.setFilter(filter);

DescribeEventAggregatesResult response =
 awsHealthClient.describeEventAggregates(request);

// print event count for each eventTypeCategory
for (EventAggregate aggregate: response.getEventAggregates()) {
    System.out.println("Event Category:" + aggregate.getAggregateValue());
    System.out.println("Event Count:" + aggregate.getCount());
 }
```

DescribeEventDetails

```
import com.amazonaws.services.health.model.DescribeEventDetailsRequest;
import com.amazonaws.services.health.model.DescribeEventDetailsResult;
import com.amazonaws.services.health.model.Event;
import com.amazonaws.services.health.model.EventDetails;
```

```
DescribeEventDetailsRequest describeEventDetailsRequest = new
 DescribeEventDetailsRequest();
// set event ARN and local value

describeEventDetailsRequest.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));
describeEventDetailsRequest.setLocale("en-US");
filter.setEventArns
DescribeEventDetailsResult describeEventDetailsResult =
 awsHealthClient.describeEventDetails(request);
EventDetails eventDetail = describeEventDetailsResult.getSuccessfulSet().get(0);

// check event-related fields
Event event = eventDetail.getEvent();
System.out.println(event.getService());
System.out.println(event.getRegion());
System.out.println(event.getAvailabilityZone());
System.out.println(event.getStartTime());
System.out.println(event.getEndTime());

// print out event description
System.out.println(eventDetail.getEventDescription().getLatestDescription());
```

DescribeAffectedEntities

```
import com.amazonaws.services.health.model.AffectedEntity;
import com.amazonaws.services.health.model.DateTimeRange;
import com.amazonaws.services.health.model.DescribeAffectedEntitiesRequest;
import
 com.amdescribeEventDetailsRequestazonaws.services.health.model.DescribeAffectedEntitiesResult;

DescribeAffectedEntitiesRequest request = new DescribeAffectedEntitiesRequest();
EntityFilter filter = new EntityFilter();

filter.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeAffectedEntitiesResult response =
 awsHealthClient.describeAffectedEntities(request);

for (AffectedEntity affectedEntity: response.getEntities()) {
    System.out.println(affectedEntity.getEntityValue());
```

```
    System.out.println(affectedEntity.getAwsAccountId());
    System.out.println(affectedEntity.getEntityArn());
 }
```

DescribeEntityAggregates

```
import com.amazonaws.services.health.model.DescribeEntityAggregatesRequest;
import com.amazonaws.services.health.model.DescribeEntityAggregatesResult;
import com.amazonaws.services.health.model.EntityAggregate;

DescribeEntityAggregatesRequest request = new DescribeEntityAggregatesRequest();

request.setEventArns(singletonList("arn:aws:health:us-
east-1::event/service/eventTypeCode/eventId"));

DescribeEntityAggregatesResult response =
 awsHealthClient.describeEntityAggregates(request);

for (EntityAggregate entityAggregate : response.getEntityAggregates()) {
    System.out.println(entityAggregate.getEventArn());
    System.out.println(entityAggregate.getCount());
 }
```

Sécurité dans AWS Health

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 exécute les AWS services 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 Health, 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,et de la législation et de la réglementation applicables.

Cette documentation vous aide à comprendre comment appliquer le modèle de responsabilité partagée lors de son utilisation AWS Health. Les rubriques suivantes expliquent comment procéder à la configuration AWS Health pour atteindre vos objectifs de sécurité et de conformité. Vous apprendrez également à utiliser d'autres AWS services qui vous aident à surveiller et à sécuriser vos AWS Health ressources.

Rubriques

Protection des données dans AWS Health

Le modèle de responsabilité AWS partagée de s'applique à la protection des données dans AWS Health. 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.
- SSL/TLS À utiliser pour communiquer avec AWS les ressources. 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 AWS Health ou d'autres Services

AWS utilisateurs de la console, de l'API ou AWS SDKs. AWS CLI 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.

Chiffrement des données

Consultez les informations suivantes sur le mode de AWS Health chiffrement des données.

Le chiffrement des données fait référence à la protection des données en transit (lorsqu'elles sont transmises du service à votre AWS compte) et au repos (lorsqu'elles sont stockées dans les AWS services). Vous pouvez protéger les données en transit à l'aide du protocole TLS (Transport Layer Security) ou au repos à l'aide du chiffrement côté client.

AWS Health n'enregistre pas d'informations d'identification personnelles (PII) telles que les adresses e-mail ou les noms des clients lors d'événements.

Chiffrement au repos

Toutes les données stockées par AWS Health sont cryptées au repos.

Chiffrement en transit

Toutes les données envoyées et sortantes AWS Health sont cryptées en transit.

Gestion des clés

AWS Health ne prend pas en charge les clés de chiffrement gérées par le client pour les données chiffrées dans le AWS Cloud.

Gestion des identités et des accès pour AWS Health

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 AWS Health les ressources. 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. AWS Health

Utilisateur du service : si vous utilisez le AWS Health service 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 nouvelles AWS Health fonctionnalités 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 AWS Health, consultez Résolution des problèmes AWS Health d'identité et d'accès.

Administrateur du service — Si vous êtes responsable des AWS Health ressources de votre entreprise, vous avez probablement un accès complet à AWS Health. C'est à vous de déterminer les AWS Health fonctionnalités et les ressources auxquelles les utilisateurs de votre 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 AWS Health, voirComment AWS Health fonctionne avec IAM.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d'écrire des politiques pour gérer l'accès à AWS Health. Pour consulter des exemples de politiques AWS Health basées sur l'identité que vous pouvez utiliser dans IAM, consultez. AWS Health exemples de politiques basées sur l'identité

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.

AWS utilisateur root du compte

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 les informations d'identification de l'utilisateur racine dans le Guide de l'utilisateur IAM.

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 une seule 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 à un service apparaissent dans votre Compte AWS répertoire 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.

AWS Health prend en charge les conditions basées sur les ressources. Vous pouvez spécifier les événements AWS Health que les utilisateurs peuvent afficher. Par exemple, vous pouvez créer une politique qui autorise uniquement un utilisateur IAM à accéder à des EC2 événements Amazon spécifiques dans le AWS Health Dashboard.

Pour de plus amples informations, veuillez consulter Ressources.

Listes de contrôle d'accès (ACL)

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.

AWS Health ne supporte pas ACLs.

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 Health fonctionne avec IAM

Avant d'utiliser IAM pour gérer l'accès à AWS Health, vous devez comprendre quelles fonctionnalités IAM sont disponibles. AWS Health Pour obtenir une vue d'ensemble de la façon dont AWS Health les autres AWS services fonctionnent avec IAM, consultez la section AWS Services qui fonctionnent avec IAM dans le Guide de l'utilisateur d'IAM.

Rubriques

- AWS Health Politiques basées sur l'identité
- AWS Health Politiques basées sur les ressources

- Autorisation basée sur les balises AWS Health
- AWS Health Rôles IAM

AWS Health Politiques basées sur l'identité

Avec les politiques basées sur l'identité IAM, vous pouvez spécifier des actions et ressources autorisées ou refusées, ainsi que les conditions dans lesquelles les actions sont autorisées ou refusées. AWS Health prend en charge des actions, ressources et clés de condition spécifiques. Pour en savoir plus sur 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.

Actions

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.

Les actions de politique en AWS Health cours utilisent le préfixe suivant avant l'action :`health:`. Par exemple, pour autoriser quelqu'un à consulter des informations détaillées sur des événements spécifiques liés à l'opération d'DescribeEventDetailsAPI, vous devez inclure l'`heath:DescribeEventDetails`action dans la politique.

Les déclarations de politique doivent inclure un `NotAction` élément `Action` ou. AWS Health définit son propre ensemble d'actions décrivant les tâches que vous pouvez effectuer avec ce service.

Pour spécifier plusieurs actions dans une seule instruction, séparez-les par des virgules, comme suit :

```
"Action": [
```

```
      "health:action1",
      "health:action2"
```

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

```
"Action": "health:Describe*"
```

Pour consulter la liste des AWS Health actions, reportez-vous à la section Actions définies par AWS Health dans le guide de l'utilisateur IAM.

Ressources

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": "*"
```

Un AWS Health événement possède le format Amazon Resource Name (ARN) suivant.

```
arn:${Partition}:health:*::event/service/event-type-code/event-ID
```

Par exemple, pour spécifier l'événement `EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456` dans votre déclaration, utilisez l'ARN suivant.

```
"Resource": "arn:aws:health:*::event/EC2/EC2_INSTANCE_RETIREMENT_SCHEDULED/
EC2_INSTANCE_RETIREMENT_SCHEDULED_ABC123-DEF456"
```

Pour spécifier tous les AWS Health événements pour Amazon EC2 qui appartiennent à un compte spécifique, utilisez le caractère générique (*).

```
"Resource": "arn:aws:health:*::event/EC2/*/*"
```

Pour plus d'informations sur le format de ARNs, consultez Amazon Resource Names (ARNs) et AWS Service Namespaces.

Certaines AWS Health actions ne peuvent pas être effectuées sur une ressource spécifique. Dans ces cas-là, vous devez utiliser le caractère générique (*).

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

AWS Health Les opérations d'API peuvent impliquer plusieurs ressources. Par exemple, l'DescribeEventsopération renvoie des informations sur les événements qui répondent à un critère de filtre spécifié. Cela signifie qu'un utilisateur IAM doit être autorisé à consulter cet événement.

Pour spécifier plusieurs ressources dans une seule instruction, séparez-les ARNs par des virgules.

```
"Resource": [
      "resource1",
      "resource2"
```

AWS Health ne prend en charge que les autorisations au niveau des ressources pour les événements de santé et uniquement pour les opérations DescribeAffectedEntitieset DescribeEventDetailsAPI. Pour de plus amples informations, veuillez consulter Conditions basées sur des ressources et des actions.

Pour consulter la liste des types de AWS Health ressources et leurs caractéristiques ARNs, reportez-vous à la section Ressources définies par AWS Health dans le guide de l'utilisateur IAM. Pour savoir grâce à quelles actions vous pouvez spécifier l'ARN de chaque ressource, consultez Actions définies par AWS Health.

Clés de condition

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.

AWS Health définit son propre ensemble de clés de condition et prend également en charge l'utilisation de certaines clés de condition globales. Pour voir toutes les clés de condition AWS globales, consultez la section Clés contextuelles de condition AWS globale dans le guide de l'utilisateur IAM.

Les opérations DescribeEventDetailsd'API DescribeAffectedEntitieset prennent en charge les clés de `health:service` condition `health:eventTypeCode` et.

Pour consulter la liste des clés de AWS Health condition, reportez-vous à la section Clés de AWS Health condition du guide de l'utilisateur IAM. Pour savoir avec quelles actions et ressources vous pouvez utiliser une clé de condition, voir Actions définies par AWS Health.

Exemples

Pour consulter des exemples de politiques AWS Health basées sur l'identité, consultez. AWS Health exemples de politiques basées sur l'identité

AWS Health Politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON qui spécifient les actions qu'un principal spécifié peut effectuer sur la AWS Health ressource et dans quelles conditions. AWS Health prend en charge les politiques d'autorisation basées sur les ressources pour les événements de santé. Les politiques basées sur les ressources permettent d'accorder une autorisation à d'autres comptes en fonction des ressources. Vous pouvez également utiliser une politique basée sur les ressources pour autoriser un AWS service à accéder à vos AWS Health événements.

Pour permettre un accès comptes multiples , vous pouvez spécifier un compte entier ou des entités IAM dans un autre compte en tant que principal dans une stratégie 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 se trouvent dans des AWS comptes différents, vous devez également accorder à l'entité principale l'autorisation d'accéder à la ressource. Accordez l'autorisation en attachant une stratégie basée sur les identités à l'entité. Toutefois, si une stratégie basée sur des ressources accorde l'accès à un principal dans le même compte, aucune autre stratégie basée sur l'identité n'est requise. Pour en savoir plus, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le guide de l'utilisateur IAM.

AWS Health prend uniquement en charge les politiques basées sur les ressources pour les opérations DescribeAffectedEntitieset DescribeEventDetailsAPI. Vous pouvez spécifier ces actions dans une politique afin de définir quelles entités principales (comptes, utilisateurs, rôles et utilisateurs fédérés) peuvent effectuer des actions sur l' AWS Health événement.

Exemples

Pour consulter des exemples de politiques AWS Health basées sur les ressources, consultez. Conditions basées sur des ressources et des actions

Autorisation basée sur les balises AWS Health

AWS Health ne prend pas en charge le balisage des ressources ou le contrôle de l'accès en fonction des balises.

AWS Health Rôles IAM

Un rôle IAM est une entité de votre AWS compte qui dispose d'autorisations spécifiques.

Utilisation d'informations d'identification temporaires avec AWS Health

Vous pouvez utiliser des informations d'identification temporaires pour vous connecter à l'aide de la fédération, endosser un rôle IAM ou encore pour endosser un rôle intercompte. Vous obtenez des informations d'identification de sécurité temporaires en appelant des opérations d' AWS STS API telles que AssumeRoleou GetFederationToken.

AWS Health prend en charge l'utilisation d'informations d'identification temporaires.

Rôles liés à un service

Les rôles liés aux AWS services permettent aux services d'accéder aux ressources d'autres services pour effectuer une action en votre nom. Les rôles liés à un service s'affichent dans votre compte IAM et sont la propriété du service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.

AWS Health prend en charge les rôles liés aux services auxquels s'intégrer. AWS Organizations Le rôle lié à un service se nomme `AWSServiceRoleForHealth_Organizations`. La politique OrganizationsServiceRolePolicy AWS gérée par Health_ est associée au rôle. La politique AWS gérée permet d'accéder AWS Health aux événements de santé à partir d'autres AWS comptes de l'organisation.

Vous pouvez utiliser cette EnableHealthServiceAccessForOrganizationopération pour créer le rôle lié au service dans le compte. Toutefois, si vous souhaitez désactiver cette fonctionnalité, vous devez d'abord appeler l'DisableHealthServiceAccessForOrganizationopération. Vous pouvez ensuite supprimer le rôle via la console IAM, l'API IAM ou AWS Command Line Interface ()AWS CLI. Pour plus d'informations, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.

Pour de plus amples informations, veuillez consulter Agrégation des AWS Health événements entre les comptes.

Rôles de service

Cette fonction permet à un service d'endosser une fonction du service en votre nom. Ce rôle autorise le service à accéder à des ressources d'autres services pour effectuer une action en votre nom. Les rôles de service s'affichent dans votre compte IAM et sont la propriété du compte. Cela signifie qu'un administrateur IAM peut modifier les autorisations associées à ce rôle. Toutefois, une telle action peut perturber le bon fonctionnement du service.

AWS Health ne prend pas en charge les rôles de service.

AWS Health exemples de politiques basées sur l'identité

Par défaut, les utilisateurs et les rôles IAM ne sont pas autorisés à créer ou modifier les ressources AWS Health . Ils ne peuvent pas non plus effectuer de tâches à l'aide de l' AWS API AWS Management Console AWS CLI, ou. Un administrateur IAM doit créer des politiques IAM autorisant les utilisateurs et les rôles à exécuter des opérations d'API spécifiques sur les ressources spécifiées dont ils ont besoin. Il doit ensuite attacher ces politiques aux utilisateurs ou aux groupes IAM ayant besoin de ces autorisations.

Pour savoir comment créer une stratégie IAM basée sur l'identité à l'aide de ces exemples de documents de stratégie JSON, veuillez consulter Création de stratégies dans l'onglet JSON dans le Guide de l'utilisateur IAM.

Rubriques

Bonnes pratiques en matière de politiques

Les politiques basées sur l'identité déterminent si quelqu'un peut créer, accéder ou supprimer AWS Health des ressources 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 AWS Health

Pour accéder à la AWS Health console, vous devez disposer d'un ensemble minimal d'autorisations. Ces autorisations doivent vous permettre de répertorier et d'afficher les informations relatives AWS Health aux ressources de votre AWS compte. Si vous créez une politique basée sur l'identité qui est plus restrictive que les autorisations minimales requises, la console ne fonctionnera pas comme prévu pour les entités (utilisateurs et rôles IAM) tributaires de cette politique.

Pour garantir que ces entités peuvent toujours utiliser la AWS Health console, vous pouvez joindre la politique AWS gérée suivante, AWSHealthFullAccess.

La `AWSHealthFullAccess` politique accorde à une entité un accès complet aux éléments suivants :

- Activer ou désactiver la fonctionnalité AWS Health d'affichage organisationnel pour tous les comptes d'une AWS organisation
- Le AWS Health Dashboard dans la AWS Health console
- AWS Health Opérations et notifications de l'API
- Afficher les informations relatives aux comptes qui font partie de votre AWS organisation
- Afficher les unités organisationnelles (UO) du compte de gestion

Example : AWSHealthFullAccess

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
```

```
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "iam:AWSServiceName": "health.amazonaws.com"
                }
            }
        }
    ]
}
```

> **Note**
>
> Vous pouvez également utiliser la politique `Health_OrganizationsServiceRolePolicy` AWS gérée afin de consulter les AWS Health événements relatifs aux autres comptes de votre organisation. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour AWS Health.

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 que vous tentez d'effectuer.

Pour plus d'informations, consultez Ajout d'autorisations à un utilisateur dans le Guide de l'utilisateur IAM.

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 l'API AWS Health Dashboard et à l' AWS Health API

Le AWS Health Dashboard est disponible pour tous les AWS comptes. L' AWS Health API n'est disponible que pour les comptes disposant d'un plan Business, Enterprise On-Ramp ou Enterprise Support. Pour de plus amples informations, veuillez consulter Support.

Vous pouvez utiliser IAM pour créer des entités (utilisateurs, groupes ou rôles), puis autoriser ces entités à accéder à l'API AWS Health Dashboard et à l' AWS Health API.

Par défaut, les utilisateurs IAM n'ont pas accès à l'API AWS Health Dashboard ou à l' AWS Health API. Vous permettez aux utilisateurs d'accéder aux AWS Health informations de votre compte en associant des politiques IAM à un seul utilisateur, à un groupe d'utilisateurs ou à un rôle. Pour plus d'informations, consultez Identités (utilisateurs, groupes et rôles) et Présentation des stratégies IAM.

Après avoir créé les utilisateurs IAM, vous pouvez leur attribuer des mots de passe individuels. Ils peuvent ensuite se connecter à votre compte et consulter les AWS Health informations en utilisant une page de connexion spécifique au compte. Pour plus d'informations, consultez Comment les utilisateurs se connectent à votre compte.

> **Note**
>
> Un utilisateur IAM autorisé à consulter AWS Health Dashboard dispose d'un accès en lecture seule aux informations de santé de tous les AWS services du compte, qui peuvent inclure, mais sans s'y limiter, des AWS ressources IDs telles que l' EC2 instance IDs Amazon, les adresses IP des EC2 instances et les notifications de sécurité générales.
> Par exemple, si une politique IAM accorde l'accès uniquement à AWS Health Dashboard et à l' AWS Health API, l'utilisateur ou le rôle auquel la politique s'applique peut accéder à toutes les informations publiées sur les AWS services et les ressources associées, même si d'autres politiques IAM n'autorisent pas cet accès.

Vous pouvez utiliser deux groupes de APIs for AWS Health.

- Comptes individuels — Vous pouvez utiliser des opérations telles que DescribeEventset DescribeEventDetailspour obtenir des informations sur les AWS Health événements de votre compte.
- Compte d'organisation : vous pouvez utiliser des opérations telles que DescribeEventsForOrganizationet DescribeEventDetailsForOrganizationpour obtenir des informations sur les AWS Health événements relatifs aux comptes qui font partie de votre organisation.

Pour plus d'informations sur les opérations d'API disponibles, consultez la référence des AWS Health API.

Actions individuelles

Vous pouvez définir l'`Action`élément d'une politique IAM sur. `health:Describe*` Cela permet d'accéder à AWS Health Dashboard la terre AWS Health. AWS Health prend en charge le contrôle d'accès aux événements basés sur le service `eventTypeCode` and.

Décrire l'accès

Cette déclaration de politique donne accès à toutes AWS Health Dashboard les opérations de l'`Describe*` AWS Health API. Par exemple, un utilisateur IAM doté de cette politique peut accéder AWS Health Dashboard à l'opération d'API AWS Management Console et appeler l'opération AWS Health `DescribeEvents` d'API.

Example : Décrire l'accès

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  }]
}
```

Refuser l'accès

Cette déclaration de politique interdit l'accès à l' AWS Health API AWS Health Dashboard et à celle-ci. Un utilisateur IAM doté de cette politique ne peut pas voir AWS Health Dashboard les opérations d'API AWS Management Console et ne peut appeler aucune des opérations d' AWS Health API.

Example : Refuser l'accès

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Deny",
    "Action": [
      "health:*"
    ],
    "Resource": "*"
  }]
}
```

Vue organisationnelle

Si vous souhaitez activer l'affichage organisationnel pour AWS Health, vous devez autoriser l'accès aux AWS Organizations actions AWS Health et.

L'`Action`élément d'une politique IAM doit inclure les autorisations suivantes :

- `iam:CreateServiceLinkedRole`

- `organizations:EnableAWSServiceAccess`
- `organizations:DescribeAccount`
- `organizations:DisableAWSServiceAccess`
- `organizations:ListAccounts`
- `organizations:ListDelegatedAdministrators`
- `organizations:ListParents`

Pour connaître les autorisations exactes requises pour chacune d'entre elles APIs, consultez la section Actions définies par AWS Health APIs et notifications dans le guide de l'utilisateur IAM.

> **Note**
>
> Vous devez utiliser les informations d'identification du compte de gestion pour qu'une organisation puisse accéder au AWS Health APIs formulaire AWS Organizations. Pour de plus amples informations, veuillez consulter Agrégation des AWS Health événements entre les comptes.

Autoriser l'accès à la vue AWS Health organisationnelle

Cette déclaration de politique donne accès à toutes AWS Health les AWS Organizations actions dont vous avez besoin pour accéder à la fonctionnalité d'affichage organisationnel.

Example : Autoriser l'accès à la vue AWS Health organisationnelle

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
```

```
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "health:*",
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

Refuser l'accès à la vue AWS Health organisationnelle

Cette déclaration de politique refuse l'accès aux AWS Organizations actions mais autorise l'accès aux AWS Health actions pour un compte individuel.

Example : Refuser l'accès à la vue AWS Health organisationnelle

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "health:*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
```

```
                "organizations:EnableAWSServiceAccess",
                "organizations:DisableAWSServiceAccess"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "organizations:ServicePrincipal": "health.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Deny",
            "Action": [
                "organizations:DescribeAccount",
                "organizations:ListAccounts",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListParents"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "arn:aws:iam::*:role/aws-service-role/health.amazonaws.com/
AWSServiceRoleForHealth*"
        }
    ]
}
```

> **Note**
>
> Si l'utilisateur ou le groupe auquel vous souhaitez accorder des autorisations possède déjà une politique IAM, vous pouvez ajouter la déclaration de politique AWS Health spécifique à cette stratégie.

Conditions basées sur des ressources et des actions

AWS Health prend en charge les conditions IAM pour les opérations DescribeAffectedEntitieset DescribeEventDetailsAPI. Vous pouvez utiliser des conditions basées sur les ressources et les actions pour limiter les événements que l' AWS Health API envoie à un utilisateur, un groupe ou un rôle.

Pour ce faire, mettez à jour le `Condition` bloc de la politique IAM ou définissez l'`Resource`élément. Vous pouvez utiliser les conditions de chaîne pour restreindre l'accès en fonction de certains champs AWS Health d'événements.

Vous pouvez utiliser les champs suivants lorsque vous spécifiez un AWS Health événement dans votre politique :

- `eventTypeCode`
- `service`

> **Remarques**
>
> - Les opérations DescribeAffectedEntitieset DescribeEventDetailsAPI prennent en charge les autorisations au niveau des ressources. Par exemple, vous pouvez créer une politique pour autoriser ou refuser des AWS Health événements spécifiques.
> - Les opérations DescribeAffectedEntitiesForOrganizationet DescribeEventDetailsForOrganizationAPI ne prennent pas en charge les autorisations au niveau des ressources.
> - Pour plus d'informations, consultez la section Actions, ressources et clés de condition AWS Health APIs et notifications dans la référence d'autorisation de service.

Example : Condition basée sur des actions

Cette déclaration de politique accorde l'accès aux opérations de l' AWS Health `Describe*`API AWS Health Dashboard et interdit l'accès à tout AWS Health événement lié à Amazon EC2.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
```

```
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "health:service": "EC2"
                }
            }
        }
    ]
}
```

Example : Condition basée sur les ressources

La stratégie suivante a le même effet, mais utilise l'élément `Resource`.

```
{
  "Version": "2012-10-17",
  "Statement": [
  {
    "Effect": "Allow",
    "Action": [
      "health:Describe*"
    ],
    "Resource": "*"
  },
  {
    "Effect": "Deny",
    "Action": [
      "health:DescribeEventDetails",
      "health:DescribeAffectedEntities"
    ],
    "Resource": "arn:aws:health:*::event/EC2/*/*"
  }]
}
```

Example : eventTypeCode état

Cette déclaration de politique accorde l'accès aux opérations de l' AWS Health `Describe*`API AWS Health Dashboard et interdit l'accès à tout AWS Health événement `eventTypeCode` correspondant`AWS_EC2_*`.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "health:Describe*",
            "Resource": "*"
        },
        {
            "Effect": "Deny",
            "Action": [
                "health:DescribeAffectedEntities",
                "health:DescribeEventDetails"
            ],
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "health:eventTypeCode": "AWS_EC2_*"
                }
            }
        }
    ]
}
```

Important

Si vous appelez les DescribeEventDetailsopérations DescribeAffectedEntitieset que vous n'êtes pas autorisé à accéder à l' AWS Health événement, l'`AccessDeniedException`erreur apparaît. Pour de plus amples informations, veuillez consulter Résolution des problèmes AWS Health d'identité et d'accès.

Résolution des problèmes AWS Health d'identité et d'accès

Utilisez les informations suivantes pour diagnostiquer et résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS Health IAM.

Rubriques

- Je ne suis pas autorisé à effectuer une action dans AWS Health
- Je ne suis pas autorisé à effectuer iam : PassRole

- Je veux afficher mes clés d'accès
- Je suis administrateur et je souhaite autoriser d'autres personnes à accéder AWS Health
- Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Health ressources

Je ne suis pas autorisé à effectuer une action dans AWS Health

S'il vous AWS Management Console indique que vous n'êtes pas autorisé à effectuer une action, vous devez contacter votre administrateur pour obtenir de l'aide. Votre administrateur est la personne qui vous a fourni votre nom d'utilisateur et votre mot de passe.

L'`AccessDeniedException`erreur apparaît lorsqu'un utilisateur n'est pas autorisé à utiliser AWS Health Dashboard les opérations de l' AWS Health API.

Dans ce cas, l'administrateur de l'utilisateur doit mettre à jour la stratégie pour autoriser l'accès de l'utilisateur.

L' AWS Health API nécessite un plan Business, Enterprise On-Ramp ou Enterprise Support auprès de AWS Support. Si vous appelez l' AWS Health API depuis un compte qui n'a pas de plan Business, Enterprise On-Ramp ou Enterprise Support, le code d'erreur suivant est renvoyé : `SubscriptionRequiredException`

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS Health.

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 exécuter une action dans AWS Health. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction 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 de connexion.

Je veux afficher mes clés d'accès

Une fois les clés d'accès utilisateur IAM créées, vous pouvez afficher votre ID de clé d'accès à tout moment. Toutefois, vous ne pouvez pas revoir votre clé d'accès secrète. Si vous perdez votre clé d'accès secrète, vous devez créer une nouvelle paire de clés.

Les clés d'accès se composent de deux parties : un ID de clé d'accès (par exemple, `AKIAIOSFODNN7EXAMPLE`) et une clé d'accès secrète (par exemple, `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`). À l'instar d'un nom d'utilisateur et un mot de passe, vous devez utiliser à la fois l'ID de clé d'accès et la clé d'accès secrète pour authentifier vos demandes. Gérez vos clés d'accès de manière aussi sécurisée que votre nom d'utilisateur et votre mot de passe.

> **Important**
>
> Ne communiquez pas vos clés d'accès à un tiers, même pour qu'il vous aide à trouver votre ID utilisateur canonique. Ce faisant, vous pourriez donner à quelqu'un un accès permanent à votre Compte AWS.

Lorsque vous créez une paire de clé d'accès, enregistrez l'ID de clé d'accès et la clé d'accès secrète dans un emplacement sécurisé. La clé d'accès secrète est accessible uniquement au moment de sa création. Si vous perdez votre clé d'accès secrète, vous devez ajouter de nouvelles clés d'accès pour votre utilisateur IAM. Vous pouvez avoir un maximum de deux clés d'accès. Si vous en avez déjà deux, vous devez supprimer une paire de clés avant d'en créer une nouvelle. Pour afficher les instructions, consultez Gestion des clés d'accès dans le Guide de l'utilisateur IAM.

Je suis administrateur et je souhaite autoriser d'autres personnes à accéder AWS Health

Pour autoriser d'autres personnes à y accéder AWS Health, vous devez accorder l'autorisation aux personnes ou aux applications qui ont besoin d'y accéder. Si vous utilisez AWS IAM Identity Center pour gérer des personnes et des applications, vous attribuez des ensembles d'autorisations aux utilisateurs ou aux groupes afin de définir leur niveau d'accès. Les ensembles d'autorisations

créent et attribuent automatiquement des politiques IAM aux rôles IAM associés à la personne ou à l'application. Pour plus d'informations, consultez la section Ensembles d'autorisations dans le guide de AWS IAM Identity Center l'utilisateur.

Si vous n'utilisez pas IAM Identity Center, vous devez créer des entités IAM (utilisateurs ou rôles) pour les personnes ou les applications qui ont besoin d'un accès. Vous devez ensuite associer une politique à l'entité qui leur accorde les autorisations appropriées dans AWS Health. Une fois les autorisations accordées, fournissez les informations d'identification à l'utilisateur ou au développeur de l'application. Ils utiliseront ces informations d'identification pour y accéder AWS. Pour en savoir plus sur la création d'utilisateurs, de groupes, de politiques et d'autorisations IAM, consultez la section Identités, politiques et autorisations IAM dans le guide de l'utilisateur IAM.

Je souhaite autoriser des personnes extérieures à mon AWS compte à accéder à mes AWS Health ressources

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 ces fonctionnalités sont prises AWS Health en charge, consultezComment AWS Health 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 des rôles liés aux services pour AWS Health

AWS Health 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. AWS Health Les rôles liés au service sont prédéfinis AWS Health et incluent toutes les autorisations dont le service a besoin Services AWS pour appeler d'autres personnes à votre place.

Vous pouvez utiliser un rôle lié à un service pour le configurer afin AWS Health d'éviter d'ajouter manuellement les autorisations nécessaires. AWS Health définit les autorisations associées à ses rôles liés aux services et, sauf indication contraire, seul AWS Health 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.

Autorisations des rôles liés à un service pour AWS Health

AWS Health possède deux rôles liés au service :

- AWSServiceRoleForHealth_Organizations— Ce rôle fait confiance à AWS Health (`health.amazonaws.com`) pour assumer le rôle d'accès Services AWS pour vous. La politique `Health_OrganizationsServiceRolePolicy` AWS gérée est attachée à ce rôle.
- AWSServiceRoleForHealth_EventProcessor— Ce rôle fait confiance au principal du AWS Health service (`event-processor.health.amazonaws.com`) pour assumer le rôle à votre place. La politique `AWSHealth_EventProcessorServiceRolePolicy` AWS gérée est attachée à ce rôle. Le directeur du service utilise le rôle pour créer une règle EventBridge gérée par Amazon pour la détection et la réponse aux AWS incidents. Cette règle est l'infrastructure dont vous avez besoin Compte AWS pour transmettre les informations de changement d'état des alarmes de votre compte à AWS Health.

Pour plus d'informations sur les politiques AWS gérées, consultezAWS politiques gérées pour AWS Health.

Création d'un rôle lié à un service pour AWS Health

Il n'est pas nécessaire de créer le rôle AWSServiceRoleForHealth_Organizations lié à un service. Lorsque vous appelez l'EnableHealthServiceAccessForOrganizationopération, AWS Health crée pour vous le rôle lié à ce service dans le compte.

Vous devez créer manuellement le rôle AWSServiceRoleForHealth_EventProcessor lié au service dans votre compte. Pour plus d'informations, consultez Création d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Modification d'un rôle lié à un service pour AWS Health

AWS Health ne vous permet pas de modifier le rôle 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 IAM Guide de l'utilisateur.

Suppression d'un rôle lié à un service pour AWS Health

Pour supprimer le AWSServiceRoleForHealth_Organizations rôle, vous devez d'abord appeler l'DisableHealthServiceAccessForOrganizationopération. Vous pouvez ensuite supprimer le rôle via la console IAM, l'API IAM ou AWS Command Line Interface ()AWS CLI.

Pour supprimer le AWSServiceRoleForHealth_EventProcessor rôle, contactez AWS Support et demandez-leur de décharger vos charges de travail de la fonction AWS Incident Detection and Response. Une fois ce processus terminé, vous pouvez supprimer l'un des rôles via la console IAM, l'API IAM ou. AWS CLI

Informations connexes

Pour plus d'informations, consultez Utilisation des rôles liés à un service dans le Guide de l'utilisateur IAM.

AWS politiques gérées pour AWS Health

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 Health possède les politiques gérées suivantes.

Table des matières

Politique gérée par AWS : AWSHealth_EventProcessorServiceRolePolicy

AWS Health utilise la politique AWSHealth_EventProcessorServiceRolePolicy AWS gérée. Cette politique gérée est attachée au rôle lié à un service `AWSServiceRoleForHealth_EventProcessor`. La politique permet au rôle lié au service d'effectuer des actions à votre place. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour AWS Health.

La politique gérée dispose des autorisations suivantes pour autoriser l'accès AWS Health à la EventBridge règle Amazon pour la détection et la réponse aux AWS incidents.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `events`— Décrit et supprime EventBridge les règles, décrit et met à jour les cibles de ces règles.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Condition": {
                "StringEquals": {"events:ManagedBy": "event-
processor.health.amazonaws.com"}
            },
            "Action": [
                "events:DeleteRule",
                "events:RemoveTargets",
                "events:PutTargets",
                "events:PutRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        },
        {
            "Action": [
                "events:ListTargetsByRule",
                "events:DescribeRule"
            ],
            "Resource": "*",
            "Effect": "Allow"
        }
    ]
}
```

Pour obtenir la liste des modifications apportées à la politique, consultezAWS Health mises à jour des politiques AWS gérées.

Politique gérée par AWS : Health_OrganizationsServiceRolePolicy

AWS Health utilise la politique Health_OrganizationsServiceRolePolicy AWS gérée. Cette politique gérée est attachée au rôle lié à un service `AWSServiceRoleForHealth_Organizations`. La politique permet au rôle lié au service d'effectuer des actions à votre place. Vous ne pouvez pas attacher cette politique à vos entités IAM. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour AWS Health.

Cette politique accorde des autorisations permettant d'accéder AWS Health aux AWS Organizations informations requises pour la vue Health Organizational.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `organizations`— Décrit les comptes contenus dans Organizations AWS Organizations et ceux Services AWS qui peuvent être utilisés avec celles-ci.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListAccounts",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:ListDelegatedAdministrators",
                "organizations:DescribeOrganization",
                "organizations:DescribeAccount"
            ],
            "Resource": "*"
        }
    ]
}
```

Pour obtenir la liste des modifications apportées à la politique, consultezAWS Health mises à jour des politiques AWS gérées.

AWS politique gérée : AWSHealthFullAccess

AWS Health utilise la politique AWSHealthFullAccess AWS gérée. La politique accorde aux entités (utilisateurs ou rôles IAM) l'accès à la AWS Health console. Pour de plus amples informations, veuillez consulter Utilisation de la console AWS Health.

Détails de l'autorisation

Cette politique inclut les autorisations suivantes.

- `organizations`— Activez ou désactivez la fonctionnalité d'affichage AWS Health organisationnel pour tous les comptes d'une AWS organisation et affichez les unités organisationnelles (UO) du compte de gestion
- `health`— Accès aux opérations et aux notifications de l' AWS Health API
- `iam`— Crée un rôle IAM lié au service AWS Health

```
{
    "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "OrganizationWriteAccess",
                "Effect": "Allow",
                "Action": [
                    "organizations:EnableAWSServiceAccess",
                    "organizations:DisableAWSServiceAccess"
                ],
                "Resource": "*",
                "Condition": {
                    "StringEquals": {
                        "organizations:ServicePrincipal": "health.amazonaws.com"
                    }
                }
            },
            {
                "Sid": "HealthFullAccess",
                "Effect": "Allow",
                "Action": [
                    "health:*",
                    "organizations:DescribeAccount",
                    "organizations:ListAccounts",
                    "organizations:ListDelegatedAdministrators",
                    "organizations:ListParents"
                ],
                "Resource": "*"
            },
            {
                "Sid": "ServiceLinkAccess",
                "Effect": "Allow",
                "Action": "iam:CreateServiceLinkedRole",
                "Resource": "*",
```

```
                "Condition": {
                    "StringEquals": {
                        "iam:AWSServiceName": "health.amazonaws.com"
                    }
                }
            }
        ]
}
```

Pour obtenir la liste des modifications apportées à la politique, consultezAWS Health mises à jour des politiques AWS gérées.

AWS Health mises à jour des politiques AWS gérées

Consultez les détails des mises à jour des politiques AWS gérées AWS Health depuis que ce service a commencé à suivre ces modifications. Pour obtenir des alertes automatiques sur les modifications apportées à cette page, abonnez-vous au flux RSS de la page Historique du document pour AWS Health.

Le tableau suivant décrit les mises à jour importantes apportées aux politiques AWS Health gérées depuis le 13 janvier 2022.

AWS Health

Modification	Description	Date
AWS politique gérée : AWSHealthFullAccess : mise à jour d'une stratégie existante	AWS Health a étendu la AWSHealth FullAccess politique AWS GovCloud (US) Regions aux régions de Chine.	16 octobre 2023
Politique gérée par AWS : Health_OrganizationsService RolePolicy : mise à jour d'une stratégie existante	AWS Health a ajouté de nouvelles AWS Organizations actions pour permettre au rôle lié à un service de décrire les comptes et les AWS services	19 juillet 2023

Modification	Description	Date
	pouvant être utilisés avec. AWS Organizations	
Journal des modifications publié	Journal des modifications pour les politiques AWS Health gérées.	13 janvier 2023

Connexion et surveillance AWS Health

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Health et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Health, signaler tout problème et prendre des mesures le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Par exemple, vous pouvez CloudWatch suivre l'utilisation du processeur ou d'autres indicateurs de vos instances Amazon Elastic Compute Cloud (Amazon EC2) et lancer automatiquement de nouvelles instances en cas de besoin. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.
- Amazon EventBridge fournit un near-real-time flux d'événements système qui décrivent les modifications apportées aux AWS ressources. EventBridge permet une informatique automatisée axée sur les événements. Vous pouvez écrire des règles qui surveillent certains événements et déclenchent des actions automatisées dans d'autres services AWS lorsque ces événements se produisent. Pour de plus amples informations, veuillez consulter Surveillance des événements AWS Health avec Amazon EventBridge.
- AWS CloudTrailcapture les appels d'API et les événements associés effectués par ou pour le AWS compte de votre compte et transmet les fichiers journaux à un compartiment Amazon Simple Storage Service (Amazon S3) que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour de plus amples informations, veuillez consulter le Guide de l'utilisateur AWS CloudTrail.

Pour de plus amples informations, veuillez consulter Surveillance AWS Health.

Validation de conformité pour AWS Health

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 Health

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.

AWS Health les événements sont stockés et répliqués dans plusieurs zones de disponibilité. Cette approche garantit que vous pouvez y accéder à partir des opérations AWS Health Dashboard ou de l' AWS Health API. Vous pouvez consulter les AWS Health événements jusqu'à 90 jours après leur survenance.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Sécurité de l'infrastructure dans AWS Health

En tant que service géré, AWS Health il est protégé par les procédures de sécurité du réseau AWS mondial décrites dans le livre blanc Amazon Web Services : présentation des processus de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder AWS Health via le réseau. Les clients doivent supporter le protocole TLS (Sécurité de la couche transport) 1.0 ou une version ultérieure. Nous recommandons TLS 1.2 ou version ultérieure. Les clients doivent aussi prendre en charge les suites de chiffrement PFS (Perfect Forward Secrecy) comme Ephemeral Diffie-Hellman (DHE)

ou Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). 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.

Analyse de configuration et de vulnérabilité dans AWS Health

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 de sécurité pour AWS Health

Consultez les meilleures pratiques suivantes pour travailler avec AWS Health.

Accorder AWS Health aux utilisateurs des autorisations minimales possibles

Suivez le principe du minimum de privilèges en utilisant l'ensemble minimum d'autorisations de stratégie d'accès pour vos utilisateurs et groupes . Par exemple, vous pouvez autoriser un utilisateur AWS Identity and Access Management (IAM) à accéder au AWS Health Dashboard. Toutefois, vous pouvez ne pas permettre à ce même utilisateur d'activer ou de désactiver l'accès à AWS Organizations.

Pour de plus amples informations, veuillez consulter AWS Health exemples de politiques basées sur l'identité.

Consultez le AWS Health Dashboard

Vérifiez AWS Health Dashboard régulièrement votre compte pour identifier les événements susceptibles d'affecter votre compte ou vos applications. Par exemple, vous pouvez recevoir une notification d'événement concernant vos ressources, telle qu'une instance Amazon Elastic Compute Cloud (Amazon EC2) qui doit être mise à jour.

Pour de plus amples informations, veuillez consulter Commencer à utiliser votre AWS Health tableau de bord.

AWS Health Intégrez Amazon Chime ou Slack

Vous pouvez l'intégrer AWS Health à vos outils de chat. Cette intégration vous permet, à vous et à votre équipe, d'être informés AWS Health des événements en temps réel. Pour plus d'informations, consultez les AWS Health outils dans GitHub.

Surveillez les AWS Health événements

Vous pouvez intégrer AWS Health Amazon CloudWatch Events afin de créer des règles pour des événements spécifiques. Lorsque CloudWatch Events détecte un événement qui correspond à votre règle, vous êtes averti et pouvez ensuite prendre des mesures. CloudWatch Les événements sont spécifiques à une région. Vous devez donc configurer ce service dans la région dans laquelle réside votre application ou votre infrastructure.

Dans certains cas, la région de l' AWS Health événement ne peut pas être déterminée. Dans ce cas, l'événement apparaît par défaut dans la région USA Est (Virginie du Nord). Vous pouvez configurer CloudWatch des événements dans cette région pour vous assurer que vous surveillez ces événements.

Pour de plus amples informations, veuillez consulter Surveillance des événements AWS Health avec Amazon EventBridge.

Agrégation des AWS Health événements entre les comptes

Par défaut, vous pouvez l'utiliser AWS Health pour afficher les AWS Health événements d'un seul AWS compte. Si vous l'utilisez AWS Organizations, vous pouvez également consulter les AWS Health événements de manière centralisée au sein de votre organisation. Cette fonctionnalité permet d'accéder aux mêmes informations que les opérations de compte unique. Vous pouvez utiliser des filtres pour afficher les événements dans des AWS régions, des comptes et des services spécifiques.

Vous pouvez agréger les événements pour identifier les comptes de votre organisation concernés par un événement opérationnel ou être avertis en cas de failles de sécurité. Vous pouvez ensuite utiliser ces informations pour gérer et automatiser de manière proactive les événements de maintenance des ressources au sein de votre organisation. Utilisez cette fonctionnalité pour rester informé des modifications à venir apportées aux AWS services susceptibles de nécessiter des mises à jour ou des modifications de code.

Il est recommandé d'utiliser la fonctionnalité d'administrateur délégué pour déléguer l'accès à la vue AWS Health organisationnelle à un compte membre. Cela permet aux équipes opérationnelles d'accéder plus facilement aux AWS Health événements de votre organisation. La fonctionnalité d'administrateur délégué vous permet de restreindre votre compte de gestion, tout en offrant aux équipes la visibilité dont elles ont besoin pour agir en cas d' AWS Health événements.

⚠ Important

- AWS Health les événements envoyés pour des comptes de votre organisation apparaîtront dans la vue organisationnelle tant que l'événement est disponible, jusqu'à 90 jours, même si un ou plusieurs de ces comptes quittent votre organisation.
- Les événements d'organisation sont disponibles pendant 90 jours avant d'être supprimés. Ce quota ne peut pas être augmenté.

Prérequis

Avant d'utiliser la vue organisationnelle, vous devez :

- faire partie d'une organisation dans laquelle toutes les fonctions sont activées ;
- Connectez-vous au compte de gestion en tant qu'utilisateur AWS Identity and Access Management (IAM) ou assumez un rôle IAM.

Vous pouvez également vous connecter en tant qu'utilisateur root (ce n'est pas recommandé) dans le compte de gestion de votre organisation. Pour plus d'informations, voir Verrouiller les clés d'accès utilisateur root de votre AWS compte dans le guide de l'utilisateur IAM.

- Si vous vous connectez en tant qu'utilisateur IAM, utilisez une politique IAM qui accorde l'accès aux actions et AWS Health Organizations, telles que la AWSHealthFullAccesspolitique. Pour de plus amples informations, veuillez consulter AWS Health exemples de politiques basées sur l'identité.

Rubriques

Activation de la vue organisationnelle

Vous pouvez utiliser la AWS Health console pour obtenir une vue centralisée des événements liés à la santé au sein de votre AWS organisation.

La vue organisationnelle est disponible dans la AWS Health console pour tous les AWS Support forfaits sans frais supplémentaires.

> **Note**
>
> Si vous souhaitez autoriser les utilisateurs à accéder à cette fonctionnalité dans le compte de gestion, ils doivent disposer d'autorisations telles que la AWSHealthFullAccesspolitique. Pour de plus amples informations, veuillez consulter AWS Health exemples de politiques basées sur l'identité.

Enabling organizational view (Console)

Vous pouvez activer la vue organisationnelle depuis la AWS Health console. Vous devez vous connecter au compte de gestion de votre AWS organisation.

Pour consulter le AWS Health tableau de bord de votre organisation

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Dans le volet de navigation, sous État de santé de votre organisation, sélectionnez Configurations.
3. Sur la page Activer l'affichage organisationnel, choisissez Activer l'affichage organisationnel.
4. (Facultatif) Si vous souhaitez apporter des modifications à vos AWS organisations, par exemple en créant des unités organisationnelles (OUs), choisissez Gérer AWS Organizations.

   Pour plus d'informations, consultez Démarrer avec AWS Organizations dans le Guide de l'utilisateur AWS Organizations .

> **Remarques**
>
> - Lorsque vous activez l'affichage AWS Health organisationnel, le processus de chargement initial du compte s'exécute en arrière-plan et peut prendre plusieurs minutes. Vous pouvez fermer la AWS Health console et y revenir plus tard, car vous n'avez pas besoin d'attendre la fin du processus. Les événements de santé historiques (ceux créés avant que vous n'activiez la fonctionnalité) peuvent prendre jusqu'à 24 heures pour apparaître dans la vue de votre organisation.
> - Si vous avez un plan Business, Enterprise On-Ramp ou Enterprise Support, vous pouvez appeler l'opération DescribeHealthServiceStatusForOrganizationAPI pour vérifier l'état du processus.
> - Lorsque vous activez cette fonctionnalité, le rôle `AWSServiceRoleForHealth_Organizations` lié au service associé à la politique `Health_OrganizationsServiceRolePolicy` AWS gérée est appliqué au compte de gestion de l'organisation. Pour de plus amples informations, veuillez consulter Utilisation des rôles liés aux services pour AWS Health.

Enabling organizational view (CLI)

Vous pouvez activer la vue organisationnelle à l'aide de l'opération EnableHealthServiceAccessForOrganizationAPI.

Vous pouvez utiliser le AWS Command Line Interface (AWS CLI) ou votre propre code pour appeler cette opération.

> **Note**
>
> - Vous devez disposer d'un plan Business, Enterprise On-Ramp ou Enterprise Support pour appeler l' AWS Health API.
> - Vous devez utiliser le point de terminaison de la région USA Est (Virginie du Nord).

Example

La AWS CLI commande suivante active cette fonctionnalité depuis votre AWS compte. Vous pouvez utiliser cette commande depuis le compte de gestion ou depuis un compte qui peut assumer le rôle avec les autorisations requises.

```
aws health enable-health-service-access-for-organization --region us-east-1
```

Les exemples de code suivants appellent l'opération EnableHealthServiceAccessForOrganizationAPI.

Python

```
import boto3

client = boto3.client('health')

response = client.enable_health_service_access_for_organization()

print(response)
```

Java

Vous pouvez utiliser le AWS SDK pour la version Java 2.0 dans l'exemple suivant.

```
import software.amazon.awssdk.services.health.HealthClient;
import software.amazon.awssdk.services.health.HealthClientBuilder;

import software.amazon.awssdk.services.health.model.ConcurrentModificationException;
```

```
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationReques
import
 software.amazon.awssdk.services.health.model.EnableHealthServiceAccessForOrganizationRespon
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationRequ
import
 software.amazon.awssdk.services.health.model.DescribeHealthServiceStatusForOrganizationResp

import software.amazon.awssdk.auth.credentials.DefaultCredentialsProvider;

import software.amazon.awssdk.regions.Region;

public class EnableHealthServiceAccessDemo {
    public static void main(String[] args) {
        HealthClient client = HealthClient.builder()
            .region(Region.US_EAST_1)
            .credentialsProvider(
                DefaultCredentialsProvider.builder().build()
            )
            .build();

        try {
            DescribeHealthServiceStatusForOrganizationResponse statusResponse =
 client.describeHealthServiceStatusForOrganization(
                DescribeHealthServiceStatusForOrganizationRequest.builder().build()
            );

            String status =
 statusResponse.healthServiceAccessStatusForOrganization();
            if ("ENABLED".equals(status)) {
                System.out.println("EnableHealthServiceAccessForOrganization already
 enabled!");
                return;
            }

            client.enableHealthServiceAccessForOrganization(
                EnableHealthServiceAccessForOrganizationRequest.builder().build()
            );

            System.out.println("EnableHealthServiceAccessForOrganization is in
 progress");
        } catch (ConcurrentModificationException cme) {
```

```
            System.out.println("EnableHealthServiceAccessForOrganization is already
 in progress. Wait for the action to complete before trying again.");
        } catch (Exception e) {
            System.out.println("EnableHealthServiceAccessForOrganization FAILED: " +
 e);
        }
    }
}
```

Pour de plus amples informations, veuillez consulter lekit SDK AWS for Java 2.0 Developer Guide.

Lorsque vous activez cette fonctionnalité, le rôle `AWSServiceRoleForHealth_Organizations` lié au service associé à la politique `Health_OrganizationsServiceRolePolicy` AWS gérée est appliqué au compte de gestion de l'organisation.

> **Note**
>
> L'activation de cette fonction est un processus asynchrone qui prend du temps. Vous pouvez appeler l'DescribeHealthServiceStatusForOrganizationopération pour vérifier l'état du processus.

Affichage de la vue organisationnelle

Vous pouvez utiliser la AWS Health console pour obtenir une vue centralisée des événements liés à la santé au sein de votre AWS organisation.

La vue organisationnelle est disponible dans la AWS Health console pour tous les AWS Support forfaits sans frais supplémentaires.

> **Note**
>
> Si vous souhaitez autoriser les utilisateurs à accéder à cette fonctionnalité dans le compte de gestion, ils doivent disposer d'autorisations telles que AWSHealthFullAccesspolitique. Pour de plus amples informations, veuillez consulter AWS Health exemples de politiques basées sur l'identité.

Viewing organizational view events (Console)

Une fois que vous avez activé l'affichage organisationnel, AWS Health affiche les événements relatifs à l'état de santé de tous les comptes de votre organisation.

Lorsqu'un compte rejoint votre organisation, il est AWS Health automatiquement ajouté à la vue organisationnelle. Lorsqu'un compte quitte votre organisation, les nouveaux événements de ce compte ne sont plus connectés à la vue organisationnelle. Toutefois, les événements existants restent et vous pouvez toujours les interroger jusqu'à la limite de 90 jours.

AWS conserve les données relatives à la politique du compte pendant 90 jours à compter de la date d'entrée en vigueur de la fermeture du compte administrateur. À la fin de la période de 90 jours, supprime AWS définitivement toutes les données relatives à la politique du compte.

- Pour conserver les résultats pendant plus de 90 jours, vous pouvez archiver les politiques. Vous pouvez également utiliser une action personnalisée avec une EventBridge règle pour stocker les résultats dans un compartiment S3.
- Tant que les données AWS de politique sont conservées, lorsque vous rouvrez le compte fermé, le compte est AWS réaffecté en tant qu'administrateur du service et récupère les données de politique de service relatives au compte.
- Pour plus d'informations, consultez Clôture d'un compte.

> **Important**
>
> Pour les clients des AWS GovCloud (US) régions :
>
> - Avant de clôturer votre compte, sauvegardez puis supprimez les ressources de votre compte. Vous n'aurez plus accès à ces informations après la clôture du compte.

> **Note**
>
> Lorsque vous activez cette fonctionnalité, la AWS Health console peut afficher les événements publics depuis le AWS Health tableau de bord — État du service au cours des 7 derniers jours. Ces événements publics ne sont pas spécifiques aux comptes de votre organisation. Événements du AWS Health tableau de bord — La santé des services fournit des informations publiques sur la disponibilité régionale des AWS services.

Vous pouvez consulter les événements d'affichage organisationnel dans les pages suivantes :.

Numéros ouverts et récents

Vous pouvez utiliser l'onglet Problèmes ouverts et récents pour consulter les événements susceptibles d'affecter votre AWS infrastructure, tels que les modifications apportées à votre organisation Services AWS et les ressources qui l'affectent.

Pour afficher les événements de l'organisation, consultez les événements

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Dans le volet de navigation, sous État de santé de votre organisation, sélectionnez Problèmes ouverts et récents pour afficher les événements récemment signalés.
3. Choisissez un événement. Dans l'onglet Détails, vous pouvez consulter les informations suivantes concernant l'événement :

   - Nom de l'événement
   - Statut
   - Région/Zone de disponibilité
   - Comptes concernés
   - L'heure de début
   - L'heure de fin
   - Catégorie
   - Description

Changements planifiés

Utilisez l'onglet Modifications planifiées pour consulter les événements à venir susceptibles d'affecter votre organisation. Ces événements peuvent inclure des activités de maintenance planifiées pour les services.

Autres notifications

Utilisez l'onglet Notifications pour consulter toutes les autres notifications et les événements en cours des sept derniers jours susceptibles d'affecter votre organisation. Cela peut inclure des événements tels que des rotations de certificats, des notifications de facturation et des failles de sécurité.

Event Log

Vous pouvez également utiliser l'onglet Journal des événements pour afficher les AWS Health événements à des fins d'organisation. La disposition et le comportement des colonnes sont similaires à ceux de l'onglet Problèmes ouverts et récents, sauf que l'onglet Journal des événements inclut des colonnes supplémentaires et des options de filtre, telles que la catégorie d'événement, le statut et l'heure de début.

Pour afficher les événements d'affichage organisationnel dans l'onglet Journal des événements

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Dans le volet de navigation, sous État de santé de votre organisation, sélectionnez Journal des événements.
3. Sous Journal des événements, choisissez le nom de l'événement. Vous pouvez consulter les informations suivantes concernant l'événement :

   - Nom de l'événement
   - Statut
   - Région/Zone de disponibilité
   - Comptes concernés
   - L'heure de début
   - L'heure de fin
   - Catégorie
   - Description

Viewing affected accounts and resources (Console)

Sous État de santé de votre organisation, vous pouvez consulter les comptes de votre organisation concernés par l'événement et toutes les ressources associées. Par exemple, s'il y a un événement à venir concernant la maintenance des instances Amazon Elastic Compute Cloud (Amazon EC2), les comptes de votre organisation dotés d' EC2 instances Amazon peuvent apparaître dans l'onglet Détails. Vous pouvez identifier les ressources spécifiques, puis contacter le propriétaire du compte.

Pour consulter les comptes et les ressources concernés

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.

2. Dans le volet de navigation, sous État de santé de votre organisation, sélectionnez l'un des onglets.
3. Choisissez un événement dont la valeur est réservée aux comptes concernés.
4. Choisissez l'onglet Comptes concernés.
5. Choisissez Afficher les détails du compte pour afficher les informations suivantes relatives aux comptes :

   - ID de compte
   - Nom du compte
   - Adresse e-mail principale
   - Unité d'organisation (UO)
6. Développez le compte pour afficher les ressources concernées.
7. S'il y a plus de 10 ressources, choisissez Afficher toutes les ressources pour les afficher.
8. Pour filtrer par ID de compte pour cet événement spécifique, procédez comme suit :

   a. Dans l'onglet Comptes concernés, choisissez Ajouter un filtre, choisissez ID de compte, puis entrez l'ID de compte. Vous ne pouvez saisir qu'un seul identifiant de compte à la fois.

   b. Choisissez Appliquer. Le compte que vous avez saisi apparaît dans la liste.

Viewing organizational view events (CLI)

Après avoir activé cette fonctionnalité, AWS Health commence à enregistrer les événements qui affectent les comptes de l'organisation. Lorsqu'un compte rejoint votre organisation, AWS Health ajoute automatiquement le compte à la vue organisationnelle.

> **Note**
>
> AWS Health n'enregistre pas les événements survenus dans votre organisation avant que vous n'activiez l'affichage organisationnel.

Lorsqu'un compte quitte votre organisation, les nouveaux événements de ce compte ne sont plus connectés à la vue organisationnelle. Toutefois, les événements existants restent et vous pouvez toujours les interroger jusqu'à la limite de 90 jours.

AWS conserve les données relatives à la politique du compte pendant 90 jours à compter de la date d'entrée en vigueur de la fermeture du compte administrateur. À la fin de la période de 90 jours, supprime AWS définitivement toutes les données relatives à la politique du compte.

- Pour conserver les résultats pendant plus de 90 jours, vous pouvez archiver les politiques. Vous pouvez également utiliser une action personnalisée avec une EventBridge règle pour stocker les résultats dans un compartiment S3.
- Tant que les données AWS de politique sont conservées, lorsque vous rouvrez le compte fermé, le compte est AWS réaffecté en tant qu'administrateur du service et récupère les données de politique de service relatives au compte.
- Pour plus d'informations, consultez Clôture d'un compte.

> **Important**
>
> Pour les clients des AWS GovCloud (US) régions :
>
> - Avant de clôturer votre compte, sauvegardez puis supprimez les ressources de votre compte. Vous n'aurez plus accès à ces informations après la clôture du compte.

Vous pouvez utiliser les opérations de l' AWS Health API pour renvoyer des événements du point de vue organisationnel.

Example : décrire les événements de la vue organisationnelle

La AWS CLI commande suivante renvoie les événements relatifs à l'état AWS des comptes de votre organisation.

```
aws health describe-events-for-organization --region us-east-1
```

Désactivation de la vue organisationnelle

Si vous ne souhaitez pas agréger les événements de votre organisation, vous pouvez désactiver cette fonctionnalité depuis le compte de gestion ou désactiver l'affichage organisationnel à l'aide de l'opération DisableHealthServiceAccessForOrganizationAPI.

Disabling organizational view events (Console)

AWS Health arrête d'agréger les événements pour tous les autres comptes de votre organisation. Vous pouvez continuer à consulter les événements précédents de votre organisation jusqu'à ce qu'ils soient supprimés.

Pour désactiver l'affichage organisationnel

1. Ouvrez votre AWS Health tableau de bord à la https://health.aws.amazon.com/health/maison.
2. Dans le volet de navigation, sous État de santé de votre organisation, sélectionnez Configurations.
3. Sur la page Activer l'affichage organisationnel, choisissez Désactiver l'affichage organisationnel.

Une fois cette fonctionnalité désactivée, elle AWS Health n'agrège plus les événements de votre organisation. Toutefois, le rôle lié au service reste dans le compte de gestion jusqu'à ce que vous le supprimiez via la console AWS Identity and Access Management (IAM), l'API IAM ou (). AWS Command Line Interface AWS CLI Pour plus d'informations, consultez Suppression d'un rôle lié à un service dans le Guide de l'utilisateur IAM.

Disabling organizational view events (CLI)

Example

La AWS CLI commande suivante désactive cette fonctionnalité de votre compte.

```
aws health disable-health-service-access-for-organization --region us-east-1
```

> **Note**
>
> Vous pouvez également désactiver la fonctionnalité organisationnelle à l'aide de l'opération Organizations Disable AWSService Access API. Une fois que vous avez appelé cette opération, AWS Health arrête l'agrégation des événements pour tous les autres comptes de votre organisation. Si vous appelez les opérations AWS Health d'API pour une vue organisationnelle, AWS Health renvoie une erreur. AWS Health continue d'agréger les événements de santé associés à votre AWS compte.

Une fois cette fonctionnalité désactivée, il AWS Health n'agrège plus les événements de votre organisation. Toutefois, le rôle lié au service reste dans le compte de gestion jusqu'à ce que vous le supprimiez via la console AWS Identity and Access Management (IAM), l'API IAM ou. AWS CLI Pour plus d'informations, consultez la section Suppression d'un rôle lié à un service dans le guide de l'utilisateur IAM.

Gestion des vues d'administrateur déléguées pour une organisation

Avec AWS Health, vous pouvez tirer parti de la fonctionnalité d'administrateur délégué AWS Organizations qui permet à un compte autre que le compte de gestion de consulter les AWS Health événements agrégés sur le AWS Health tableau de bord ou par programmation via l'AWS Health API. La fonction d'administrateur délégué permet aux différentes équipes de consulter et de gérer les événements sanitaires au sein de votre organisation en toute flexibilité. Dans la mesure du AWS possible, il est recommandé de déléguer des responsabilités en dehors du compte de gestion.

Table des matières

Enregistrement d'un administrateur délégué pour votre vue organisationnelle

Après avoir activé la vue organisationnelle pour votre organisation, vous pouvez enregistrer jusqu'à cinq comptes membres dans votre organisation en tant qu'administrateur délégué. Pour ce faire, appelez l'opération RegisterDelegatedAdministratorAPI. Une fois que vous avez enregistré les comptes des membres, ceux-ci sont des comptes d'administration délégués et peuvent accéder à la vue AWS Health organisationnelle depuis le AWS Health tableau de bord. Si le compte dispose d'un plan Business, Enterprise On-Ramp ou Enterprise Support, les administrateurs délégués peuvent utiliser l' AWS Health API pour accéder à la vue AWS Health organisationnelle.

Pour établir un administrateur délégué, depuis le compte de gestion de votre organisation, appelez la commande suivante AWS Command Line Interface (AWS CLI). Vous pouvez utiliser cette commande depuis le compte de gestion ou depuis un compte qui peut assumer le rôle avec les AWS Identity and Access Management autorisations requises. Dans l'exemple de commande suivant, remplacez ACCOUNT_ID par l'ID du compte de membre que vous souhaitez enregistrer avec le principal de AWS Health service « health.amazonaws.com ».

```
aws organizations register-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Une fois qu'un administrateur délégué est enregistré, vous avez une visibilité sur tous les AWS Health événements affectant les comptes de votre organisation. Vous pouvez consulter l'historique des événements survenus au cours des 90 derniers jours ou depuis que la fonctionnalité d'affichage organisationnel a été activée pour la première fois, selon la date la plus récente. Notez que l'activation de la fonctionnalité d'administrateur délégué est un processus asynchrone qui prend jusqu'à une minute.

Supprimer un administrateur délégué de votre vision organisationnelle

Pour supprimer l'accès d'un administrateur délégué, appelez l'opération DeregisterDelegatedAdministratorAPI.

Depuis le compte de gestion de votre organisation, appelez la AWS CLI commande suivante pour supprimer un compte membre en tant qu'administrateur délégué. Dans l'exemple de commande suivant, remplacez ACCOUNT_ID par l'ID du compte membre que vous souhaitez supprimer.

```
aws organizations deregister-delegated-administrator --account-id ACCOUNT_ID --service-
principal  health.amazonaws.com
```

Surveillance des événements AWS Health avec Amazon EventBridge

Vous pouvez utiliser Amazon EventBridge pour détecter les AWS Health événements et y réagir. Ensuite, en fonction des règles que vous créez, EventBridge invoque une ou plusieurs actions cibles lorsqu'un événement correspond aux valeurs que vous spécifiez dans une règle. Selon le type d'événement, vous pouvez saisir des informations sur l'événement, initier des événements supplémentaires, envoyer des notifications, prendre des mesures correctives ou effectuer d'autres actions. Par exemple, vous pouvez AWS Health recevoir des notifications par e-mail si vous disposez de AWS ressources dont les mises à jour sont programmées, telles que des instances Amazon Elastic Compute Cloud (Amazon EC2). Compte AWS

Remarques

- AWS Health organise des événements dans la mesure du possible. La livraison des événements n'est pas toujours garantie EventBridge.
- Toutes EventBridge les règles que vous créez ne peuvent recevoir des notifications que pour votre Compte AWS. Pour recevoir des événements organisationnels pour d'autres comptes au sein du vôtre AWS Organizations, consultez la section Agrégation d' AWS Health événements à l'aide de la vue organisationnelle et de l'accès administrateur délégué.

Vous pouvez choisir entre plusieurs types de cibles dans EventBridge le cadre de votre AWS Health flux de travail, notamment :

- AWS Lambda fonctions
- Amazon Kinesis Data Streams
- Files d'attente Amazon Simple Queue Service (Amazon SQS)
- Cibles intégrées (telles que les actions CloudWatch d'alarme)
- Rubriques Amazon Simple Notification Service (Amazon SNS)

Par exemple, vous pouvez utiliser une fonction Lambda pour transmettre une notification à un canal Slack lorsqu'un AWS Health événement se produit. Vous pouvez également utiliser Lambda

EventBridge pour envoyer des notifications personnalisées par texte ou SMS avec Amazon SNS lorsqu' AWS Health un événement se produit.

Pour des exemples d'automatisation et d'alertes personnalisées que vous pouvez créer en réponse à AWS Health des événements, consultez les AWS Health outils dans GitHub.

Rubriques

Création de EventBridge règles de Région AWS couverture

Vous devez créer une EventBridge règle pour chaque région pour laquelle vous souhaitez recevoir AWS Health des événements. Si vous ne créez pas de règle, vous ne recevrez aucun événement. Par exemple, pour recevoir des événements de la région USA Ouest (Oregon), vous devez créer une règle pour cette région.

La configuration d'une règle supplémentaire dans une région de sauvegarde ajoute un niveau de résilience supplémentaire à vos flux de travail, si votre règle principale est affectée par un événement en cours. Les événements publics pour AWS Health sont envoyés simultanément à la région concernée et à une région secondaire. Consultez À propos des événements publics pour AWS Health pour plus d'informations. Pour toutes les régions de la partition AWS standard, vous pouvez

configurer une règle dans l'ouest des États-Unis (Oregon) en tant que sauvegarde afin de continuer à recevoir des événements même si votre région principale est affectée par un problème persistant. La région de sauvegarde pour la région USA Ouest (Oregon) est la région USA Est (Virginie du Nord).

Par exemple, si vous surveillez des événements dans la région Europe (Francfort) et que cette région est temporairement indisponible, vous AWS Health diffuserez également cet événement dans la région de l'ouest des États-Unis (Oregon). Ensuite, votre EventBridge règle de sauvegarde envoie l'événement aux cibles que vous avez spécifiées. Pour créer une règle de sauvegarde, suivez la procédure ci-dessous Configuration d'une EventBridge règle pour envoyer des notifications concernant des événements dans AWS Health et utilisez la région de l'ouest des États-Unis (Oregon).

Certains AWS Health événements ne sont pas spécifiques à une région. Les événements qui ne sont pas spécifiques à une région sont appelés événements mondiaux. Il s'agit notamment des événements envoyés pour AWS Identity and Access Management (IAM). Pour recevoir des événements internationaux, vous devez créer une règle pour la région USA Est (Virginie du Nord) pour la région principale et pour la région USA Ouest (Oregon) en tant que région secondaire.

Pour recevoir des événements internationaux dans le AWS GovCloud (US), vous devez créer une règle dans la région AWS GovCloud (ouest des États-Unis).

Surveillance des événements publics et spécifiques au compte pour AWS Health

Lorsque vous créez une EventBridge règle pour surveiller des événements AWS Health, celle-ci propose à la fois des événements spécifiques au compte et des événements publics :

- Les événements spécifiques au compte affectent votre compte et vos ressources, tels qu'un événement vous informant d'une mise à jour requise d'une EC2 instance Amazon ou d'autres événements de modification planifiés.
- Les événements publics apparaissent sur le AWS Health tableau de bord — État des services. Les événements publics ne sont pas spécifiques à la disponibilité régionale d'un service Comptes AWS et ne fournissent pas d'informations publiques à ce sujet.

> **Important**
>
> Pour recevoir les deux types d'événements, votre règle doit utiliser la `"source": [ "aws.health"]` valeur. Les caractères génériques, tels que ceux qui `"source": [ "aws.health*"]` ne correspondent à aucun événement, ne correspondent au modèle à surveiller.

Si vous surveillez des événements publics à partir d'un Région AWS, nous vous recommandons de créer une règle de sauvegarde. Les événements publics pour AWS Health sont envoyés simultanément à la région concernée et à une région secondaire. Il est recommandé de dédupliquer les AWS Health événements à l'aide d'EventArn et de CommunicationID, car ceux-ci restent cohérents pour les AWS Health messages envoyés à la région de sauvegarde.

Vous pouvez déterminer si un événement est public ou spécifique à un compte dans EventBridge, à l'aide du eventScopeCode paramètre. Les événements peuvent avoir le `PUBLIC` ou`ACCOUNT_SPECIFIC`. Vous pouvez également filtrer votre règle en fonction de ce paramètre.

Exemple : événements publics pour Amazon Elastic Compute Cloud

L'événement suivant montre un problème opérationnel pour Amazon EC2 dans la région USA Est (Virginie du Nord).


```
{
    "version": "0",
    "id": "fd9d4512-1eb0-50f6-0491-d016ae56aef0",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-02-15T10:07:10Z",
    "region": "us-east-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:us-east-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Wed, 15 Feb 2023 22:07:07 GMT",
```

```
        "lastUpdatedTime": "Wed, 15 Feb 2023 22:07:07 GMT",
        "statusCode": "open",
        "eventRegion": "us-east-1",
        "eventDescription": [{
            "latestDescription": "We are investigating increased API Error rates and
 Latencies for Amazon Elastic Compute Cloud in the US-EAST-1 Region.",
            "language": "en_US"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"

    }
}
```

Installation d'un rôle lié à un service pour utiliser la détection et la réponse aux AWS incidents

Si vous utilisez AWS Incident Detection and Response pour votre compte, vous devez installer le rôle `AWSServiceRoleForHealth_EventProcessor` lié au service dans votre compte.

Ce rôle fait confiance au directeur du `event-processor.health.amazonaws.com` service pour assumer le rôle. La politique `AWSHealth_EventProcessorServiceRolePolicy` AWS gérée est attachée à ce rôle. Cette politique répertorie les autorisations que le rôle peut effectuer, par exemple en appelant d'autres personnes Services AWS pour vous.

Ce rôle crée ensuite une règle EventBridge gérée par Amazon dans votre compte. La règle est nomméeAWSHealthEventProcessor-DO-NOT-DELETE. Cette règle constitue l'infrastructure requise pour votre compte afin de EventBridge pouvoir transmettre les informations de changement d'état des alarmes de votre compte à AWS Health.

Informations connexes

Pour en savoir plus, consultez les sujets suivants :

- Utilisation des rôles liés aux services pour AWS Health
- Politique gérée par AWS : AWSHealth_EventProcessorServiceRolePolicy

Afficher les listes paginées d' AWS Health événements sur EventBridge

AWS Health prend en charge la pagination des AWS Health événements lorsque la liste des messages dépasse `resources` ou `affectedEntities` fait en sorte que la taille EventBridge du message dépasse la limite de 256 Ko.

AWS Health inclut tous les `detail.affectedEntities` champs `resources` et tous les champs du message. Si cette liste `resources` et ces `detail.affectedEntities` valeurs dépassent 256 Ko, AWS Health divisez l'événement médical en plusieurs pages et publiez ces pages sous forme de messages individuels dans. EventBridge Chaque page conserve `eventARN` les mêmes `communicationId` valeurs pour aider à recombiner la liste des pages `resources` ou une `detail.affectedEntities` fois celles-ci reçues.

Ces messages supplémentaires peuvent générer des messages inutiles, par exemple lorsque la EventBridge règle est dirigée vers une interface lisible par l'homme telle que le courrier électronique ou le chat. Les clients dont les notifications sont lisibles par l'homme peuvent ajouter un filtre pour que le `detail.page` champ ne traite que la première page, ce qui élimine les messages inutiles créés à partir des pages suivantes.

Dans le schéma, chaque communicationID inclut le numéro de page avec un trait d'union après le communicationID, même s'il n'y a qu'une seule page. Les champs `detail.page` et `detail.totalPages` décrivent le numéro de page actuel et le nombre total de pages de l' AWS Health événement. Les informations contenues dans chaque message paginé sont les mêmes, à l'exception de la liste de `detail.affectedEntities` ou`resources`. Ces listes peuvent être reconstruites une fois que toutes les pages ont été reçues. Les pages des ressources et entités concernées sont indépendantes de la commande.

Agrégation d' AWS Health événements à l'aide de la vue organisationnelle et de l'accès administrateur délégué

AWS Health prend en charge la vue organisationnelle et l'accès administrateur délégué pour les AWS Health événements publiés sur Amazon EventBridge. Lorsque la vue organisationnelle est activée AWS Health, le compte de gestion ou un compte d'administrateur délégué reçoit un flux unique d' AWS Health événements provenant de tous les comptes de votre organisation dans AWS Organizations.

Cette fonctionnalité est conçue pour fournir une vue centralisée afin de faciliter la gestion AWS Health des événements au sein de votre organisation. La configuration de l'affichage organisationnel et d'une EventBridge règle dans le compte de gestion ne désactive pas EventBridge les règles des autres comptes de votre organisation.

Pour plus d'informations sur l'activation de la vue organisationnelle et de l'accès administrateur délégué AWS Health, consultez la section Agrégation des AWS Health événements.

Intégration de la surveillance des AWS Health événements et des notifications avec JIRA et ServiceNow

Vous pouvez intégrer AWS Health des événements à JIRA et ServiceNow recevoir des informations opérationnelles et de compte, préparer les modifications planifiées et gérer les événements de santé à l'aide du Service Management Connector (SMC). L'intégration avec SMC AWS Health peut utiliser les événements Health envoyés pour créer, EventBridge cartographier et mettre à jour automatiquement des tickets et ServiceNow des incidents JIRA.

Vous pouvez utiliser la vue organisationnelle et l'accès administrateur délégué pour gérer facilement les événements de santé au sein de l'organisation dans JIRA et ServiceNow intégrer les AWS Health informations directement dans le flux de travail de votre équipe.

Pour plus d'informations sur ServiceNow l'intégration à l'aide du SMC, consultez la section Intégration AWS Health dans ServiceNow.

Pour plus d'informations sur l'intégration de JIRA Management Cloud à l'aide du SMC, consultez AWS Health JIRA.

Configuration d'une EventBridge règle pour envoyer des notifications concernant des événements dans AWS Health

Vous pouvez créer une EventBridge règle pour être informé des AWS Health événements survenus dans votre compte. Avant de créer des règles d'événement pour AWS Health, procédez comme suit :

- Familiarisez-vous avec les événements, les règles et les cibles dans EventBridge. Pour plus d'informations, consultez Qu'est-ce qu'Amazon EventBridge ? dans le guide de EventBridge l'utilisateur Amazon et dans Nouveau EventBridge — Suivez et répondez aux modifications apportées à vos AWS ressources.

- Créez la ou les cible(s) à utiliser dans vos règles d'événement.

Pour créer une EventBridge règle pour AWS Health

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Pour modifier le Région AWS, utilisez le sélecteur de région dans le coin supérieur droit de la page. Choisissez la région dans laquelle vous souhaitez suivre les AWS Health événements.
3. Dans le volet de navigation, choisissez Règles.
4. Choisissez Create rule (Créer une règle).
5. Sur la page Define rule detail (Définir les informations de la règle), saisissez un nom et une description pour votre règle.
6. Conservez les valeurs par défaut pour Event bus (Bus d'événement) et Rule Type (Type de règle), puis choisissez Next (Suivant).
7. Sur la page Créer un modèle d'événement, dans Source d'événement, sélectionnez AWS événements et événements EventBridge partenaires.
8. Sous Modèle d'événement, dans Source d'événement, sélectionnez Services AWS.
9. Sous Modèle d'événement, pour Service AWS, choisissez Health.
10. Pour Type d'événement, choisissez l'une des options suivantes.
    - Specific Health Abuse Events : créez une règle pour les AWS Health événements dont le nom du type d'événement contient le mot`Abuse`.
    - Événements de santé spécifiques : créez une règle pour les événements spécifiques Service AWS, tels qu'Amazon EC2.
11. Vous pouvez choisir n'importe quel service ou Service (s) spécifique (s). Si vous avez choisi un service spécifique, choisissez l'une des options suivantes :
    - Choisissez N'importe quelle catégorie de type d'événement pour créer une règle qui s'applique à toutes les catégories de types d'événements.
    - Choisissez une ou plusieurs catégories de type d'événement spécifiques, puis choisissez une valeur dans la liste, telle que issue, AccountNotification ou ScheduledChange.

> **Tip**
>
> - Pour surveiller tous les AWS Health événements relatifs à un service spécifique, nous vous recommandons de choisir N'importe quelle catégorie de type d'événement et N'importe quelle ressource. Cela garantit que votre règle surveille tous les AWS Health

événements, y compris les nouveaux codes de type d'événement, pour le service que vous avez spécifié. Pour un exemple de règle, consultez tous les EC2 événements Amazon.

- Vous pouvez créer une règle pour surveiller plusieurs catégories de services ou d'événements. Pour ce faire, vous devez mettre à jour manuellement le modèle d'événement de la règle. Pour de plus amples informations, veuillez consulter Création d'une règle pour plusieurs services et catégories.

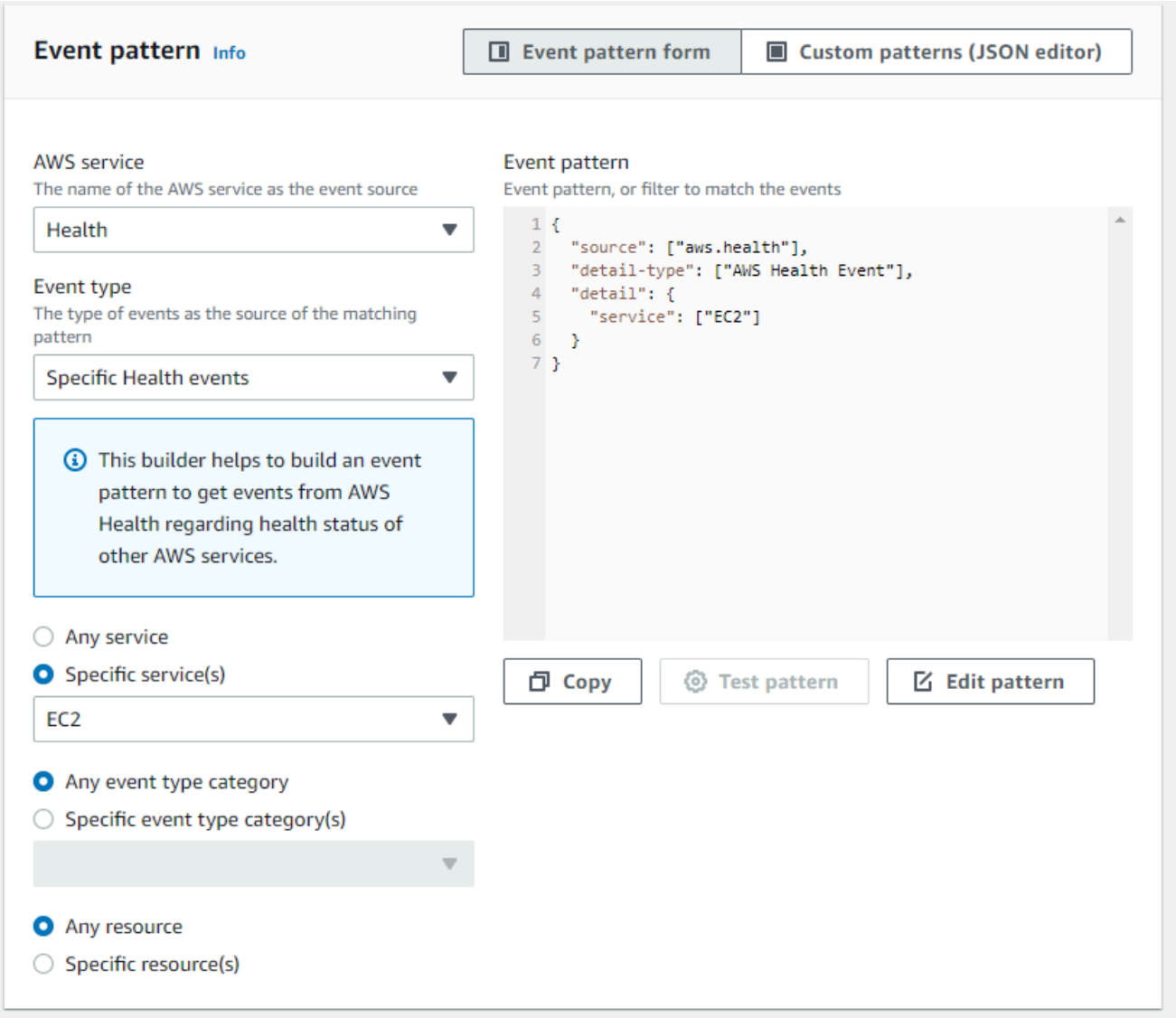
12. Si vous avez choisi une catégorie de service et de type d'événement spécifique, choisissez l'une des options suivantes pour les codes de type d'événement.
    - Choisissez N'importe quel code de type d'événement pour créer une règle qui s'applique à tous les codes de type d'événement.
    - Choisissez un ou plusieurs codes de type d'événement spécifiques, puis choisissez une ou plusieurs valeurs dans la liste. Cela crée une règle qui s'applique uniquement à des codes de type d'événement spécifiques. Par exemple, si vous choisissez **`AWS_EC2_INSTANCE_STOP_SCHEDULED`**et **`AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`**, votre règle s'applique uniquement à ces événements lorsqu'ils se produisent dans votre compte.
13. Choisissez l'une des options suivantes pour les ressources concernées.
    - Choisissez N'importe quelle ressource pour créer une règle qui s'applique à toutes les ressources.
    - Choisissez Ressource (s) spécifique (s) et saisissez une ou plusieurs ressources. IDs Par exemple, vous pouvez spécifier un ID d' EC2 instance Amazon, par exemple*`i-EXAMPLEa1b2c3de4`*, pour surveiller les événements qui n'affectent que cette ressource.
14. Passez en revue la configuration de vos règles afin qu'elle réponde à vos exigences en matière de surveillance des événements.
15. Choisissez Suivant.
16. Sur la page Sélectionner une ou plusieurs cibles, choisissez le type de cible que vous avez créé pour cette règle, puis configurez les options supplémentaires requises pour ce type. Par exemple, vous pouvez envoyer l'événement à une file d'attente Amazon SQS ou à une rubrique Amazon SNS.
17. Choisissez Suivant.
18. (Facultatif) Sur la page Configure tags (Configurer des étiquettes), ajoutez des étiquettes, puis choisissez Next (Suivant).

- Remarque : les balises ne sont actuellement pas envoyées par la source aws.health dans. EventBridge

19. Sur la page Vérifier et créer, examinez la configuration de votre règle et assurez-vous qu'elle répond à vos exigences en matière de surveillance d'événements.
20. Choisissez Créer une règle.

Example : Règle pour tous les EC2 événements Amazon

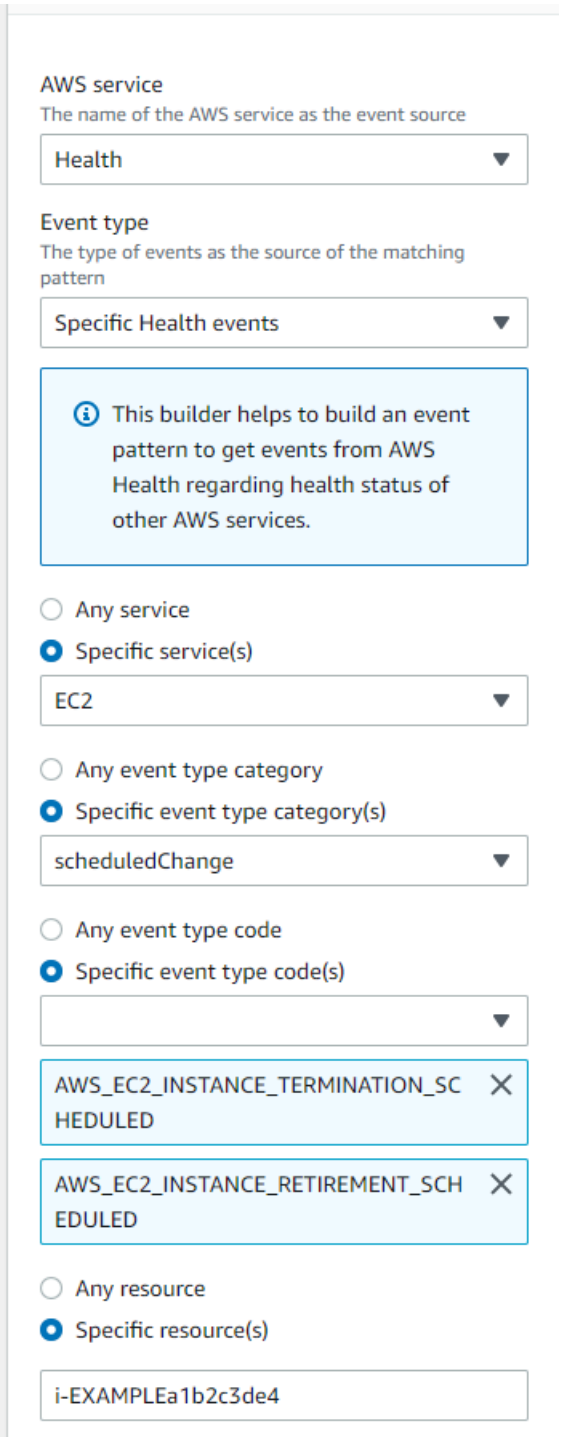
L'exemple suivant crée une règle qui EventBridge surveille tous les EC2 événements Amazon, y compris les catégories de types d'événements, les codes d'événements et les ressources.



Example : Règle pour des EC2 événements Amazon spécifiques

L'exemple suivant crée une règle afin de EventBridge contrôler les éléments suivants :

- Le EC2 service Amazon
- Catégorie de type d'événement ScheduledChange
- Les codes de type d'événement pour `AWS_EC2_INSTANCE_TERMINATION_SCHEDULED` et `AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED`
- L'instance avec l'ID `i-EXAMPLEa1b2c3de4`



Création d'une règle pour plusieurs services et catégories

Les exemples de la procédure précédente vous montrent comment créer une règle pour une seule catégorie de service et de type d'événement. Vous pouvez également créer une règle pour plusieurs catégories de services et de types d'événements. Cela signifie qu'il n'est pas nécessaire de créer une

règle distincte pour chaque service et chaque catégorie que vous souhaitez surveiller. Pour ce faire, vous devez modifier le modèle d'événement, puis saisir vos modifications manuellement.

Vous pouvez utiliser l'une des options suivantes.

Pour ajouter des services et des catégories à une règle existante

1. Dans la EventBridge console, sur la page Règles, choisissez le nom de la règle.
2. Dans le coin supérieur droit, choisissez Modifier.
3. Choisissez Suivant.
4. Pour Modèle d'événement, choisissez Modifier le modèle, puis entrez vos modifications dans le champ de texte.
5. Choisissez Suivant jusqu'à ce que vous atteigniez la page de révision et de mise à jour.
6. Choisissez Mettre à jour la règle pour enregistrer vos modifications.

Pour ajouter des services et des catégories pour une nouvelle règle

1. Suivez la procédure décrite Configuration d'une EventBridge règle pour envoyer des notifications concernant des événements dans AWS Health à l'étape 9.
2. Au lieu de choisir un seul service ou une seule catégorie dans les listes, dans le champ Modèle d'événement, choisissez Modifier le modèle.
3. Entrez vos modifications dans le champ de texte. Consultez l'exemple de modèle suivant comme modèle pour créer votre propre modèle d'événement.
4. Passez en revue votre modèle d'événement, puis suivez le reste de la procédure Configuration d'une EventBridge règle pour envoyer des notifications concernant des événements dans AWS Health pour créer votre règle.

Utilisez l'API ou AWS Command Line Interface (AWS CLI)

Pour une règle nouvelle ou existante, utilisez l'opération d'PutRuleAPI ou la `aws events put-rule` commande pour mettre à jour le modèle d'événement. Pour un exemple de AWS CLI commande, voir put-rule dans la référence des AWS CLI commandes.

Example Exemple : plusieurs catégories de services et de types d'événements

Le modèle d'événement suivant crée une règle pour surveiller les événements pour les catégories `issue`,`accountNotification`, et type d'`scheduledChange`événement pour trois AWS services : Amazon EC2, Amazon EC2 Auto Scaling et Amazon VPC.

```
{
  "detail": {
    "eventTypeCategory": [
      "issue",
      "accountNotification",
      "scheduledChange"
    ],
    "service": [
      "AUTOSCALING",
      "VPC",
      "EC2"
    ]
  },
  "detail-type": [
    "AWS Health Event"
  ],
  "source": [
    "aws.health"
  ]
}
```

Configuration d'Amazon Q Developer dans les applications de chat pour envoyer des notifications concernant des événements dans AWS Health

Vous pouvez recevoir des AWS Health événements directement dans vos clients de chat, tels que Slack et Amazon Chime. Vous pouvez utiliser cet événement pour identifier les problèmes AWS de service récents susceptibles d'affecter vos AWS applications et votre infrastructure. Vous pouvez ensuite vous connecter à votre AWS Health tableau de bord pour en savoir plus sur la mise à jour. Par exemple, si vous surveillez le type d'`AWS_EC2_INSTANCE_STOP_SCHEDULED`événement dans votre AWS compte, celui-ci AWS Health peut apparaître directement sur votre chaîne Slack.

Prérequis

Avant de commencer, vous devez disposer des éléments suivants :

- Un client de chat configuré avec Amazon Q Developer dans les applications de chat. Vous pouvez configurer Amazon Chime et Slack. Pour plus d'informations, consultez Getting started with Amazon Q Developer in chat applications in chat dans le Guide de l'administrateur d'Amazon Q Developer in chat applications.
- Rubrique Amazon SNS que vous avez créée et à laquelle vous êtes abonné. Si vous avez déjà une rubrique SNS, vous pouvez utiliser une rubrique existante. Pour plus d'informations, consultez Prise en main d'Amazon SNS dans le Guide du développeur Amazon Simple Notification Service.

Pour recevoir des AWS Health événements avec Amazon Q Developer dans des applications de chat

1. Suivez la procédure décrite à Configuration d'une EventBridge règle pour envoyer des notifications concernant des événements dans AWS Health l'étape 13.

   a. Lorsque vous avez fini de configurer le modèle d'événement à l'étape 13, ajoutez une virgule à la dernière ligne du modèle et ajoutez la ligne suivante pour supprimer les messages de discussion inutiles des événements paginés AWS Health . Consultez Afficher les listes paginées d' AWS Health événements sur EventBridge.

      ```
      "detail.page": ["1"]
      ```

   b. Lorsque vous choisissez la cible à l'étape 14, choisissez une rubrique SNS. Vous utiliserez cette même rubrique SNS dans la console Amazon Q Developer dans les applications de chat.

   c. Effectuez le reste de la procédure pour créer la règle.

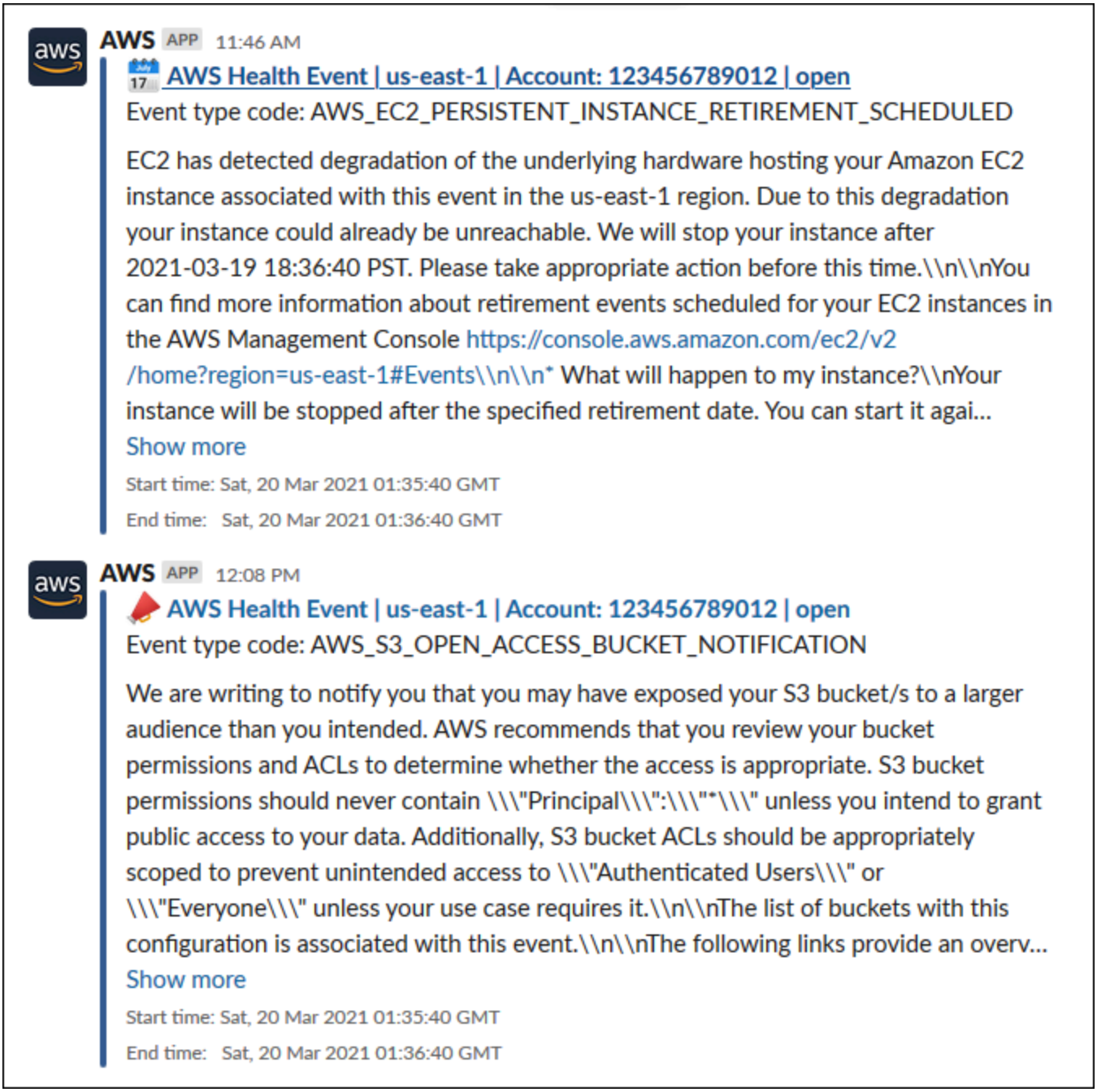
2. Accédez à Amazon Q Developer dans la console des applications de chat.
3. Choisissez votre client de chat, tel que le nom de votre chaîne Slack, puis choisissez Modifier.
4. Dans la section Notifications - facultatif, pour Rubriques, choisissez la même rubrique SNS que celle que vous avez spécifiée à l'étape 1.
5. Choisissez Save (Enregistrer).

   Lorsque AWS Health vous envoyez un événement EventBridge qui correspond à votre règle, l' AWS Health événement apparaît dans votre client de chat.

6. Choisissez le nom de l'événement pour voir plus d'informations dans votre AWS Health tableau de bord.

Example : AWS Health événements envoyés à Slack

Voici un exemple de deux AWS Health événements pour Amazon EC2 et Amazon Simple Storage Service (Amazon S3) dans la région USA Est (Virginie du Nord) qui apparaissent sur le canal Slack.



Exécution automatique d'opérations sur EC2 les instances en réponse à des événements dans AWS Health

Vous pouvez automatiser les actions qui répondent aux événements planifiés pour vos EC2 instances Amazon. Lorsque AWS Health vous envoyez un événement à votre AWS compte, votre EventBridge règle peut alors invoquer des cibles, telles que des documents AWS Systems Manager d'automatisation, pour automatiser les actions en votre nom.

Par exemple, lorsqu'un événement de retrait d' EC2 instance Amazon est planifié pour une instance EC2 soutenue par Amazon Elastic Block Store (Amazon EBS) AWS Health , le type d'événement sera envoyé à votre tableau de `AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED` bord. AWS Health Lorsque votre règle détecte ce type d'événement, vous pouvez automatiser l'arrêt et le démarrage de l'instance. Ainsi, vous n'avez pas à effectuer ces actions manuellement.

> **Note**
>
> Pour automatiser les actions de vos EC2 instances Amazon, celles-ci doivent être gérées par Systems Manager.

Pour plus d'informations, consultez Automating Amazon EC2 with EventBridge dans le guide de l' EC2 utilisateur Amazon.

Prérequis

Vous devez créer une politique AWS Identity and Access Management (IAM), créer un rôle IAM et mettre à jour la politique de confiance du rôle avant de pouvoir créer une règle.

Créer une politique IAM

Suivez cette procédure pour créer une politique gérée par le client pour votre rôle. Cette politique autorise le rôle à effectuer des actions en votre nom. Cette procédure utilise l'éditeur de politique JSON dans la console IAM.

Pour créer une stratégie IAM

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, choisissez Politiques.

3. Sélectionnez Create policy (Créer une politique).
4. Choisissez l'onglet JSON.
5. Copiez le JSON suivant, puis remplacez le JSON par défaut dans l'éditeur.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ssm:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": [
        "arn:aws:sns:*:*:Automation*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::123456789012:role/AutomationEVRole"
    }
```

```
  ]
}
```

a. Dans le `Resource` paramètre, pour Amazon Resource Name (ARN), entrez votre identifiant de AWS compte.

b. Vous pouvez également remplacer le nom du rôle ou utiliser le nom par défaut. Cet exemple utilise *`AutomationEVRole`*.

6. Choisissez Suivant : Balises.
7. (Facultatif) Vous pouvez utiliser des balises comme paires clé-valeur pour ajouter des métadonnées à la politique.
8. Choisissez Suivant : Vérification.
9. Sur la page Révision de la politique, entrez un nom, par exemple *`AutomationEVRolePolicy`* et une description facultative.
10. Consultez la page Résumé pour voir les autorisations autorisées par la politique. Si vous êtes satisfait de votre politique, choisissez Créer une politique.

Cette politique définit les actions que le rôle peut prendre. Pour plus d'informations, consultez Création de politiques IAM (console) dans le Guide de l'utilisateur IAM.

Créer un rôle IAM

Après avoir créé la politique, vous devez créer un rôle IAM, puis associer la politique à ce rôle.

Pour créer un rôle pour un AWS service

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le volet de navigation, sélectionnez Rôles, puis Créer un rôle.
3. Pour Select type of trusted entity (Sélectionner le type d'entité de confiance), choisissez Service AWS .
4. Choisissez EC2le service que vous souhaitez autoriser à assumer ce rôle.
5. Choisissez Suivant : Autorisations.
6. Entrez le nom de la stratégie que vous avez créée*`AutomationEVRolePolicy`*, par exemple, puis cochez la case à côté de la stratégie.
7. Choisissez Suivant : Balises.

8. (Facultatif) Vous pouvez utiliser des balises comme paires clé-valeur pour ajouter des métadonnées au rôle.
9. Choisissez Next: Review (Suivant : Vérification).
10. Pour le Nom du rôle, saisissez *AutomationEVRole*. Ce nom doit être le même que celui qui apparaît dans l'ARN de la politique IAM que vous avez créée.
11. (Facultatif) Dans le champ Role description (Description du rôle), saisissez la description du nouveau rôle.
12. Passez en revue les informations du rôle, puis choisissez Créer un rôle.

Pour plus d'informations, consultez la section Création d'un rôle pour un AWS service dans le Guide de l'utilisateur IAM.

Mettre à jour la politique de confiance

Enfin, vous pouvez mettre à jour la politique de confiance pour le rôle que vous avez créé. Vous devez suivre cette procédure afin de pouvoir choisir ce rôle dans la EventBridge console.

Pour mettre à jour la politique de confiance pour le rôle

1. Connectez-vous à la console IAM AWS Management Console et ouvrez-la à https://console.aws.amazon.com/iam/l'adresse.
2. Dans le panneau de navigation, choisissez Roles (Rôles).
3. Dans la liste des rôles de votre AWS compte, choisissez le nom du rôle que vous avez créé, par exemple*AutomationEVRole*.
4. Sélectionnez l'onglet Relations d'approbation, puis Modifier la relation d'approbation.
5. Pour le document de stratégie, copiez le code JSON suivant, supprimez la politique par défaut et collez le code JSON copié à sa place.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": [
                    "ssm.amazonaws.com",
                    "events.amazonaws.com"
                ]
```

```
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

6. Choisissez Mettre à jour la politique d'approbation.

Pour plus d'informations, consultez la section Modification d'une politique d'approbation des rôles (console) dans le guide de l'utilisateur IAM.

Créez une règle pour EventBridge

Suivez cette procédure pour créer une règle dans la EventBridge console afin d'automatiser l'arrêt et le démarrage des EC2 instances dont le retrait est prévu.

Pour créer une règle EventBridge pour les actions automatisées de Systems Manager

1. Ouvrez la EventBridge console Amazon à l'adresse https://console.aws.amazon.com/events/.
2. Sous Events (Événements) dans le panneau de navigation, choisissez Rules (Règles).
3. Sur la page Créer une règle, entrez le nom et la description de votre règle.
4. Sous Define pattern (Définir un modèle), choisissez Event pattern (Modèle d'événement), puis Pre-defined pattern by service (Modèle prédéfini par service).
5. Pour Service Provider (Fournisseur de service), sélectionnez AWS.
6. Dans Nom du service, choisissez Health.
7. Dans Type d'événement, sélectionnez Specific Health events.
8. Choisissez Service (s) spécifique (s), puis choisissez EC2.
9. Choisissez une ou plusieurs catégories de type d'événement spécifiques, puis choisissez ScheduledChange.
10. Choisissez un ou plusieurs codes de types d'événements spécifiques, puis choisissez le code du type d'événement.

    Par exemple, pour les instances basées sur Amazon EC2 EBS, choisissez. **AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED** Pour les EC2 instances basées sur le stockage d'instances Amazon, choisissez. **AWS_EC2_INSTANCE_RETIREMENT_SCHEDULED**
11. Choisissez N'importe quel type de ressource.

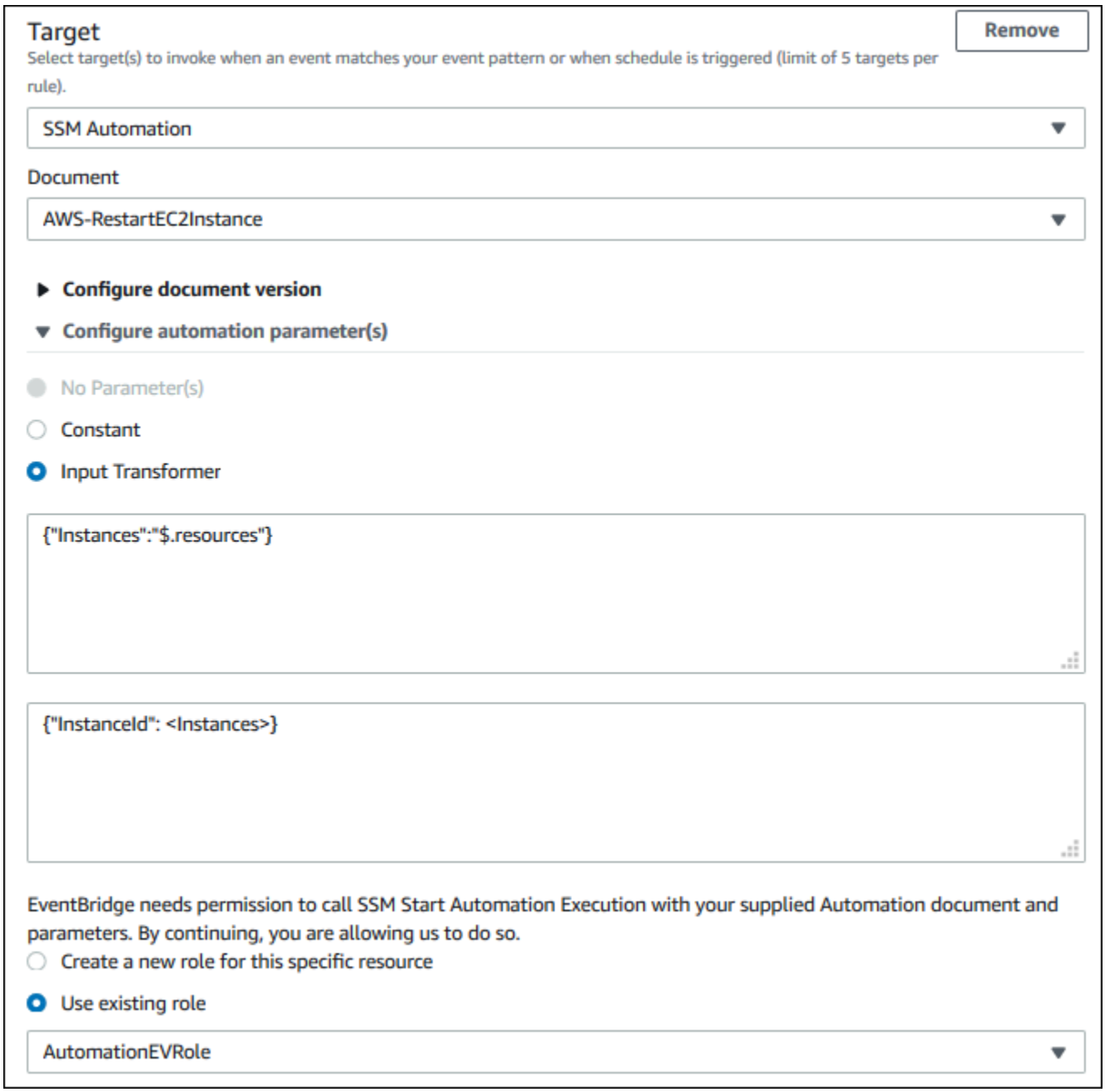
Votre modèle d'événement ressemblera à celui de l'exemple suivant.

Example

```
{
  "source": [
    "aws.health"
  ],
  "detail-type": [
    "AWS Health Event"
  ],
  "detail": {
    "service": [
      "EC2"
    ],
    "eventTypeCategory": [
      "scheduledChange"
    ],
    "eventTypeCode": [
      "AWS_EC2_PERSISTENT_INSTANCE_RETIREMENT_SCHEDULED"
    ]
  }
}
```

12. Ajoutez le document cible de Systems Manager Automation. Sous Sélectionner les cibles, pour Target, choisissez SSM Automation.
13. Pour Document, sélectionnez `AWS-RestartEC2Instance`.
14. Développez les paramètres de configuration de l'automatisation, puis choisissez Input Transformer.
15. Dans le champ Chemin d'entrée, entrez**`{"Instances":"$.resources"}`**.
16. Pour le deuxième champ, entrez**`{"InstanceId": <Instances>}`**.
17. Choisissez Utiliser le rôle existant, puis choisissez le rôle IAM que vous avez créé, tel que*`AutomationEVRole`*.

    Votre cible doit ressembler à l'exemple suivant.



> **Note**
>
> Si vous ne possédez pas de rôle IAM disposant des autorisations requises EC2 et de la relation de confiance de Systems Manager, votre rôle n'apparaîtra pas dans la liste. Pour de plus amples informations, veuillez consulter Prérequis.

18. Sélectionnez Créer.

Si un événement correspondant à votre règle se produit sur votre compte, il EventBridge sera envoyé à la cible que vous avez spécifiée.

Référence : Amazon EventBridge schéma AWS Health des événements

Le schéma des AWS Health événements est le suivant. Le contenu du paramètre details est présenté dans un second tableau. Des exemples de charges utiles sont fournis après les tables de schéma.

AWS Health schéma d'événement

AWS Health schéma d'événement

Paramètre	Description	Obligatoire
Version	EventBridge version, actuellement « 0 ».	Oui
id	Identifiant unique de l'EventBridge événement.	Oui
type de détail	Le type de détail. Pour les AWS Health événements, les valeurs prises en charge sont `&AWS Health Event` et `AWS Health`	Oui

Paramètre	Description	Obligatoire
	`Abuse Event`	
source	La source du bus d'événements. Pour les AWS Health événements, la valeur prise en charge est `aws.health`	Oui

Paramètre	Description	Obligatoire
account	L'identifiant du compte auquel l'AWS Health événement a été envoyé. **Note** Pour les vues organisationnelles, il s'agit d'un compte différent du compte concerné s'il est reçu dans le compte de gestion ou le compte d'adminis	Oui

Paramètre	Description	Obligatoire
	trateur délégué.	
time	Heure à laquelle la notification a été envoyée EventBridge. Format : `yyyy-mm-ddThh:mm:ssZ` .	Oui

Paramètre	Description	Obligatoire
region	Le Région AWS destinataire de la notification. **Note** Ce champ n'indique pas la région concernée par cet AWS Health événement. Ces informations sont publiées dans`detailRegion`.	Oui

Paramètre	Description	Obligatoire
resources	Décrit la liste des ressources concernées, le cas échéant, au sein d'un compte. Ce champ est vide si aucune ressource n'est référencée.	Non
détail	Section contenant les détails de l'AWS Health événement, comme décrit dans le tableau qui suit immédiatement celui-ci.	Oui

Contenu du schéma du paramètre « details »

Le tableau suivant décrit le contenu du paramètre de détail dans le schéma AWS Health d'événement.

AWS Health schéma d'événement : contenu détaillé des paramètres

contenu du paramètre « détail »	Description	Obligatoire
ARN de l'événement	L'identifiant unique de l' AWS Health événement pour la région spécifique, y compris la région et l'identifiant de l'événement. **Note** L'ARN d'un événement n'est pas propre à une région Compte AWS ou à une région spécifique.	Oui
web	Les Service AWS personnes touchées par l' AWS Health événement. Par exemple, Amazon EC2, Amazon Simple Storage Service, Amazon Redshift ou Amazon Relational Database Service.	Oui
eventTypeCode	Identifiant unique du type d'événement. Par exemple : `AWS_EC2_INSTANCE_NETWORK_MAINTENANCE_SCHEDULED` et `AWS_EC2_INSTANCE_REBOOT_MAINTENANCE_SCHEDULED`. Les événements inclus `MAINTENANCE_SCHEDU`	Oui

contenu du paramètre « détail »	Description	Obligatoire
	`LED` sont généralement reportés environ deux semaines avant l'heure de début. **Note** Tous les nouveaux événements du cycle de vie planifiés ont le type d'événement`AWS_{SERVICE}_PLANNED_LIFECYCLE_EVENT` .	
eventTypeCategory	Code de catégorie d'événement. Les valeurs prises en charge incluent `issue`,`accountNotification` ,`investigation` , et`scheduledChange` .	Oui
eventScopeCode	Indique si l' AWS Health événement est spécifique au compte ou public. Les valeurs prises en charge sont `ACCOUNT_SPECIFIC` ou `PUBLIC`.	Oui

contenu du paramètre « détail »	Description	Obligatoire
Numéro de communication	Identifiant unique pour cette communication relative à l' AWS Health événement. Les messages portant le même identifiant de communication peuvent être des messages de sauvegarde ou des pages d'un seul AWS Health événement . Cet identifiant peut être utilisé avec l'identifiant du compte pour dédupliquer les messages. Grâce à la prise en charge de la pagination des AWS Health événements, l'identifiant de communication inclut le numéro de page afin que l'identifiant de communication reste unique sur toutes les pages, par exemple 12345678910-1. Pour de plus amples informations, veuillez consulter Afficher les listes paginées d' AWS Health événements sur EventBridge.	Oui

contenu du paramètre « détail »	Description	Obligatoire
startTime	L'heure de début de l' AWS Health événement, au format`DoW, DD, MMM, YYYY, HH:MM:SS TZ`. L'heure de début peut se situer dans le futur pour les événements planifiés.	Oui
endTime	L'heure de fin de l' AWS Health événement, au format :`DoW, DD MMM YYYY HH:MM:SS TZ`. L'heure de fin ne peut pas être spécifiée pour les événements planifiés pour une date future.	Non
lastUpdatedTime	L'heure de la dernière mise à jour de l' AWS Health événement, au format`DoW, DD MMM YYYY HH:MM:SS TZ`.	Oui
statusCode	État de l' AWS Health événement. Les valeurs prises en charge incluent `open`,`closed`, et`upcoming`.	Oui
Région de l'événement	La région touchée décrite par cet AWS Health événement.	Oui

contenu du paramètre « détail »	Description	Obligatoire
Description de l'événement	Section qui décrit l' AWS Health événement. Cela inclut les champs de langue et de texte décrivant l'événement. • language — Le code de la langue utilisée lors de l' AWS Health événement . Cela est généralement déterminé par la région dans laquelle l'événement est publié. Par exemple, dans la `us-east-1` Région, c'est généralement le `casen_US`. • LatestDescription — Décrit l' AWS Health événement tel qu'il est rendu par l' AWS Health API et apparaît généralement sur le AWS Health tableau de bord. **Note** Pour les événements publics, il contient uniquement la dernière mise à jour et non l'historique complet de l'événement.	Oui

contenu du paramètre « détail »	Description	Obligatoire
Métadonnées de l'événement	Métadonnées d'événement supplémentaires qui peuvent être fournies pour l' AWS Health événement. • <metadata key 1>— Chaînes de paires clé-valeur de métadonnées : « keystring1" : « keyvalue1" Les paires clé-valeur pour les métadonnées des événements sont déterminé es par le service qui a envoyé l' AWS Health événement.	Non

contenu du paramètre « détail »	Description	Obligatoire
Entités concernées	Tableau qui décrit la valeur des ressources et l'état des ressources affectées dans le cadre de l' AWS Health événement. • EntityValue — ID de ressource/entité. • LastUpdatedTime — Heure à laquelle le statut de cette ressource/entité a été mis à jour pour la dernière fois, au format. `DoW, DD MMM YYYY HH:MM:SS TZ` • status — État de la ressource/entité affectée. Les valeurs prises en charge incluent `IMPAIRED` `UNIMPAIRED` `PENDING`,`RESOLVED`, et`UNKNOWN`.	Non

contenu du paramètre « détail »	Description	Obligatoire
page	La page que représente ce message. Pour de plus amples informations, veuillez consulter Afficher les listes paginées d' AWS Health événements sur EventBridge. **Note** La pagination s'effectue uniquement sur les ressources. Si la limite de taille de 256 Ko est dépassée pour une autre raison, la communication échouera.	Oui
Nombre total de pages	Le nombre total de pages consacrées à cet événement de santé. Pour de plus amples informations, veuillez consulter Afficher les listes paginées d' AWS Health événements sur EventBridge. Vous pouvez utiliser cette valeur pour déterminer si vous avez reçu toutes les pages d'une communication de plusieurs pages pour un compte.	Oui

contenu du paramètre « détail »	Description	Obligatoire
Compte concerné	L'identifiant du compte concerné. Cela peut être différent de la valeur du `account` champ si cet événement de santé est envoyé à un compte faisant partie d'un compte AWS Organizations et est reçu sur le compte de gestion ou le compte d'administrateur délégué.	Oui

Événement de santé publique - Problème EC2 opérationnel d'Amazon


```
{
    "version": "0",
    "id": "7bf73129-1428-4cd3-a780-95db273d1602",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2023-01-27T09:01:22Z",
    "region": "af-south-1",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:af-south-1::event/EC2/AWS_EC2_OPERATIONAL_ISSUE/
AWS_EC2_OPERATIONAL_ISSUE_7f35c8ae-af1f-54e6-a526-d0179ed6d68f",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_OPERATIONAL_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "PUBLIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 27 Jan 2023 06:02:51 GMT",
        "endTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "lastUpdatedTime": "Fri, 27 Jan 2023 09:01:22 GMT",
        "statusCode": "open",
        "eventRegion": "af-south-1",
```

```
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "Current severity level: Operating normally\n
\n[RESOLVED] \n\n [03:15 PM PST] We continue see recovery \n\nThe following AWS
 services were previously impacted but are now operating normally: APPSYNC, BACKUP,
 EVENTS."
        }],
        "affectedEntities": [],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Événement spécifique au compte : problème avec l'API Elastic Load Balancing

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-10T06:27:57Z",
    "region": "ap-southeast-2",
    "resources": [],
    "detail": {
        "eventArn": "arn:aws:health:ap-southeast-2::event/
AWS_ELASTICLOADBALANCING_API_ISSUE_90353408594353980",
        "service": "ELASTICLOADBALANCING",
        "eventTypeCode": "AWS_ELASTICLOADBALANCING_API_ISSUE",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 10 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 10 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "ap-southeast-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
```

```
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
    }
}
```

AWS Health Événement spécifique au compte : dégradation des performances du disque Amazon EC2 Instance Store

```
{
    "version": "0",
    "id": "121345678-1234-1234-1234-123456789012",
    "detail-type": "AWS Health Event",
    "source": "aws.health",
    "account": "123456789012",
    "time": "2022-06-03T06:27:57Z",
    "region": "us-west-2",
    "resources": [
        "i-abcd1111"
    ],
    "detail": {
        "eventArn": "arn:aws:health:us-west-2::event/
AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED_90353408594353980",
        "service": "EC2",
        "eventTypeCode": "AWS_EC2_INSTANCE_STORE_DRIVE_PERFORMANCE_DEGRADED",
        "eventTypeCategory": "issue",
        "eventScopeCode": "ACCOUNT_SPECIFIC",
        "communicationId": "01b0993207d81a09dcd552ebd1e633e36cf1f09a-1",
        "startTime": "Fri, 3 Jun 2022 05:01:10 GMT",
        "endTime": "Fri, 3 Jun 2022 05:30:57 GMT",
        "statusCode": "open",
        "eventRegion": "us-west-2",
        "eventDescription": [{
            "language": "en_US",
            "latestDescription": "A description of the event will be provided here"
        }],
        "affectedEntities": [{
            "entityValue": "i-abcd1111"
        }],
        "page": "1",
        "totalPages": "1",
        "affectedAccount": "123456789012"
```

```
    }
}
```

Surveillance AWS Health

La surveillance joue un rôle important dans le maintien de la fiabilité, de la disponibilité AWS Health et des performances de vos autres AWS solutions. AWS fournit les outils de surveillance suivants pour surveiller AWS Health, signaler tout problème et prendre des mesures le cas échéant :

- Amazon CloudWatch surveille vos AWS ressources et les applications que vous utilisez AWS en temps réel. Vous pouvez collecter et suivre les métriques, créer des tableaux de bord personnalisés, et définir des alarmes qui vous informent ou prennent des mesures lorsqu'une métrique spécifique atteint un seuil que vous spécifiez. Pour plus d'informations, consultez le guide de CloudWatch l'utilisateur Amazon.

  Vous pouvez utiliser Amazon EventBridge pour être informé AWS Health des événements susceptibles d'affecter vos services et ressources. Par exemple, si vous AWS Health publiez un événement concernant vos EC2 instances Amazon, vous pouvez utiliser ces notifications pour prendre des mesures et mettre à jour ou remplacer vos ressources selon vos besoins. Pour de plus amples informations, veuillez consulter Surveillance des événements AWS Health avec Amazon EventBridge.
- AWS CloudTrail capture les appels d'API et les événements associés effectués par ou pour le compte de votre AWS compte et envoie les fichiers journaux dans un compartiment Amazon S3 que vous spécifiez. Vous pouvez identifier les utilisateurs et les comptes appelés AWS, l'adresse IP source à partir de laquelle les appels ont été effectués et la date des appels. Pour plus d'informations, consultez le Guide de l'utilisateur AWS CloudTrail.

Rubriques

Journalisation des appels d' AWS Health API avec AWS CloudTrail

AWS Health est intégré à AWS CloudTrail un service qui fournit un enregistrement des actions entreprises par un utilisateur, un rôle ou un AWS service dans AWS Health. CloudTrail capture les appels d'API AWS Health sous forme d'événements. Les appels capturés incluent des appels provenant de la AWS Health console et des appels de code vers les opérations de l' AWS Health API. Si vous créez un suivi, vous pouvez activer la diffusion continue d' CloudTrail événements vers un compartiment Amazon S3, y compris les événements pour AWS Health. Si vous ne configurez pas

de suivi, vous pouvez toujours consulter les événements les plus récents dans la CloudTrail console dans Historique des événements. À l'aide des informations collectées par CloudTrail, vous pouvez déterminer la demande qui a été faite AWS Health, 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 en savoir plus CloudTrail, notamment comment le configurer et l'activer, consultez le guide de AWS CloudTrail l'utilisateur.

AWS Health informations dans CloudTrail

CloudTrail est activé sur votre AWS compte lorsque vous le créez. Lorsqu'une activité événementielle prise en charge se produit dans AWS Health, cette activité est enregistrée dans un CloudTrail événement avec d'autres événements AWS de service dans l'historique des événements. Vous pouvez consulter, rechercher et télécharger les événements récents dans votre AWS compte. Pour plus d'informations, consultez la section Affichage des événements à l'aide de l'historique des CloudTrail événements.

Pour un enregistrement continu des événements de votre AWS compte, y compris des événements pour AWS Health, créez un parcours. Un suivi permet CloudTrail de fournir des fichiers journaux à un compartiment Amazon S3. Par défaut, lorsque vous créez un parcours dans la console, celui-ci s'applique à toutes les AWS régions. Le journal de suivi consigne les événements de toutes les régions dans la partition AWS , et il livre les fichiers journaux dans le compartiment Amazon S3 de votre choix. En outre, vous pouvez configurer d'autres AWS services pour analyser plus en détail les données d'événements collectées dans les CloudTrail journaux et agir en conséquence. Pour plus d'informations, consultez les ressources suivantes :

- Vue d'ensemble de la création d'un journal d'activité
- CloudTrail Services et intégrations pris en charge
- Configuration des notifications Amazon SNS pour CloudTrail
- Réception de fichiers CloudTrail journaux de plusieurs régions et réception de fichiers CloudTrail journaux de plusieurs comptes

Toutes les opérations d' AWS Health API sont enregistrées CloudTrail et documentées dans la référence AWS Health d'API. Par exemple, les appels aux `DescribeAffectedEntities` opérations `DescribeEventsDescribeEventDetails`, et génèrent des entrées dans les fichiers CloudTrail journaux.

AWS Health prend en charge la journalisation des actions suivantes sous forme d'événements dans les fichiers CloudTrail journaux :

- Si la demande a été faite avec des informations d'identification root ou IAM
- Si la demande a été effectuée avec des informations d'identification de sécurité temporaires pour un rôle ou un utilisateur fédéré
- Si la demande a été faite par un autre AWS service

Pour plus d'informations, consultez la section Élément userIdentity CloudTrail .

Vous pouvez stocker vos fichiers journaux dans votre compartiment Amazon S3 aussi longtemps que vous le souhaitez. Vous pouvez également définir des règles de cycle de vie d'Amazon S3 pour archiver ou supprimer les fichiers journaux automatiquement. Par défaut, vos fichiers journaux sont chiffrés avec le chiffrement côté serveur (SSE) d'Amazon S3.

Pour être averti lors de la livraison des fichiers journaux, vous pouvez configurer CloudTrail pour publier des notifications Amazon SNS lorsque de nouveaux fichiers journaux sont livrés. Pour plus d'informations, consultez Configuration des notifications Amazon SNS pour CloudTrail.

Vous pouvez également agréger les fichiers AWS Health journaux de plusieurs AWS régions et de plusieurs AWS comptes dans un seul compartiment Amazon S3.

Pour plus d'informations, consultez les sections Recevoir les fichiers journaux de CloudTrail de plusieurs régions et Recevoir les fichiers journaux de CloudTrail de plusieurs comptes.

Exemple : entrées de fichier AWS Health journal

Un suivi est une configuration qui permet de transmettre des événements sous forme de fichiers journaux à un compartiment Amazon S3 que vous spécifiez. CloudTrail les fichiers journaux contiennent une ou plusieurs entrées de journal. Un événement représente une demande unique provenant de n'importe quelle source et inclut des informations sur l'action demandée, la date et l'heure de l'action, les paramètres de la demande, etc. CloudTrail les fichiers journaux ne constituent pas une trace ordonnée des appels d'API publics, ils n'apparaissent donc pas dans un ordre spécifique.

L'exemple suivant montre une entrée de CloudTrail journal illustrant l'DescribeEntityAggregatesopération.

```
{
```

```
   "Records": [
   {
   "eventVersion": "1.05",
   "userIdentity": {
      "type": "IAMUser",
      "principalId": "AIDACKCEVSQ6C2EXAMPLE",
      "arn": "arn:aws:iam::123456789012:user/JaneDoe",
      "accountId": "123456789012",
      "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
      "userName": "JaneDoe",
      "sessionContext": {"attributes": {
         "mfaAuthenticated": "false",
         "creationDate": "2016-11-21T07:06:15Z"
      }},
      "invokedBy": "AWS Internal"
    },
   "eventTime": "2016-11-21T07:06:28Z",
   "eventSource": "health.amazonaws.com",
   "eventName": "DescribeEntityAggregates",
   "awsRegion": "us-east-1",
   "sourceIPAddress": "203.0.113.0",
   "userAgent": "AWS Internal",
   "requestParameters": {"eventArns": ["arn:aws:health:us-east-1::event/EBS/
EBS_LOST_VOLUME/EBS_LOST_VOLUME_123"]},
   "responseElements": null,
   "requestID": "05b299bc-afb9-11e6-8ef4-c34387f40bd4",
   "eventID": "e4deb9dc-dbc2-4bdb-8515-73e8abcbc29b",
   "eventType": "AwsApiCall",
   "recipientAccountId": "123456789012"
   }
   ],
   ...
}
```

Historique du document pour AWS Health

Le tableau suivant décrit la documentation de cette version de AWS Health.

- Version de l'API : 2016-08-04

Le tableau suivant décrit les mises à jour importantes apportées à la AWS Health documentation à compter du 28 août 2020. Vous pouvez vous abonner à un flux RSS pour recevoir les notifications sur les mises à jour.

Modification	Description	Date
Section mise à jour : Activation de la vue organisationnelle	Ajout d'informations à la section Notes indiquant que tous les événements de santé historiques au sein de votre organisation sont AWS Health automatiquement agrégés lorsque vous activez la vue organisationnelle. Les événements historiques peuvent prendre jusqu'à 24 heures pour apparaître dans la vue de votre organisation. Pour plus d'informations, voir Activation de l'affichage organisationnel	27 juin 2025
Section mise à jour : Agrégation des AWS Health événements entre les comptes	Suppression de la note qui AWS Health ne montre pas les événements survenus avant que vous n'activiez l'affichage organisationnel. Pour plus d'informations, consultez la section Agrégation des AWS	27 juin 2025

	Health événements entre les comptes	
WorkDocs obsolète	Suppression des références à la version obsolète WorkDocs dans les événements du cycle de vie planifiés pour. AWS Health	19 juin 2025
Ajout d'une note concernant le calendrier de migration des notifications AWS gérées	Ajout d'une note concernant les dates clés pour la migration des e-mails vers les notifications AWS gérées dans Notifications des utilisateurs AWS. Pour plus d'informations, consultez la section Gérer AWS Health les notifications dans Notifications des utilisateurs AWS.	28 avril 2025
Événements du cycle de vie planifiés actualisés	Mise à jour des événements du cycle de vie planifiés pour indiquer que les AWS Health événements restent ouverts pendant 4 ans au lieu de 90 jours pour les ressources non résolues. Pour plus d'informations, consultez la section À quoi dois-je m'attendre lorsque je reçois une notification d'événement lié au cycle de vie planifié ? section dans Événements du cycle de vie planifiés pour AWS Health.	18 avril 2025

Mise à jour de la description de la liste des ressources concernées pour les événements du cycle de vie planifiés	La liste des ressources concernées pour les événements du cycle de vie planifiés est généralement actualisée toutes les 24 heures, mais l'état actuel des ressources peut prendre jusqu'à 72 heures. Pour plus d'informations, consultez la section Détails des événements dans Afficher les événements de votre compte dans le AWS Health tableau de bord.	7 avril 2025
Ajout d'une FAQ pour gérer AWS Health les notifications dans Notifications des utilisateurs AWS	Pour plus d'informations, consultez la section Gérer les notifications dans la Notifications des utilisateurs AWS FAQ.	18 février 2025
Ajout d'informations concernant les demandes adressées IPv6 uniquement aux points de terminaison.	Pour plus d'informations, consultez la section Choix des points de terminaison pour les demandes AWS Health d'API.	28 janvier 2025
Gérez AWS Health les notifications dans Notifications des utilisateurs AWS	Pour plus d'informations, voir Gérer les notifications dans Notifications des utilisateurs AWS.	16 janvier 2025
JSON corrigé dans la surveillance AWS Health des événements avec Amazon EventBridge	Pour plus d'informations, consultez la section Surveillance AWS Health des événements avec Amazon EventBridge.	3 septembre 2024

Informations mises à jour sur le téléchargement des ressources concernées	Pour plus d'informations, consultez la section Affichage des ressources concernées.	27 juillet 2024
La confidentialité du trafic interréseau a été supprimée de la documentation de la section AWS Health Sécurité	Pour plus d'informations, consultez la section Sécurité dans AWS Health.	27 mars 2024
Mise à jour du AWS Health tableau de bord — État du service et événements du cycle de vie planifiés pour AWS Health la documentation.	Pour plus d'informations, consultez AWS Health Tableau de bord — État du service et Événements du cycle de vie planifiés pour AWS Health.	15 février 2024
Suppression d'une double bullet dans Création d'une EventBridge règle pour AWS Health	Suppression d'une double bullet dans Creating an EventBridge rule for AWS Health.	4 décembre 2023
Documentation ajoutée pour les événements du cycle de vie planifiés	Pour plus d'informations, consultez la section Événements du cycle de vie planifiés pour AWS Health.	31 octobre 2023
Documentation mise à jour pour `AWSHealthFullAccess`	Vous pouvez désormais utiliser la politique `AWSHealthFullAccess` gérée dans le AWS GovCloud (US) Regions. Voir les politiques AWS gérées pour AWS Health.	16 octobre 2023

Ajout de documentation pour configurer les notifications AWS utilisateur dans AWS Health.	Vous pouvez désormais configurer les notifications AWS utilisateur dans AWS Health. Pour plus d'informations, voir Configurer les notifications AWS utilisateur pour AWS Health.	30 août 2023
Ajout de la documentation relative à la fonctionnalité d'administrateur délégué dans la section Agrégation AWS Health des événements.	Pour plus d'informations, consultez la section Vue organisationnelle de l'administrateur délégué.	27 juillet 2023
Mise à jour de la politique SLR	Mise à jour de la politique AWS gérée : Health_OrganizationsServiceRolePolicy. Pour plus d'informations, consultez Politiques gérées par AWS pour AWS Health.	19 juillet 2023
AWS Health le schéma prend désormais en charge les métadonnées des événements	Vous pouvez désormais recevoir les métadonnées des AWS Health événements. Pour plus d'informations, consultez la section Surveillance AWS Health des événements avec Amazon EventBridge.	20 juin 2023

Documentation mise à jour pour Amazon EventBridge	Vous pouvez désormais utiliser une EventBridge règle Amazon pour surveiller à la fois les événements publics et spécifiques au compte. Pour plus d'informations, consultez la section Surveillance AWS Health des événements avec Amazon EventBridge.	2 mai 2023
Documentation ajoutée pour les politiques AWS gérées	Ajout de documentation sur les politiques AWS gérées pour AWS Health et l'utilisation de rôles liés à un service pour. AWS Health	18 janvier 2023
Ajout de la documentation sur le réglage du fuseau horaire	Utilisez la nouvelle fonctionn alité de fuseau horaire pour afficher le AWS Health tableau de bord dans votre fuseau horaire local ou en UTC. Pour plus d'informations, consultez Commencer à utiliser votre AWS Health tableau de bord — État de votre compte et AWS Health Tableau de bord — État des services.	21 septembre 2022
Documentation mise à jour	Ajout de documentation pour AWS Health Aware. Pour plus d'informations, consultez AWS Health Aware.	25 mai 2022

Documentation mise à jour	Le Service Health Dashboard et le AWS Personal Health Dashboard ont été rebaptisés AWS Health Tableau de bord. Pour plus d'informations, consultez Commencer à utiliser votre AWS Health tableau de bord — État de votre compte et AWS Health Tableau de bord — État des services.	28 février 2022
Documentation mise à jour pour Amazon EventBridge	Nouveau sujet sur l'utilisation AWS Health d'Amazon EventBridge pour surveiller les événements liés à la santé. Pour plus d'informations, consultez la section Surveillance AWS Health des événements avec Amazon EventBridge.	3 février 2022
Documentation mise à jour	Si vous avez un plan Enterprise On-Ramp Support, vous pouvez utiliser l' AWS Health API.	24 novembre 2021
Documentation ajoutée	Nouveau sujet pour les AWS Health concepts. Pour plus d'informations, voir Concepts pour AWS Health.	29 juillet 2021

Documentation mise à jour pour les CloudWatch événements	Ajout d'une section expliquant comment créer une règle pour plusieurs catégories de services et de types d'événements. Pour plus d'informations, consultez la section Création d'une règle pour plusieurs services et catégories.	7 mai 2021
Documentation mise à jour pour les CloudWatch événements	Mise à jour de la section pour automatiser AWS Systems Manager les actions relatives aux règles Amazon CloudWatch Events. Pour plus d'informations, consultez Automatiser les actions pour les EC2 instances Amazon.	28 avril 2021
Documentation mise à jour pour les CloudWatch événements	Ajout d'une section pour recevoir AWS Health les événements dans votre client de chat. Pour plus d'informations, consultez la section Réception d' AWS Health événements avec Amazon Q Developer dans les applications de chat.	16 mars 2021

Documentation mise à jour	Les rubriques suivantes ont été mises à jour : • Mise à jour de la rubrique « Agrégation d' AWS Health événements » • Réorganisation et mise à jour de la rubrique Monitor for AWS Health events with Amazon CloudWatch Events • Mise à jour de la section sur les conditions basées sur les ressources et les actions	29 janvier 2021
Ajout du AWS Health tableau de bord pour une vue organisationnelle dans la AWS Health console	Vous pouvez utiliser la AWS Health console pour activer la fonctionnalité d'afficha ge organisationnel. Vous pouvez ensuite consulter les événements de santé relatifs aux comptes des membres de votre AWS organisation.	14 décembre 2020
Démonstration des terminaux à haute disponibilité	Vous pouvez utiliser l'exemple de code pour déterminer le point de terminaison régional actif et AWS la région de signature pour AWS Health.	22 octobre 2020
Mises à jour du guide de AWS Health l'utilisateur	Mises à jour de l'organisation et ajout d'un flux RSS afin que vous puissiez vous abonner aux dernières mises à jour de la AWS Health documentation.	28 août 2020

Mises à jour antérieures

Modification	Description	Date
Mise à jour de la rubrique de la vue organisationnelle pour inclure des exemples.	Consultez Agrégation des AWS Health événements entre les comptes.	3 juin 2020
Sécurité et AWS Health	Ajout d'informations sur les considérations de sécurité lors de l'utilisation d' AWS Health. Consultez Sécurité dans AWS Health.	5 mai 2020
Ajout d'une nouvelle section expliquant comment utiliser la vue organisationnelle pour les événements regroupés de tous les comptes dans AWS Organizations.	Consultez Agrégation des AWS Health événements entre les comptes.	18 décembre 2019
Ajout d'une nouvelle section « Conditions basées sur les ressources et les actions » pour expliquer les restricti ons relatives aux événement s imposées par l'API. AWS Health	Consultez Gestion des identités et des accès pour AWS Health.	2 août 2018
Ajout d'une note concernan t la visibilité des AWS Health informations.	Consultez Gestion des identités et des accès pour AWS Health.	le 16 août 2017
Edition du service	AWS Health publié.	1er décembre 2016

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.